INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU* EM DIREITO
DOUTORADO EM DIREITO CONSTITUCIONAL

GETÚLIO VELASCO MOREIRA FILHO

MECANISMOS REGULATÓRIOS EM MATÉRIA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS: DO MODELO REGULATÓRIO ESTATAL AOS MODELOS HÍBRIDOS DE REGULAÇÃO PÚBLICO-PRIVADA

BRASÍLIA - DF
2023

GETÚLIO VELASCO MOREIRA FILHO

MECANISMOS REGULATÓRIOS EM MATÉRIA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS: DO MODELO REGULATÓRIO ESTATAL AOS MODELOS HÍBRIDOS DE REGULAÇÃO PÚBLICO-PRIVADA

Tese de Doutorado desenvolvida sob a orientação da Profª. Drª. Laura Schertel Ferreira Mendes e apresentada ao PPGD/IDP como requisito parcial para a obtenção do título de Doutor em Direito Constitucional.

BRASÍLIA - DF

2023

Código de catalogação na publicação – CIP

M838 Moreira Filho, Getúlio Velasco

Mecanismos regulatórios em matéria de privacidade e proteção de dados pessoais: do modelo regulatório estatal aos modelos híbridos de regulação público-privada / Getúlio Velasco Moreira Filho. Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2023.

393 f.

Tese - Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, Doutorado em Direito Constitucional, 2023.

Orientador(a): Prof. Dr. Laura Schertel Ferreira Mendes

1. Proteção de dados 2. Regulação. 3. Modelo regulatório. I.Título

CDDIR 341.2732

Elaborada pela Biblioteca Ministro Moreira Alves

GETÚLIO VELASCO MOREIRA FILHO

MECANISMOS REGULATÓRIOS EM MATÉRIA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS: DO MODELO REGULATÓRIO ESTATAL AOS MODELOS HÍBRIDOS DE REGULAÇÃO PÚBLICO-PRIVADA

Tese de Doutorado desenvolvida sob a orientação da Profª. Drª. Laura Schertel Ferreira Mendes e apresentada ao PPGD/IDP como requisito parcial para a obtenção do título de Doutor em Direito Constitucional.

Aprovado em: 16/06/2023

BANCA EXAMINADORA

Profª. Drª. Laura Schertel Ferreira Mendes
Orientadora
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

Prof. Dr. Osmar Mendes Paixão Côrtes
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

Prof. Dr. Guilherme Pereira Pinheiro
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

Profª. Drª. Bianca Kremer Nogueira Corrêa
Universidade Federal Fluminense -UFF
Membro Externo

"Com o desenvolvimento da televisão e o avanço técnico que possibilitou a recepção e a transmissão simultâneas por intermédio do mesmo aparelho, a vida privada chegou ao fim. (...) A possibilidade de obrigar todos os cidadãos a observar estrita obediência às determinações do Estado e completa uniformidade de opinião sobre todos os assuntos existia pela primeira vez."

Orwell, George. 1984 (p. 274).

Em memória ao Professor Danilo Cesar Maganhoto Doneda,

cujo brilhantismo o tempo jamais esmaecerá.

AGRADECIMENTOS

É comum vermos em agradecimentos como este a menção de que a escrita de uma tese é um trabalho solitário. A assertiva tem um fundo de verdade. Contudo, em verdade, jamais estamos sós.

Certo de que nada se faz sozinho, agradeço, a Deus por findar este trabalho de incansáveis horas de estudo e escrita.

Agradeço à minha orientadora, Profª. Drª. Laura Schertel Ferreira Mendes por sua enorme paciência, por seu brilhantismo (ímpar àqueles que militam na área do direito digital), por suas substanciais contribuições e, acima de tudo, por sua leveza em conduzir essa jornada comigo e sempre caminhar ao meu lado.

Agradeço ao Prof. Dr. Osmar Mendes Paixão Côrtes, à Profª. Drª. Bianca Kremer Nogueira Corrêa, ao Prof. Dr. Guilherme Pereira Pinheiro, e ao Prof. Dr. Danilo Cesar Maganhoto Doneda (*in memoriam*), pelas valiosas contribuições que moldaram o resultado desta pesquisa.

Agradeço, ainda, às punjantes instituições que possibilitaram que esse trabalho fosse possível, em especial, ao Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) e todo seu corpo docente e administrativo que me forneceram os instrumentos necessário à condução desta pesquisa.

Ao Tribunal de Contas do Estado de Mato Grosso e ao Ministério Público de Contas do Estado de Mato Grosso, sem os quais esse trabalho não seria possível.

À minha equipe de trabalho, cuja dedicação me permitiu mais tranquilidade para conduzir os estudos que levaram a este trabalho.

E, a todos, que direta ou indiretamente me ajudaram a formar o trabalho que ora se apresenta.

Por fim, mas de forma alguma menos importante, à minha família, cujo apoio integral e inabalável me sustentou por todos esses anos de trabalho e dedicação. Meu amor por vocês é incondicional.

Sem mais delongas: ao trabalho.

RESUMO

O objeto da tese circunscreve-se à utilização de mecanismos regulatórios de natureza híbrida na seara da privacidade e proteção de dados pessoais. O problema por ela abordado é representado pela pergunta: "como se garantir um adequado grau de intervenção regulatória de modo a se conciliar a proteção de direitos fundamentais dos cidadãos, sem sufocar a capacidade atuação dos agentes privados, responsáveis, em grande medida pela inovação e pelo desenvolvimento em nossas sociedades?". Para investigar o tema analisou-se diferentes graus de intervenção do Estado na regulação da privacidade e proteção de dados pessoais. Em um primeiro momento abordou-se como os modelos produtivos se desenvolveram, desde a primeira revolução industrial até a indústria 4.0. Percebeu-se aí os problemas gerados por formas de produzir que fogem ao controle estatal, por meio da inovação, acarretando, frequentemente, cenários de exploração de grupo vulneráveis, como os trabalhadores. Nessa mesma seção também foram abordados a economia de dados, os conceitos fundamentais às novas tecnologias e uma gama de benefícios, mas sobretudo, riscos que elas despertam. Na segunda seção analisou-se as teorias regulatórias do ciberespaço e como elas influenciaram nos modelos de regulação postos. A partir dessas teorias o trabalho se debruçou a analisar os modelos de proteção de dados americano, europeu, uruguaio e brasileiro. Esses modelos apresentam diferentes níveis de intervenção estatal e, sobretudo, os dois primeiros, influenciaram a construção das diversas legislações ao redor do mundo. Também na segunda seção avaliou-se a origem do direito à proteção de dados e como este foi tutelado pelos citados modelos regulatórios. Na terceira seção, fez-se um contraponto em relação à primeira, demonstrando-se as diversas modalidades de falhas regulatórias a que o modelo estatal de regulação está sujeito. Assim, começou-se a avaliar a construção de um modelo híbrido de regulação que conciliasse interesses estatais e de mercado. Esse modelo proposto, chamado de modelo sistemático-dialógico de regulação, foi na sequência detalhado e esmiuçado seu funcionamento. Também foram apresentadas algumas vantagens expectáveis no modelo e algumas possíveis desvantagens. Ao final chegou-se à conclusão de que, enquanto um sistema integrado, o modelo dialógico tem a aptidão de fomentar uma cultura de proteção de dados pessoais em diferentes níveis; de repartir responsabilidade entre atores públicos e privados (gerando, inclusive, diminuição de custos, em alguns cenários); e de promover um diálogo mais abrange e menos propenso a cair em erros comum de cenários regulatórios exclusivamente estatais ou exclusivamente autorregulatórios. Não obstante, reconheceu-se que, como um modelo

projetado (ainda não implementado), os resultados devem ser submetidos a novas investigações empíricas, capazes de analisar o efeito prático do sistema no mercado e na atitude dos titulares de dados. Todavia, do ponto de vista teórico, o modelo demonstra se sustentar, de modo que se espera que possa oferecer novos horizontes na seara da proteção de dados pessoais no Brasil na busca de se salvaguardar os direitos dos titulares de dados pessoais, sem que isso represente um obstáculo ao desenvolvimento tecnológico, e à busca de uma sociedade digital livre, próspera e segura.

ABSTRACT

The object of the thesis is limited to regulatory mechanisms of a hybrid nature in the area of privacy and protection of personal data. The problem addressed by it is represented by the question: "how to guarantee an adequate degree of regulatory intervention in order to reconcile the protection of fundamental rights of citizens, without stifling the capacity to act by private agents, responsible, to a large extent, for innovation and for development in our societies? To investigate the subject, different degrees of State intervention in the regulation of privacy and protection of personal data were analyzed. At first, it was discussed how production models developed, from the first industrial revolution to industry 4.0. It was noticed there the problems generated by ways of producing that escape state control, through innovation, often resulting in scenarios of exploitation of vulnerable groups such as workers. In this same section, the economy of data, the fundamental concepts of new technologies and a range of benefits, but above all, risks that they raise are also addressed. In the second section, the regulatory theories of cyberspace were analyzed and how they influenced the proposed regulatory models. Based on these theories, the work focused on analyzing the American, European, Uruguayan and Brazilian data protection models. These models present different levels of state intervention and, above all, the first two, influenced the construction of different legislations around the world. The second section also evaluated the origin of the right to data protection and how it was safeguarded by the aforementioned regulatory models. In the third section, a counterpoint was made in relation to the first section, demonstrating the different types of regulatory failures to which the state model of regulation is subject. Thus, the construction of a hybrid model of regulation that reconciled state and market interests began to be evaluated. This proposed model, called the systematic-dialogical

model of regulation, was subsequently detailed and its functioning in detail. Some expected advantages of the model and some possible disadvantages were also presented. In the end, it was concluded that, while an integrated system, the dialogic model has the ability to foster a culture of personal data protection at different levels; sharing responsibility between public and private actors (even generating cost reductions in some scenarios); and to promote a model of dialogue that is more comprehensive and less prone to falling into the common mistakes of exclusively state or exclusively self-regulatory regulatory scenarios. Nevertheless, it was recognized that, as a projected model (not yet implemented), the results must be subjected to further empirical investigations capable of addressing the practical effect of the system on the market and on the attitude of data subjects. However, from a theoretical point of view, the model proves to be sustainable, so it is expected that it can offer new horizons in the field of personal data protection in Brazil in order to safeguard the rights of holders of personal data, without this representing an obstacle to technological development, and the pursuit of a free, prosperous and secure digital society.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

INTRODUÇÃO

As transformações digitais ocorridas nas últimas décadas configuraram novos cenários nos quais direito, política, economia, cultura e sociedade, acabaram por conformar-se e adaptar-se.

A invenção da máquina à vapor (Indústria 1.0), a descoberta da eletricidade (Indústria 2.0), a automatização e a digitalização (Indústria 3.0), a inteligência artificial[1], o aprendizado de máquina[2], o *big data*, a computação em nuvem[3] e a internet das coisas[4] (Indústria 4.0) aos poucos, delinearam novas maneiras de se viver, se produzir e se relacionar.

Esses novos hábitos, surgidos a partir da inserção da tecnologia nas tarefas mais comezinhas da vida moderna, levaram a profundas modificações por todos os lados. Na economia, por exemplo, as tecnologias da informação e comunicação conduziram a uma expressiva desmaterialização dos meios de produção.

Os bens intangíveis, oriundos do intelecto humano, tornaram-se os grandes geradores de riqueza nos últimos anos.[5] A valorização da informação e do conhecimento

---

[1] Termo utilizado para definir o processo que capacita computadores e máquinas a performar tarefas de forma inteligente. MOOR, James. The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years. **AI Magazine**. Palo Alto: Association for the Advancement of Artificial Intelligence, v. 27, n. 4, p. 87–91, 2006, p. 87.

[2] O termo aprendizado de máquina, "*machine learning*", foi cunhado em 1959, três anos após a primeira referência à inteligência artificial, para designar o campo de estudo que dá aos computadores a habilidade de aprender sem serem explicitamente programados. MOOR, James. The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years. **AI Magazine**. Palo Alto: Association for the Advancement of Artificial Intelligence, v. 27, n. 4, p. 87–91, 2006, p. 87. SAMUEL, A. L. Some studies in machine learning using the game of checkers. **IBM Journal of Research and Development**. New York, v. 3, n. 3, p. 210–229, 1959.

[3] Ou *cloud computing* refere-se à disponibilização sob demanda de recursos computacionais, especialmente armazenamento de dados e capacidade de processamento, sem o gerenciamento ativo direto do utilizador, por meio de servidores remotos conectados à internet, a chamada "nuvem". Ver: Luís Antunes sobre a definição e benefícios dessa tecnologia, especialmente, em termos de economia de recursos. ANTUNES, Luís. **Pôr em Prática o RGPD: o que muda para nós? E para as organizações?**. Lisboa: FCA, 2018, p. 35.

[4] Terminologia empregada por Ashton, para designar aparelhos e utensílios com tecnologia de aprendizagem de máquina, aptidão de coleta e interpretação de dados autônoma, além da aptidão de se comunicar entre si e com a rede. ASHTON, Kevin. That 'Internet of Things' Thing. **RFID Journal**, 2009. Disponível em: http://www.rfidjournal.com/articles/view?4986. Acesso em: 10 jun. 2021.

[5] *Cf.* a análise trazida pela revista Forbes em artigo intitulado "Covid-19 provoca a maior aceleração da riqueza em toda a história da humanidade", que avalia a distribuição da riqueza ao longo dos últimos dois séculos: *"(...) Por quase toda a história humana, a riqueza foi dinástica. Os John D. Rockefellers e Henry Fords de um século atrás desencadearam a primeira era do empreendedorismo, mas mesmo esses sucessos se transformaram em fortunas familiares consolidadas. A primeiríssima lista Forbes 400 dos norte-americanos mais ricos, em 1982, continuava repleta da prole deles, assim como de muitos Mellons, DuPonts e outros – cerca de 63% daquela lista de ricos inaugural era formada por herdeiros. Muitos dos demais tinham um histórico que envolvia começar a vida já em situação bastante favorável, nos moldes de Rupert Murdoch ou Donald Trump. A revolução tecnológica mudou essa dinâmica aqui e no mundo inteiro.*

como espécies de capital passou a ser a marca das sociedades pós-industriais, naquela que recebeu a alcunha de "sociedade da informação".[6]

Esse movimento é notado, entre outros, por Barlow,[7] ao lembrar que, no passado, as grandes economias eram estruturadas em torno da propriedade de bens materiais. No atual contexto, entretanto, a informação e os dados subverteram esse papel, "avançando sobre a posição econômica dos átomos"[8] para se tornar o capital mais valioso do novo século.

Para se perceber essa mudança, basta pensarmos no valor econômico das *big techs,*[9] no crescimento exponencial das *fintechs,*[10] na figura das *bitcoins* ou na própria economia de compartilhamento – que torna cada vez mais irrelevante a propriedade dos bens, à medida que seu uso é suscetível de vasto compartilhamento.

Esse estado de coisas (*Sachverhalt*), atualmente convertidas em *bits*, ante os fenômeno da disrupção[11] e digitalização,[12] acabou por inaugurar um novo modelo produtivo, identificado por Zuboff como "o capitalismo de vigilância",[13] por meio do qual

---

Em 2002, 52% dos bilionários globais da Forbes – uma estreita maioria – eram pessoas que enriqueceram por esforço próprio, sendo 59% entre os norte-americanos. Dez anos atrás, esse total havia disparado para 69% em nível mundial". Essa mudança se deu especialmente, em razão do surgimento das empresas de tecnologia, no vale do silício, como explica mais à frente a matéria. LANE, Randall. Covid-19 provoca a maior aceleração da riqueza em toda a história da humanidade. **Forbes Brasil**. São Paulo, 2021. Disponível: https://forbes.com.br/forbes-money/2021/04/covid-19-provoca-a-maior-aceleracao-da-riqueza-em-toda-a-historia-da-humanidade/. Acesso em: 29 abr. 2021.

[6] Expressão atribuída a Machlup. *Cf*. MACHLUP, Fritz. **The production and distribution of knowledge in the United States**. Princeton, Princeton University Press, 1962.

[7] BARLOW, John. Selling Wine Without Bottles: The Economy of Mind on the Global Net. **Duke Law & Technology Review**, Durham, v. 18, n. 1, 2019. ISSN: 2328-9600. Disponível em: https://scholarship.law.duke.edu/dltr/vol18/iss1/3. Acesso em: 3 maio. 2021.

[8] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 42.

[9] Isto é: das grandes empresas de tecnologia, como a Google, a Microsoft, a Apple e a Tesla, por exemplo.

[10] OLIVEIRA, Madalena Perestrelo de. As recentes tendências da FinTech: disruptivas e colaborativas. CORDEIRO, António Menezes, OLIVEIRA, Ana Perestrelo, DUARTE, Diogo Pereira (coord.). **Fintech: Desafios da Tecnologia Financeira.** 2. ed. Coimbra: Almedina. p. 63-73.

[11] Conceito abordado por Bower e Christensen para designar inovações tecnológicas com potencial disruptivo, isto é: de inaugurar um novo seguimento de produto ou tecnologia aptos a colocar fim a modelos e seguimentos pretéritos. Assim, nem toda inovação tecnológica é disruptiva, mas apenas aquela com potencial de substituir, na competição de marcado, modelos e opções do passado. BOWER, Joseph L; CHRISTENSEN, Clayton M. Disruptive Technologies: Catching the Wave. **Harvard Business Review (HBR)**, 1995. Disponível em: https://hbr.org/1995/01/disruptive-technologies-catching-the-wave. Acesso em: 25 out. 2022.

[12] Digitalização é o processo de transformar um documento físico para o formato digital, através de dispositivos e instrumentos apropriados. É um termo genérico utilizado para descrever a transformação digital da sociedade e da economia, também chamado de desmaterialização.

[13] Expressão cunhada por Shoshana Zuboff, para designar: "1. Uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas; 2. Uma lógica econômica parasítica na qual a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento; 3. Uma funesta mutação do capitalismo marcada por concentrações de riqueza, conhecimento e poder sem precedentes na história da humanidade; 4. A estrutura que serve de base para a economia de vigilância; 5. Uma ameaça tão significativa para a

dados e metadados são produzidos, coletados e analisados a todo instante, num persistente monitoramento de hábitos, preferências e aspirações.

Esse sistema somente é possível na medida em que grande parte de nossos hábitos, na sociedade da informação, como pagar por produtos, viajar, enviar mensagens, clicar em *hyperlinks* ou, simplesmente, escutar músicas e fazer ligações, se arrisca a deixar um rastro digital (*digital trace*), condicionando em maior ou menor medida, nossas escolhas, hábitos e preferências. Aquilo que somos, fomos e seremos – presente, passado e futuro.

A partir dessa percepção, situada no campo de alargados controle e vigilância, é que Bauman diagnostica uma viragem no papel da privacidade, apontando que, na atualidade, tudo aquilo que é privado passa a ser feito potencialmente em público – e está potencialmente disponível para consumo público de alguma maneira.[14]

A distinção entre as esferas pública e privada, portanto, tem a sua razão de ser (*raison d'être*) atenuada, anunciando, para os mais enérgicos, o prelúdio da "morte da privacidade" ("*la morte della privacy*").[15]

---

natureza humana no século XXI quanto foi o capitalismo industrial para o mundo natural nos séculos XIX e XX; 6. A origem de um novo poder instrumentário que reivindica domínio sobre a sociedade e apresenta desafios surpreendentes para a democracia de mercado; 7. Um movimento que visa impor uma nova ordem coletiva baseada em certeza total; 8. Uma expropriação de direitos humanos críticos que pode ser mais bem compreendida como um golpe vindo de cima: uma destituição da soberania dos indivíduos". ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução George Schlesinger. Rio de Janeiro: Intrínseca, 2021, p. 13.

[14] BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. São Paulo: Zahar, 2013, p. 22.

[15] Para se entender melhor a expressão Ugo Pagallo faz referência ao escândalo do programa Prism da Agência de Segurança Nacional Americana (NSA), que eclodiu em 2013, após as revelações de Edward Snowden, transformando-se em um indicativo daquilo que muitos evocaram como a "morte da privacidade", dado o arsenal de meios técnicos de vigilância disponíveis com o recolha de metadados sobre comunicações eletrônicas, sistemas de filtragem ou geoposicionamento por satélite (GPS), câmaras de circuito fechado (CCTV), dados biométricos e os demais vestígios e conteúdos digitais difundidos com e-mails, compras através de cartões de crédito e operações bancárias, reservas de automóvel ou hotel, todas coletadas e processadas em bancos de dados gigantescos. Argumenta o autor que a tese da "morte da privacidade" nada mais é do que uma simplificação jornalística, ela teve, e ainda é, um grande sucesso, pois sintetiza a sensação de desorientação causada pela revolução tecnológica em curso. No original: "Molto prima dello scandalo del programma Prisma dell'Agenzia di sicurezza nazionale americana (NSA), scoppiato nel 2013 a séguito delle rivelazioni di Edward Snowden, è indicativo che in molti abbiano evocato la "morte della privacy", stante l'arsenale dei mezzi tecnici messi a disposizione con la raccolta di metadati sulle comunicazioni elettroniche, sistemi di filtraggio o di geo-posizionamento satellitare (GPS), telecamere a circuito chiuso (CCTV), dati biometrici e ulteriori tracce e contenuti digitali disseminati con le email, acquisti tramite carte di credito e operazioni bancarie, prenotazioni di macchine o alberghi, il tutto poi raccolto e processato in gigantesche banche dati. Sebbene, come argomenteremo, la tesi della "morte della privacy" non è che una semplificazione giornalistica, essa ha avuto, e riscuote tuttora di, un grande successo, perché sintetizza il senso di spaesamento provocato dalla rivoluzione tecnologica in corso.". PAGALLO, Ugo. **Il diritto nell'età dell'informazione**: Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti. Torino: G. Giappichelli Editore, 2014, p. 5.

A perspectiva pessimista, no entanto, se contrapõe à uma espécie de "vício pelas Tecnologias de Informação e Comunicação",[16] sintetizado com exatidão pelo sociólogo polonês na passagem: "*o velho pesadelo pan-óptico ([do] 'Nunca estou sozinho') [foi] agora transformado na esperança de 'Nunca mais vou ficar sozinho' (abandonado, ignorado e desprezado, banido e excluído), o medo da exposição foi abafado pela alegria de ser notado*".[17]

E essa alegria, explica a razão, em grande medida, de não mais se cogitar de uma privacidade fechada, isto é: de uma privacidade excludente, fora das redes, no sentido em que foi inicialmente concebida; mas de uma privacidade abrandada, que convive com as tecnologias e processos sociais em rede.

Para ilustrar o ponto de vista, é suficiente correlacionar os dados a respeito da participação das crianças e adolescente nas redes socais – o recorte sobre esse grupo de pessoas se dá pela especial condição de vulnerabilidade desses indivíduos, a justificar um controle mais próximo sobre os riscos a que estão expostos.[18]

Nesse sentido, os números levantados pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), ligado ao Comitê Gestor da Internet no Brasil (CGI.br), demonstram que, em 2015, cerca de 87% das crianças e jovem de 9 a 17 anos já possuía algum perfil em redes sociais[19].

As informações mais recentes do indicador[20] revelam um novo crescimento nas faixas etárias maiores, perfazendo 97% dos adolescentes entre 15 e 17 anos: quase a sua totalidade.[21]

---

[16] Expressão empregada por Ugo Pagallo. *Cf:* PAGALLO, Ugo. **Il diritto nell'età dell'informazione**: Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti. Torino: G. Giappichelli Editore, 2014, p. 1.

[17] BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. São Paulo: Zahar. p. 22-23.

[18] Para se ilustrar tais riscos, basta a conferência dos respectivos indicadores nas pesquisas citadas, dentre os quais se notam desde situações de discriminação e ofensas ao contato com conteúdos sensíveis.

[19] Por grupo de faixa etária, a pesquisa identificou que 96% dos adolescentes de 15 a 17 anos possuíam perfil em redes sociais, 93%, na faixa dos 13 e 14 anos, 79%, entre as crianças de 11 e 12 anos de idade e, finalmente, 63% entre as crianças de 9 e 10 anos de idade. BRASIL. Comitê Gestor da Internet no Brasil – CGI.br. **Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC Kids online Brasil 2015**. Núcleo de Informação e Coordenação do Ponto BR [editor]. São Paulo: Comitê Gestor da Internet no Brasil, 2016, p. 170. Disponível em: https://cetic.br/media/docs/publicacoes/2/TIC_Kids_2015_LIVRO_ELETRONICO.pdf. Acesso em: 10 out. 2021.

[20] BRASIL. Comitê Gestor da Internet no Brasil – CGI.br. **Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC Kids online Brasil 2018**. Núcleo de Informação e Coordenação do Ponto BR [editor]. São Paulo: Comitê Gestor da Internet no Brasil, 2019, p. 170. Disponível em: https://cetic.br/media/docs/publicacoes/2/TIC_Kids_2015_LIVRO_ELETRONICO.pdf. Acesso em: 10 out. 2021.

[21] Na contramão disso, possivelmente em razão da melhor compreensão sobre os riscos associados à utilização das redes sociais por crianças e adolescentes, viu-se uma diminuição, ainda que pequena, em

Se considerarmos que esses dados se referem ao ano de 2018, quando o percentual de domicílios que utilizavam a internet era de aproximadamente 79,1%, conforme a Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD-Contínua) do IBGE;[22] e que essa proporção já teria sofrido um incremento na casa dos 3,6 pontos percentuais, passando para 82,7%[23] dos domicílios no ano 2019;[24] somos capazes de antever um número ainda maior de usuário nesse novo contexto informacional.

Todas essas evidências denotam o apreço social pela convivência em rede, sendo um dos grandes desafios da atualidade conciliar a exposição digital com a preservação de um núcleo essencial de direitos relativos à privacidade e à proteção de dados pessoais.

O desafio aumenta à medida que despontam um sem-número de riscos aos usuários das tecnologias digitais, como a tomada de decisões automatizadas com potencial discriminatório;[25] o roubo de identidade, o aumento do número de fraudes, inclusive bancárias e casos de engenharia social;[26] a disseminação de *fake news* fabricadas e direcionada à medida, com o especial intuito de influir a percepção de um grupo de indivíduos sobre determinado assunto – condicionando, especialmente, o sentido de voto de bolsões de cidadãos em eleições futuras;[27] além dos notórios casos de vazamentos de dados, com potencial danoso ainda incerto em toda sua extensão, a exemplo da situação

relação à utilização das redes sociais pelas demais faixas etárias, perfazendo 88% dos adolescentes entre 13 e 14 anos, 70% entre as crianças de 11 e 12 anos de idade e 58% entre as de 9 e 10 anos de idade. BRASIL. Comitê Gestor da Internet no Brasil – CGI.br. **Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil : TIC Kids online Brasil 2018**. Núcleo de Informação e Coordenação do Ponto BR [editor]. São Paulo: Comitê Gestor da Internet no Brasil, 2019, p. 170. Disponível em: https://cetic.br/media/docs/publicacoes/2/TIC_Kids_2015_LIVRO_ELETRONICO.pdf. Acesso em: 10 out. 2021.

[22] BRASIL. Instituto Brasileiro de Geografia e Estatística – IBGE. **PNAD Contínua TIC 2019: internet chega a 82,7% dos domicílios do país**. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/30521-pnad-continua-tic-2019-internet-chega-a-82-7-dos-domicilios-do-pais. Acesso em: 5 out. 2021.

[23] BRASIL. Instituto Brasileiro de Geografia e Estatística – IBGE. **PNAD Contínua TIC 2019: internet chega a 82,7% dos domicílios do país**. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/30521-pnad-continua-tic-2019-internet-chega-a-82-7-dos-domicilios-do-pais. Acesso em: 5 out. 2021.

[24] Isso, antes mesmo da expansão forçada das Tecnologias de Informações e Comunicação (TICs) pelas medidas de distanciamento social ocasionadas pela pandemia da COVID-19.

[25] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Revista Direito Público**, Brasília, v. 16, n. 90, p. 39–64, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em: 2 maio 2021.

[26] CASE, Tony. WTF is jobfishing (and how to avoid it). **Worklife**. [s.l.], 2022. Disponível em: https://www.worklife.news/talent/wtf-is-jobfishing-and-how-to-avoid-it/. Acesso em: 25 jun. 2022.

[27] MARS, Amanda. Como a desinformação influenciou nas eleições presidenciais? **El País**. Nova York, 2018. Disponível em: https://brasil.elpais.com/brasil/2018/02/24/internacional/1519484655_450950.html. Acesso em: 25 jun. 2022.

envolvendo a *Cambridge Analytica*[28] ou os dois megavazamentos de dados pessoais que atingiram milhões de brasileiros em 2021.[29]

Essa miríade de riscos, no entanto, coloca em xeque o poder do Estado de dar respostas adequadas às incursões de entidades públicas e privadas sobre a vida particular e os dados pessoais de seus cidadãos. Enquanto o progresso parece caminhar a passos largos, a regulação está sempre há alguns distância em seu encalço.[30] E esse cenário ganha uma tônica diferente à medida que se nota faltar fôlego ao ente público nesse percurso. A escassez de seus recursos e a percepção de que os problemas aos quais são convocados a atuar, além de múltiplos e dinâmicos, transcendem os interesses e as fronteiras nacionais, parecendo minar sua capacidade de resolvê-los de modo isolado.[31]

A policontextualidade, a multiplicidade e a correlação entre os problemas enfrentados na sociedade da informação parecem demonstrar que cada vez mais as nações precisam cooperar entre si e com atores privados, especialmente em matérias cada vez mais complexas, dinâmicas e com alto grau de especialização.

Dessa necessidade, exsurge o problema a ser tratado nessa pesquisa: como garantir um adequado grau de intervenção regulatória de modo a se conciliar a proteção de direitos fundamentais dos cidadãos, sem sufocar a capacidade de atuação dos agentes privados, responsáveis, em grande medida, pela inovação e pelo desenvolvimento em nossas sociedades? A disrupção, a convergência[32] e a digitalização parecem colocar

---

[28] CONFESSORE, Nicholas. Cambridge Analytica and Facebook: the scandal and the fallout so far. **The New York Times**. New York, 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 05 maio 2021. ALVES, Paulo. Facebook e Cambridge Analytica: sete fatos que você precisa saber. **TechTudo**. São Paulo, 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/03/facebook-e-cambridge-analytica-sete-fatos-que-voce-precisa-saber.ghtml. Acesso em 05 maio 2021.

[29] CORACCINI, Raphael. Fotos e até salários estão entre os dados vazados de 223 milhões de brasileiros. **CNN Brasil**. São Paulo, 2021. Disponível em: https://www.cnnbrasil.com.br/business/2021/01/27/fotos-e-ate-salarios-estao-entre-os-dados-vazados-de-223-milhoes-de-brasileiros. Acesso em 5 maio 2021. SAMBRANA, Carlos. Exclusivo: Novo vazamento expõe mais de 100 milhões de contas de celular. **NEOFeed**. São Paulo, 2021. Disponível em: https://neofeed.com.br/blog/home/exclusivo-novo-vazamento-expoe-mais-de-100-milhoes-de-contas-de-celular/. Acesso em: 5 maio 2021.

[30] Fato natural, diante da disruptividade tecnológica, contudo, seus efeitos não deixam de nos preocupar.

[31] OTERO, Paulo. **Manual de Direito Administrativo**. vol. 1. Coimbra: Almedina, 2013, p. 515.

[32] A convergência é frequentemente definida, em termo gerais e simplificados, como um processo pelo qual as telecomunicações, as tecnologias da informação e as mídias em geral, setores que originalmente operam largamente de forma independente uns dos outros, passam a se desenvolver conjuntamente. Isso tem ocorrido em níveis diferentes, por exemplo, nas infraestruturas, nos dispositivos destinados aos usuários finais ou em serviços. Segundo Stobbe e Just, podemos definir convergência como um processo de mudança qualitativa que conecta dois ou mais mercados existentes, anteriormente distintos. A força motriz desse processo seria o desenvolvimento de uma nova tecnologia ou a integração de diversas tecnologias que permitem infraestruturas, dispositivos destinados a usuários finais ou serviços adquirirem novas funcionalidades. Outra importante fonte de convergência de mercado, para os autores, é a mudança nas características de um produto resultando em novas tecnologias (convergência do produto). STOBBE, Antje;

obstáculos sensíveis à regulação do ciberespaço, impondo que alternativas sejam pensadas, especialmente soluções conciliatórias e de natureza híbrida (coparticipativas).

Nesse passo, como hipótese levantada pela pesquisa, encontra-se o desenvolvimento de um sistema de controle e fiscalização dialógico que englobe mecanismos de conformação democrática entre agentes públicos e privados, sem olvidar a adoção de um sistema de *enforcement*, que permita tutelar adequadamente os direitos à privacidade e à proteção de dados constitucionalmente assegurados.[33]

A hipótese a ser testada é a de que o desenvolvimento de códigos de conduta, mecanismos de certificação, selos, marcas de proteção de dados e listagens, poderiam prover um modelo regulatório dinâmico e coeso para a proteção de dados pessoais, capaz de equilibrar e conciliar uma atuação pública e privada cooperativa.

Assim, para investigar o assunto, a pesquisa divide-se em três partes, avaliando diferentes formas de se conceber o papel do Estado como agente regulador. A primeira delas, centrará seu foco na análise sobre o desenvolvimento das estruturas produtivas ao longo dos séculos e de como a ausência de regulação por parte do Estado é capaz de levar a cenários exploração de grupos vulneráveis como os trabalhadores

Busca-se, também, demonstrar como saímos de um modo de produzir centrado em bens materiais para outro fundado na economia de dados.

Na sequência, entendidos o contexto histórico, passamos à análise dos principais riscos associados às novas tecnologias, não, sem antes, entender a nova gramática engendrada por tais artifícios.

A primeira parte, assim, traz os alicerces da pesquisa, avaliando os modelos produtivos ao longo dos séculos e como eles se refletiram na vida da população, até chegarmos à forma de produzir atual, fundada na coleta de dados e informações. Ali repousando, caminhamos para entender como essas novas tecnologias funcionam, os benefícios que apresentam, mas sobretudo, os riscos que despontam nesse novo cenário.

Desse modo, a primeira seção, com um certo pé no passado, fará um retrospecto histórico,[34] além da abordagem dos riscos e benefícios a que essas novas tecnologias nos sujeitam.

JUST, Tobias. The dawn of technological convergence. Economics 56. **Deutsche Bank Research**. Frankfurt a.M., may 3, 2006, p. 3.

[33] Este último, recentemente alçado à categoria de direito fundamental pela Emenda Constitucional n.º 115/2022, não obstante a academia já defendesse a existência desse direito, como a Professora Laura Schertel Ferreira Mendes.

[34] Não tão remoto, na medida em que vemos a sua repetição em maior ou medida em situações que se transformam e reconfiguram, como o trabalho análogo ao escravo e a escravidão moderna.

A segunda parte, com uma perspectiva mais atual, abordará as "Estruturas de regulação", analisando, em um primeiro momento, as teorias relativas à regulação do cyberespaço, para depois, fixarmo-nos no desenvolvimento dos principais modelos regulatórios em matéria de privacidade e proteção de dados pessoais, em diferentes contextos: na Europa (com algum enfoque na experiência Alemã, berço da proteção de dados); nos Estados Unidos da América; e na América Latina (com destaque para o Uruguai, que apresenta um modelo peculiar de proteção de dados, e o Brasil, objeto de nossas formulações futuras).

Essa perspectiva dos principais modelos regulatórios (o europeu e o estadunidense, acompanhada de alguma ponderação sobre outros modelos regulatórios mais restritos, como o uruguaio) permitirá que saibamos em que passo estamos e qual o estado da arte no que se refere à regulação da matéria.

A segunda parte, ainda que mais voltada à atualidade, não se esquece de considerar como é que aqui se chegou, abordando o alvorecer do direito à proteção de dados pessoais e como foram desenvolvidos os modelos atuais, explicando, com alguma racionalidade, os diferentes papéis exercidos pelo Estado em cada um deles.

A terceira parte, como contraponto à primeira, buscará demonstrar que também a regulação estatal também não é indene a falhas. Essas falhas serão detalhadas e abordadas a partir da literatura internacional e nacional no estudo de regulação, que reúne um amplo arcabouço teórico tanto sobre as distorções provocadas pelo Poder Público quanto pelo Mercado, mormente quando tratamos de regular assuntos complexos, como as tecnologias digitais.

A partir disso, o terceiro capítulo volta-se para a proposição de uma teoria conciliadora e híbrida, que possa reunir e promover o diálogo entre atores públicos e privados, na busca de colmatar lacunas e falhas regulatórias.

Esse modelo híbrido é por nós intitulado de modelo regulatório sistemático-dialógico, na medida em que busca reunir elementos informativos e promover o diálogo entre agentes públicos e privados (por meio dos códigos de conduta), além de incentivos à observância das regras acordadas (mecanismos de certificação, selos e marcas de privacidade) e de desincentivos a seu descumprimento (listagens ou listas-sujas),[35] integrados na forma de um sistema de estímulos positivos e negativos na busca de um propósito definido.

[35] Sem excluir outras formas de atuação da Autoridade de Controle.

Esse sistema, na sequência, será estudado em pormenor, analisando como alguns desses mecanismos já são aplicados e seu potencial de aplicação ao contexto da privacidade e proteção de dados pessoais.

Por fim, algumas vantagens e desvantagens do modelo proposto são analisadas. Esses diferentes predicados são abordados de forma individual pela literatura, em relação a cada um dos diferentes mecanismos propostos. Não obstante, o que se espera ser a maior contribuição do trabalho, é passar a enxergá-los como mecanismos coesos e capazes de, apoiado uns nos outros, buscar suprir diferentes lacunas e necessidades que sozinhos não poderiam colmatar.

O referencial teórico da pesquisa girará em torno das teorias da regulação, sobretudo da regulação do cyberespaço e da privacidade e proteção de dados pessoais. A pesquisa se utilizará do método dedutivo e da pesquisa bibliográfica-exploratória, para entender como os mecanismos em análise poderiam ser empregados na proteção dos direitos fundamentais dos cidadãos-usuários.

Esquadrinha-se por um modelo regulatório responsável, transparente e aberto à participação dos interessados, especialmente dos criadores de tecnologia, contemplando a inovação com responsabilidade, naquilo que o Professor Emérito de Direito Público da Universidade de Hamburgo, Wolfgang Hoffmann-Riem, defende como a "responsabilidade pela criação", exortando o papel não só do Estado, mas do mercado e dos desenvolvedores nas repercussões práticas de suas criações.

O objetivo geral de toda essa incursão é oferecer novos horizontes à proteção de dados pessoais no Brasil de forma a se salvaguardar os direitos dos titulares de dados pessoais, sem que representem um obstáculo ao desenvolvimento tecnológico, na busca de uma sociedade digital livre, próspera e segura.

PARTE I – O PROGRESSO E A GRAMÁTICA DAS NOVAS TECNOLOGIAS: ENTENDENDO O QUADRO COMUNICATIVO E OS RISCOS ASSOCIADOS

Antes de darmos início a uma análise mais específica sobre a regulação das Tecnologias da Informação e Comunicação (TIC's), nada mais oportuno que abordarmos a forma com que o progresso tecnológico repercutiu socialmente ao longo dos anos e os caminhos que nos levaram a um modelo produtivo baseado na utilização em larga escala de dados pessoais.

Essa primeira abordagem nos servirá para entender de que forma a inovação, sem qualquer espécie de intervenção, pode representar um sério risco à garantia de um patamar civilizatório mínimo de direitos. Isso porque estimula práticas exploratórias aviltantes de uma série de direitos, como saúde, liberdade, dignidade, e a própria existência de populações vulneráveis.

A análise sobre os processos e os modos de produção trazem uma perspectiva bastante autêntica a respeito das consequência de uma regulação frágil ou inexistente, que se contraporá, mais a frente à existência de mecanismos regulatórios mais fechados e seus potenciais efeitos.

Nas próximas linhas, segue-se um apanhado histórico e teórico, direcionado aos propósitos do trabalho, acerca das revoluções industriais e da vida em sociedade ao longo nos últimos séculos.

1. Da máquina à nuvem:[36] o desenvolvimento do atual modelo de economia baseado em dados.

"A cada dia, novas tecnologias fazem do hoje algo muito diverso do que foi o ontem", [37] com essas palavras o Ministro do Supremo Tribunal Federal, Luiz Fux, faz a abertura do livro do Professor e procurador da República, João Paulo Lordelo,

[36] Expressão cunhada por Ana Carolina Reis Paes Leme, para designar o processo de transformação transcorrido desde a primeira revolução industrial até os dias atuais, marcado pelo fenômeno da digitalização e desmaterialização. Conforme aponta: "Primeiro, veio o carvão. Com sua queima, ele aqueceu a água, que virou vapor e empurrou o pistão. O pistão pôde mover a primeira máquina e assim a humanidade converteu uma nuvem de vapor em movimento. Nos dias de Hoje, com a internet, a nuvem de vapor da máquina industrial se tornou uma nuvem de bits". LEME, Ana Carolina Reis Paes. **Da máquina à nuvem**: caminhos para o acesso à justiça pela via de direitos dos motoristas da Uber. São Paulo: LTr, 2019, p. 67.

[37] FUX, Luiz. Apresentação, *In*: LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. São Paulo: Juspodivm, 2022, p. 9.

"Constitucionalismo digital e devido processo legal"[38]. Em singelas palavras o Ministro nos recorda da capacidade de transformação proporcionada pelo saber científico e pela tecnologia.

Essas transformações, ao longo da história, foram agrupadas em verdadeiros marcos epistemológicos, representativos das formas de produção e do modo de vida das pessoas nos últimos séculos. Referimo-nos àquilo que se denominou de revoluções industriais.[39]

A Primeira Revolução Industrial ocorreu na segunda metade do século XVIII (1760 – 1840) e representou o primeiro paradigma na área de produção em grande escala,[40] tendo como foco as fábricas instaladas em aglomerados urbanos, que, mais tarde, se expandiram por toda a Europa. A moderna industrialização substituía o modelo de trabalho artesanal e manufatureiro, pelo assalariado, com o uso de máquinas que acarretaram profundas alterações sociais e econômicas.[41] [42]

Iniciada na Inglaterra e se espraiando na sequência pelo restante da Europa Ocidental e pelos Estados Unidos, a primeira revolução industrial foi marcada pela introdução das máquinas nos processos produtivos, pela fabricação de produtos químicos e pela expansão do transporte de pessoas e de produtos por meio das ferrovias e dos navios à vapor.[43] [44]

Os avanços dos métodos de produção agrícolas contribuíram de forma significativa no processo de industrialização inglês, mormente em razão da confluência

---

[38] LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. São Paulo: Juspodivm, 2022.

[39] "A palavra "revolução" denota mudança abrupta e radical. Em nossa história, as revoluções têm ocorrido quando novas tecnologias e novas formas de perceber o mundo desencadeiam uma alteração profunda nas estruturas sociais e nos sistemas econômicos." SCHWAB, Klaus. **A Quarta Revolução Industrial**. Tradução de Daniel Moreira Miranda. 1. ed., São Paulo: Edipro, 2016, p. 8.

[40] CFA. Conselho Federal de Administração. **Conheça as quatro Revoluções Industriais que moldaram a trajetória do mundo**. Disponível em: https://cfa.org.br/as-outras-revolucoes-industriais/. Acesso em: 19 outubro 2022.

[41] COSTA, Aline Moreira da; ALMEIDA, Victor Hugo de. Meio ambiente do trabalho: uma abordagem propedêutica. In: FELICIANO, Guilherme Guimarães et al. (Coord.). **Direito ambiental do trabalho**: apontamentos para uma teoria geral. São Paulo: LTr, v. 3, 2017, p. 50.

[42] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[43] CFA. Conselho Federal de Administração. **Conheça as quatro Revoluções Industriais que moldaram a trajetória do mundo**. Disponível em: https://cfa.org.br/as-outras-revolucoes-industriais/. Acesso em: 19 outubro 2022.

[44] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

de três grandes fatores: a ampliação da produção alimentícia; a disponibilização de mão de obra, decorrente do êxodo rural;[45] e a expansão da produção de matérias-primas.[46]

As alterações promovidas pelo advento do ambiente fabril ocasionaram significativas mudanças para a população egressa do campo, que viu intensificada a exploração de sua mão de obra por meio de um novo sistema marcado pela hierarquização, pela extensão do ritmo laboral (agora, controlado por máquinas), e pelo aumento de sua subordinação – representada pela estipulação de uma jornada laboral fadigosa, com controle de pontualidade e do trabalho prestado. [47] [48]

A mecanização do trabalho conquanto tenha propiciado a ampliação do consumo por meio do incremento da produtividade e da diminuição dos preços, também levou às enfermidades ocupacionais e ao aumento dos acidentes laborais, haja vista a exaustão do trabalhador; a existência de ambientes insalubres; e a insuficiente instrução sobre o manejo dos maquinários.

A numerosa mão de obra disponível propiciava que operários pudessem ser coisificados e descartados, em especial nos casos de acidentes de trabalho ou de adoecimento, quando apenas lhes restava serem socorridos pelas casas de caridade, em razão da inexistência de um ordenamento jurídico protetivo, quer de natureza trabalhista, quer relacionado à seguridade social.[49] [50]

---

[45] Isso se deu porque, com a evolução da capacidade de aproveitamento do solo, em razão da introdução de inovações tecnológicas, os trabalhadores, que antes se viam presos à terra em uma relação de colonato, foram afugentados do campo pelos senhores, proprietários de terra, levando a um aumento considerável de mão de obra na zona urbana, disponível para ser empregadas na crescente produção industrial. GUIMARÃES, Pollyanna Silva. **A tecnologia aliada à Construção do Direito do Trabalho**. São Paulo: LTr, 2016, p. 34-35.

[46] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[47] COSTA, Aline Moreira da; ALMEIDA, Victor Hugo de. Meio ambiente do trabalho: uma abordagem propedêutica. In: FELICIANO, Guilherme Guimarães et al. (Coord.). **Direito ambiental do trabalho**: apontamentos para uma teoria geral. São Paulo: LTr, v. 3, 2017, p. 50.

[48] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[49] COSTA, Aline Moreira da; ALMEIDA, Victor Hugo de. Meio ambiente do trabalho: uma abordagem propedêutica. In: FELICIANO, Guilherme Guimarães et al. (Coord.). **Direito ambiental do trabalho**: apontamentos para uma teoria geral. São Paulo: LTr, v. 3, 2017, p. 50.

[50] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

Essa primeira miragem do passado evidencia um quadro de exploração humana diretamente propiciado pela tecnologia. O ambiente fabril levou à possibilidade de mecanização da produção, rompendo com o modo de produzir artesanal. O ser humano "livre" passa a ser utilizado como espécie de insumo no processo produtivo, marcado por um ritmo de trabalho intenso. A marca da disrupção, ao pôr termo ao modelo de produção manufatureiro, instaurou um processo produtivo mecanicista, no qual latente os abusos, representados por jornadas exaustiva e a pela inexistência de um aparato jurídico-protetivo ao trabalhador.

A segunda revolução industrial (1850-1945), de outro lado, envolveu o desenvolvimento das indústrias química, elétrica, de petróleo e aço, além do progresso dos meios de transporte e comunicação.[51]

Atrelados a essa segunda revolução surgiram os dois primeiros modelos produtivos de larga escala: o taylorismo e o fordismo, frutos da intensificação da produção pelas tecnologias emergentes no período.

A forma de organização da produção desenvolvida por Taylor tinha como principal objetivo racionalizar o trabalho e, assim, aumentar sua produtividade. O Taylorismo visava alcançar a fragmentação máxima do trabalho, de forma a minimizar os movimentos e tarefas supérfluas, assim como o tempo para sua realização e aprendizado.[52]

Conforme aponta Lemes,[53] ele foi responsável por uma verdadeira revolução na estrutura produtiva da empresa. Previu a especialização e a divisão das tarefas e instituiu a hierarquia na produção, com a presença do chefe. Os seus estudos de ergonomia levaram-no a projetar um sistema produtivo em que havia certa sinergia entre máquina e homem, a fim de otimizar a produção no menor tempo possível. [54] [55]

---

[51] CFA. Conselho Federal de Administração. **Conheça as quatro Revoluções Industriais que moldaram a trajetória do mundo**. Disponível em: https://cfa.org.br/as-outras-revolucoes-industriais/. Acesso em: 19 outubro 2022.

[52] Taylor dividiu a execução do trabalho em movimentos individuais, analisou-os para determinar quais eram essenciais e, cronometrando as atividades realizadas por cada funcionário, estabeleceu um sistema remuneratório segundo a produtividade de cada indivíduo. Cf. TAYLOR, Frederick Winslow. **The Principles of Scientific Management**. 1911. Disponível em: https://www.gutenberg.org/ebooks/6435. Acesso em: 05 nov. 2022.

[53] LEME, Ana Carolina Reis Paes. **Da máquina à nuvem**: caminhos para o acesso à justiça pela via de direitos dos motoristas da Uber. São Paulo: LTr, 2019, p. 67-68.

[54] LEME, Ana Carolina Reis Paes. **Da máquina à nuvem**: caminhos para o acesso à justiça pela via de direitos dos motoristas da Uber. São Paulo: LTr, 2019, p. 67-68.

[55] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

Aproveitando-se de sua formação como engenheiro, Taylor planejou, organizou e racionalizou a produção, atribuindo à chefia a incumbência de cronometrar o tempo de execução das tarefas.

As teorias tayloristas, desenvolvidas na Europa, foram, mais tarde, aprimoradas por Ford, em sua fábrica de automóveis nos Estados Unidos da América. Suas principais contribuições foram a padronização da produção; o emprego de esteiras rolantes e linhas de montagem; a diminuição do tempo de produção ao padronizar os modelos e designar movimentos repetitivos aos seus funcionários; a rígida divisão de tarefas; bem como o barateamento dos produtos e a produção em massa. A partir disso, Ford promoveu o acréscimo da esteira de produção, que ditavam a velocidade da execução das tarefas, e promoveu a alienação do processo produtivo, na medida em que o trabalhador passou a saber fazer tão somente uma parcela do produto final.[56] [57]

A segunda revolução industrial, conforme assinala Harvey,[58] foi responsável, também pelo consumo em massa, para fazer frente à crescente produtiva. A divisão do dia de trabalho em "oito horas e cinco dólares" intentava, em parte, sujeitar o trabalhador a adquirir a disciplina necessária à operação da linha de montagem com alta produtividade, e, de outro lado, lhe proporcionar renda e tempo de lazer suficientes para que os produtos produzidos em larga escala fossem consumidos.[59]

A segunda revolução trouxe o início de alguma regulamentação, ainda que servindo aos propósitos de manutenção do consumo, como foi o caso da limitação da carga horária de trabalho, que antes chegava a mais de 16 horas diárias e passaria a girar entre 8 horas diária. No entanto, essas concessões se deram, como dito, com um propósito específico: o aumento do consumo, face o salto produtivo representado pelo aumento de eficiência na realização de tarefas, agora cronometradas, com metas a serem cumpridas e controladas por uma esteira de produção que ditava o ritmo do trabalho.

---

[56] LEAL, Carla Reita Faria; RODRIGUES, Débhora Renata Nunes. A precarização do trabalho na era digital e seu impacto no equilíbrio laboral-ambiental. **Veredas do Direito**, Belo Horizonte, v. 17, p. 137-165, 2020.

[57] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[58] HARVEY, David. **Condição pós-moderna**: uma pesquisa sobre as origens da mudança cultural. Tradução de Adail Ubirajara Sobral e Maria Stela Gonçalves. 17. ed. São Paulo: Edições Loyola, 2008, p. 122.

[59] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

A Terceira Revolução Industrial (1950–2010), por sua vez, também chamada de Revolução Informacional, teve seu foco no desenvolvimento da eletrônica e representou uma verdadeira modernização da indústria. Esse período foi marcado pela substituição gradual da mecânica analógica pela digital, pelo uso de microcomputadores e pela criação da internet (1969) – na época, chamada pelo governo americano de Arpanet. [60] [61]

Também nesse período tem início o fenômeno da digitalização e a invenção da robótica.

A modernização dos meio de produção, agora digitais, levou à ruptura do modelo fordista-taylorista, pois, nas palavras Guimarães,[62] este não se mostrava mais apto a suprir as necessidades advindas da complexidade tecnológica, que instalava a imperatividade da intelectualidade para a execução das atividades, requerendo, assim, destreza do trabalhador.[63] [64]

Além da valorização do trabalho intelectual, esse período é marcado pela alavancagem dos processos produtivos e comerciais em escala global. O encurtamento das distâncias em razão dos meios de comunicação e transporte levou à possibilidade de uma produção flexível, informada por dados de demanda e consumo, e pela produção e prestação de bens e serviços em diferentes partes do mundo.

Conforme destaca Harvey,[65] esse cenário conduziu à reformulação do sistema produtivo, representado pelo que se denominou de "regime de acumulação flexível", amparado na "flexibilidade dos processos de trabalho, dos mercados de trabalho, dos produtos e padrões de consumo", caracterizando-se pela emersão de novos setores de produção, mercados, modos de provisão de serviços financeiros e, acima de tudo, "taxas

[60] CFA. Conselho Federal de Administração. **Conheça as quatro Revoluções Industriais que moldaram a trajetória do mundo**. Disponível em: https://cfa.org.br/as-outras-revolucoes-industriais/. Acesso em: 19 outubro 2022.
[61] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.
[62] GUIMARÃES, Pollyanna Silva. **A tecnologia aliada à Construção do Direito do Trabalho**. São Paulo: LTr, 2016, p. 39-40.
[63] LEAL, Carla Reita Faria; RODRIGUES, Débhora Renata Nunes. A precarização do trabalho na era digital e seu impacto no equilíbrio laboral-ambiental. **Veredas do Direito**, Belo Horizonte, v. 17, p. 137-165, 2020.
[64] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.
[65] HARVEY, David. **Condição pós-moderna**: uma pesquisa sobre as origens da mudança cultural. Tradução de Adail Ubirajara Sobral e Maria Stela Gonçalves. 17. ed. São Paulo: Edições Loyola, 2008, p. 140.

altamente intensificadas de inovação comercial, tecnológica e organizacional", por todo o globo.[66]

Trata-se da globalização mercadológica, que tem seus contornos traçados nesse período. A forma produtiva, desde a invenção da internet, conduziu a modificações na exploração do trabalho humano, com a valorização do trabalho intelectual (imaterial), corporificado em máquinas, utensílios, *softwares*, programas e projetos.[67]

A Terceira Revolução Industrial permitiu o desenho de um novo sistema de produção,[68] tendo como um de seus precursores Eiji Toyoda, que buscava a eliminação das perdas e uma produtividade qualitativa.[69] Leme[70] esclarece que Eiji Toyota e o engenheiro Taiichi Ohno, após observarem o modelo implantado na *Ford Motors*, estabeleceram, em 1970, uma forma de administração que coordenava a produção de acordo com a demanda específica de veículos variados, o chamado "*just in time"*. Assim nasceu o sistema toytista de produção, também chamado de "produção flexível".[71]

Segundo Antunes[72] (2011, p. 33-34), o atendimento do modelo toyotista requereu a "flexibilização dos trabalhadores" por meio de direitos flexibilizados, que viabilizaram que se dispusesse da força de trabalho em razão direta das "necessidades do mercado consumidor", de modo que o modelo em tela se sustentou em um quantitativo mínimo de trabalhadores, o qual era majorado com base, *v. g.*, em horas extras, trabalhadores temporários ou subcontratação.[73]

---

[66] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[67] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[68] ANTUNES, Ricardo. **Adeus ao trabalho?** ensaio sobre as metamorfoses e a centralidade do mundo do trabalho. 15. ed. São Paulo: Cortez, 2011, p. 32.

[69] MARTINEZ, Luciano; MALTEZ, Mariana. O direito fundamental à proteção em face da automação. **Revista de direito do trabalho**, São Paulo, SP, v. 43, n. 182, p. 21-59, out. 2017,

[70] LEME, Ana Carolina Reis Paes. **Da máquina à nuvem**: caminhos para o acesso à justiça pela via de direitos dos motoristas da Uber. São Paulo: LTr, 2019, p. 69.

[71] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[72] ANTUNES, Ricardo. **Adeus ao trabalho?**: ensaio sobre as metamorfoses e a centralidade do mundo do trabalho. 15. ed. São Paulo: Cortez, 2011, p. 33-34.

[73] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

Diferentemente do taylorismo, que atingiu sobremaneira a saúde física do trabalhador, Oliveira[74] salienta que os novos padrões gerenciais advindos do modelo japonês impactaram também na saúde psicossocial dos indivíduos, citando, por exemplo, a experiência vivenciada no Japão em que o estresse dos trabalhadores "sob as práticas de gestão enxuta" resultou no que se denominou de Karoshi, ou seja, a morte por exaustão, por excesso de trabalho.[75]

Marca esse período um momento de fuga a qualquer espécie de regulação. A evolução dos meios de comunicação e transporte permitiu que a produção dos mais variados componentes, insumos e serviços pudesse ser feita à quilômetros de distância de onde o bem ou serviço é consumido, geralmente, em países nos quais a regulação de direitos e garantias trabalhistas são escassos ou apresentam baixo nível de proteção. Isso se reflete no fenômeno do *Dumping Social*, que consiste na busca de vantagens competitivas (diminuição do custo da produção) por meio da migração (instalação da produção em países com legislações flexíveis) ou da infração a direitos trabalhistas.[76]

O fenômeno, possibilitado pela globalização, é facilmente percebido ao se verificar a procedência de grande parte das mercadorias consumidas em escala global. Atualmente, o emprego da tecnologia tem permitido que até mesmo serviços sejam prestados à distância, com destaque para as atividades de suporte tecnológico, atendimento ao consumidor e telemarketing.

É também nesse período que os dados de consumo e de produção começam a despontar como elemento da organização e manejo da produção, por natureza, flexível,

---

[74] OLIVEIRA, Simone. A qualidade da qualidade: uma perspectiva em saúde do trabalhador. **Cad. Saúde Públ.**, Rio de Janeiro, 13 (4), pp. 625-634, out-dez, 1997. p. 632. Disponível em: https://www.scielosp.org/pdf/csp/1997.v13n4/625-634/pt. Acesso em: 21 meio 2020, p. 632-633.

[75] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[76] Cf. BUELENS, Jan; RIGAUX, Marc. (eds.). **From Social Competition to Social Dumping**. Antwerp and Portland: Intersentia (Cambridge Core), 2016. O livro traz uma visão europeia sobre o fenômeno, considerando os diferentes países que compõe o Bloco Europeu e o Mercado Comum Europeu. Na obra, o Dumping Social é tratado como um fenômeno controverso. É considerado a partir da existência de um baixo nível de proteção social ou de baixos padrões trabalhistas nas legislações nacionais que acabam por permitir que fornecedores de bens e serviços ofertem seus produtos e atividades a um custo mais baixo. A controvérsia surge ao avaliar se essa estratégia constitui uma tática legítima ou não. No âmbito europeu, por exemplo, é discutido se ela decorre legitimamente do poder conferido a cada Estados-Membros de regular seus sistemas de segurança social de forma autônoma ou se constitui uma vantagem competitiva ilegítima, dando lugar a uma 'race to the bottom' (uma corrida pela precarização) nas legislações nacionais de segurança social. O livro discute a repercussão de diferentes níveis de proteção social sob a perspectiva dos direitos fundamentais dos trabalhadores. A análise é interessante pois não se restringe ao *locus* comum em que o fenômeno é avaliado, a saber, os países asiáticos e subdesenvolvidos, que, usualmente, têm baixos níveis de proteção e se tornam grandes centros de fabricação de insumos e de mão de obra barata.

modulando a intensidade produtiva consoante a necessidade, de forma a se poupar insumos, mão de obra e tempo de produção. Ocorre que, para se ajustar a esse cenário de produção flexível, também são flexibilizados direitos sociais e trabalhistas, como a sucessiva recorrência a horas-extras (às vezes, além do permitido), a contratos temporários, subcontratações e terceirizações, nem sempre lícitas, para não se falar em quadros ainda mais graves como as situações de trabalho análogo ao escrevo e a escravidão moderna.

Em suma, o cenário demonstra a conformação dos arranjos produtivos à interferência estatal, num movimento centrífugo às tentativas de regulação pelo direito.

A quarta revoluções industrial (ou indústria 4.0), por fim, designa o período mais recente em que vivemos. O termo foi cunhado originalmente por Klaus Schwab[77] e popularizou-se durante o Fórum Mundial Econômico de 2016.

A quarta revolução industrial faz referência às novas ondas tecnológicas, como o advento dos *smartphones*, da inteligência artificial, da aprendizagem de máquina, do *Big Data*, da Computação em nuvem, das plataformas virtuais, dos aplicativos e das *startups,*[78] tendo como marco temporal a virada do último século (2010 – até atualmente).

A existência de uma nova etapa "revolucionária", no entanto, ainda é objeto de debate. Isso porque, para alguns autores, a quarta revolução industrial não representaria uma verdadeira clivagem, mas a continuação da etapa produtiva anterior. Nesse sentido, Johngo Lee e Keun Lee[79] defendem que as cinco tecnologias[80] representativas da indústria 4.0 não trariam uma radical inovação se comparadas com aquelas desenvolvidas até a década de 2010.[81]

Trata-se, no entanto, de uma posição diversa daquele defendida por Klaus Schwab,[82] para quem a humanidade estaria no início de um novo ciclo, caracterizado pela

---

[77] SCHWAB, Klaus. **A quarta Revolução Industrial**. Tradução de Daniel Moreira Miranda. 1. ed., São Paulo: Edipro, 2016.

[78] Termo utilizado para designar uma "empresa emergente" que tem como objetivo principal desenvolver ou aprimorar um modelo de negócio, preferencialmente escalável, disruptivo e repetível. Para alguns, trata-se de um modelo de negócios, sendo questionável atrelá-los à forma de empresa.

[79] LEE, Jongho; LEE, Keun. Is the fourth industrial revolution a continuation of the third industrial revolution or something new under the sun? Analyzing technological regimes using US patent data. ***Industrial and Corporate Change***, vol. 30, n. 1, 2021, p. 157, para os quais o estágio atual de desenvolvimento é uma mera continuação do anterior, não havendo inovações suficientes que pudessem distingui-lo e emancipá-lo do anterior.

[80] A saber: a impressão 3D; o Big Data; a Internet das Coisas (IoT), a Inteligência Artifical (AI); e a computação em nuvem (cloud computing).

[81] LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. São Paulo: Juspodivm, 2022, p. 83-84.

[82] SCHWAB, Klaus. **A quarta Revolução Industrial**. Tradução de Daniel Moreira Miranda. 1. ed., São Paulo: Edipro, 2016.

intensa presença da internet móvel na vida das pessoas; pelo desenvolvimento de sensores e processadores cada vez menores e mais poderosos; pelo uso da inteligência artificial em larga escala; pelas aplicações do *Big Data*; pela interconexão entre aparelhos pela internet das coisas (IoT); e pelo desenvolvimento de programas com aprendizado de máquina (*machine learning*).[83]

Apesar da crítica minoritária, a quarta revolução industrial espraiou-se pela literatura. Segundo destaca Lordelo:[84]

> Analisando a literatura sobre o assunto, é possível compreender que, apesar da precisão dos argumentos de Lee e Lee, a expressão "quarta revolução industrial" já é uma realidade. Exemplo disso é o trabalho de Luciano Floridi,[85] para quem, assim como as revoluções tecnológicas anteriores, a quarta revolução foi capaz de abalar os limites do autoconhecimento. Nesse sentido, estaríamos diante de um novo tipo de iluminismo capaz de permitir a compreensão do ser humano como um novo tipo de organismo. Segundo o autor, a humanidade está aceitando paulatinamente a ideia pós-Turing no sentido de que não somos seres newtonianos ou agentes únicos, mas sim organismos informacionais (*inforgs*) em um ambiente informacional (*inforphere*). Essa aceitação decorre da transição da *história* para a *hiper-história* e da dependência em tecnologias da informação e comunicação (ICTs). Nessa nova revolução copernicana, os seres humanos não podem mais ser considerados o centro da infosfera. Isso porque nossas memórias, decisões, tarefas diárias e outras atividades são constantemente delegadas a agentes artificiais.
>
> Seja como for – estejamos ou não em uma etapa tecnológica essencialmente nova ou em uma continuidade da terceira revolução –, o fato é que, especialmente a partir da década de 2010, os produtos e serviços digitais adentraram fortemente a vida das pessoas.

Ademais, para o autor, "cada vez mais, as relações humanas são marcadas pela intermediação de ferramentas tecnológicas complexas, cujo uso tem promovido profundas transformações nos variados campos de interação social".[86] Embora ainda estejamos no início dessa revolução, já podemos notar cenários surpreendentes e vislumbrar potenciais de aplicação que, de fato, nos fazem refletir sobre a chegada do futuro.

---

[83] FUX, Luiz. Apresentação, *In*: LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. São Paulo: Juspodivm, 2022, p. 9.
[84] LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. São Paulo: Juspodivm, 2022, p. 84-85.
[85] FLORIDI, Luciano. *The 4th revolution.* How the infosphere is reshaping human reality. Oxford: Oxford University Press, 2014.
[86] LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. São Paulo: Juspodivm, 2022, p. 85.

Alguns desses potenciais serão tratados mais à frente, destacando-se, para se ilustrar um pouco desse cenário, a possibilidade de utilização do *Big Data* aliado ao sequenciamento genético para a produção de terapias customizadas a nível celular; a nanotecnologia e computação quântica; o melhoramento humano (*human enhancement*); a constituição e funcionamento de lojas e serviços pelo metaverso; entre outros potenciais diversos de aplicação, alguns já em utilização.

Schwab[87] ainda aponta que:

> A quarta revolução industrial (...) não diz respeito apenas a sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo. Ondas de novas descobertas ocorrem simultaneamente em áreas que vão desde o sequenciamento genético até a nanotecnologia, das energias renováveis à computação quântica. O que torna a quarta revolução industrial fundamentalmente diferente das anteriores é a fusão dessas tecnologias e a interação entre os domínios físicos, digitais e biológicos.

O autor ainda retrata a rápida difusão dessas novas tecnologias. Enquanto o tear mecanizado (a marca da primeira revolução industrial) levou quase 120 anos para se espalhar para fora da Europa e a segunda revolução industrial ainda precisa ser plenamente vivida por 17% da população mundial – eis que quase 1,3 bilhão de pessoas ainda não têm acesso à eletricidade no mundo – a internet se espalhou pelo globo em menos de uma década.[88]

No campo produtivo, consoante aponta Schwab,[89] as "empresas digitais" geraram mais riqueza com um número muito reduzido de trabalhadores, podendo, em determinados casos, chegar a um custo irrisório ou inexistente à manutenção e ao desenvolvimento de suas atividades. Essa "revolução informacional" criou o que Supiot[90] chamou de trabalhador conectado, que precisa realizar os desígnios estabelecidos, respondendo prontamente aos sinais recebidos. [91]

---

[87] SCHWAB, Klaus. **A quarta Revolução Industrial**. Tradução de Daniel Moreira Miranda. 1. ed., São Paulo: Edipro, 2016, p. 9.

[88] Não obstante o exposto, mais da metade da população mundial, 4 bilhões de pessoas, ainda não tinha acesso à internet. SCHWAB, Klaus. **A quarta Revolução Industrial**. Tradução de Daniel Moreira Miranda. 1. ed., São Paulo: Edipro, 2016, p. 13.

[89] SCHWAB, Klaus. **A quarta Revolução Industrial**. Tradução de Daniel Moreira Miranda. 1. ed., São Paulo: Edipro, 2016, p. 19-21.

[90] SUPIOT, Alain. Por uma reforma digna do nome. E se refundarmos a legislação trabalhista?. **Le Mond Diplomatique**, França, Ed. 123, 4 out. 2017. Disponível em: https://diplomatique.org.br/reforma-trabalhista-na-franca-e-se-refundarmos-a-legislacao/. Acesso em: 15 set. 2022.

[91] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In:

Os novos modelos de negócio, emergentes na última década (2010) têm como marco a liquidez das relações negociais (os trabalhadores são contratados ou acionados para realização de tarefas singulares, desfazendo-se sua vinculação ao término da atividade),[92] a rapidez (própria dos meios tecnológicos) e a maximização do desempenho (fruto de uma sociedade de autoexploração, que coloca o indivíduo como único responsável por seu próprio sucesso).[93] [94]

O marco desses novos modelos de negócio são as plataformas digitais. Prassl, em recente trabalho publicado pela Universidade de Oxford, intitulado "*Human as a service: The promisse and perils of work in the gig economy*",[95] analisa a forma como essas plataformas buscam a desregulação no campo socio-trabalhista.

O autor relata uma espécie de farsa, que utiliza as linhas do código para esconder o trabalhador que, factualmente, realiza a atividade. Ele relembra que na década de 1770, foi apresentada à corte de Maria Theresa em Viena o primeiro robô jogador de xadrez completamente autômato do mundo – *the Mechanical Turk* (o Turco Mecânico) A máquina, teria a capacidade de reconhecer as estratégias de seus oponentes, pinçar as peças de xadrez e fazer suas próprias jogadas de forma automatizada.[96]

Ao longo dos anos, o Truco Mecânico (*the Mechanical Turk*) atraiu a atenção internacional, hipnotizada pela destreza da máquina. Apesar de muitas tentativas de revelar seus segredos (Edgar Allen Poe teria tido sua chance e Napoleão Bonaparte teria sido pego trapaceando contra a máquina), a tecnologia que permitia a proeza mágica, permaneceu um mistério até pouco antes de sua destruição em um incêndio no século XIX. [97]

LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[92] BAUMAN, Zygmunt. **Modernidade líquida**. Tradução Plínio Dentzein. Rio de janeiro: Zahar, 2001.

[93] Cf. HAN, Byung-Chul. Byung-Chul Han: "Hoje o indivíduo se explora e acredita que isso é realização". GELI, Carles. **El país**, Barcelona, 2018. Disponível em: https://brasil.elpais.com/brasil/2018/02/07/cultura/1517989873_086219.html. Acesso em: 27 out. 2022. HAN, Byung-Chul. Exaustos-e-correndo-e-dopados: Na sociedade do desempenho, conseguimos a façanha de abrigar o senhor e o escravo no mesmo corpo. BRUM, Eliane. **El país**, Barcelona, 2016. Disponível em: https://brasil.elpais.com/brasil/2016/07/04/politica/1467642464_246482.html. Acesso em: 27 out. 2022. HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Paulo Giachini. Petrópolis: Vozes, 2019.

[94] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[95] PRASSL, Jeremias. **Human as a service**: The promisse and perils of work in the gig economy. Oxford: Oxford University Press, 2018.

[96] PRASSL, Jeremias. **Human as a service**: The promisse and perils of work in the gig economy. Oxford: Oxford University Press, 2018.

[97] PRASSL, Jeremias. **Human as a service**: The promisse and perils of work in the gig economy. Oxford: Oxford University Press, 2018.

Ponderando-se que levaria mais de um século e meio até que o IBM *Deep Blue* enfrentasse e derrotasse o campeão mundial de xadrez Garry Kasparov nos anos 90, Prassl, indaga: "como o engenheiro austríaco Wolfgang von Kempelen conseguiu criar um robô de xadrez no século XVIII?". A resposta era bastante simples: agachado em um compartimento secreto dentro do tabuleiro de xadrez do Turco Mecânico havia um jogador humano, movendo as peças ao redor do quadro acima. Durante as apresentações pré-jogo, o operador era, literalmente, escondido por detrás da tecnologia moderna, movendo-se entre rodas giratórias, mostradores brilhantes e mecanismos complicados, que distraíam o público da verdade por dentro da máquina. [98] [99]

Mais de dois séculos depois o CEO da Amazon, Jeff Bezos, produziu uma plataforma pela qual se podia solicitar uma série de pequenas tarefas e por meio da qual uma multidão de indivíduos poderia, discretamente, realizá-las em alguns minutos, nominando essa plataforma de Amazon Mechanical Turk (MTurk).[100] [101]

O autor refere-se a uma das muitas plataformas que fazem parte daquilo que, atualmente se denomina de *gig economy (economia de "bicos").*

De Stefano,[102] consultor da OIT (Organização Internacional do Trabalho), aponta que o fenômeno da *gig economy* desenvolve-se em duas principais formas de trabalho: o *crowdwork* e o *work on-demand via apps.* A primeira modalidade, na descrição de Feliciano e Pasqualeto[103] abrange "plataformas virtuais de trabalho coletivo, destinadas à captação de prestações laborais, em um universo virtualmente global de potenciais prestadores, para o cumprimento de uma série de tarefas adredemente ordenada (*tasks*)". Em outros termos: ambientes virtuais de intermediação de trabalho, que reúnem

---

[98] PRASSL, Jeremias. **Human as a service**: The promisse and perils of work in the gig economy. Oxford: Oxford University Press, 2018.

[99] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[100] PRASSL, Jeremias. **Human as a service**: The promisse and perils of work in the gig economy. Oxford: Oxford University Press, 2018.

[101] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v. , p. 53-94.

[102] DE STEFANO, Valerio. The rise of the "just-in-time workforce": on-demand work, crowdwork and labour protection in the "gig-economy". Geneva: ILO, 2016. **Conditions of work and employment series**. n. 71. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_443267.pdf. Acesso em: 10 set. 2022.

[103] FELICIANO, Guilherme Guimarães; PASQUALETO, Olívia de Quintana Figueiredo. (Re)descobrindo o direito do trabalho: gig economy, uberização do trabalho e outras reflexões. In: FELICIANO, Guilherme Guimarães; MISKULIN, Ana Paula Silva Campos (Org.) **Infoproletários e a uberização do trabalho**: direito e justiça em um novo horizonte de possibilidades. São Paulo: LTr Editora, 13-20, 2019.

organizações a potenciais trabalhadores, para o desempenho de pequenas tarefas, sob uma remuneração pré-determinada pelo próprio ofertante. [104]

Essas tarefas envolvem atividades como a simples validação de dados e respostas a questionários e pesquisas, até serviços de ordem mais subjetiva, como a avaliação e moderação de conteúdo.[105]

Já a segunda modalidade, o trabalho sob demanda via aplicativo, corresponde à "execução de atividades tradicionais como transporte e limpeza, por exemplo, em que a força de trabalho é canalizada por aplicativos gerenciados por corporações, que também intervêm na definição de padrões mínimos de qualidade e na seleção e gestão da força de trabalho". [106] [107]

O modelo de negócios, outra vez, aproveita-se da possibilidade de escapar da regulação para conseguir uma redução dos custos de produção e, assim, vantagem competitiva. Conforme avalia Prassl,[108] a tecnologia é o coração desse novo modelo de negócios. Segundo ele:

> A internet facilita a comunicação na velocidade da luz – independentemente se os usuários estão na mesma vizinhança ou em diferentes hemisférios do globo. Algoritmos podem processar um vasto número de transações por segundos, levando em conta um número quase ilimitado de variáveis relevantes. Smartphones e tablets colocam poder de processamento nas palmas e bolsos de consumidores e trabalhadores; satélites de GPS calculam com precisão suas localizações e os mecanismos de pagamento por meio do telefone celular torna o dinheiro obsoleto.
> Tecnologia, no entanto, não apenas viabiliza relações na gig-economy, ela também muda nossa percepção sobre o que está atrás das cenas. Quando tocamos ao longo de bem desenhados aplicativos para conseguirmos uma refeição ou assistimos a um pequeno símbolo de

[104] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v., p. 53-94.
[105] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v., p. 53-94.
[106] FELICIANO, Guilherme Guimarães; PASQUALETO, Olívia de Quintana Figueiredo. (Re)descobrindo o direito do trabalho: gig economy, uberização do trabalho e outras reflexões. In: FELICIANO, Guilherme Guimarães; MISKULIN, Ana Paula Silva Campos (Org.) **Infoproletários e a uberização do trabalho**: direito e justiça em um novo horizonte de possibilidades. São Paulo: LTr Editora, 13-20, 2019.
[107] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v., p. 53-94.
[108] PRASSL, Jeremias. **Human as a service**: The promisse and perils of work in the gig economy. Oxford: Oxford University Press, 2018.

> carro se aproximar num mapa, é fácil que a linha que separa algoritmos e seres humanos se torne turva: ambos parecem inexplicavelmente envolvidos em se obter a conclusão da tarefa. A Professora Lilly Irani da Universidade da Califórnia, San Diego, fez o primeiro destaque de como a ênfase da gig economy na tecnologia nos leva a perceber 'pessoas como parte da infraestrutura computacional ... Nesse mundo ... alguns se tornam criadores enquanto outros se tornam computadores. As plataformas de gig-economy, em outros palavras, tornam o trabalho menos visível, mesmo onde um elemento de interação física ainda permanece. Em um mundo de humanos como serviços, Irani argumenta que os trabalhadores são 'deixados à distância e organizados à bel prazer dos inventores'. Como resultado, 'histórias de desigualdade de direitos, compensações e segurança não são aberrações, mas constitutivas dos papéis e ideologias de trabalho de alta tecnologia'.
> Por mais invisível que seja, o trabalho é fundamental para a gig economia: sem acesso a grandes grupos de trabalhadores sob demanda, seria impossível para plataformas e aplicativos oferecer qualquer um dos "bicos", tarefas e corridas que eles oferecem. Jeff Bezos admite isso quando fala em usar colegas de trabalho para entregar 'Inteligência artificial' - e nomeia, descaradamente, a plataforma da Amazon de Mechanical Turk, depois da infame farsa do xadrez do século XVIII. [109] [110]

A narrativa demonstra como a percepção de que há seres humanos por trás dos serviços prestados por plataformas e aplicativos digitais pode ser diluída e mascaradas pelas linhas de código.

---

[109] Tradução do autor. PRASSL, Jeremias. **Human as a service**: The promisse and perils of work in the gig economy. Oxford: Oxford University Press, 2018, p. 05-06. No original: "The Internet facilitates communication at lightning speed—regardless of whether users are in the same neighbourhood or at different ends of the globe. Algorithms can crunch vast numbers of transactions in seconds, taking into account a near-unlimited number of relevant variables. Smartphones and tablets have put powerful processors in the palms and pockets of consumers and workers; GPS satellites accurately calculate their location and mobile payment mechanisms have made cash obsolete.
Technology, however, doesn't just enable gig-economy transactions; it also shapes our perceptions of what's going on behind the scenes. When we tap along through a well-designed app to pick a meal or watch a small car symbol inch closer on a map, it's easy for the lines between algorithms and humans to become blurred: both appear inextricably involved in getting the job done. Professor Lilly Irani of University of California San Diego was amongst the first to highlight how the gig economy's emphasis on technology leads us to perceive 'people as computational infrastructure . . . In this world . . . some become creators while others become computers.'12
Gig-economy platforms, in other words, make labour less visible, even where an element of physical interaction remains. In a world of humans as a service, Irani argues, workers are 'kept at a distance and organized for innova- tors' pleasures'.13 As a result, 'stories of uneven rights, compensation and safety are not aberrations, but rather constitutive of the roles and ideologies of high-technology work'.14
Invisible though it might be, labour is central to the gig economy: with- out access to large pools of on-demand workers, it would be impossible for platforms and apps to deliver any of the gigs, tasks, and rides they offer. Jeff Bezos admitted as much when he spoke of using crowdworkers to deliver 'artificial artificial intelligence'—and brazenly named Amazon's new plat- form after the infamous eighteenth-century chess hoax".

[110] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v., p. 53-94.

Esses indivíduos, por detrás das linhas de códigos, no entanto, não gozam de um sistema de proteção legal e econômico, a exemplo da garantia de salário-mínimo, de uma jornada de trabalho salubre ou de qualquer proteção social e previdenciária.[111]

A falsa atração desse modelo de produção reside aí: tal como a infraestrutura de tecnologia da informação (TI), grandes forças de trabalho são caras para se estruturar e manter. Enquanto servidores precisam ser energizados e resfriados; trabalhadores precisam receber salários, serem treinados e pagos – independentemente do aumento ou da diminuição da demanda. No entanto, uma vez que os trabalhadores se tornem serviços ou mercadorias,[112] essas responsabilidades podem ser evitadas, diminuindo os preços para os consumidores e aumentando o lucro de empregadores. [113]

Biewald, CEO da plataforma concorrente da MTurk, a CrowdFlower, resume o tipo de negócios:

> Antes da Internet, seria realmente difícil encontrar alguém, sentá-lo por dez minutos, fazer com que ele trabalhe para você e despedi-lo, depois desses dez minutos trabalhados. Mas com a tecnologia, você pode realmente encontrá-los, pagá-los uma quantia pequena de dinheiro e depois se livrar deles quando não precisar mais deles. [114] [115]

A lógica por trás disso, é, mais uma vez, o descarte. Sem garantias de qualquer natureza, o trabalhador da *gig economy* se vê em semelhante situação de desamparo ao

---

[111] Supiot assevera que nos "Estados Unidos e no Reino Unido, diversas jurisdições reclassificaram como contrato de trabalho assalariado os contratos de motoristas da Uber", eis que a argumentação de que as plataformas digitais levam ao "ressurgimento do trabalho independente é negada pelos fatos". SUPIOT, Alain. Por uma reforma digna do nome. E se refundarmos a legislação trabalhista?. **Le Mond Diplomatique**, França, Ed. 123, 4 out. 2017. Disponível em: https://diplomatique.org.br/reforma-trabalhista-na-franca-e-se-refundarmos-a-legislacao/. Acesso em: 15 set. 2022.

[112] Importa lembrar que em 1944 foi editada a Declaração de fins e objetivos da Organização Internacional do Trabalho (Declaração de Filadélfia), na qual consagrou-se o princípio da vedação à mercantilização do trabalho, prescrevendo, a declaração que "o trabalho não é mercadoria", repousando nesse preceito um dos princípios fundamentais da Organização. OIT. Organização Internacional do Trabalho. **Constituição da Organização Internacional Do Trabalho**. Declaração de Filadélfia. Filadélfia, 1944. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/---ilo-brasilia/documents/genericdocument/wcms_336957.pdf. Acesso em: 23 out. 2022.

[113] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v., p. 53-94.

[114] ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021, v., p. 53-94.

[115] Tradução do autor. No Original: "Before the Internet, it would be really difficult to find someone, sit them down for ten minutes and get them to work for you, and then fire them after those ten minutes. But with technology, you can actually find them, pay them the tiny amount of money, and then get rid of them when you don't need them anymore". MARVIT, Moshe Z. **How crowdworkers became the ghosts in the digital machine**. The Nation, 2014. Disponível em: https://www.thenation.com/article/archive/how-crowdworkers-became-ghosts-digital-machine/. Acesso em: 23 out. 2022.

trabalhador da primeira revolução industrial, se vendo obrigado a jornadas exaustivas (já que não há garantia de salário-mínimo) e descoberto de qualquer proteção social, especialmente, quando mais precisa: em caso de acidente, adoecimento ou na velhice.

Prassl[116] arremata expondo o problema central dessas plataformas: "isso tudo parece bom - até que você se coloque no lugar do trabalhador cujo trabalho tornou-se um serviço, para ser comprado e comercializado como qualquer outra mercadoria".

O movimento pendular entre regulação e desregulação é a marca da disrupção tecnológica, como se pôde perceber até então.

A escolha dessa abordagem teórica, partindo-se da posição do trabalhador na sociedade tem a finalidade de apontar, com precisão, os impactos dessas tecnologias sobre a vida humana. Isso porque o trabalhador representa uma classe vulnerável aos efeitos do mercado e das formas como o sistema produtivo se regula. Considerando que "em nossa história, as revoluções têm ocorrido quando novas tecnologias e novas formas de perceber o mundo desencadeiam uma alteração profunda nas estruturas sociais e nos sistemas econômicos",[117] a construção dessa narrativa socioprodutiva não poderia ser ignorada.

Os avanços e retrocessos no campo da regulação estatal são marcas presentes ao longo do tempo e que se evidenciam com muito mais nitidez a partir de uma visão holística dos sistemas socioprodutivos. Notar esse movimento pendular e como ele se molda às novas tecnologias descortina uma face central da pesquisa: o modo como o Estado enxerga seu papel diante dos desafios que a tecnologia reconduz o ser humano.

Além disso, as correlações entre o trabalho e todos os demais aspectos da vida é fundamental, na medida em que, conforme destaca Redinha, o ser humano em sua prestação laboral não prossegue "apenas um modo de subsistência, mas também um meio de realização pessoal, profissional e social".[118]

Não obstante, ainda nos resta uma última tarefa: apontar, precisamente, como a economia se modificou para essa nova estrutura que têm em suas bases a utilização maciça de dados pessoais.

A resposta a esse questionamento acena para todo o movimento que se viu até aqui. Em todos os modelos produtivos, assistimos aos esforços (de Taylor, Ford e Toyota,

---

[116] PRASSL, Jeremias. **Human as a service**: The promisse and perils of work in the gig economy. Oxford: Oxford University Press, 2018, p. 05.
[117] SCHWAB, Klaus. **A Quarta Revolução Industrial**. Tradução de Daniel Moreira Miranda. 1. ed., São Paulo: Edipro, 2016, p. 8.
[118] REDINHA, Maria Regina Gomes. **Da protecção da personalidade no Código do Trabalho**. In: Fernandes, F., & Redinha, M., Para Jorge Leite: escritos jurídico-laborais. p. 819-853. Coimbra: Coimbra Editora, 2014.

por exemplo) em busca de uma economia nos custos de produção, ora com foco nas máquinas, ora sob o trabalhador; ora o capital humano, ora material.

No entanto, com o poder de processamento de dados cada vez maior e eficiente, viu-se a possibilidade de se realizar tarefas cada vez mais complexas em menos tempo e com menores custos, a partir da produção de modelos matemáticos de caráter preditivo, inclusive sobre o consumo.

Embora esta já fosse uma variável considerada em diversos modelos de produção (veja-se a divisão da jornada de trabalho em oito horas, apresentada por Ford para estimular o mercado), ao se possibilitar a análise de grandes conjuntos de dados (o *Big Data*), somado à utilização da inteligência artificial e do aprendizado de máquina, permitiu-se a produção de modelos muito mais precisos, além da capacidade de, no campo do marketing, influenciar o consumo.

Na "sociedade da informação",[119] fruto da intensa utilização das Tecnologias de Informação e Comunicação (TICs), instalou-se um "capitalismo de vigilância",[120] dependente, cada vez mais de dados e metadados de potenciais consumidores. A ideia de produção flexível, nesse contexto, pode chegar a níveis muito mais confiáveis e, até mesmo, criar outras demandas de consumo.[121]

Conhecendo-se o usuário, a partir de seus rastros digitais (*digital trace* – incluindo seus dados pessoais) é possível prever e condicionar seu comportamento, com bastante precisão e grande valor comercial – e até político, como se viu recentemente.[122]

---

[119] *Cf.* MACHLUP, Fritz. **The production and distribution of knowledge in the United States**. Princeton, Princeton University Press, 1962.

[120] Expressão cunhada por Shoshana Zuboff, para designar: "1. Uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas; 2. Uma lógica econômica parasítica na qual a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento; 3. Uma funesta mutação do capitalismo marcada por concentrações de riqueza, conhecimento e poder sem precedentes na história da humanidade; 4. A estrutura que serve de base para a economia de vigilância; 5. Uma ameaça tão significativa para a natureza humana no século XXI quanto foi o capitalismo industrial para o mundo natural nos séculos XIX e XX; 6. A origem de um novo poder instrumentário que reivindica domínio sobre a sociedade e apresenta desafios surpreendentes para a democracia de mercado; 7. Um movimento que visa impor uma nova ordem coletiva baseada em certeza total; 8. Uma expropriação de direitos humanos críticos que pode ser mais bem compreendida como um golpe vindo de cima: uma destituição da soberania dos indivíduos". ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução George Schlesinger. Rio de Janeiro: Intrínseca, 2021, p. 13.

[121] Um exemplo interessante dessa criação de demanda foi a introdução do IPad pela Apple, que surgiu como um híbrido entre um computador e um smartphone. A estratégia de marketing da empresa se refletiu em alto número de vendas, em um mercado totalmente projetado e criado pela empresa.

[122] MARS, Amanda. Como a desinformação influenciou nas eleições presidenciais? **El País**. Nova York, 2018. Disponível em: https://brasil.elpais.com/brasil/2018/02/24/internacional/1519484655_450950.html. Acesso em: 25 jun. 2022.

Essas relações, logo mais serão exploradas em espaço reservado a compreendê-las, estudando seu funcionamento e os riscos a eles associados.

Antes disso, dedicaremos algumas linhas para falar sobre o progresso e como este se dissociou, ao longo do tempo, de um vetor axiológico, o que permite explicar a razão pela qual o quadro de exploração humana abordado até aqui parece ter sido, em alguma medida tolerado.

2. O valor do Progresso e da Tecnologia

No curso da história, o discurso sobre o progresso[123] caminhou entre percepções otimista – nas quais essa ideia transfigurava-se em um vetor do desenvolvimento, com objetivos claros e universais de avanço da humanidade; e pessimistas – sobretudo no pós-segunda-guerra, com a tecnologia sendo utilizada para subjugar povos e nações.[124]

O primeiro período, demarcado por um vetor humanista que associava o progresso a um estágio maior de desenvolvimento civilizatório, tem como marco autores renascentistas e humanistas. Essas correntes de pensamento colocavam o ser humano como o centro de toda a técnica e da racionalidade. A oração *De Dignitate hominis*, escrita em 1486 por Pico della Mirandola, reflete essa centralidade do homem no universo do seguinte modo:

> Finalmente, o supremo artífice estabeleceu que seria comum, àquele a quem não pudera dar nada de próprio, tudo aquilo que era particular a cada um dos outros seres. (18) Logo, Ele tomou o homem, criatura de imagem indefinida, e, tendo-o colocado no centro do mundo, falou-lhe

[123] Para uma noção acurada da noção de progresso e suas implicações, ver: DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 55-62. Há de se ressaltar que nem sempre a ideia de progresso esteve associada à tecnologia. Na antiguidade clássica ela sequer existia, como aponta Danilo Doneda, isso porque a vida era vista como um eterno ciclo. Foi somente na renascença que o homem tomou consciência de seu poder de intervir e modificar, muitas vezes permanentemente, os espaços que ocupa. Isso é expresso na seguinte passagem: "A natureza dos outros seres, uma vez definida, é limitada pelas leis que ditamos. No teu caso serás tu, livre de qualquer limitação, de acordo com o seu arbítrio, depositado por mim em suas mãos, a decidir sobre ela". Giovanni Pico della Mirandola. De dignitate hominis (1486). A partir da renascença e do humanismo o homem toma conhecimento de sua capacidade de intervir sobre todas as coisas e de ditar avanços e melhorias propiciados pela ciência. Nas palavras de Doneda "Hoje, verificamos que a consciência do poder da técnica e de suas possibilidades como instrumento de mudança já estava clara durante o Renascimento – basta fazer menção aos tantos projetos de Leonardo da Vinci, uma personalidade que certamente encontrou ambiente cultural propício para conceber ideias que poderiam de fato operar mudança, desde as mais teoréticas até suas "máquinas de guerra" que habitualmente oferecia aos Medici". DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 55-62.

[124] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 55-62.

> assim: «não te demos um lugar determinado, nem um aspecto que te seja próprio, nem dom algum peculiar, a fim de que tu, ó Adão, obtenhas e possuas, segundo o teu desejo e por tua decisão, aquele lugar, aquele aspecto, aqueles dons que tu mesmo tiveres escolhido. (19) Para os demais, a natureza, uma vez definida, é encerrada dentro de leis prescritas por nós. (20) Tu, porém, não constrangido por limites de nenhum tipo, segundo o teu arbítrio, em cujas mãos te coloquei, definirás para ti a tua lei. (21) Eu te coloquei no centro do mundo, a fim de que daí possas observar mais comodamente tudo o que existe no mundo. (22) Não te fizemos nem celeste nem terreno, nem mortal nem imortal, a fim de que tu, como livre e honorário executor e escultor de ti próprio, te modelasses na forma que tu mesmo preferisses. (23) Poderás degenerar-te até as formas inferiores, que são feras; poderás, por decisão de teu espírito, regenerar-te até as superiores, que são divinas.[125]

Os ideais humanistas e renascentistas mais tarde se uniram às correntes iluministas do século XVII. O ideal de progresso, nesse período, passou a se assemelhar a um verdadeiro imperativo lógico, pelo qual cada geração se valeria das conquistas e conhecimentos da geração anterior e as aperfeiçoaria, dando um passo rumo a um estágio civilizatório superior. Via-se a noção de progresso como uma escala sucessiva, na qual aquilo que se encontra cronologicamente adiante estaria mais bem colocado, em uma espécie de escala valorativa.[126] Essa concepção encontrou expressão na obra de Turgot, em seu discurso *Sur les progrès successifs de l'esprit humain*, de 1750,[127] e teve sua sistematização mais famosa na obra clássica do seu discípulo, o enciclopedista Condorcet, *Esquisse d'un tableau historique des progrès de l'esprit humain*, de 1795. [128]

Tais ideários, difundidos pelo movimento iluminista, se fizeram presentes, mais tarde, também no pensamento do século XIX, representado pelo positivismo de Augusto Comte e pelas teses evolucionistas de Charles Darwin e Herbert Spencer, os quais identificaram uma noção de progresso a partir da evolução das formas de vida, das mais simples até as mais complexas, conforme analisa Doneda.[129]

---

[125] MIRANDOLA, Pico Della. **Discurso sobre a dignidade do homem**. Belo Horizonte: Editora Âyiné, 2021, [p. 323] Edição do Kindle.
[126] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 55-62.
[127] TURGOT, Anne-Robert-Jacques. **Oeuvres de Turgot**. 1975. Disponível em: https://www.institutcoppet.org/turgot-discours-sur-les-progres-successifs-de-lesprit-humain-1750/. Acesso em: 22 ago. 2022.
[128] CONDORCET, Jean-Antoine-Nicolas de Caritat. **Esquisse d'un tableau historique des progrès de l'esprit humain**. Bibliothèque nationale de France. Disponível em: https://gallica.bnf.fr/ark:/12148/bpt6k281802. Acesso em: 22 ago. 2022.
[129] MIRANDOLA, Pico Della. **Discurso sobre a dignidade do homem**. Trad. Elaine Cristine Sart. Belo Horizonte: Editora Âyiné, 2021, [p. 323] Edição do Kindle.

O período otimista, entretanto, não reinou por muito tempo, nem de forma absoluta, tendo sido permeado por momentos de ceticismo.

Hegel, por exemplo, notava certo imobilismo na natureza, apontando que nada de realmente novo se poderia esperar – *Nihil sub sole novum* – "nada de novo sob o sol". Para ele, as aparentes inovações nada mais seriam que um jogo polimórfico de estruturas, constatando que o único espaço no qual, de fato, poderia surgir algo de "novo" seria o espírito.[130] [131]

Soma-se a isso o fato de que começa a ser percebido um movimento de distanciamento entre a técnica e seus objetivos humanístico. A técnica passa a voltar-se para si mesma e a ignorar qualquer limite.

Surge, no século XX, a ideia de progresso pelo progresso, isto é: a ideia de progresso como um fim em si mesmo, passando a regular as diversas relações entre a sociedade e a tecnologia. Na brilhante colocação de Danilo Doneda:

> Nesse (...) período vem à tona uma faceta da tecnologia explorada por diversos estudiosos: seu desprezo por limites que lhe sejam extrínsecos – ou, em outras palavras, por quaisquer limites que sejam. Eligio Resta, sociólogo do direito, procura demarcar esse desprezo, afirmando que a utopia do direito estaria em pretender que nós não possamos fazer aquilo que somos capazes de fazer: matar, desflorestar, roubar. Tais limites, caros ao direito, não existem na lógica da tecnologia. "O código do poder fazer é o código da tecnologia, que vive da pesquisa de níveis crescentes de potência para alcançar um grau maior do poder fazer". Para Agostino Carrino, "O progresso, de um valor, ideia ou mito, tornou-se em um fato que, como tal, subtrai-se a qualquer discurso normativo (...). O progresso agora é a aceleração do tempo, não mais em direção a um determinado objetivo, porém como objetivo em si. O progresso é o progredir no progresso. E assim ele evita qualquer controle, qualquer questionamento sobre os seus fins."
> O fato de que o progresso tenha transformado a técnica de um simples instrumento a um fim em si mesma foi preocupação de alguns dos filósofos da Escola de Frankfurt. A técnica teria se tornado, ela própria, um sujeito impessoal, capaz de impor sua lógica inerente à sociedade, constituindo-se assim em um simulacro da vontade: a "vontade da técnica", perdendo assim definitivamente seu caráter instrumental e neutro.[132]

[130] HEGEL. Georg F. *Apud* DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 58.
[131] MIRANDOLA, Pico Della. **Discurso sobre a dignidade do homem**. Belo Horizonte: Editora Âyiné, 2021, [p. 323] Edição do Kindle.
[132] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 59-60.

A perda de qualquer elemento valorativo na técnica e no progresso os transforma em uma ferramenta despida de significado próprio, capaz das piores tragédias,[133] ou das maiores proezas.[134] A ela já não são imbuídos elementos extrínsecos, bastando-se a si própria.

Essa perda de um fio condutor axiológico na noção de progresso embora tenha acabado por lapidá-la, trouxe, porém, uma série de consequências ignoradas, diante de uma pureza que não se conformava mais com elementos externos às ciências tecnológicas. [135]

A tensão entre otimismo e pessimismo acabou acedendo a uma aparente instrumentalização e privatização da tecnologia, separando-a de outros elementos e repousando sobre cada indivíduo a valoração sobre a essência de uma determinada tecnologia, bem como a responsabilidade de dela fazer bom. Nas palavras de Doneda:[136]

> (...), hoje, dificilmente é possível compreender o progresso de uma perspectiva unilateral. A ideia de progresso trazia originariamente um universalismo que foi arrefecendo com o tempo. Para Zygmunt Bauman, o progresso, como tantos outros parâmetros da vida moderna, foi desregulamentado, isto é, a valoração de uma determinada "novidade" passou a ser feita livre e individualmente; e privatizado, isto é, espera-se que toda pessoa, também individualmente, lance mão de seus próprios recursos para obter uma condição mais satisfatória e deixe para trás uma eventual condição desfavorável.

Tal neutralidade aparente, no entanto, volta a dar indícios de que ser apenas ilusória. Como será retratado mais à frente, é difícil se falar em neutralidade quando toda tecnologia é resultado do trabalho humano, que guarda em si opiniões, valores e julgamentos – idiossincrasias – que podem ser embutidos, consciente ou inconscientemente, no fruto de seu trabalho, especialmente quando falamos em algoritmos.

Ao abordarmos adiante esse conceito, veremos que os algoritmos expressam seleções e escolhas; que se fundam em conjunto de dados e informações às vezes

---

[133] Basta referir-se à invenção da bomba atômica, ao período de corrida armamentista-tecnológica que tomou lugar no pós-guerra; ou das diversas experiências levadas a efeito durante o regime nazista.
[134]

[135] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 59-60.
[136] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 62.

enviesados; que são passíveis de toda espécie de erro, muito embora sua aparente correção e neutralidade seja defendida com vigor.

Na passagem seguinte, considerando que as Tecnologias de Informação e Comunicação (TIC's) engendraram uma gramática própria, abordaremos os principais conceitos relativos a essas tecnologias, para, na sequência, tratarmos, efetivamente, de sua aplicação.

3. A gramática das novas Tecnologias de Informação e Comunicação (as TIC's)

Partindo-se do pressuposto de que em toda comunicação a precisão vocabular é fundamental, traremos nessa seção alguns dos conceitos fundamentais relacionados às novas tecnologias, para que sua aplicação possa ser abordada nas seções seguintes com alguma compreensão por parte do leitor a respeito de seu conteúdo e funcionamento.

Aproveitando-se da analogia feita por Doneda[137] em relação ao livro de Carl Schmitt *Der nomos der Erde*[138] assinalamos uma diferença de substância entre o real e o virtual. Em seus termos:

> Carl Schmitt (...) confrontava o direito da terra com o direito do mar. A terra, para ele, teria moldado o direito através de sua materialidade; as suas possibilidades e limitações e o processo pelo qual se dá a sua apropriação – o nomos – teriam condicionado a própria estrutura do direito. "A Terra traz em seu próprio solo linhas e limites, pedras de confins, muros, casas e outros edifícios. [...] Família, estirpe, classe, tipos de propriedade e de vizinhança, mas também formas de poder e de domínio, fazem-se nela publicamente visíveis". Ao contrário da terra, o mar se constituiria em um espaço diverso, marcado por uma espécie de liberdade que não se encontra sobre a terra. O direito do mar apresenta, consequentemente, uma gramática diversa, baseada na utilização por diversos sujeitos de um espaço que a princípio é livre.

[137] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 62.

[138] "Carl Schmitt em seu livro *Der nomos der Erde*, confrontava o direito da terra com o direito do mar. A terra, para ele, teria moldado o direito através de sua materialidade; as suas possibilidades e limitações e o processo pelo qual se dá a sua apropriação – o nomos – teriam condicionado a própria estrutura do direito. "A Terra traz em seu próprio solo linhas e limites, pedras de confins, muros, casas e outros edifícios. [...] Família, estirpe, classe, tipos de propriedade e de vizinhança, mas também formas de poder e de domínio, fazem-se nela publicamente visíveis". Ao contrário da terra, o mar se constituiria em um espaço diverso, marcado por uma espécie de liberdade que não se encontra sobre a terra. O direito do mar apresenta, consequentemente, uma gramática diversa, baseada na utilização por diversos sujeitos de um espaço que a princípio é livre. DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 62.

Essa contraposição entre terra e mar, é facilmente extensível ao mundo físico e ao cyberespaço. Enquanto no primeiro os limites são rígidos e bem demarcados, o segundo é fluido e tido com um espaço de ampla liberdade. Tratando-se de sistemas diferentes, torna-se necessário entender a linguagem que rege esse outro sistema, compreendendo, em alguma medida, seu funcionamento e potencialidades.

Para tanto, partiremos da partícula fundamental das novas Tecnologias de Informação e Comunicação (TICs): os dados, cujo paralelo, no mundo físico, seria o próprio átomo e sua subestruturas.

3.1. Dados e metadados.

O termo "dados", conforme assinala David Michael,[139] em essência, refere-se a tudo aquilo que é capaz de ser registrado. Uma produção ao vivo, um testemunho ou uma conversa não serão dados a menos que sejam gravados. O autor aponta, nesse sentido, que o termo "gravado" pode ser entendido de diferentes formas, como o registro de áudio, de vídeo, alfabético ou numérico. Michael avalia que "a maior parte das coisas que chamamos de dados são combinações de conteúdos visuais e alfanuméricos que comunicam algo ou que entretém".[140]

Hoffmann-Riem,[141] por sua vez, pondera que os dados, na literatura da teoria da informação, são tidos "como sinais ou símbolos de mensagens que podem ser formalizados e (arbitrariamente) reproduzidos e facilmente transportados com a ajuda de meios técnicos adequados". Como tais, os dados não têm significado, mas podem ser portadores de informações codificadas, de forma que, nos termos propostos pelo autor[142]:

> o significado é atribuído a eles quando entram em um processo de comunicação de informações por um remetente e geração de informações pelo destinatário, ou seja, [quando] tornam-se o objeto de comunicação. Essa comunicação pode ocorrer entre humanos, mas também entre humanos e máquinas ou entre máquinas.

---

[139] MICHAEL, David. What and Where Is My Data. **GP Solo**, vol. 34, n. 2, mar./abr. 2017, p. 46-49, p. 47. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/gpsolo34&i=132. Acesso em: 5 out. 2021.

[140] Tradução do autor. No original: "Most things we call data are combinations of visual alpha- numeric content that communicates or entertains". MICHAEL, David. "What and Where Is My Data." MICHAEL, David. What and Where Is My Data. **GP Solo**, vol. 34, n. 2, mar. /abr. 2017, p. 46-49, p. 47. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/gpsolo34&i=132. Acesso em: 5 out. 2021.

[141] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Rio de Janeiro: Forense, 2021, p. 34-35.

[142] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Rio de Janeiro: Forense, 2021, p. 34-35.

Michael[143] refere existir dois tipos diferentes de dados: os dados de conteúdo e os metadados. Os dados de conteúdo consistem no próprio registro da comunicação, enquanto os metadados são informações a respeito desse conteúdo, como seu autor, data de criação, local de armazenamento, proprietário, localização (em registros fotográficos, utilizando-se o GPS dos smartphones, por exemplo), entre outros.

O autor afirma que documentos que são "herdados" de outros arquivos, geram metadados, permitindo-se, *v.g.* identificar o nome de um cliente em uma cadeia de edições. Além disso, os dados de conteúdo podem ser classificados com uma infinidade de *tags* (marcadores), que podem ser utilizadas para categorizar e organizar o conteúdo sem a necessidade de a eles propriamente se aceder (acessá-los).

O autor[144] ainda divide os dados em mais seis classificações, referindo-se aos dados estruturados (dados gerenciados, formando estruturas como bancos de dados) e não estruturados (dados brutos, ainda não rotulados, tratados ou gerenciados); dados digitais e analógicos (terminologia utilizada pelo autor para distinguir entre dados eletrônicos e dados impressos); bem como dados primários e secundários (sendo os dados secundários, aqueles derivados de outros dados, tidos por primários).[145]

Outra categoria importante ao objeto do trabalho é a noção de dados pessoais. Tal categoria decorre de previsão normativa, estando descrita na legislação brasileira como sento toda "informação relacionada a pessoa natural identificada ou identificável", nos termos do artigo 5º inciso I, da Lei nº 13.709/2018.[146]

Na legislação europeia, de onde se inspira o normativo nacional, a previsão do conceito encontra-se insculpida no artigo 4º, nº. 1 do Regulamento Geral de Proteção de Dados,[147] significando "qualquer informação relativa a uma pessoa singular identificada

---

[143] MICHAEL, David. What and Where Is My Data. **GP Solo**, vol. 34, n. 2, mar./abr. 2017, p. 46-49, p. 47. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/gpsolo34&i=132. Acesso em: 5 out. 2021.

[144] MICHAEL, David. What and Where Is My Data. **GP Solo**, vol. 34, n. 2, mar./abr. 2017, p. 46-49, p. 47-48. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/gpsolo34&i=132. Acesso em: 5 out. 2021.

[145] O autor aponta como objeto de interesse da distinção, saber que os dados primários podem perder suas propriedades ao serem copiados (essa cópia trata-se de um dado secundário), sendo necessário se assegurar a sua integridade (por meio de cópias estáticas, por exemplo), ao deles se utilizar como meio de prova. MICHAEL, David. What and Where Is My Data. **GP Solo**, vol. 34, n. 2, mar. /abr. 2017, p. 46-49, p. 48. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/gpsolo34&i=132. Acesso em: 5 out. 2021

[146] BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 nov. 2022.

[147] UE. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

ou identificável". Hoffmann-Riem,[148] complementando a informação, esclarece que será dado pessoal todo aquele que se referir a:

> uma pessoa singular que possa ser identificada, direta ou indiretamente, em particular por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador *on-line* ou um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.

É esse conjunto de dados que, de alguma maneira, referem-se e permitem identificar um indivíduo que são chamados de dados pessoais.

De outra banda, a terminologia "dados pessoais sensíveis" remete a uma categoria especial de dados pessoais, que demandam uma proteção maior, porquanto veiculam informações potencialmente discriminatórias ou que colocam seu titular em risco, a exemplo dos dados sobre origem racial ou étnica, convicções religiosas, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referentes à saúde ou à vida sexual, os dados genéticos ou biométrico, consoante aponta o artigo 5º inciso II, da Lei nº 13.709/2018.[149]

Na legislação europeia, utilizada como parâmetro de comparação, a categoria "dado pessoal sensível" encontra apoio no artigo 9º do Regulamento Geral de Proteção de Dados, abrangendo nessa espécie os dados que revelam a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como os dados genéticos e os dados biométricos que permitam identificar um indivíduo de forma inequívoca, os dados relativos à saúde, à vida sexual e à orientação sexual de uma pessoa. Encontram-se abrangidos na categoria, também, os dados relativos às condenações penais, por força do artigo 6º da Convenção 108 do Conselho da Europa (Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal).[150]

Esses dados constituem categoria especialmente protegida, se submetendo a um regime diferenciado de tratamento, no qual, em regra, se proíbe o seu tratamento, exceto

---

Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0679. Acesso em: 3 set. 2021.

[148] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Rio de Janeiro: Forense, 2021, p. 35.

[149] BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 nov. 2022.

[150] ANTUNES, Luís. **Pôr em Prática o RGPD: o que muda para nós? E para as organizações?** Lisboa: FCA, 2018, p. 35.

nas hipóteses legalmente estipuladas, em razão do risco inerente a essas informações, seja no campo da discriminação, seja relativa ao roubo de identidade, à possibilidade de perdas financeiras, prejuízos à reputação, perdas de confidencialidade de informações protegidas por sigilo profissional, inversão não autorizada da pseudonimização, ou quaisquer outros danos de natureza econômica ou social.[151]

Cabe notar, entretanto, que os dados, à partida não sensíveis podem levar à descoberta de dados sensíveis. Isto é: o cruzamento de informações pode resultar em um caractere sensível. O gênero de um indivíduo, associado ao nome de seu cônjuge, por exemplo, pode facilmente levar à descoberta da orientação sexual de uma pessoa.

É isso o que revela a teoria do mosaico, segundo a qual, embora um dado isolado possa parecer sem importância, esse dado combinado a diversos outros pode levar à criação de um retrato bastante completo e fidedigno do indivíduo sem a sua participação, tornando o ser humano um "cidadão transparente ou de cristal",[152] despido de sua privacidade. Conforme expõem Conesa:[153]

> Existem dados a priori irrelevantes do ponto de vista do direito e da intimidade que, entretanto, em conexão com outros, talvez também irrelevantes, podem servir para tornar completamente transparente a personalidade do cidadão, tal qual ocorre com as pequenas peças que formam os mosaicos, que em si não dizem nada, mas unidas podem formar conjuntos plenos de significado.

Com efeito, a quantidade maciça de dados extraídos todos os dias já permite que sistemas algorítmicos possam realizar os mais diversos tipos de previsão, como identificar comportamentos psicológicos, predizer características pessoais (como orientação

---

[151] DUARTE, Tatiana. Artigo 9.º. *In:* PINHEIRO, Alexandre Sousa. **Comentários ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018, p. 234-334, p. 236-237.

[152] LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí, v. 14. n. 2, p. 27–53, 2009. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/1767. Acesso em: 7 mar. 2021.

[153] Tradução do autor. No original: "*Existen datos a priori irrelevantes desde el punto de vista del derecho a la intimidad y que, sin embargo, en conexión con otros, quizá también irrelevantes, pueden servir para hacer totalmente transparente la personalidad del ciudadano, al igual que ocurre con las pequeñas piedras que forman los mosaicos, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significados*". CONESA, F. **Derecho a la intimidad, informática y Estado de Derecho**. Valencia: Universidad, 1984, p. 44-45.

política, religiosa e, até sexual);[154] além de detectar hábitos de consumo e outras variáveis economicamente exploráveis.[155]

Como o conjunto de dados disponível em escala mundial não para de crescer, as potencialidades do tratamento de dados apresentam-se como um universo em expansão. Nesse passo, pesquisa realizada pela *International Data Corporation*[156] revela que o conjunto de informações disponíveis em escala global, a chamada "*Global Datasphere*", cresce de modo exponencial, tendo passado da marca de 2 zettabytes em 2010, para 33 zettabytes em 2018, com previsão de que esse número chegue a 175 zettabytes até 2025.

Para se ter uma ideia da imensidão desses números, um zettabyte corresponde a uma potência de 10^{21} (1.000.000.000.000.000.000.000 bytes), isto é: 1 trilhão de gigabytes. Se fosse possível armazenar toda essa informação em DVDs, ter-se-ia uma pilha de discos capaz de ir 23 vezes à lua ou circundar a terra 222 vezes.

Do mesmo modo, se alguém tentasse fazer o download da *Datasphere*, a uma velocidade de 25 Mb/s (a velocidade média de conexão nos EUA), demoraria 1.8 bilhão de anos, caso a tarefa fosse realizada por uma única pessoa, e, mesmo que todas as pessoas ao redor do mundo ajudassem, ainda assim, o trabalho levaria 81 dias para ser concluído.[157]

Esses números dão a dimensão da importância do assunto, à frente detalhadas. Assim, para o ponto, interessa que se entendam as diferentes categorias de dados; que se

---

[154] Nesse sentido, pesquisa realizada pela Universidade de Cambridge e pela *Microsoft Research*, demonstrou que registros digitais de comportamento facilmente acessíveis, como curtidas no *Facebook*, podem ser usados para prever automaticamente e com precisão uma variedade de atributos pessoais altamente sensíveis, incluindo: orientação sexual, etnia, pontos de vista religiosos e políticos, traços de personalidade, inteligência, felicidade, uso de substâncias viciantes, separação dos pais, idade e sexo. A análise apresentada baseou-se em um conjunto de dados de mais de 58.000 voluntários que forneceram seus *likes* no *Facebook*, perfis demográficos detalhados e os resultados de vários testes psicométricos. O modelo proposto usa redução de dimensionalidade para o pré-processamento dos dados de *likes*, que são então inseridos em regressão logística/linear para prever perfis psicodemográficos individuais. O modelo discrimina corretamente homens homossexuais e heterossexuais em uma proporção de acerto de 88% dos casos, Afro-americanos e caucasianos americanos em 95% dos casos, e entre democratas e republicanos em 85% dos casos. KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. **Proceedings of the National Academy of Sciences of the United States of America**, Washington, v. 110, n. 15, p. 5802–5805, 2013. ISSN: 00278424. DOI: 10.1073/pnas.1218772110. Disponível em: www.pnas.org/cgi/doi/10.1073/pnas.1218772110. Acesso em: 13 mar. 2021.

[155] LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí, v. 14. n. 2, p. 27–53, 2009, p. 36. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/1767. Acesso em: 7 mar. 2021, p. 269.

[156] REINSEL, David; GANTZ, John; RYDNING, John. International Data Corporation. **The Digitization of the World:** from Edge to Core. Framingham, 2018. Disponível em: https://www.seagate.com/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. Acesso em: 9 mar. 2021.

[157] REINSEL, David; GANTZ, John; RYDNING, John. International Data Corporation. **The Digitization of the World:** from Edge to Core. Framingham, 2018. Disponível em: https://www.seagate.com/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. Acesso em: 9 mar. 2021.

tenha a compreensão da imensidão de informações disponíveis globalmente; e de como esses dados podem se conectar, formando um perfil cada vez mais fiel do ser humano real, com potenciais de aplicação às mais diversas áreas e finalidades.

3.2. Algoritmos

A segunda noção de máxima importância para as Tecnologias de Informação e Comunicação (TICs) é a ideia de algoritmo. A esse respeito, Pedro Domingos,[158] professor de ciências da computação da Universidade de Washington, ensina que algoritmo "é uma sequência de instruções que informa ao computador o que ele deve fazer". Laura Schertel Mendes e Marcela Mattiuzo[159] enfatizam que um algoritmo é comumente descrito como "um conjunto de instruções, organizadas de forma sequencial, que determina como algo deve ser feito". É, nada mais, que "uma fórmula na qual tarefas são colocadas em uma ordem específica para atingir determinado objetivo".[160]

A função de um algorítmico é fazer com que os componentes mecânicos de computadores executem operações matemáticas, de modo a produzir resultados úteis. Para isso, opera uma linguagem de programação que possibilita aos componentes mecânicos compreenderem e executarem essas tarefas de ordem lógico-matemático. A partir desse ponto, o algoritmo pode ser chamado de programa. [161]

Hoffmann-Riem,[162] por sua vez, aponta que:

> O termo algoritmo é antigo. Inicialmente, ele foi usado para designar apenas uma regra de ação clara que é usada para resolver certos problemas em etapas individuais definidas. (...)
> [Aponta que] para uso em computadores, os algoritmos são escritos em linguagem digital processável por máquina e a respectiva tarefa é processada com a ajuda de um número finito de etapas individuais predefinidas. (...). Na maioria dos casos (...) os algoritmos individuais são partes de sistemas algorítmicos complexos. Eles consistem em

[158] DOMINGOS, Pedro. **The master algorithm:** how the quest for the ultimate learning machine will remake our world. New York: Basic Books, 2015, p. 1.
[159] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Revista Direito Público**, Brasília, v. 16, n. 90, p. 39–64, 2019, p. 41. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em: 2 maio 2021.
[160] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Revista Direito Público**, Brasília, v. 16, n. 90, p. 39–64, 2019, p. 41. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em: 2 maio 2021.
[161] DOMINGOS, Pedro. **The master algorithm:** how the quest for the ultimate learning machine will remake our world. New York: Basic Books, 2015, p. 4.
[162] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Rio de Janeiro: Forense, 2021, p. 34-35.

> *software* (programas) e *hardware* [componentes físicos] e muitas vezes estão ligados a outros componentes de *software*.

Os algoritmos estão presentes nas mais diversas máquinas, sistemas, utensílio e, até mesmo, na internet. Com a evolução tecnológica, eles estão presentes por todos os lados. São exemplos disso, os aparelhos inteligentes, os sistemas preditivos em mecanismos de buscas, as recomendações feitar em plataformas de *streaming*, entre outros.

O desenvolvimento da Internet das Coisas (IoT – Internet of Things),[163] das casas inteligentes e dos sistemas de conectividade (que interligam dos lares aos veículos) tornaram corriqueira a existência de algoritmos na contemporaneidade.

Eles, em geral, são utilizados para automatizar tarefas, fazer previsões ou indicar decisões a serem tomadas. São, em si, um conjunto de regras, e, como tais, ao se inserirem na vida humana, influenciam comportamentos, escolhas e preferência. Como bem pontua Wolfgang Hoffmann-Riem[164]:

> (...) algoritmos mudam nossa percepção do mundo, afetam nosso comportamento influenciando decisões e são uma importante fonte de ordem social. Grande parte de nossas atividades diárias em geral e nosso consumo de mídia em particular são cada vez mais influenciados por algoritmos que funcionam nos bastidores. Algoritmos são usados para monitorar nosso comportamento e interesses e para prever nossas necessidades e ações futuras. Eles orientam nossas ações e assim determinam, entre outras coisas, o sucesso econômico dos produtos e serviços. Eles formam a base técnico-funcional de novos serviços e modelos de negócios que se sobrepõem ou deslocam os modelos de negócios tradicionais. Os campos em que os sistemas algorítmicos são importantes são múltiplos. Palavras-chaves específicas incluem a Internet das Coisas; produção industrial usando sistemas ciberfísicos; robótica incluindo carros automotores; portais de avaliação; computação em nuvem; gestão de fluxos financeiros; diagnósticos médicos; espionagem e sabotagem; ou o controle digital de serviços existenciais de interesse geral (por exemplo, nas áreas de energia e transporte). Os algoritmos são cada vez mais utilizados não só em áreas privadas/comerciais, mas também no cumprimento de tarefas governamentais.

[163] Terminologia utilizada para designar aparelhos e utensílios com aprendizagem de máquina, aptidão de coleta e interpretação de dados autônoma, além de capacidade de comunicação entre si e com a rede. ASHTON, Kevin. That 'Internet of Things' Thing. **RFID Journal**, 2009. Disponível em: http://www.rfidjournal.com/articles/view?4986. Acesso em: 10 jun. 2021.

[164] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Rio de Janeiro: Forense, 2021, p. 34-35.

É esse potencial de aplicação quase ilimitado que revela a importância dos algoritmos para a sociedade pós-contemporânea, especialmente, quando esses algoritmos são dotados da capacidade de simular inteligência e de aprenderem por si sós, melhorando seu próprio código.

3.3. Inteligência artificial e aprendizagem de máquina

A ideia de Inteligência Artificial remonta um famoso estudo realizado por James Moor no ano de 1956.[165] Em seu ensaio, o autor aponta que "cada aspecto do aprendizado ou qualquer característica da inteligência humana pode, em princípio, ser tão precisamente descrita que uma máquina seja capaz de simulá-la".[166]

O termo aprendizado de máquina (*machine learning*), por sua vez, foi cunhado em 1959, três anos após a primeira referência à inteligência artificial, para designar o campo de estudo que dá aos computadores a habilidade de aprender sem serem explicitamente programados.[167]

Para melhor explicar o conceito, Pedro Domingos[168] aponta que:

> todo algoritmo tem uma entrada (*input*) e uma saída (*output*): os dados entram no computador, o algoritmo faz o que precisa ser feito com eles, e um resultado é produzido. O *machine learning* faz o contrário: entram os dados e o resultado desejado, e é produzido o algoritmo que transforma a relação entre dado e resultado verdadeira. Algoritmos inteligentes – também conhecidos como *learners* – são algoritmos que criam outros algoritmos. Com o *machine learning*, os computadores escrevem seus próprios programas, para que não tenhamos de fazê-lo.

A técnica do *machine learning*, que consiste em espécie de inteligência artificial, procura fazer referências e predições, a partir de um conjunto maciço de dados. A

---

[165] Atualizado e republicado em 2006.

[166] Tradução do autor. No original: "(...) every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it". MOOR, James. The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years. **AI Magazine**. Palo Alto: Association for the Advancement of Artificial Intelligence, v. 27, n. 4, p. 87–91, 2006, p. 87.

[167] SAMUEL, A. L. Some studies in machine learning using the game of checkers. **IBM Journal of Research and Development**. New York, v. 3, n. 3, p. 210–229, 1959.

[168] Tradução do autor. No original: "every algorithm has an input and an output: the data goes into the computer, the algorithm does what it will with it, and out comes the result. Machine learning turns this around: in goes the data and the desired result and out comes the algorithm that turns one into the other. Learning algorithms—also known as learners—are algorithms that make other algorithms. With machine learning, computers write their own programs, so we don't have to". DOMINGOS, Pedro. **The master algorithm:** how the quest for the ultimate learning machine will remake our world. New York: Basic Books, 2015, p. 6.

programação, a partir de certos parâmetros definidos, é capaz de encontrar padrões de comportamento nos dados alimentados, correlacionando-os, em busca do resultado almejado.

Funciona de forma parecida com um GPS. Dá-se um conjunto de dados (rotas), e a missão do algoritmo é encontrar a melhor rota até o ponto de chegada (resultado esperado). Dentre os conjuntos de dados, nesse exemplo, estariam os diversos caminhos existentes, pontos de partida e chegada, fluxo de veículos, comprimento das rodovias, podendo ser otimizados à medida que se aumente o conjunto de dados, como informações sobre obras, semáforos, se se trata de uma região com grande número de assaltos ou outros indicadores de violência, a existência de buracos, pedágios, etc.

Essa tecnologia está presente em serviços eletrônicos customizados (como players de música capazes de indicar *singles* com base nas preferências do usuário e, até mesmo, levando em conta o humor do usuário), em serviços de publicidade direcionada que rastreiam a atividade do indivíduo na web para lhe oferecer serviços e produtos com base em suas preferências, ou nas assistentes virtuais, capazes de se adaptar ao padrão de comportamento do usuário, além de diversas outras aplicações.

Hoffmann-Riem,[169] vai mais além na abordagem desses conceitos, apresentando algumas questões bastantes atuais, como o *deep lerning* e o desenvolvimento de redes neurais artificiais, veja-se:

> Atualmente, as capacidades computacionais e de análise dos computadores estão sendo expandidas e as possibilidades de aplicação e desempenho dos algoritmos estão crescendo e mudando rapidamente. A chamada inteligência artificial é particularmente importante para isso. Esse termo refere-se em particular ao esforço de reproduzir digitalmente estruturas de decisão semelhantes às humanas, ou seja, de projetar um computador de tal forma e, em particular, de programá-lo usando as chamadas redes neurais[170] de tal forma que possa processar os problemas da maneira mais independente possível e, se necessário, desenvolver ainda mais os programas utilizados.
> (...)
> O uso da inteligência artificial para o desenvolvimento de sistemas de aprendizagem está sendo promovido atualmente. Isto inclui a chamada máquina de aprendizagem. É usada para reconhecer padrões, avaliar imagens, traduzir linguagem em textos, apoiar decisões (como pontuação, *ranking*, previsão). Visa também o domínio de tarefas particularmente complexas, como a produção industrial com a ajuda de robôs ou a avaliação de imagens de raios X em medicina e outras. Mas

[169] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Rio de Janeiro: Forense, 2021, p. 35-37.
[170] O autor refere-se a redes de neurônios artificiais que são simuladas a partir de redes neurais naturais.

> os algoritmos podem fazer ainda mais. Cada vez mais, os sistemas de aprendizagem algorítmica são capazes de se adaptar a novas situações problemáticas de forma independente e de continuar a escrever seus próprios programas. Os algoritmos de aprendizagem são assim programados não só para resolver problemas específicos, mas também para aprender como os problemas são resolvidos. Eles devem então ser capazes de se desenvolver independentemente da programação humana. Falamos de *Deep Learning* quando o sistema aprende a compreender inter-relações, estruturas e arquiteturas sem intervenção humana adicional, de tal forma que pode melhorar seu desempenho de forma independente. A capacidade de aprendizagem do sistema condiciona assim seu processo de forma independente. As etapas individuais como tais permanecem deterministicamente controladas, mas existem em grande número e muitas vezes estão dinamicamente ligadas umas às outras, de modo que é difícil ou, em muitos casos, quase impossível reconstruir a determinação. Tais programas, que dependem da capacidade de aprender, são utilizados, por exemplo, no processamento de imagem e fala, robótica e prognóstico. A programação humana que antes era necessária para a programação de algoritmos e sistemas algorítmicos complexos está se tornando cada vez menos importante nos sistemas de aprendizagem, com a consequência de que os passos individuais e sua interação, bem como a lógica utilizada para eles, não são mais compreensíveis para os programadores. Andrew Tutt formula o seguinte sobre tais sistemas de aprendizagem: "Even if we can fully describe what makes them work, the actual mechanisms by which they implement their solutions are likely to remain opaque: difficult to predict and sometimes difficult to explain. And as they become more complex and more autonomous, that difficulty will increase"[171].

Dois são os pontos que merecem destaque na fala do professor Hoffmann-Riem: o rápido incremento no desempenho dos algoritmos, alavancado pelo barateamento e acréscimo de performance dos componentes eletrônicos; e a opacidade dos algoritmos dotados de inteligência artificial, na medida em que detém capacidade de alterar seu próprio código e fazer correlações a partir dos dados de que dispõe.

Sobre o primeiro aspecto, não poderíamos deixar apontar a denominada "Lei de Moore". Em 1965, Gordon E. Moore foi convidado a enviar um artigo para a revista *Electronics* com o intuito de apontar tendências para o futuro da tecnologia. Pensando nisso, ele revisou os dados sobre a produção de chips de silício da *Fairchild* e descobriu que o número de transistores em um chip de silício dobrava a cada ano.[172] A partir desses

[171] Tradução do autor: "mesmo se pudéssemos descrever completamente o que os faz funcionar, o verdadeiro mecanismo pelo qual implementam suas soluções ainda permaneceria, muito provavelmente, opaco: eles são difíceis de prever e difíceis de explicar. E à medida que se tornam mais complexos e mais autônomos, essa dificuldade irá aumentar".

[172] MOORE, Gordon M. Cramming more components onto integrated circuits. **Electronics**, [S. l.], v. 38, n. 8, p. 114, 1965. Disponível em: https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf. Acesso em: 12 nov. 2021.

dados ele propôs em seu artigo que essa taxa de crescimento se manteria praticamente estável nos anos seguintes. Em 1975 Moore apresentou uma revisão de seu artigo propondo uma taxa de duplicação mais conservadora: a cada 2 anos.[173]

Embora não seja uma lei no sentido matemático, a Lei de Moore acabou por se confirmar: a cada 18 meses, um transistor[174] teria a metade do tamanho do transistor atual.

---

[173] LOEFFLER, John. No More Transistors: The End of Moore's Law. **Interesting Engineering**. Delaware, 2018. Disponível em: https://interestingengineering.com/no-more-transistors-the-end-of-moores-law. Acesso em: 12 nov. 2021.

[174] Para entender melhor a importância dos transistores, recorre-se às lições de Pedro Domingos, no seguinte sentido: "Os computadores são compostos por bilhões de minúsculos interruptores chamados transistores, e os algoritmos ligam e desligam esses interruptores bilhões de vezes por segundo. O algoritmo mais simples é: desligue um interruptor. O estado de um transistor contém um único *bit* de informação: um, se o transistor estiver ativado, e zero, se estiver desativado. Um único *bit* em algum local dos computadores de um banco informa se nossa conta tem ou não saldo. Outro *bit* dos computadores da administração da previdência social informa se estamos vivos ou mortos. O segundo algoritmo mais simples é: combine dois *bits*. Claude Shannon, conhecido como o pai da teoria da informação, foi a primeira pessoa a entender que o que os transistores fazem, quando ligam e desligam em resposta a outros transistores, chama-se raciocínio. (Essa foi sua tese de mestrado no MIT – a mais importante tese de mestrado de todos os tempos.) Se o transistor A só liga quando os transistores B e C estão ligados, ele está envolvido em um pequeno esforço de raciocínio lógico. Se A liga quando B ou C está ligado, essa é outra minúscula operação lógica. E se A liga sempre que B está desligado, e vice-versa, é uma terceira operação. Acredite ou não, todos os algoritmos, não importando sua complexidade, podem ser reduzidos a apenas três operações: E, OU e NÃO. (...) Combinando várias dessas operações, podemos executar cadeias complexas de raciocínio lógico. Frequentemente as pessoas acham que os computadores só lidam com números, mas não é isso que ocorre. Os computadores são pura lógica. Os números e a aritmética são feitos de lógica, assim como tudo o mais que existe em um computador. Deseja somar dois números? Há uma combinação de transistores que faz a soma. (...) No entanto, seria proibitivamente caro se tivéssemos de construir um novo computador para cada tarefa diferente que quiséssemos executar. Em vez disso, um computador moderno é um vasto conjunto de transistores que pode fazer várias coisas, dependendo dos transistores que forem ativados. Michelangelo dizia que ele apenas via a estátua dentro do bloco de mármore e removia o excesso até ela ser revelada. Da mesma forma, um algoritmo desativa os transistores excedentes no computador até a função pretendida ser executada, seja o piloto automático de uma aeronave ou um novo filme da Pixar". No original: "An algorithm is a sequence of instructions telling a computer what to do. Computers are made of billions of tiny switches called transistors, and algorithms turn those switches on and off billions of times per second. The simplest algorithm is: flip a switch. The state of one transistor is one bit of information: one if the transistor is on, and zero if it's off. One bit somewhere in your bank's computers says whether your account is overdrawn or not. Another bit somewhere in the Social Security Administration's computers says whether you're alive or dead. The second simplest algorithm is: combine two bits. Claude Shannon, better known as the father of information theory, was the first to realize that what transistors are doing, as they switch on and off in response to other transistors, is reasoning. (That was his master's thesis at MIT—the most important master's thesis of all time.) If transistor A turns on only when transistors B and C are both on, it's doing a tiny piece of logical reasoning. If A turns on when either B or C is on, that's another tiny logical operation. And if A turns on whenever B is off, and vice versa, that's a third operation. Believe it or not, every algorithm, no matter how complex, can be reduced to just these three operations: AND, OR, and NOT. (…) By combining many such operations, we can carry out very elaborate chains of logical reasoning. People often think computers are all about numbers, but they're not. Computers are all about logic. Numbers and arithmetic are made of logic, and so is everything else in a computer. Want to add two numbers? There's a combination of transistors that does that. (…) It would be prohibitively expensive, though, if we had to build a new computer for every different thing we want to do. Rather, a mod- ern computer is a vast assembly of transistors that can do many different things, depending on which transistors are activated. Michelangelo said that all he did was see the statue inside the block of marble and carve away the excess stone until the statue was revealed. Likewise, an algorithm carves away the excess transistors in the computer until the intended function is revealed, whether it's an airliner's autopilot or a new Pixar movie. DOMINGOS, Pedro. **The master algorithm:** how the quest for the ultimate learning machine will remake our world. New York: Basic Books, 2015, p. 1-3. Para uma outra definição ainda mais técnica a

Isso significa que mais transistores poderiam ser colocados em um chip, o que impulsionaria o crescimento da capacidade de computação nos último 40 anos a níveis exponenciais.[175]

Hoje já se cogita o fim da Lei de Moore diante da capacidade de se comprimir transistores cada vez menores – já na casa dos nanômetros – em um único chip, sem perda energética por sua conversão em calor.

Já quanto à opacidade dos algoritmos e os problemas daí decorrentes, seja no campo da discriminação, seja em relação à proteção de direitos fundamentais como a privacidade, são assuntos tratados em diversas obras como The Black Box Society,[176] do jurista Frank Pasquale, Weapons of Math Destruction,[177] da matemática Cathy O'Neil e Automating Inequality,[178] da cientista política Virginia Eubanks.

Todas elas abordam diferentes perspectivas dos potenciais riscos associados aos algoritmos dotados de inteligência artificial, que serão tratados com mais profundidade na seção seguinte.

Entretanto, para o momento, cabe a este tópico introduzir ao leitor a ideia de Inteligência Artificial e Aprendizagem de Máquina, permitindo que se perceba à grosso modo como funcionam, seus potenciais de uso e alguns riscos a elas atrelados. Não se poderia, ainda, encerrar essa discussão sem fazer remissão à Proposta de Regulamento do

---

respeito do funcionamento de transistores e porque a Lei de Moore estaria próximo de seu fim, veja-se: LOEFFLER, John. No More Transistors: The End of Moore's Law. **Interesting Engineering**. Delaware, 2018. Disponível em: https://interestingengineering.com/no-more-transistors-the-end-of-moores-law. Acesso em: 12 nov. 2021. JURVETSON, Steve. Transcending Moore's Law with Molecular Electronics and Nanotechnology. **Nanotechnology Law & Business**, vol. 1, n. 1, 2004, p. 70-90. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/nantechlb1&i=72. Acesso em: 24 nov. 2021.

[175] LOEFFLER, John. No More Transistors: The End of Moore's Law. **Interesting Engineering**. Delaware, 2018. Disponível em: https://interestingengineering.com/no-more-transistors-the-end-of-moores-law. Acesso em: 12 nov. 2021.

[176] "*The black box society: the secret algorithms that control money and information",* escrito por Frank Pasquale e publicado pela Harvard Univerty Press, chama atenção para a opacidade dos algoritmos no sistema financeiro e informacional. PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2016.

[177] A obra "*Weapons of math destruction: How big data increases inequality and threatens democracy*", analisa diversas situações em que modelos matemáticos construídos por cientistas de dados aumentaram ou reforçaram desigualdades existentes. O livro explora diversos casos concretos relativos a algoritmos pouco transparentes (opacos), que em larga escala e com grande potencial danoso à vida das pessoas. O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016.

[178] O livro analisa o forte escrutínio digital, sinalização e perpassa a questão da opacidade. Trabalha, como hipótese central, a ideia de que grupos marginalizados estão mais suscetíveis à coleta de dados pessoais pois são beneficiários de políticas sociais, estando mais vulneráveis ao monitoramento estatal. Esses dados, no entanto, acabam por reforçar a marginalidade, quando tais grupos são alvo de algoritmos preditivos, análises de risco e sistemas automáticos de elegibilidade, em espécie de "sinalização vermelha coletiva", que alimenta um ciclo de injustiças – na designação da autora: *a feedback loop of injustice.* EUBANKS, Virginia. **Automating inequality**: how high-tech tools profile, police, and punish the poor. New York: St. Martin's Press, 2018.

Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento sobre inteligência artificial).[179]

Citado diploma é uma das primeiras propostas de normatização que trata de forma especial e autônoma da inteligência artificial, diante das diferentes implicações de seu uso. Para efeitos do regulamento entende-se como «Sistema de inteligência artificial» (sistema de IA), um programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas em anexo próprio,[180] capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage.

O regulamento já deixa antever um traço fundamental tratado por Hoffmann-Riem: a percepção de que os algoritmos, como regras, influenciam nossos comportamentos. Eles acabam por interagir com o ambiente em que estão inseridos e, de certo modo, os regulam. De igual forma, moldam esses ambientes trazendo novas implicações, necessidades e comportamentos em uma área específica, como foi, por exemplo, a introdução dos algoritmos de alta frequência nos mercados de negócios (*algorithmic trading*).

É por isso que o regulamento, segundo a proposta em construção, almeja garantir que os sistemas de IA colocados e utilizados no mercado da União sejam seguros e respeitem a legislação em vigor, sobretudo em matéria de direitos fundamentais e dos valores perseguidos pela União Europeia, garantindo a segurança jurídica para facilitar os investimentos e a inovação no domínio da IA. Busca, ademais, aperfeiçoar a governança e a aplicação efetiva da legislação em vigor em matéria de direitos

---

[179] UE. União Europeia. **Proposta de Regulamento do Parlamento Europeu e do Conselho harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial)**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN. Acesso em: 22 nov. 2021.

[180] ANEXO I - TÉCNICAS E ABORDAGENS NO DOMÍNIO DA INTELIGÊNCIA ARTIFICIAL - referidas no artigo 3.º, ponto 1

a) Abordagens de aprendizagem automática, incluindo aprendizagem supervisionada, não supervisionada e por reforço, utilizando uma grande variedade de métodos, designadamente aprendizagem profunda;

b) Abordagens baseadas na lógica e no conhecimento, nomeadamente representação do conhecimento, programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, sistemas de raciocínio (simbólico) e sistemas periciais;

c) Abordagens estatísticas, estimação de Bayes, métodos de pesquisa e otimização. UE. União Europeia. **Proposta de Regulamento do Parlamento Europeu e do Conselho harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial)**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN. Acesso em: 22 nov. 2021.

fundamentais e dos requisitos de segurança aplicáveis aos sistemas de IA; facilitar o desenvolvimento de um mercado único para as aplicações de IA legítimas, seguras e de confiança; e evitar a fragmentação do mercado.

A principal preocupação da recente proposta é conciliar a proteção de direitos fundamentais à abertura à inovação, sendo o esforço cognitivo nessa direção a tendência das ciências jurídicas como um todo; em especial, a busca pela efetividade normativa.

3.4. Big data

O termo Big Data, de outro lado, é utilizado para designar as tecnologias digitais capazes de lidar com grandes volumes de informações e as várias possibilidades de combinação, avaliação e processamento desses mesmos dados.

Amy Affelt[181] aponta que:

> Os “Dados brutos” sempre foram parte integrante do trabalho em empresas e escritórios (...). Mas, nos últimos anos, assistimos a uma explosão na quantidade de dados que estão sendo coletados. Literalmente, cada clique em cada site pode ser considerado um dado que um terceiro pode querer monitorar ou coletar. Embora esse volume de dados não sejam novidade para bibliotecários e profissionais da informação, a mídia tomou conhecimento dessa expansão e a chamou "Big Data". De acordo com um estudo da McKinsey, a quantidade de dados coletados deve crescer 40% ao ano. Da mesma forma, 15 dos 17 setores da indústria nos Estados Unidos têm mais dados armazenados por empresa do que a Biblioteca do Congresso Americano. O

[181] Tradução do autor. No original: “"Raw data" has always been part and parcel to work in corporations and law firms. But recent years have seen an explosion in the amount of data being collected. Literally, every click on every website can be considered data that a third-party may want to monitor or collect. While massive amounts of data are nothing new to librarians and information professionals, the news media has taken notice and termed this explosion "Big Data." According to a McKinsey study, the amount of data collected is poised to grow at 40% per year. Similarly, 15 of 17 industry sectors in the United States have more data stored per company than the Library of Congress. The growth in data has also lead to growth in revenue. International Data Corporation projects that in 2015, revenue from Big Data will be $16.9B, up from $3.2B in 2010.
Gartner coined the phrase "The V's of Big Data," establishing its unique characteristics as volume, meaning the sheer amount of data being collected, velocity, or the speed at which it is being collected (almost real-time in many cases), and variety, or the myriad of formats in which the data appears (ascii, plain text, audio, video, tweets, server log files, etc.). Information professionals have the skills to determine which data is truly useful and from credible sources, and we also are uniquely positioned to derive the value from the data for our constituents. “Value” is the most important v, because, as Jeanne Johnson writes in Financial Executive, extracting value from data is "challenging, risky, and expensive." It is challenging because it is hard to know which data should be tracked and used, and it is risky and expensive for a firm to undertake Big Data initiatives, spending vast sums of money to create datasets that may or may not be useful and may or may not be owned by the firm, since intellectual property laws applicable to datasets resulting from Big Data collation are in a nascent stage”. AFFELT, Amy. Big Data, Big Opportunity. **Australian Law Librarian**, vol. 21, n. 2, 2013, p. 78-89. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/auslwlib21&i=86. Acesso em: 21 nov. 2021.

> crescimento dos dados também levou ao crescimento da receita. A International Data Corporation projeta que, em 2015, a receita proveniente do Big Data será de US$ 16,9 bilhões, acima dos US$ 3,2 bilhões em 2010.
> O Gartner cunhou a frase "Os V's do Big Data", estabelecendo suas características únicas como: o volume, significando a grande quantidade de dados sendo coletados; a velocidade, representando a rapidez com que estão sendo recolhidos (quase em tempo real em muitos casos); e a variedade, destacando a miríade de formatos em que os dados aparecem (ascii, textos simples, áudio, vídeo, tweets, arquivos de log de servidor etc.). Os profissionais da informação têm as habilidades para determinar quais dados são realmente úteis e de fontes confiáveis, e estão em uma posição privilegiada para extrair o valor dos dados àqueles que representam. "Valor" é o v mais importante, porque, como Jeanne Johnson escreve em *Financial Executive*, extrair valor dos dados é "desafiador, arriscado e caro". É um desafio porque é difícil saber quais dados devem ser rastreados e usados, e é arriscado e caro para uma empresa empreender iniciativas de Big Data, gastando grandes somas de dinheiro para criar conjuntos de dados que podem ou não ser úteis e podem ou não ser propriedade da empresa, uma vez que as leis de propriedade intelectual aplicáveis aos conjuntos de dados resultantes da comparação de Big Data estão em um estágio inicial.

O maciço conjunto de dados do Big Data é especialmente importante porque permite a criação de modelos matemáticos mais acurados. Para os matemáticos e estatísticos, quanto maior a quantidade de dados disponíveis, mais precisa a determinação de um modelo, com menor chance de erros ou desvios.

Essa é uma preocupação expressa, em certa medida, por Amy Affelt,[182] ao descrever os riscos envolvendo a utilização do Big Data, ainda que tenha escrito suas anotações nos idos de 2013.

A constatação de que a precisão dos modelos matemáticos empregados no Big Data está diretamente relacionada à quantidade de dados sobre os quais estes são construídos, revela uma aparente antinomia entre a utilização desta tecnologia e a regulação geral envolvendo a proteção de dados pessoais (consubstanciada nos princípios da limitação, proporcionalidade e finalidade).

Essa perspectiva denota, desde já, que o Regulamento Geral de Proteção de Dados (ou nossa Lei Geral de Proteção de Dados), por ser uma norma de caráter abrangente e genérica não dará conta de todos os problemas envolvendo as novas tecnologias, tanto assim que a União Europeia e o Brasil já estudam marcos legais

[182] AFFELT, Amy. Big Data, Big Opportunity. **Australian Law Librarian**, vol. 21, n. 2, 2013, p. 78-89. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/auslwlib21&i=86. Acesso em: 21 nov. 2021.

relacionados a outras tecnologias, como a inteligência artificial, frequentemente empregada de forma associada ao Big Data.

3.4.1. Sobre o termo e sua evolução

Ainda falando sobre o *Big Data*, ao se buscar por uma definição do termo, corriqueiramente a literatura nos remete aos 5V's, atualmente 7V's. É exemplo disso a lição da Professora portuguesa Paula Ribeiro Alves[183] segundo a qual:

> A *big data* tem vindo a ser objeto de várias tentativas de definição, com pouco sucesso.[184]
> Melhores resultados têm sido obtidos com a identificação e autonomização de suas características.
> No início, foram identificadas o Volume, a Variedade e a Velocidade, significando que estamos perante uma quantidade enorme de informação, estruturada e não estruturada, proveniente de várias fontes e que, para ser interessante, tem de ser trabalhada muito rapidamente.
> Depois juntaram-se a Veracidade e o Valor, quando se começou a perceber que muita da informação que estava *online* não era verdadeira e havia que fazer uma triagem e quando começou a ficar evidente o valor da *big data.* Quem consegue criar melhores algoritmos e minerar melhor os dados passa a ter uma mercadoria para vender. Essa informação vai permitir orientar publicidade, aliciar clientes, avaliar o risco, gerir com mais eficácia e responder a muitas questões.
> Atualmente, autonomizaram-se mais duas características num total de sete, a Variabilidade e a Visualização, considerando que a informação se altera ao longo do tempo é necessário ter em conta essa variação e considerando que é importante mostrar os resultados das análises de modos cada vez mais interessantes, apelativos e interativos.

Outros, como Ana Alves Leal[185], mantém-se na simplicidade de um conceito mais enxuto, todavia bastante funcional, não obstante ainda se refira a três dos sete V's:

---

[183] ALVES, Paula Ribeiro. Os desafios digitais no mercado segurador. In **Fintech: Desafios da Tecnologia Financeira**. 2ª ed. Coimbra: Almedina, 2019, p. 28-62, p. 34-35.

[184] Refira-se, a título de exemplo, "Big data is the capacity to analyse a variety of (unstructured) data sets from a wide range of sources.", no Green Paper on mobile health ("mHrealth"), da Comissão Europeia, 2014, disponível em: https://ec.europa.eu/digitalsingle-market/en/news/green-paper-mobile-health-mhealth e "Big data" is a term for the collection of large an complex data sets and the analysis of these data sets for relationships. The quantity of data in these sets prevents traditional methods of analysis from being effective. Rather than focusing on precise relationships between individual pieces of data, big data uses various algorithms and techniques to infer general trends over the entire set. What count is the quantity rather the quality. Big data looks for the correlation rather than the causation – the "what" rather than the "why.", in: https://epic.org/privacy/big-data/, consultados em 29/03/2017 e em 07/01/2019.

[185] LEAL, Ana Alves. Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação. In Fintech: Desafios da Tecnologia Financeira. 2ª ed. Coimbra: Almedina, 2019, p. 79-218, p. 81.

> No domínio da tecnologia da informação, utiliza-se a designação «big data» (em português, «megadados», «dados massivos» ou «dados em larga escala») para referir conjuntos de informação em larga escala, cuja dimensão excede a capacidade e impossibilita (ou, pelo menos, dificulta) a aptidão das ferramentas dos tradicionais *softwares* de recolha, armazenamento, gestão e análise de bases de dados.
> Diz-se serem estes conjuntos de informação caracterizados por "três V's": *volumetria* (grandes volumes de dados gerados em cada segundo), *variedade* (os dados são fornecidos em diferentes tipos de formatos e recolhidos através de diversas formas, correspondendo sobretudo a dados não estruturados) e *velocidade de atualização* (o conteúdo dos dados está em constante mutação, sendo gerados grandes volumes de dados por segundo, o que impulsiona a necessidade de processamento desses dados em tempo real).

Por fim, socorrendo-se às ideias de Hoffmann-Riem,[186] tem-se que:

> O termo Big Data refere-se a situações em que as tecnologias digitais são utilizadas para lidar com grandes e diversas quantidades de dados e às várias possibilidades de combinação, avaliação e processamento desses dados por autoridades privadas e públicas em diferentes contextos. Cinco características são frequentemente utilizadas para identificar Big Data: Os cinco "Vs". As possibilidades de acesso a enormes quantidades de dados digitais (*High Volume*), de diferentes tipos e qualidade, assim como diferentes formas de coleta, armazenamento e acesso (*High Variety*), e a alta velocidade do seu processamento (*High Velocity*). O uso da inteligência artificial em particular torna possível novas e altamente eficientes formas de processamento de dados, bem como a verificação de sua consistência e garantia de qualidade (*Veracity*). Além disso, os Big Data são objeto e base de novos modelos de negócios e de possibilidades para diversas atividades de valor agregado (*Value*). Big Data é utilizado para diversos fins, tais como controle de comportamentos individuais e coletivos, registro de tendências de desenvolvimento, possibilitando novos tipos de produção e distribuição e cumprimento de tarefas estatais, mas também para novas formas de ilegalidade, especialmente crimes cibernéticos. Exemplos de aplicações para o uso de Big Data são: comunicação eletrônica (por exemplo, com smartphones); interação e comunicação em mídias sociais; tecnologias de rede (*smart home*, medidor inteligente); sistemas de assistência linguística como o Alexa da Amazon; vigilância eletrônica; uso de cartões de crédito ou de clientes; mobilidade inteligente etc.

A definição de Big Data, como visto, não é unívoca, o que dificulta que aqui seja apresentado apenas um ponto de vista. Não obstante, para descrever esse grande conjunto de dados, em geral, a doutrina opta por elencar suas características, de forma a qualificar se um conjunto de dados se subsome a essa categoria funcional.

---

[186] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Rio de Janeiro: Forense, 2021, p. 34-35.

Assim, ao menos três características são unânimes em qualquer definição de Big Data, caracterizando-o: a existência de um grande volume de dados, com grande variedade e alta velocidade de processamento. Embora outras características tenham se somado a essas três principais ao longo dos anos, especialmente por necessidades mercadológicas (como é exemplo o sétimo "v", visualização, fruto da necessidade de interfaces cada vez mais intuitivas e visuais, o que explica o clamor por tecnologias que proporcionem praticidade e intuitividade),[187] ao menos essas três características originárias devem se fazer presente para que estejamos diante dessa categoria de dados.

Sem embargos, para lidar com esses conjuntos de dados gigantesco outras tecnologias têm de se aliar para que se produzam resultados úteis, surgindo daí o termo *Big Data Analytics*.

3.4.2. Big data analytics

O *Big Data Analytics*, por fim, é a combinação de técnicas (como o uso da inteligência artificial) para a realização de análises sobre um grande conjunto de dados. Hoffmann-Riem, avalia que essas análises podem ser dos seguintes tipos:[188]

> 1. A análise descritiva (...) utilizada para peneirar e preparar o material para fins de avaliação. Um campo de exemplo é o uso de Big Data para Data Mining e para registro e sistematização dos dados (especialmente priorização, classificação e filtragem).
> 2. A análise preditiva visa identificar indicadores para uma possível relação causal – ainda em grande parte desligada de um processo de entendimento – mas (pelo menos até agora apenas) sob a forma de correlações estatisticamente significativas; nesta base, os eventos devem ser previstos com uma certa probabilidade. O objetivo é fornecer ideias para o comportamento humano e, por exemplo, identificar tendências de desenvolvimento e padrões de comportamento a fim de prever comportamentos futuros e, com base nisso, ser capaz de tomar decisões na forma de Tomada de Decisão Automatizada (ADM). A análise preditiva pode ser usada, por exemplo, para registrar as preferências e desejos do consumidor (*Predictive Consumer Interests*) ou para *Predictive Policing*.
> 3. A análise prescritiva visa a recomendações de ação, a fim de utilizar conhecimentos descritivos e preditivos para atingir objetivos

[187] Como exemplo podemos notar a significativa diferença em nossos controles remotos atualmente. Os muitos botões e comandos outrora existentes foram substituídos por interfaces, cada vez mais enxutas, existindo pouco mais de uma dezena de botões na maioria dos controles remotos dos mais modernos aparelhos eletrônicos. Ou, ainda, a adoção do *visual law* na área do direito; ou o próprio metaverso, que é exemplo claro da possibilidade de interatividade e visualização, levados ao extremo, talvez.

[188] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Rio de Janeiro: Forense, 2021, p. 34-35.

> específicos, tais como seleção personalizada em preços ou estratégias e táticas para influenciar atitudes e comportamentos, incluindo a influência na formação da opinião pública, bem como na percepção e apoio/prevenção de desenvolvimentos sociais.

Tais técnicas permitem diversas aplicações, tanto na área privada (política de crédito bancário, disponibilização de serviços financeiros, como cartões de crédito, além de outras análises complexas), quanto pública (sistemas preditivos utilizados em Tribunais, análises e comparação de políticas públicas, entre outras).

As consequências dessas técnicas sobre populações mais vulneráveis, entretanto, é fartamente catalogada na literatura, como os ensaios de Sweeney,[189] Richardson, Schultz e Crawford,[190] e Bertrand e Mullainathan,[191] por exemplo. Dois deles abordando vieses raciais nos algoritmos de entrega de anúncios (propensos a apresentarem publicidade relacionada à sistemas de buscas por fichas criminais a pessoas negras) e de seleção a vagas de emprego. O terceiro, por seu turno, relacionado à violação de direitos civis em razão da utilização de sistemas de policiamento preditivo nos Estados Unidos da América.

O trabalho de Richardson, Schultz e Crawford argumenta que em várias jurisdições os sistema preditivos são construídos com base em dados produzidos durante períodos já documentados de más práticas e políticas falhas, racialmente enviesadas e, às vezes, ilegais ("policiamento sujo"). Essas práticas e políticas de policiamento moldam o ambiente e a metodologia pela qual os dados são criados, o que aumenta o risco desses dados serem imprecisos, distorcidos ou sistematicamente tendenciosos ("dados sujos"). A premissa do estudo é de que se os sistemas de policiamento preditivo forem informados por tais dados, eles não poderão escapar dos legados das práticas de policiamento ilegais ou tendenciosas sobre as quais foram construídos.

Além disso, os fornecedores desses sistemas de policiamento preditivo não fornecem garantias suficientes de que seus sistemas atenuam ou segregam adequadamente esses dados, representando uma possível ameaça aos direitos civis da população negra estadunidense.

---

[189] SWEENEY, Latanya. Discrimination in Online Ad Delivery. **SSRN Electronic Journal**. 2013. Disponível em: https://doi.org/10.2139/ssrn.2208240. Acesso em: 17 jun. 2022.
[190] RICHARDSON, Rashida; SCHULTZ, Jason M.; CRAWFORD, Kate. **Dirty data, bad predictions: how civil rights violations impact police data, predictive policing systems, and justice**. 2019. New York: New York University Law Review, p. 192–233.
[191] BERTRAND, Marianne; MULLAINATHAN, Sendhil. **Are Emily and Greg More Employable than Lakisha and Jamal?**: A Field Experiment on Labor Market Discrimination. 2003. Disponível em: URL: https://doi.org/10.4324/9780429499821-53. Acesso em: 15 jun. 2022.

Postas algumas das premissas fundamentais para análise dos sistemas algorítmicos, trataremos em algumas linhas como eles são planejados e executados.

3.5. A construção algorítmica

Baer descreve a construção dos modelos algorítmicos em cinco etapas: o *design* do modelo, a engenharia de dados, a montagem do modelo, sua validação, e, por fim, sua implementação.

O autor[192] discorre que a primeira etapa (projeto) define a estrutura geral do modelo e como ele deve funcionar (seus *inputs* e *outputs*), algo não muito diferente do plano que um arquiteto executa para a construção de uma casa nova. A segunda etapa (engenharia de dados) é responsável por preparar os dados usados para estimar os coeficientes do algoritmo e abrange todas as atividades de engenharia, desde os dados que se pretende coletar (na analogia do projeto de uma casa, estaríamos falando da seleção dos materiais) até os colocar ordenadamente em uma grande "tabela" ou banco de dados. Essa tarefa se mostra bastante complexa, utilizando o autor da analogia aos ladrilhos de um banheiro; ordená-los envolve selecionar e inspecionar cada ladrilho, descartar os quebrados e cortar alguns no comprimento certo para se encaixarem nos cantos e fendas do desenho projetado.

A terceira etapa é a montagem do modelo. Para Baer,[193] trata-se do coração de seu desenvolvimento, pois é aqui que os dados brutos são transformados em uma equação, com coeficientes derivados por meio de técnicas estatísticas. A validação do modelo, por sua vez, consiste na busca por uma revisão independente que possa afirmar sua adequação para uso.

---

[192] Tradução do autor. No original: 1. Model design defines the overall structure of the model, such as what shall go in and what shall come out of it—not unlike the plan an architect makes for the construction of a new house. 2. Data engineering prepares the data used to estimate the coefficients of the algorithm. It covers all activities from identifying the data you want to collect (in our architecture analogy, this first substep is placing an order for construction materials) to putting all data neatly into one or more large tables—with most challenges hiding behind the notion of "neatly." (Just think of bathroom tiles—if you want to have that perfect bathroom, the tiler should carefully inspect each tile, dispose of the broken ones, and cut some tiles just to the right length to fit into corners and crevices.). BAER, Tobias. **Understand, Manage, and Prevent Algorithmic Bias**. Kaufbeuren: Apress, 2019, p. 30.

[193] Tradução do autor. No original: 3. Model assembly is the heart of model development . Here the raw data is transformed into an equation, with coefficients derived through statistical techniques. 4. Model validation is an independent review and assertion of the model's fitness for use. 5. Model implementation is the deployment of the model in actual business operations. Let's discuss each step in a bit more detail, in particular the two steps most important for taming biases: data engineering and model assembly. BAER, Tobias. **Understand, Manage, and Prevent Algorithmic Bias**. Kaufbeuren: Apress, 2019, p. 30.

Por fim, a implementação nada mais é que a utilização do modelo em operações de negócio reais. Esmiuçando todas as etapas, Baer sistematiza: [194]

> 1. O design do modelo garante que este apoie seu objetivo estratégico, definindo o resultado a ser previsto, em que tipo de população ele é desenvolvido, quais dados preditivos são usados e qual metodologia de modelagem é aplicada.
> 2. A engenharia de dados prepara os dados apropriados para o desenvolvimento do modelo, definindo uma amostra adequada; realizando a coleta de dados brutos e a divisão da amostra em três partes para desenvolvimento, teste e validação; garante a alta qualidade dos dados, identificando e eliminando problemas com eles; e faz a agregação dos dados granulares.
> 3. A montagem do modelo produz o algoritmo real. Esta etapa envolve sete subetapas, a saber, a exclusão de registros inadequados com base em critérios lógicos; o desenvolvimento de novos recursos; a eliminação de recursos que são inúteis ou redundantes; a estimativa inicial dos coeficientes do modelo e seu ajuste iterativo; a calibração dos resultados do modelo e regras de decisão em torno deles; e a documentação do modelo.
> 4. A validação do modelo é um processo de governança para determinar de forma independente sua adequação para uso.
> 5. A implementação do modelo o insere nas operações de negócios reais; isso envolve, em particular, alimentar entradas de dados no modelo e vincular as saídas do modelo às decisões de negócios.

A partir desse quadro tem-se uma visão geral a respeito da construção dos modelos algoritmos, processo que envolve desde a seleção e preparação de dados até a verificação de conformidade do modelo, em etapa de validação.

Entre essas etapas, no entanto, um sem-número de intercorrências podem acontecer, seja na captura dos dados que alimenta, na filtragem desses mesmo dados ou, até, na construção do modelo que depende de certas assunções, às vezes problemáticas, como se verá no caso de Sara Wysocki.

---

[194] Tradução do autor. No original: "Model design ensures that the model supports its strategic objective by defining the outcome to be predicted, on what kind of population it is developed, which predictive data is used, and what modeling methodology is applied. Data engineering prepares appropriate data for the model development by defining a suitable sample; collecting raw data; splitting the sample in three parts for development, testing, and validation; ensuring high data quality by identifying and cleaning issues with the data; and aggregating granular data. Model assembly produces the actual algorithm. This step involves seven substeps, namely the exclusion of inappropriate records based on logical criteria, the development of new features, the elimination of features that are useless or redundant, an initial estimate of the model coefficients, their iterative tuning, the calibration of model outputs and decision-rules around them, and the documentation of the model. Model validation is a governance process to independently ascertain the model's fitness for use. Model implementation deploys the model in actual business operations; this involves in particular feeding data inputs into the model and linking model outputs to business decisions. BAER, Tobias. **Understand, Manage, and Prevent Algorithmic Bias**. Kaufbeuren: Apress, 2019, p. 39.

Finda essa última etapa a respeito dos conceitos que envolvem a linguagem das tecnologias da informação, passaremos a analisar alguns riscos em potencial dessas novas tecnologias, que a regulação em matéria de privacidade e proteção de dados pessoais busca evitar, nem sempre com sucesso.

4. O uso dos dados e seus efeitos sociais: o controle digital do comportamento

4.1. O uso preditivo de dados e outras aplicações algorítmicas

Desde o início da era digital, a tomada de decisões nas áreas de finanças, emprego, política, saúde e serviços humanos passou por mudanças significativas. Quarenta anos atrás, quase todas as principais decisões que envolviam a vida das pessoas – se lhe é oferecido um emprego, uma hipoteca, um seguro, crédito bancário ou um serviços do governo – eram tomadas por seres humanos. Essas decisões por mais padronizadas e baseadas em processos atuariais (técnicas específicas de análise de riscos e expectativas), contavam, de algum modo, com o discernimento humano.[195]

Hoje, cedeu-se muito desse poder de tomada de decisão para máquinas sofisticadas. Sistemas automatizados de elegibilidade, algoritmos de classificação e modelos de risco preditivos que controlam quais bairros são policiados, quais famílias obtêm os recursos necessários, quem é selecionado para vagas de emprego e quem é investigado por fraude, por exemplo.[196]

Ao contrário do que se pode pensar os algoritmos (modelos lógico-matemáticos adotados a partir de algoritmos) não estão apenas em aspectos banais da vida das pessoas, mas em áreas cada vez mais cruciais da vida humana, como na segurança pública, em políticas educacionais, assistenciais ou, até criminais.

Esses algoritmos, no entanto, podem apresentar um impacto significativamente desproporcional, injusto ou discriminatório na vida das pessoas, o que levou a cientista de dados, Cathy O'Neil[197], a nomear modelos potencialmente danosos de "Armas de destruição matemática" (no inglês: "Weapons of math destruction").

---

[195] EUBANKS, Virginia. **Automating inequality**: how high-tech tools profile, police, and punish the poor. New York: St. Martin's Press, 2018, p. 3.
[196] EUBANKS, Virginia. **Automating inequality**: how high-tech tools profile, police, and punish the poor. New York: St. Martin's Press, 2018, p. 3.
[197] Ph.D. em matemática pela Universidade de Harvard.

O trocadilho com a expressão “Armas de destruição em massa” (“Weapons of mass destruction”) foi utilizado pela autora para designar algorítmicos pouco transparentes (opacos), com atuação em larga escala e grande potencial danoso à vida das pessoas.[198]

O’Neil analisa em sua obra diversas situações em que tais modelos matemáticos construídos por cientistas de dados se tornaram problemáticos. Para que se entenda o argumento da autora, antes de abordar três dos casos por ela expostos, examinaremos algumas considerações sobre a construção de tais modelos matemáticos.

4.2. Os modelos matemáticos

Um modelo matemático, como aponta O’Neil,[199] nada mais é do que uma representação abstrata de algum processo aplicável a muitos casos, seja em um jogo de beisebol, em uma cadeia de suprimentos de uma empresa de petróleo, em ações de um governo estrangeiro ou em uma ida ao cinema. Quer esteja sendo executado em um programa de computador ou mentalmente, o modelo (construído a partir de um ou vários algoritmos) capta o que sabemos sobre um assunto e usa esses dados para prever as respostas possíveis em várias situações.[200] Esses modelos, dizem o que uma pessoa pode esperar e orientam sua tomada de decisão.

A construção de um modelo leva em conta diversos dados de entrada (*input*s) e de saída (*outputs* ou resultados), assim como as etapas ordenadas para a realização desses resultados. A autora exemplifica a situação a partir de um modelo informal que ela utiliza todos os dias:

> Como mãe de três filhos, preparo as refeições em casa (...). Cada noite, quando começo a cozinhar uma refeição em família, interna e intuitivamente construo um modelo para a situação. Eu sei que um dos meus filhos adora frango (mas odeia hambúrgueres), enquanto outro come apenas o macarrão (com queijo parmesão ralado extra). Mas também tenho de levar em conta que o apetite das pessoas varia de dia para dia, então uma mudança pode pegar meu modelo de surpresa. Há alguma incerteza inevitável envolvida.

---

[198] O’NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 42.
[199] O’NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p.18.
[200] O’NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p.18.

> Os dados de entrada para esse modelo são as informações que tenho sobre minha família, os ingredientes que tenho em mãos ou que sei que estarão disponíveis, e minha própria energia, tempo e ambição na cozinha. Os dados de saída são como e o que decidirei cozinhar. A avaliação do modelo é medida pelo sucesso da refeição, pelo quão satisfeita minha família parece no final dela, quanto eles comeram e quão saudável a comida era. Ver o quão bem é recebido e o quanto é apreciada a comida me permite atualizar meu modelo para a próxima vez que cozinhar. As atualizações e ajustes tornam o que os estatísticos chamam de "modelo dinâmico".[201]

O problema desses modelos está no fato de que eles refletem os julgamentos e as prioridades de seus criadores. E, embora em certas situações, como em uma indicação musical ou na seleção daquilo que vai parar em sua caixa de spam, pareça simples, outras são muito mais problemáticas.

Para ilustrar a situação, vamos ao primeiro caso relatado por O'Neil.[202]

4.1.1. O caso das escolas do distrito de Washington

Em 2007, o novo prefeito de Washington, D.C., Adrian Fenty, estava determinado a reverter a situação das escolas de baixo desempenho da cidade. Ele detinha um trabalho difícil pela frente: na época, apenas um em cada dois alunos do ensino médio permanecia na escola após a nona série, e, apenas 8% dos alunos da oitava série, apresentavam um bom desempenho em matemática. A teoria corrente era a de que os alunos não estavam aprendendo o suficiente porque seus professores não estavam fazendo um bom trabalho.[203]

---

[201] Tradução do autor. No original: "*As a mother of three, I cook the meals at home—my husband, bless his heart, cannot remember to put salt in pasta water. Each night when I begin to cook a family meal, I internally and intuitively model everyone's appetite. I know that one of my sons loves chicken (but hates hamburgers), while another will eat only the pasta (with extra grated parmesan cheese). But I also have to take into account that people's appetites vary from day to day, so a change can catch my model by surprise. There's some unavoidable uncertainty involved. The input to my internal cooking model is the information I have about my family, the ingredients I have on hand or I know are available, and my own energy, time, and ambition. The output is how and what I decide to cook. I evaluate the success of a meal by how satisfied my family seems at the end of it, how much they've eaten, and how healthy the food was. Seeing how well it is received and how much of it is enjoyed allows me to update my model for the next time I cook. The updates and adjustments make it what statisticians call a "dynamic model*". O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 18.

[202] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 3.

[203] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 3.

Então, em 2009, Michelle Rhee, nomeada por Fenty para preencher o cargo de chanceler das escolas de Washington, desenvolveu uma ferramenta de avaliação dos professores chamada IMPACT, que procurava medir o desempenho do professor e extirpar do sistema os maus profissionais; é o que a engenharia de dados chama de otimização. Assim, ao final do ano letivo de 2009-10, o distrito demitiu todos os professores cujas pontuações estabelecidas pelo sistema estava entre os 2% piores no ranking criado. No final do ano seguinte, outros 5%, ou 206 professores, foram expulsos.[204]

Sarah Wysocki, uma professora da quinta série, não parecia ter nenhum motivo para se preocupar. Ela estava na *MacFarland Middle School* por apenas dois anos, mas já estava recebendo excelentes críticas de seu diretor e dos pais de seus alunos. Em uma de suas avaliações foi elogiada por sua atenção às crianças; outra a apontou como "uma das melhores professoras" com quem já teve contato. No entanto, ainda assim, no final do ano escolar de 2010-11, Wysocki recebeu uma pontuação extremamente baixa em sua avaliação realizada pela ferramenta IMPACT.[205]

O problema de Wysocki era claro: o novo sistema de pontuação conhecido como modelagem de valor-agregado, de algum modo, fazia com que as notas dos alunos superassem as críticas positivas dos administradores da escola e da comunidade escolar.[206] A modelagem parecia até fazer sentido, na medida em que um administrador que tivesse qualquer relação pessoal ou de amizade com um professor poderia influir no resultado da avaliação, de modo que o sistema parecia conferir um peso menor a avaliações e críticas de ordem subjetiva.

Tal situação deixou o distrito sem escolha a não ser demiti-la, junto com 205 outros professores que tiveram pontuações abaixo do limite mínimo no IMPACT.

Wysocki, é claro, achava que os dados eram terrivelmente injustos e ela queria saber de onde vinham. Questionava como uma boa professora poderia obter notas tão ruins? Qual foi a medição do modelo de valor agregado? Mas como ela veio a perceber, essas questões eram complexas.[207]

---

[204] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 3.
[205] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 4.
[206] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 4.
[207] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 4.

Em sua origem, o sistema analisado foi criado por uma empresa de consultoria, a *Mathematica Policy Research* situada em Princeton e contratada pelo distrito de Washington para desenvolvê-lo. O desafio da *Mathematica* era medir o progresso educacional dos alunos do distrito e então calcular quanto de seu avanço ou declínio poderia ser atribuído a seus professores. Isso não foi fácil, é claro. Os pesquisadores sabiam que muitas variáveis, desde as origens socioeconômicas dos alunos até os efeitos intrínsecos às dificuldades de aprendizagem, poderiam afetar os resultados dos alunos. Os algoritmos tiveram que fazer concessões para tais diferenças, que representavam uma das razões de serem tão complexos.[208]

Na verdade, tentar reduzir o comportamento, o desempenho e o potencial humanos a algoritmos não é uma tarefa fácil, como avalia O'Neil. Tentar calcular o impacto que uma pessoa pode ter sobre outra ao longo de um ano letivo é muito complexo. A própria professora, Sarah Wysock, argumentava: "Há tantos fatores envolvidos na aprendizagem e no ensino que seria muito difícil medir todos eles".[209] Além do mais, tentar pontuar a eficácia de um professor analisando os resultados do teste de apenas 25 ou 30 alunos seria estatisticamente incorreto, afirma O'Neil. Os números são muito pequenos, considerando todas as variáveis que podem influir no caso.[210]

No entanto, quando o sistema de pontuação da Mathematica marca Sarah Wysocki e 205 outros professores como ruins, o distrito os despede. Mas como saber se ele estava correto? Aparentemente, isso não é importante. O próprio sistema determina quem são os profissionais insuficientes e é assim que são vistos. Duzentos e seis professores "ruins" deixaram de compor o sistema de ensino. Esse fato por si só parece demonstrar a eficácia do modelo de valor agregado, na medida em que está "expurgando" do distrito profissionais de baixo desempenho. Assim, ao invés de buscar a verdade, o sistema de pontuação passa a representá-la (a incorporá-la), tornando-se o principal medidor de sucesso desses indivíduos. Como avalia O'Neil, no campo algorítmico muitas suposições deletérias são camufladas pela matemática e não são testadas ou questionadas.[211]

---

[208] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 4.
[209] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 5.
[210] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 5.
[211] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 5.

Após alguma insistência, Sarah Wysocki não foi capaz de encontrar alguém que lhe explicasse sua baixa pontuação. Como pôde perceber, o modelo em si era uma caixa preta, seu conteúdo um segredo corporativo fortemente guardado. Durante anos, os professores de Washington reclamaram das pontuações e clamaram por detalhes de seu conteúdo. A resposta padrão era a de que se tratava de um algoritmo muito complexo.[212]

Ainda assim, Wysocki estava ciente de que as notas dos testes padronizados de seus alunos contavam muito na fórmula matemática. E, aqui, ela teve algumas suspeitas.

Antes de começar o que seria seu último ano na *MacFarland Middle School*, ela ficou satisfeita em ver que seus novos alunos da quinta série haviam obtido resultados surpreendentemente bons em seus testes no final de ano anterior. Na *Barnard Elementary School*, de onde vieram muitos dos alunos de Sarah, 29 por cento dos alunos foram classificados em um "nível de leitura avançado". Isso era cinco vezes a média do distrito escolar. No entanto, quando as aulas começaram, ela viu que muitos de seus alunos tinham dificuldade para ler até mesmo frases simples.[213]

O tempo se passou e investigações do *Washington Post* e do *USA Today* revelaram um alto nível de rasuras nos testes padronizados em 41 escolas do distrito, incluindo *Barnard*. Uma alta taxa de respostas corrigidas aponta para uma maior probabilidade de trapaça. Em algumas escolas o percentual de salas de aula suspeitas chegava a até 70 por cento. O que isso teria a ver com o algoritmo? Um par de coisas.

Em primeiro lugar, os algoritmos de avaliação dos professores são uma ferramenta poderosa para modificação comportamental. Esse é o propósito deles, e, nas escolas de Washington, os administradores do distrito usaram uma dupla política de incentivos e punições (conhecida como *sticks and carrots*).[214]

Os professores sabiam que, se seus alunos tropeçassem no teste, seus próprios empregos estavam em risco. Isso deu a eles uma forte motivação para garantir que os alunos fossem aprovados, especialmente porque a Grande Recessão de 2008 atingiu o mercado de trabalho. Ao mesmo tempo, se seus alunos superassem os de seus colegas, professores e administradores poderiam receber um bônus de até US $ 8.000.[215]

---

[212] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 8.
[213] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 8-9.
[214] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 9.
[215] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 9.

Se forem adicionados esses incentivos poderosos às evidências do caso – o alto número de rasuras e as pontuações anormalmente altas nos testes – havia motivos para suspeitar que os professores da quarta série, curvando-se ao medo ou à ganância, corrigiram os exames de seus alunos. É concebível, então, que os alunos da quinta série de Sarah Wysocki tenham começado o ano letivo com notas artificialmente infladas. Se assim fosse, seus resultados no ano seguinte fariam parecer que eles perderam desempenho na quinta série – e que seu professor teve um resultado inferior. Wysocki estava convencida de que foi isso o que aconteceu com ela. Essa explicação se encaixava nas observações de pais, colegas e de seu diretor de que ela era realmente uma boa professora. Isso esclareceria a confusão.[216]

O'Neil relata que Sarah Wysocki tinha um caso forte em mãos, mas pouco conseguiu diante do sistema informático, pois ele não ouve, nem se dobra. Além disso, quando fica claro que os sistemas automatizados estão incorretos de alguma forma esdrúxula e sistemática, os programadores voltarão e ajustarão os algoritmos.[217] Contudo, na maioria das vezes os programas entregam veredictos inflexíveis, e os seres humanos que os aplicam só podem dar de ombros.[218]

E foi exatamente essa a resposta que Sarah Wysocki finalmente obteve do distrito escolar. Jason Kamras, administrador do distrito, disse mais tarde ao Washington Post que as rasuras eram "sugestivas" e que os números podiam estar errados na classe da quinta série de Wysocki, mas a evidência não era conclusiva.[219]

Ele disse, dessa forma, que Sarah foi tratada com justiça. Veja-se, no entanto, o paradoxo: um algoritmo processa uma série de estatísticas e apresenta a probabilidade de que uma certa pessoa seja uma péssima contratação. Essa probabilidade é destilada em uma pontuação, que pode virar a vida de alguém de cabeça para baixo. E, no entanto, quando essa pessoa reage ao sistema, a evidência compensatória, indicativa do erro, é apenas "sugestiva" e, simplesmente, não funciona.[220]

---

[216] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 9.
[217] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 9.
[218] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 9.
[219] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 10.
[220] O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 10.

Após todo a situação e o choque de sua demissão, Sarah Wysocki ficou sem emprego por apenas alguns dias. Ela tinha muitas pessoas, incluindo seu diretor, para atestá-la como uma boa profissional, e, desse modo, ela prontamente conseguiu um emprego em uma escola em um distrito rico no norte da Virgínia, que não utilizava o IMPACT. Então, graças a um modelo altamente questionável, uma escola em um distrito pobre e com dificuldades perdeu uma boa professora, e uma escola rica, que não demitia pessoas com base nas pontuações de seus alunos, ganhou uma.[221]

A narrativa de O'Neil, é perturbadora sob dois aspectos bastante relevantes: a) a existência de uma situação de injustiça perpetrada pelo Estado; e b) para a qual ninguém era capaz de fornecer uma resposta minimamente aceitável. A questão, que deveria ter sido respondida pela própria Administração, no entanto, acabou por se arrastar e culminou em um prejuízo a um sistema de ensino em um distrito pobre e com dificuldades.

O caso demonstra o potencial nocivo dos algoritmos, em especial sobre populações que já se encontram em certa desvantagem. Como conclui O'Neil[222] o modelo utilizado nas escolas de Washington, DC, que avaliava os professores principalmente com base nas pontuações dos testes dos alunos, ignorava o quanto os professores envolviam os alunos, trabalhavam em habilidades específicas, lidavam com a gestão da sala de aula, ou ajudavam os alunos com problemas pessoais e familiares.

É extremamente simples sacrificar precisão e percepção pela eficiência. Ainda assim, da perspectiva dos administradores, ele fornecia uma ferramenta eficaz para descobrir centenas de professores aparentemente com baixo desempenho, mesmo correndo o risco de interpretar mal alguns deles. Essa situação, segundo a autora, demonstra o ponto essencial desta seção: o fato de que os modelos algorítmicos, apesar de sua reputação de imparcialidade, refletem objetivos e idiossincrasias (ideologias).[223]

Basta um exemplo simples para entender a questão: se, por exemplo, naquele modelo informal de alimentação familiar ali no início da seção, a autora eliminasse a possibilidade de se comer um determinado prato, por considerá-lo não saudável, como a carne vermelha, estaria impondo sua própria ideologia ao modelo alimentar. E isso é algo que as pessoas fazem sem pensar duas vezes, pois, os valores individuais de cada um

[221] O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 9.
[222] O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 20.
[223] O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 20.

influenciam suas escolhas, os dados que escolhem coletar e até as perguntas que buscam fazer. Assim, apesar da aparência de neutralidade: "modelos são opiniões embutidas na matemática".[224]

4.1.2. O caso Kyle Behm

O segundo caso a ser tratado, retratado no livro de Cathy O'Neil refere-se a um jovem chamado Kyle Behm que teve de pedir licença de seus estudos na Universidade de *Vanderbilt* para se tratar de um transtorno bipolar.

Um ano e meio depois, Kyle estava suficientemente saudável para voltar aos estudos. Por volta dessa época, ele soube por um amigo de uma vaga de emprego de meio período na empresa *Kroger*. Era apenas um trabalho de tempo parcial e um salário-mínimo em um supermercado, mas parecia algo certo. Seu amigo, que estava deixando o emprego, poderia atestar sua aptidão para a vaga. Para um aluno de alto desempenho como Kyle, a inscrição parecia uma mera formalidade.[225]

Mas Kyle nunca foi chamado para uma entrevista. Quando ele perguntou, seu amigo explicou que ele havia sido sinalizado ("*red-lighted*") pelo teste de personalidade que havia feito quando se candidatou ao emprego. O teste fazia parte de um sistema automatizado de seleção de funcionários desenvolvido pela *Kronos*, uma empresa que licenciava *softwares* de contratação em diversas lojas. Ao contar a seu pai, Roland, advogado, o que havia acontecido, este lhe questionou que tipo de perguntas haviam aparecido no teste. Kyle disse que elas eram muito parecidas com o teste do "Modelo de Cinco Fatores" que ele recebeu no hospital enquanto estava em tratamento de seu transtorno bipolar. Esse teste classifica as pessoas quanto à extroversão, afabilidade, conscienciosidade, neuroticismo e abertura a ideias.[226]

No início, perder um emprego de meio período e salário-mínimo por causa de um teste questionável não parecia grande coisa. Assim, Roland Behm incentivou seu filho a se inscrever em outros lugares, no entanto, Kyle voltava sempre com as mesmas notícias.

---

[224] O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 20.
[225] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 106.
[226] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 107.

As empresas para as quais ele estava se candidatando estavam usando o mesmo tipo de teste e ele não estava recebendo qualquer oferta.[227]

Kyle, à essa altura, se sentia fracassado. Poucos anos antes havia obtido notas quase perfeitas em seus exames de seleção e ingressado na Universidade de *Vanderbilt*. Agora, não conseguia sequer um emprego de meio período. O jovem, como relatou seu pai, Roland a O'Neil, sentia-se "quebrado". (Na transcrição original da fala – Kyle: "If I can't get a part-time minimum-wage job, how broken am I?". Isto é: "Se não consigo um emprego de meio período e salário-mínimo, quão "quebrado" eu estou?").[228]

Roland, no entanto, não se contentou com a situação. As perguntas sobre saúde mental pareciam estar excluindo seu filho do mercado de trabalho. Ele decidiu investigar e logo descobriu que o uso de testes de personalidade para contratações era bastante comum entre as grandes corporações. E, ainda assim, ele encontrou poucos desafios legais para essa prática. Como ele explica a O'Neil, as pessoas que se candidatam a um emprego e são dispensadas raramente ficam sabendo que foram rejeitadas por causa dos resultados dos testes. Mesmo quando o sabem, não é provável que consigam entrar em contato com um advogado.[229]

Diante da situação Roland decidiu, então, enviar notificações a sete empresas - *Finish Line, Home Depot, Kroger, Lowe's, PetSmart, Walgreen Co. e Yum Brands* - informando-as de sua intenção de ingressar com uma ação coletiva alegando que o uso do exame durante o processo de candidatura a emprego era ilegal, argumentando que o teste da *Kronos* poderia ser considerado um exame médico, cujo uso na contratação seria ilegal de acordo com o *Americans with Disabilities Act (ADA)* de 1990.[230]

Em resposta à notificação, a empresa *PetSmart* explicou que teria adquirido a ferramenta de avaliação de candidatos da empresa *Kronos* no ano de 2005, sendo ela a responsável por seu desenvolvimento e testagem.[231]

---

[227] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 107.
[228]O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 107.
[229] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 107.
[230] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 107.
[231] "A Kronos elaborou as questões de avaliação, realizou todos os testes de validação e ajudou a *PetSmart* a escolher a configuração do teste para cada vaga de contratação". Tradução do autor. No original: "Kronos drafted the assessment questions, conducted all validation testing, and helped PetSmart choose the configuration of tests for each position". TIMMONS, Kelly Cahill. Pre-Employment Personality Tests, Algorithmic Bias, and the Americans with Disabilities Act. **Penn State Law Review**, v. 125, n. 2, winter

Segundo informado pela *PetSmart* a *Kronos* teria calibrado os testes de modo que 50% dos candidatos recebessem "Pontuação Verde", 25% recebessem uma "Pontuação Amarela" e 25% recebessem uma "Pontuação Vermelha". Os testes seriam feitos por meio do computador e os resultados enviados aos gerentes de contratação da *PetSmart* com determinação "Verde", "Amarela" ou "Vermelha" para cada candidato, de acordo com o posto de trabalho a que submetida a aplicação (candidatura). A carta encaminhada, no entanto, acaba por reconhecer que a "*PetSmart* desencorajava a contratação de candidatos que recebessem uma avaliação geral vermelha nos testes da *Kronos*".[232]

A empresa explicou ainda que:

> A *PetSmart* incorporou as avaliações da *Kronos* em seus processos seletivos porque, entre outras coisas, acreditava que as avaliações haviam sido desenvolvidas especificamente como um mecanismo de seleção no contexto empregatício. A *PetSmart* também acreditava que as avaliações não eram derivadas de nenhum exame médico ou de qualquer teste usado anteriormente no contexto médico ou psicológico, e que não foram projetados para diagnosticar quaisquer condições médicas ou psicológicas. Além disso, a PetSmart entendeu que as avaliações nunca foram vendidas ou usadas para fins de diagnóstico de deficiências médicas, deficiências de ordem psicológicas ou similares e que as avaliações atendiam a todos os outros requisitos legais e regulamentares, incluindo sua conformidade com a ADA e a legislação estadual. Em suma, a *PetSmart* acreditava que as avaliações da *Kronos* ajudariam a identificar candidatos com maior probabilidade de serem bem-sucedidos no trabalho e de permanecerem em seus empregos por mais tempo – ambas características diretamente ligadas às necessidades de negócio da *PetSmart*, satisfação do consumidor e sucesso do associado.[233]

2021, p. 389-452, p. 420. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/dlr125&i=405. Acesso em: 28 jan. 2022.

[232] TIMMONS, Kelly Cahill. Pre-Employment Personality Tests, Algorithmic Bias, and the Americans with Disabilities Act. **Penn State Law Review**, v. 125, n. 2, winter 2021, p. 389-452, p. 421. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/dlr125&i=405. Acesso em: 28 jan. 2022.

[233] Tradução do autor. No original: "PetSmart incorporated the Kronos assessments into its job application process because, among other things, it believed that the assessments had been specifically developed as a selection device in the employment context. PetSmart also believed that the assessments were not derived from any medical examinations or tests used previously in the medical or psychological context and were not designed to be diagnostic of any medical or psychological conditions. Further, PetSmart understood that the assessments had never been marketed or used for purposes of diagnosing medical disabilities, psychological impairments, or the like and that the assessments met all other legal and regulatory requirements, including compliance with the ADA and state law. In sum, PetSmart believed that Kronos' [sic] assessments would help it identify applicants who were more likely to demonstrate successful on-the-job behaviors and to remain in their jobs for a longer period of time—both features directly linked to PetSmart's business needs, customer satisfaction, and associate success.". TIMMONS, Kelly Cahill. Pre-Employment Personality Tests, Algorithmic Bias, and the Americans with Disabilities Act. *Penn State Law Review*, vol. 125, n. 2, winter 2021, p. 389-452, p. 421. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/dlr125&i=405. Acesso em: 28 jan. 2022.

A *PetSmart* afirmou, ainda, que não havia evidências de que as avaliações tivessem um impacto desigual sobre os candidatos com deficiência e que desde que começou a usar as avaliações, suas pontuações gerais de satisfação dos clientes aumentaram, enquanto a rotatividade de funcionários em suas lojas diminuiu drasticamente.[234]

As explicações, no entanto, não pareciam encontrar suporte na realidade, especialmente tendo em conta que para todas as empresas usuárias dos sistemas, ainda que atuassem em diferentes áreas de mercado e as aplicações se direcionassem a diferentes postos de trabalho, pressupondo-se diferentes necessidades, permaneciam sinalizando e reprovando Kyle.

Reforça o argumento o fato de que em outra ação judicial,[235] anterior à notificação de Roland e Kyle, a ferramenta desenvolvida pela empresa *Kronos* já teria sido acusada de promover uma análise enviesada, com potencial discriminatório, inclusive, contra outra pessoa com deficiência, tendo as partes entrado em acordo naquele procedimento, de forma que a empresa se comprometeu a revisar e eliminar de seu teste perguntas que pudessem ter o efeito discriminatório alegado.

Analisando o caso, Kelly Timmons, professora associada da Universidade de Geórgia, argumenta que:

> Ele era um jovem inteligente e trabalhador com transtorno bipolar que procurava um emprego de salário-mínimo enquanto frequentava a faculdade, e sete empresas o rejeitaram devido ao seu desempenho em seu teste de personalidade pré-admissional. (...) A *PetSmart* declara que "não vê evidências de que indivíduos com deficiência tenham um desempenho diferente de quaisquer outros indivíduos nas avaliações da *Kronos*", mas o que sabemos do litígio EEOC (Equal Employment Opportunity Commission) v. *Kronos* é que a *Kronos* nunca realizou análise de impacto adverso em relação às pessoas com deficiência. Empregadores como a *PetSmart* deveriam querer saber se os testes de personalidade pré-admissionais que usam tendem a excluir indivíduos com deficiência, de forma que deveriam exigir que os fornecedores desses testes obtivessem esse tipo de informação. Além disso, os fornecedores desses testes estariam mais bem equipados para comercializar seus produtos se pudessem assegurar aos compradores

[234] TIMMONS, Kelly Cahill. Pre-Employment Personality Tests, Algorithmic Bias, and the Americans with Disabilities Act. **Penn State Law Review**, v. 125, n. 2, winter 2021, p. 389-452, p. 421-422. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/dlr125&i=405. Acesso em: 28 jan. 2022.

[235] Veja a seção "C. ADA Challenges to Personalitu Testing" em TIMMONS, Kelly Cahill. Pre-Employment Personality Tests, Algorithmic Bias, and the Americans with Disabilities Act. **Penn State Law Review**, vol. 125, n. 2, winter 2021, p. 389-452, p. 413 e ss. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/dlr125&i=405. Acesso em: 28 jan. 2022.

> que investigaram o impacto de seus produtos em indivíduos com deficiência.
> Estaríamos confiantes em afirma que a baixa pontuação de Kyle no teste de personalidade significa que ele não conseguiria desempenhar com sucesso as funções dos cargos que buscou na *PetSmart* ou em outras empresas? Ou o principal benefício do teste é o fato de oferecer aos empregadores uma maneira rápida e fácil de reduzir o volume de solicitações e candidaturas que deveria considerar?[236]

Considerando toda a situação, Kyle e seu pai apresentaram queixas à EEOC (Equal Employment Opportunity Commission – Comissão de Igualdade de Oportunidades de Emprego) contra todas as sete empresas por violarem o *Americans with Disabilities Act (ADA).*

Ao que tudo indica, o teste, porquanto padronizado e semelhante a uma avaliação psicológica, acabava por impedir o acesso de várias pessoas com alguma doença mental, ainda que sob controle e adequado acompanhamento, ao mercado de trabalho. Importa notar que o transtorno apresentado por Kyle amolda-se perfeitamente ao conceito de deficiência pela Convenção das Nações Unidas sobre os Direitos das Pessoas com Deficiência, na medida em que resulta da interação entre uma incapacidade de longo prazo e as diversas barreiras ambientais (como comportamentais, sociais ou ambientais) que impedem sua participação plena e efetiva na sociedade, em condições de igualdade com os demais indivíduos, veja-se:[237]

> Artigo 1º - Objeto
> 1 - O objeto da presente Convenção é promover, proteger e garantir o pleno e igual gozo de todos os direitos humanos e liberdades fundamentais por todas as pessoas com deficiência e promover o respeito pela sua dignidade inerente.

---

[236] Tradução do autor. No original: "He was a smart, hardworking young man with bipolar disorder looking for a minimum-wage job while attending college, and seven companies rejected him due to his performance on their pre-employment personality test. (...) PetSmart stated that it had "seen no evidence that qualified individuals with disabilities perform differently than others on the Kronos assessments," but we know from the EEOC v. Kronos litigation that Kronos never performed adverse-impact analysis with respect to disability. Employers like PetSmart should want to know if the pre- employment personality tests they use tend to screen out individuals with disabilities, so they should demand that test vendors attempt to obtain this information. Test vendors, moreover, would be better equipped to market their products if they could assure employers that they have investigated the products' impact on individuals with disabilities. Are we confident that Kyle's low score on the personality test meant that he could not successfully perform the duties of the positions he sought at PetSmart or the other companies? Or is a primary benefit of the test the fact that it gives employers a quick and easy way to narrow the volume of applications they must consider?". TIMMONS, Kelly Cahill. Pre-Employment Personality Tests, Algorithmic Bias, and the Americans with Disabilities Act. **Penn State Law Review**, v. 125, n. 2, winter 2021, p. 389-452, p. 438. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/dlr125&i=405. Acesso em: 28 jan. 2022.

[237] CDPC. **Convenção sobre os Direitos das Pessoas com Deficiência e seu Protocolo Facultativo**. Nova York, 2006. Disponível em: http://www.pcdlegal.com.br/convencaoonu/wp-content/themes/convencaoonu/downloads/ONU_Cartilha.pdf. Acesso em: 29 jun. 2022.

> 2 - As pessoas com deficiência incluem aqueles que têm incapacidades duradouras físicas, mentais, intelectuais ou sensoriais, que em interação com várias barreiras podem impedir a sua plena e efetiva participação na sociedade em condições de igualdade com os outros.

Como diagnostica O'Neil:[238]

> Os candidatos a empregos, especialmente aqueles que aplicam para um emprego de salário-mínimo e são rejeitados raramente descobrem o porquê. No caso, foi apenas porque ocorreu de o amigo de Kyle ouvir sobre a razão de sua rejeição e lhe contar que este chegou a saber. Mesmo assim, o caso com a grande empresa Kronos não teria ido a lugar nenhum se o pai de Kyle não fosse um advogado com tempo e dinheiro suficientes para montar um amplo desafio legal à empresa. Isso raramente acontece com candidatos a cargos de baixo nível hierárquico. Finalmente, considere o círculo vicioso que o teste de personalidade da Kronos engendra. Acendendo uma luz vermelha às pessoas com certos problemas de saúde mental acaba por privar esses indivíduos de encontrar um emprego normal, de viver uma vida norma, isolando-os ainda mais. Isso é exatamente o que o Americans with Disabilities Act é suposto prevenir.

Por fim, cabe apontar que Kelly Timmons[239] assinala estar sendo conduzida uma investigação pela Comissão sobre o uso de avaliações de personalidade pré-admissionais por parte da *Kroger* e da *PetSmart*.

Aponta,[240] ainda que Kyle e seu pai teriam negociado acordos com dois dos empregadores. A Lowe's, um dos empregadores do acordo, emitiu um comunicado à imprensa sobre mudanças em seu processo de inscrição *on-line* para funcionários. De acordo com o comunicado, a Lowe's fez uma parceria com o Judge David L. Bazelon Center for Mental Health Law "para modificar o processo de teste *on-line* buscando melhor assegurar que ele não impeça, de forma desnecessária, pessoas com deficiências

---

[238] Tradução do autor. No original: "Job candidates, especially those applying for minimum-wage work, get rejected all the time and rarely find out why. It was just chance that Kyle's friend happened to hear about the reason for his rejection and told him about it. Even then, the case against the big Kronos users would likely have gone nowhere if Kyle's father hadn't been a lawyer, one with enough time and money to mount a broad legal challenge. This is rarely the case for low-level job applicants. * Finally, consider the feedback loop that the Kronos personality test engenders. Red-lighting people with certain mental health issues prevents them from having a normal job and leading a normal life, further isolating them. This is exactly what the Americans with Disabilities Act is supposed to prevent". O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 112.

[239] TIMMONS, Kelly Cahill. Pre-Employment Personality Tests, Algorithmic Bias, and the Americans with Disabilities Act. *Penn State Law Review*, vol. 125, n. 2, winter 2021, p. 389-452, p. 422. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/dlr125&i=405. Acesso em: 28 jan. 2022.

[240] TIMMONS, Kelly Cahill. Pre-Employment Personality Tests, Algorithmic Bias, and the Americans with Disabilities Act. *Penn State Law Review*, vol. 125, n. 2, winter 2021, p. 389-452, p. 422. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/dlr125&i=405. Acesso em: 28 jan. 2022.

(especialmente as relacionadas à saúde mental) de encontrarem empregos e ofertar valiosas contribuições para sua força de trabalho". [241]

No entanto, infelizmente, a história de Kyle Behm teve um final trágico. Em 27 de agosto de 2019,[242] ele perdeu a batalha que travava desde o segundo de faculdade contra a bipolaridade, tirando sua própria vida aos 29 anos de idade. A história Kyle é referida no documentário "Persona: The Dark Truth Behind Personality Tests".

4.1.3. Perfilização, acesso ao crédito e feedback looping

Os dois primeiros casos narrados dão uma boa dimensão sobre os efeitos perversos que algoritmos podem trazer à vida das pessoas. Ambos os casos se valem de acontecimentos na vida de pessoas reais (Sarah Wysocki e Kyle Behm) para fornecerem as razões substanciais de iniquidade dos modelos criados. Essas narrativas pessoalizam a problemática, permitindo compreender que por trás das máquinas e algoritmos encontram-se pessoas reais, por eles impactadas.

Em contraposição, neste terceiro tópico, os casos retratados abordarão situações em que todo um grupo de pessoas é afetado, na medida em que esses indivíduos não são mais vistos como tais, mas como parte de um grupo que os define, quer concordem ou não; quer se comportem como a maioria ou não. É o que conveniou-se chamar de *profiling* ou perfilização.

O termo *profiling* ou perfilização[243] emergiu de uma conhecida prática anglo-saxônica, o *psychological profiling*, que consiste na criação de um perfil psicológico de um indivíduo, em especial, para fins de política criminal. A técnica se popularizou, sobretudo, a partir de um grande número de séries e filmes investigativos, sobretudo

[241] Tradução do autor. No original: "to modify the online testing process to better ensure it does not unnecessarily prevent people with mental health disabilities from finding jobs and making valuable contributions to the workforce". TIMMONS, Kelly Cahill. Pre-Employment Personality Tests, Algorithmic Bias, and the Americans with Disabilities Act. *Penn State Law Review*, vol. 125, n. 2, winter 2021, p. 389-452, p. 422. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/dlr125&i=405. Acesso em: 28 jan. 2022.

[242] Conforme informações obtidas no aviso disponibilizado na página do crematório de Geórgia. Disponível em: https://www.csog.com/obit/kyle-lawton-behm/. Acesso em: 02 fev. 2021.

[243] Na tradução aqui adotada, também visível em: ZANATTA, Rafael Augusto Ferreira. **Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais**. 2018. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais/download. Acesso em: 15 jun. 2019. Zanatta, t

estadunidenses, nas quais o perfil psicológico de assassinos em série são traçados na busca de tentar prever o comportamento delitivo desses indivíduos.

Para melhor entender as origens do *psychological profiling*, Ronald N. Turco faz um breve retrospecto sobre a técnica, relacionando alguns dos trabalhos precursores da técnica. Veja-se: [244]

> O desenvolvimento de perfis psicológicos e a compreensão do comportamento de indivíduos data de tempos antigos. O homem sempre esteve interessado em entender seus adversários, competidores e, até mesmo, seus amigos. O pioneiro trabalho de Freud no desenvolvimento da psicanálise [New Introductory Lectures on Psycho-Analysis] proveu uma estrutura geral para o estudo e predição do comportamento humano (Freud, 1933).
> Como consequência direta desse trabalho o autor dedicou-se ao desenvolvimento de uma compreensão psicológica ou "perfil" de Woodrow Wilson, o 20º presidente dos Estados Unidos. Freud nunca conheceu Wilson, mas colaborou com Bullitt, ex-diplomata dos Estados Unidos. Bullitt trabalhou para Wilson e acreditava que detinha informações suficientes para a condução de um estudo sobre o ex-presidente. O rascunho final da obra foi preparado em 1939, ano da morte de Freud. O livro resultante do trabalho foi publicado em 1967 e não foi muito bem recebido (Freud and Bullitt, 1967). Houve

[244] Tradução do autor. No original: "The development of psychological profiles and an understanding of individuals dates to ancient times. Man has always been interested in understanding his adversaries, competitors and even his friends. The pioneering work of Freud in developing psychoanalysis provided a framework for study and for predic- tion of human behavior (Freud, 1933). One direct outgrowth of this work was the development of a psychological understanding or "profile" of Woodrow Wilson, the 20th president of the United States. Freud never met Wilson yet he collaborated with Bullitt, a former U.S. diplomat. Bullitt worked for Wilson and believed that he had sufficient information to assemble for a study of Wilson. The final draft was prepared in 1939, the year of Freud's death. The book was published in 1967 and was not well received (Freud and Bullitt, 1967). There was considerable criticism about the manner of the study and even that such an exercise would be undertaken (Tuchman, 1967). The development of a psychological profile of a public figure that met with more acceptance was prepared by Langer (1972). The Office of Strategic Services during World War II asked Langer to prepare a profile of Adolph Hitler. Langer, a psychoanalyst, was eager to take on this task. Among Langer's most significant successes was his prediction of Hitler's death. Langer predicted Hitler's death as a suicide, in addition to the nature and the circumstances in which Hitler would turn his aggression upon the German people. Langer was remarkably accurate. His profile was classified "top secret" for many years. It was finally published in 1972 (Langer, 1972; Bromberg, 1974). Laswell's (1960) detailed studies ushered in an era of more sophisticated psychobiography of historical figures and their psychopathology. A practical application of Laswell's work was discussed by Wedge (Wedge, 1968). Wedge prepared a psychological profile for President Kennedy's Vienna Summit Meet- ing in 1961 with Kruschev. This included information on "how to" negotiate with the Soviet leader as well as some interpretations and some predictions of his behavior. Post (1973; 1983) studied the effects of the aging process on leadership and developed a sophisticated method of studying terrorists. He has provided valuable insight into the conscious and the unconscious patterns of thinking and emotions of terrorists. Post postulated ideas regarding terrorist's political affiliations and motivations. [...]. Clutterbuck (1976) was another individual who studied terrorism and brought scholarship, military experience, political shrewdness and direct "hands on" experience to the study of terrorist's profiles. He taught at the University of Exeter in Devon, England where his reputation earned him the title "the terrorismman.". TURCO, Ronald N. Psychological Profiling. **International Journal of Offender Therapy and Comparative Criminology**, vol. 34, n. 2, September 1990, p. 147-154. HeinOnline, Disponível em: https://heinonline.org/HOL/P?h=hein.journals/ijotcc34&i=152. Acesso em: 10 fev. 2022.

> consideráveis críticas sobre a forma como o estudo foi conduzido e, até mesmo, sobre a realização dessa espécie de estudo (Tuchman, 1967).
> O desenvolvimento de um perfil psicológico de uma autoridade pública que encontrou maior aceitação foi elaborado por Langer (1972). O Escritório de Serviços Estratégicos durante a Segunda Guerra Mundial pediu a Langer que preparasse um perfil de Adolph Hitler. Langer, um psicanalista, estava ansioso para assumir a tarefa. Entre os sucessos mais significantes de Langer esteve a predição da morte de Hitler. Langer previu a morte de Hitler como suicídio, além da natureza e das circunstâncias em que Hitler voltaria sua agressão contra o povo alemão. Langer foi notavelmente preciso. O perfil por ele realizado foi classificado como "ultrassecreto" por muitos anos. Em 1972, foi, finalmente, publicado (Langer, 1972; Bromberg, 1974).
> Os estudos detalhados de Laswell (1960) deram início a uma era de psicobiografia mais sofisticadas de figuras históricas e suas psicopatologias. Uma aplicação prática do trabalho de Laswell foi discutida por Wedge (Wedge, 1968). Wedge preparou um perfil psicológico para a Reunião de Cúpula do Presidente Kennedy em Viena, em 1961, com Kruschev. Esse estudo incluiu informações sobre como negociar com o líder soviético, bem como certas interpretações e algumas previsões de seu comportamento. Post (1973; 1983), por sua vez, estudou os efeitos do processo de envelhecimento de lideranças e desenvolveu um método sofisticado de estudo de terroristas. Ele forneceu informações valiosas sobre os padrões conscientes e inconscientes de pensamento e emoções dos terroristas. Ele apresentou ainda ideias sobre afiliações políticas e motivações dos terroristas. (...)
> Por fim, Clutterbuck (1976) foi outro autor que estudou terrorismo e trouxe erudição, experiência militar, astúcia política e experiência direta de campo para o estudo dos perfis dos terroristas. Ele lecionou na Universidade de Exeter em Devon, Inglaterra, onde sua reputação lhe rendeu o título de "o homem terrorista".

O exame do autor demonstra uma evolução das técnicas de análise comportamental e de perfilhamento de certos indivíduos sob o interesse do Estado. Os trabalhos, como visto, tinham um eminentemente caráter político-estratégico, embora, mais tarde, a técnica tenha se popularizado na investigação criminal, no enfrentamento ao terrorismo e na persecução criminal de assassinos em série.

Conquanto o *psychological profiling* e a noção de perfilização que aqui se desenvolvem tenham bases comuns, é necessário entender como esse tipo de técnica acabou por se espraiar da psicologia, política e investigação criminal para uma centena de aplicações corriqueiras, como a busca por crédito bancário em nossa sociedade.

Busca-se, a seguir, avaliar a interseção entre o *psychological profiling* e as técnicas de análise de dados.

Nesse passo, um dos primeiros estudos a tratar do *profiling* como técnica incorporada às Tecnologias da Informação e Comunicação é o artigo de Nancy Reichman:

"*Computer Matching: Toward Computerized Systems of Regulation*",[245] de 1987.[246] O ensaio de Reichman fornece uma visão geral sobre o "*computer matching*", ou, em tradução direta: a correspondência computacional, identificando-a como uma das novas formas de controle social gerada por meios informáticos.[247]

O trabalho de Nancy Reichman fornece indício de que o controle e a vigilância deixariam de ser exercidos apenas no berço do Estado, para se tornarem difusos e onipresentes na sociedade da informação. As técnicas por ela analisadas, àquela altura, já eram aplicadas a diferentes áreas da vida, como a segurança social ou a análise de seguros. Assim, remete-se à algumas das lições da autora para entender a técnica do *profiling* e como era aplicada há mais de quatro décadas: [248]

---

[245] Este artigo examina a correspondência computacional, uma das muitas novas tecnologias que estão mudando os contornos da atividade regulatória. Uma de suas formas envolve a comparação direta de variáveis em duas ou mais bases de dados distintas. Ela é usada para cruzar, verificar e filtrar as informações encontradas nessas bases de dados. Outra forma dessa técnica envolve a criação de perfis de prováveis infratores e ofensas. Para isso, distintos itens de dados são correlacionados para avaliar o quão perto uma pessoa ou evento chega de um modelo predeterminado relacionado à infração; à quebra de uma regra. Ambas as formas de correspondência computacional permitem a regulação separada e em particular de atores e eventos. Embora a correspondência ocorra em muitos contextos regulatórios, este artigo se concentra especificamente na tendência geral e na dinâmica da correspondência de computadores em programas governamentais. Faz parte de um projeto maior que examina o impacto da tecnologia nas políticas e processos de controle social (Marx e Reichman, 1984; Reichman e Marx, 1985). Tradução do Autor. No original: "This paper examines computer matching, one of the many new techno- logies that are changing the contours of regulatory activity. One form of matching involves the direct computerized comparison of variables in two or more distinct data bases. It is used to cross-check, verify and screen information found in those data bases. Another form of computerized data matching involves the profiling of likely offenders and offenses. Distinct data items are correlated in order to assess how close a person or event comes to a predetermined model of rule breaking. Both forms of computer matching permit regulation divorced from particular actors and events. Although matching occurs in many regulatory contexts, this paper focuses specifically on the general trend toward and dynamics of computer matching in government programs. It is part of a larger project examining the impact of technology on the policies and processes of social control (Marx and Reichman, 1984; Reichman and Marx, 1985)". REICHMAN, Nancy. Computer Matching: Toward Computerized Systems of Regulation. **Law & Policy**. vol. 9, n. 4, October 1987, p. 387-416. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/lawpol9&i=397. Acesso em: 19 fev. 2022.

[246] Há referências, também em: RULE, James B. **Private Lives and Public** Surveillance: Social Control in the Computer Age. New York: Schocken Books, 1974, nas quais o autor descreve técnicas de vigilância que se amoldam à perfilização, mas, ainda, sem assim caracterizá-las. Entretanto, esta parece ser a mais antiga referência sobre o assunto, ainda que indireta, valendo a sua menção.

[247] Discutem-se os desenvolvimentos administrativos e legislativos que incentivam o uso desta técnica. Os trade-offs entre o aumento da eficácia e eficiência regulatória, por um lado, e os direitos dos indivíduos, por outro, são discutidos.

[248] Tradução do autor. No original: "Profiling, a more sophisticated type of matching, has been used to locate potential violators and violations when regulators have some general knowledge about the characteristics of offending behavior but no precise information about who the violators are. Profiles can be used to seek them out. The Social Security Administration, for example, has developed computer profiles based on characteristics such as the claimant's age, type of injury, and magnitude of claim to identify fraud-prone claimants in their Disability Program. On the basis of similarity to those profiles disability payments have been discontinued, in some cases even before any human contact was established with the alleged defrauder (US Senate Committee on Governmental Affairs, 1982; 17). To locate persons who fail to file tax returns or under-report their income, the IRS recently purchased lists that market research firms use to target consumers. The lists contain household names and estimates of their income. They are compiled

A criação de perfis, um tipo mais sofisticado de correspondência computacional, tem sido usada para localizar potenciais infratores e potenciais violações quando os agentes reguladores têm algum conhecimento geral sobre as características do comportamento ofensivo, mas nenhuma informação precisa sobre quem são os infratores. Os perfis podem ser usados para procurá-los. A Administração do Seguro Social, por exemplo, desenvolveu perfis de computador com base em características como idade do reclamante, tipo de lesão e magnitude das queixas para identificar reclamantes propensos a fraudes em seu programa relacionado à deficiência. Com base na semelhança com esses perfis os pagamentos por invalidez foram descontinuados, em alguns casos, mesmo antes de qualquer contato humano ser estabelecido com o suposto fraudador (US Senate Committee on Governmental Affairs, 1982; 17). Para localizar pessoas que não apresentam declarações de impostos ou que não declaram seus rendimentos, o IRS comprou recentemente listas que as empresas de pesquisa de mercado usam para atingir consumidores. As listas contêm nomes de famílias e estimativas de sua renda. Elas são compiladas a partir de dados públicos (como registros telefônicos e de serviços

---

from public data (telephone and utility records, applications for motor vehicle licenses, aggregate Census data and the like). The IRS is matching the commercially compiled estimated household income lists with lists of taxpayers to identify those individuals who may have failed to file income tax returns. Commissioner Egger reported to Congress that the Internal Revenue Service is seeking only information needed to determine whether there was an obligation to file. Consequently, estimated annual income is of primary importance. But other information, such as age and the number of people in the household may also be looked at because these factors affect filing requirement (as quoted in Baker, et al., 1985; 2). Profiles have been used preventively as well. The Federal Insurance Adminstration uses computerized profiles developed by Arson Early Warning Systems to cancel insurance on inner city properties with high risk of arson. The logic here is that by canceling the insurance you negate at least one of the profit motives for the crime. Cancellation criteria are based on a profile identified as being a significant indicator of arson. Variables of interest include among others: unpaid taxes, code violations, vacancy rates, and previous fires at site (Insurance Committee for Arson Control, Fact Sheet # 13; 1981). The U.S. Drug Enforcement Agency is one of a number of federal, state and local agencies that participated in the Prescription Abuse Data Synthesis Project (PADS) sponsored by the American Medical Association. PADS is a copyrighted data analysis model which combines the records of drug manufacturers and distributors, state medicaid, health, and vital statistics records with drug enforcement records to ". . .define the nature, extent and source of prescription drug abuse and diversion within the state and to provide a basis for developing programs and strategies to curtail these problems" (Colorado Department of Health, 1985). One outcome of this combination of records is the ability to target potential problem pharmacies and physicians overprescribing and diverting con- trolled substances from their intended use. Computer profiling also is being used to scan the marketplace for evidence of illegal activity. The Departments of Transportation and Justice use profiling to identify highway construction contract bid-rigging. Certain indicators present in the bidding process suggest a strong possibility of illegal activity and investigation into the contract process automatically begins. The indicators derived from current and previous bids include: ... (1) certain bidders who do not bid against each other; (2)the bid winner repeatedly subcontracts work to firms who bid higher; (3) a particular contractor always wins in certain geographical areas; (4) certain contractors who bid frequently but never win; (5) identical bids are made for particular contract items (PCIE, 1983; 25). (...) These diverse examples demonstrate the range of uses to which computer matching may be put. They also serve to illustrate the potential reach of this technique. Anyone who has filed a tax return, received veterans benefits, or participated either as a beneficiary or contractor in a social welfare program has been subject to some form of computerized record matching. Although it will not be discussed here, record matching is flourishing in the private sector as well. Insurance companies, credit companies, banks, mass marketing firms, as well as other private enterprises maintain systems of records to monitor the behavior of clients or potential clients. REICHMAN, Nancy. Computer Matching: Toward Computerized Systems of Regulation. **Law & Policy**. vol. 9, n. 4, October 1987, p. 387-416. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/lawpol9&i=397. Acesso em: 19 fev. 2022.

públicos, solicitações de licenças de veículos automotores, dados agregados do Censo e informações similares). O IRS está comparando as listas compiladas de renda familiar estimada com as listas de contribuintes para identificar aqueles indivíduos que podem ter deixado de apresentar declarações de imposto de renda. O Comissário Egger informou ao Congresso que o Internal Revenue Service (Receita Federal) está "... buscando apenas as informações necessárias para determinar se haveria a obrigação do contribuinte declarar renda ao fisco. Consequentemente, a renda anual estimada é de primordial importância. Mas outras informações, como idade e número de pessoas no domicílio também podem ser observadas porque esses fatores afetam a exigência de declaração à Autoridade Fiscal" (como citado em Baker, et al., 1985; 2).

Os perfis também têm sido usados preventivamente. A Administração Federal de Seguros usa perfis computadorizados desenvolvidos pela Arson Early Warning Systems para cancelar o seguro em propriedades no centro da cidade com alto risco de incêndio criminoso. A lógica aqui é que ao cancelar o seguro você evita pelo menos um dos principais motivos para o crime. Os critérios de cancelamento são baseados em um perfil indicativo de significativas chances de ocorrência de um incêndio criminoso. As variáveis de interesse incluem, entre outras: impostos não pagos, violações à lei, taxas de desocupação e incêndios anteriores no local (Comitê de Seguros para Controle de Incêndios, Fact Sheet 13; 1981). A Agência Antidrogas dos EUA é uma das várias agências federais, estaduais e locais que participaram do Projeto de Síntese de Dados de Abuso de Prescrição (PADS) patrocinado pela Associação Médica Americana. O PADS é um modelo de análise de dados protegido por direitos autorais que combina os registros de fabricantes e distribuidores de medicamentos, da assistência médica estatal, de registros de saúde e de estatísticas vitais em registros de ações de repressão às drogas com a finalidade de "... definir a natureza, extensão e fonte do abuso e desvio de medicamentos prescritos dentro do Estado, além de fornecer uma base para o desenvolvimento de programas e estratégias para reduzir esses problemas" (Departamento de Saúde do Colorado, 1985). Um dos produtos dessa combinação de registros é a capacidade de sinalizar farmácias potencialmente problemáticas e médicos que prescrevem medicamentos em excesso ou desviam as substâncias controladas de seu uso pretendido.

A criação de perfis de computador também está sendo usada para verificar o mercado em busca de evidências de atividades ilegais. Os Departamentos de Transporte e Justiça usam perfis para identificar fraudes em contratos de construção de rodovias. Certos indicadores presentes no processo licitatório sugerem uma forte possibilidade de atividade ilegal e a apuração do processo de contratação automaticamente tem início. Os indicadores derivados de licitações atuais e anteriores incluem: "... (1) determinados licitantes que não concorrem entre si; (2) o vencedor da licitação subcontrata repetidamente o trabalho para empresas que oferecem propostas mais altas; (3) um determinado contratante sempre vence em determinadas áreas geográficas; (4) certos empreiteiros que licitam com frequência, mas nunca vencem; (5) licitações idênticas são feitas para determinados itens do contrato" (PCIE, 1983; 25). (...)

Esses diversos exemplos demonstram a variedade de usos para os quais a correspondência computacional pode ser colocada. Servem, também, para ilustrar o alcance potencial desta técnica. Qualquer pessoa que

> tenha apresentado uma declaração de imposto de renda, recebido benefícios de veteranos ou participado como beneficiário ou contratado de um programa de bem-estar social está sujeito a alguma forma de comparação de registros computadorizados. Embora não seja discutido aqui, a correspondência de registros também está florescendo no setor privado. Seguradoras, empresas de crédito, bancos, empresas massivas de marketing, bem como outras empresas privadas, mantêm sistemas de registros para monitorar o comportamento de clientes ou clientes em potencial.

A contribuição de Reichman é bastante interessante para se perceber que já no século passado a perfilização era praticada, prevendo-se que se espalhasse como, de fato, veio a ocorrer.

Não obstante, apesar de retratar uma das primeiras referências na literatura sobre o *prolifing*, foi a obra de Roger Clark, "*Profiling: A Hidden Challenge to the Regulation of Data Surveillance*", que, de fato, buscou tratar do assunto com minucia.

Datado de 1993, seis anos depois do ensaio de Reichman, Clark identifica a perfilização como uma técnica de vigilância, o que poderia explicar, de certo modo, como um mecanismo de política externa e criminal veio a ser utilizado em larga escala na vida moderna. Tal assertiva dialoga com a ideia de um "capitalismo de vigilância", cunhada por Shoshana Zuboff, que vê na previsão e monitoramento dos comportamentos de usuários e consumidores a matéria-prima ou lubrificante para o funcionamento das engrenagens do hodierno sistema de acúmulo de capital.

A ideia central é que o controle do mercado e de maiores parcelas do lucro vêm àqueles que detêm melhores informações estratégicas, seja para agir atempadamente no mercado, seja para conhecer melhor seus consumidores e hábitos de consumo; ou, ainda, para lidar com competidores. E seriam justamente essas as razões, ainda que aplicadas ao campo da política, que conduziram aos primeiros estudos sobre a perfilização no campo da psicologia.

Nota-se que, na nas raízes dessas técnicas, encontra-se uma essência ligada à vigilância e ao controle social, há muito diagnosticada por Reichman e Clarke.

Com efeito, o ensaio de Clarke, é, de fato, o pioneiro a tratar de modo claro e profundo do conceito. Seu trabalho tinha o escopo de definir e descrever a perfilização; avaliar suas implicações sociais; e estabelecer a necessidade de regulamentação do seu uso.

Clarke procura analisar o conceito sob as perspectivas pública e privada, traçando uma definição que pudesse ser aplicada nos dois campos. Assim, para o autor, *profiling* consiste em:

> "uma técnica pela qual um conjunto de características de uma classe particular de pessoas é inferida, a partir de experiências passadas, e os acervos de dados são então pesquisados por indivíduos com um ajuste próximo a esse conjunto de características".[249]

Um perfil, como aponta o ensaio, nada mais é que uma "representação esquemática de certos interesses e padrões comportamentais".[250] Esse perfil pode dizer respeito a uma pessoa em particular (como no caso de perfis psicológicos), ou a um grupo de pessoas, das quais se espera um determinado comportamento, em um determinado contexto (o perfil comportamental de adolescentes, por exemplo).

Clarke aponta que as etapas no processo de criação de perfil podem ser resumidas da seguinte forma:

> - **descrever a classe de pessoas** (...)
> - **usar a experiência existente para definir um perfil dessa classe de pessoas**. É provável que isso se baseie, pelo menos em parte, em conhecimento informal, referências à literatura de disciplinas e profissões subjacentes, além de discussões dentro da organização e com funcionários de outras organizações com interesses semelhantes.
> (...)
> - **expressar o perfil formalmente**, talvez incluindo o uso de ponderações para refletir o grau de correlação entre a característica e o alvo, limites abaixo dos quais a correlação é baixa e acima dos quais é alta, além de relações condicionais complexas entre os fatores (por exemplo, o fator x é indicativo, mas apenas se os fatores y e z estiverem ambos acima dos níveis de limiar particulares);
> - **adquirir dados relativos à população relevante**; por exemplo:
> - no caso de clientes: a base de dados de clientes da organização e as bases de dados dos fornecedores (como listas de endereços);
> - no caso dos trabalhadores: a base de dados de pessoal e os registos das empresas de colocação de pessoal;

[249] Tradução do autor. No original: "Profiling is a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data- holdings are then searched for individuals with a close fit to that set of characteristics.". CLARKE, Roger. Profiling: A Hidden Challenge to the Regulation of Data Surveillance. **Journal of Law and Information Science**, vol. 4, no. 2, 1993, p. 403-419. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/jlinfos4&i=405. Acesso em: 19 fev. 2022.

[250] Tradução livre e adaptada. No original: "The sense in which the term 'profile' is used in this paper is "... [the] schematic representation of [a] person's interests for use in information retrieval" (Concise Oxford, 1976, p.885). The term 'profiling' refers to the process of creating and using such a profile.". CLARKE, Roger. Profiling: A Hidden Challenge to the Regulation of Data Surveillance. **Journal of Law and Information Science**, vol. 4, no. 2, 1993, p. 403-419. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/jlinfos4&i=405. Acesso em: 19 fev. 2022.

- no caso de propensões dos alunos nas artes e no esporte: escola, clube e talvez registros médicos;
- no caso de pacientes: prontuários médicos, registros de clínicas, registros de hospitais e informações de histórico familiar de uma localidade, por exemplo, de Utah;
- nos casos de potenciais criminosos e de perfis de adolescentes: registros escolares, bancos de dados de agências de assistência social e registros médicos e psiquiátricos de médicos, clínicas e hospitais;
- no caso de contribuintes: o histórico de declarações fiscais, informação de fluxos de caixa de empregadores, instituições financeiras e outras organizações, além de análises estatísticas dessas e outras bases de dados;
- no caso de viajantes: registos de voos de ida e de volta e de movimentos de viagem; e
- no caso de ativistas clandestinos: associações com dissidentes conhecidos e listas de assinaturas de literatura subversiva;

- **pesquisar os dados de indivíduos cujas características estejam de acordo com o perfil**. É altamente provável que isso envolva suporte computacional, especialmente quando o conjunto de dados é grande (por exemplo, contribuintes), complexo de processamento (por exemplo, análises psicossociais) ou o tempo disponível é curto (por exemplo, listas de passageiros de aeronaves);
- **agir em relação a esses indivíduos**; por exemplo:
  - enviar publicidade selecionada para clientes selecionados ou perspectivas;
  - convocar estudantes, funcionários ou futuros nomeados para entrevista;
  - aconselhar pacientes ou estudantes e/ou seus pais e professores;
  - aconselhar adolescentes e potenciais criminosos violentos e suas famílias, associados e colegas de trabalho;
  - sujeitar os contribuintes a auditoria;
  - entrevistar passageiros e/ou revistar bagagens e corpos; e
  - impor medidas repressivas ao ativista identificado.[251]

[251] Tradução do autor. No original: "**describe the class of person**, (...); **use existing experience to define a profile of that class of person**. This is likely to be based at least in part on informal knowledge, references to the literature of underlying disciplines and professions, and discussions within the organisation and with staff of other organisations with similar interests. (...) **express the profile formally**, perhaps including the use of weightings to reflect the degree of correlation between the characteristic and the target, thresholds below which the correlation is low and above which it is high, and complex conditional relationships among the factors (e.g. factor x is indicative, but only if factors y and z are both above particular threshold levels); **acquire data concerning a relevant population**; for example: - in the case of customers: the organisation's customer database, and the databases of mailing list suppliers; - in the case of employees: the personnel database, and the records of staff placement companies; - in the case of students' propensities in the arts and sport: school, club and perhaps medical records; - in the case of patients: medical records from doctors, clinics, hospitals and registries, and family history information, e.g. from Utah; - in the cases of potential criminals and of adolescents: school records, welfare agency databases, and the medical and psychiatric records of doctors, clinics and hospitals; - in the case of taxpayers: the historical record of tax returns, cash flow information from employers, financial institutions and other organisations, and statistical analyses of those and other databases; - in the case of travellers: inbound and outbound flight and voyage movement records; and - in the case of underground activists: associations with known dissidents, and subscription lists to subversive literature; **search the data for individuals whose characteristics comply with the profile**. This is highly likely to involve computer support, especially where the data-set is large (e.g. taxpayers), the processing complex (e.g. psycho-social analyses), or the time available short (e.g. lists of aircraft passengers); **take action** in relation to those individuals; for example: - mail selected advertising to selected customers or prospects; - call students, employees or prospective appointees for interview; -

É a partir da inferência entre os padrões estabelecidos em um certo perfil que os indivíduos são classificados como a ele pertencentes ou não, assumindo-se um determinado resultado pré-ordenado com grande probabilidade de ocorrência, como a inadimplência, por exemplo.

Essa, aliás, é uma das principais aplicações das técnicas de perfilização, como se sentirá nas próximas linhas, a partir da descrição de O'Neil,[252] sobre o acesso ao crédito bancário. Para tanto, a autora[253] inicia com uma breve regressão para ilustrar como eram feitas as análises de crédito, dependentes de um sem número de critérios subjetivos, conforme se verá:

> Se você quisesse um carro novo ou uma hipoteca, você colocaria sua melhor roupa e faria uma visita ao banqueiro. E como membro da sua comunidade esse banqueiro provavelmente saberia diversos detalhes da sua vida. Ele saberia sobre suas idas à igreja, ou a falta delas. Saberia todas as histórias sobre os desentendimentos do seu irmão mais velho com a lei. Saberia o que seu chefe (e amigo dele de golfe) pensa sobre você como trabalhador. Saberia, naturalmente, a sua raça e grupo étnico, e, ainda, daria uma checada nos números em seu formulário de aplicação.
> Os quatro primeiros fatores, em geral, acabam por encontrar, conscientemente ou não, um caminho até a ponderação feita pelo banqueiro. E há boas chances de que ele seja mais propenso a confiar em pessoas de seus próprios círculos. Isso é da natureza humana. Mas também significava que para milhões de americanos o *status quo* pré-digital era tão terrível quanto alguns [dos algoritmos atuais] (...). Forasteiros, inclusive minorias e mulheres, eram rotineiramente excluídos do acesso ao crédito. Eles teriam que montar um impressionante orçamento ou carteira – e, ainda, buscar por banqueiros de mente aberta caso necessitassem de um empréstimo. Simplesmente não era justo. Foi, então, que surgiu um algoritmo, e as coisas melhoraram.[254]

---

counsel patients or students and/or their parents and teachers; - counsel adolescents and potential violent criminals, and their families, associates and workmates; - subject tax-payers to audit; - interview passengers and/or conduct luggage- and body- searches; and - impose repressive measures on the activist. CLARKE, Roger. Profiling: A Hidden Challenge to the Regulation of Data Surveillance. **Journal of Law and Information Science**, vol. 4, no. 2, 1993, p. 403-419. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/jlinfos4&i=405. Acesso em: 19 fev. 2022.

[252] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 168.

[253] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 168-169.

[254] Tradução do autor. No original: "If you wanted a new car or a mortgage, you'd put on your Sunday best and pay a visit. And as a member of your community, this banker would probably know the following details about your life. He'd know about your churchgoing habits, or lack of them. He'd know all the stories about your older brother's run-ins with the law. He'd know what your boss (and his golfing buddy) said about you as a worker. Naturally, he'd know your race and ethnic group, and he'd also glance at the numbers on your application form. The first four factors often worked their way, consciously or not, into the banker's judgment. And there's a good chance he was more likely to trust people from his own circles. This was only

O algoritmo mencionado por O'Neil[255], chamado "FICO", foi desenvolvido pelo matemático Earl Isaac e pelo engenheiro Bill Fair com a finalidade de avaliar o risco que um indivíduo teria de se tornar inadimplente em um empréstimo.

O modelo, baseado em uma pontuação, era alimentado a partir de uma fórmula que analisava exclusivamente as finanças do mutuário (principalmente sua carga de dívidas e suas contas) e seus registros de pagamentos. A pontuação, por óbvio, não levava em consideração a cor de pele do indivíduo nem outros aspectos étnicos-sociais. E isso, nas palavras da autora, "acabou sendo ótimo para o setor bancário na medida em que previu o risco com muito mais precisão e abriu as portas para milhões de novos clientes". [256].

O modelo ainda hoje é usado por agências de crédito como a *Experian*, a *Transunion* e a *Equifax*, cada uma, no entanto, contribuindo com fontes diferentes de informações para chegar a suas próprias avaliações.

A autora ressalta[257] que embora essas pontuações tenham muitos atributos louváveis, como o fato de poderem ser ajustadas para torná-las mais precisas;[258] serem relativamente transparentes;[259] e de fazerem parte de uma indústria regulamentada nos Estados Unidos,[260] fato é que seu uso se proliferou descontroladamente. Hoje, segundo O'Neil "estamos cercados de todas as maneiras concebíveis por estatísticas e pela

human. But it meant that for millions of Americans the predigital status quo was just as awful as some of the WMDs I've been describing. Outsiders, including minorities and women, were routinely locked out. They had to put together an impressive financial portfolio - and then hunt for open-minded bankers. It just wasn't fair. And then along came an algorithm, and things improved.". O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 16-169.

[255] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 168-169.

[256] Tradução do autor. No original: "And it turned out to be great for the banking industry, because it predicted risk far more accurately while opening the door to millions of new customers". O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 168-169.

[257] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 169.

[258] Se mutuários com pontuações altas se mostrarem inadimplentes em empréstimos com mais frequência do que o modelo poderia prever, a FICO e as agências de crédito podem ajustar a precisão desses modelos.

[259] O sítio eletrônico da empresa FICO na internet, por exemplo, oferece simples instruções sobre como melhorar sua pontuação: reduzir dívidas, pagar em dia suas contas, diminuir os pedidos de novos cartões de crédito etc.

[260] Se qualquer pessoa tiver dúvidas sobre sua pontuação nos EUA, ela tem o direito legal de solicitar seu relatório de crédito, que inclui todas as informações que vão para a pontuação, como seu registro de hipoteca e pagamentos, sua dívida total e a porcentagem de crédito disponível que ela está usando. Embora o processo possa ser bastante lento, como aponta O'Neil, se alguém encontrar erros, pode corrigi-los.

matemática, em uma colcha de retalhos formada por dados que abrangem desde nossos códigos postais a registros de navegação na Internet e compras recentes". [261]

Muitos desses modelos "pseudocientíficos", como intitulados pela autora, tentam prever a credibilidade de um indivíduo, dando-lhe os chamados scores. Esses números, que raramente são vistos, abrem portas para alguns enquanto as fecham para outros. E, ao contrário das pontuações do "FICO" com as quais se assemelham, elas são arbitrárias, inexplicáveis, não regulamentadas e muitas vezes injustas, conforme pondera.[262]

Para entender melhor o panorama, alguns exemplos são dados por O'Neil.[263] O primeiro é de uma empresa na Virgínia, nos Estados Unidos da América chamada *Neustar*. A *Neustar* oferecia serviços de segmentação de clientes para outras empresas, incluindo um serviço que ajudava a gerenciar o tráfego de *call centers*.

Essa tecnologia permitia classificar, em uma espécie de hierarquia, as ligações recebidas, a partir dos dados disponíveis sobre os respectivos chamadores. Os que estivessem no topo eram considerados mais rentáveis e eram rapidamente canalizados para um operador humano.

Aqueles no final da lista, menos rentáveis, esperavam muito mais tempo para serem atendidos ou eram despachados para um centro terceirizado (*call center*) já abarrotado, onde eram atendidos, em sua maioria, por máquinas.

Outro arquétipo estudado pela autora[264] foi o de empresas de cartão de crédito, como a *Capital One*, que utilizava algoritmos para estabelecer uma pontuação e encontrar clientes em potencial.

Os algoritmos utilizados por essas empresas, no entanto, eram capazes de acessar dados de navegação dos usuários na web e analisar seus padrões de compras para determinar clientes em potencial. Isso era feito a partir do itens buscados pelo potenciais cliente. É que as chances de uma pessoa clicando sobre anúncios de carros de luxo ser mais rentável do que um indivíduo buscando por um carro usado na internet é bem alta.[265]

---

[261] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 169.
[262] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 169.
[263] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 170.
[264] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 170.
[265] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 170.

A maioria dos sistemas de pontuação também utiliza a localização do computador do visitante, o que, quando combinado com dados imobiliários, pode resultar em inferências sobre o poder aquisitivo do usuário. Uma pessoa utilizando um computador em uma região nobre representa uma melhor perspectiva de negócio para essas empresas do que outra pessoa localizada em uma região periférica.[266]

O problema desses sistemas de escores se apresenta, entretanto, quando se considera o efeito de *feedback loop* (de retroalimentação) gerado. Isso porque haverá grandes chances de que o sistema de pontuação dê ao mutuário residente em uma região periférica uma pontuação baixa. E, então, este será direcionado à oferta de um cartão de crédito, por exemplo, para um grupo demográfico de maior risco, significando menos crédito disponível e juros mais altos para aqueles que já estão em uma situação difícil.[267]

O *feedback loop* pode ser visto mais facilmente quando se fala em empregabilidade. Nesse sentido, uma pesquisa realizada pela *Society for Human Resources Management* apontou que quase a metade dos empregadores estadunidenses selecionam potenciais contratações analisando relatórios de crédito de seus aplicantes, e às vezes, até de seus funcionários atuais, sobretudo quando aplicam para uma promoção.[268]

Antes de as empresas realizarem essas verificações, elas devem primeiro pedir o consentimento do empregado ou candidato a emprego. Mas isso geralmente é pouco mais do que uma formalidade; em muitas empresas, aqueles que se recusam a entregar seus dados de crédito sequer são considerados para o trabalho. E se o histórico de crédito deles for ruim, há uma boa chance de que serão preteridos.[269]

Outra pesquisa, do ano de 2012, sobre dívida de cartão de crédito em famílias de média e baixa renda deixou esse ponto muito claro. Um em dez participantes relataram ter ouvido dos empregadores que históricos de crédito ruins minaram suas chances de contratação, e ninguém sabe precisar ao certo quantos foram desqualificados exclusivamente por seus relatórios de crédito.[270]

---

[266] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 175.
[267] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 176.
[268] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 170.
[269] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 170.
[270] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 170.

Embora a lei estadunidense estipule que os empregadores devem alertar candidatos quando problemas de crédito os desqualificam, alguns deles simplesmente dizem aos candidatos que não são adequados ao posto de trabalho ou que outros candidatos eram mais bem qualificados que eles. [271]

A prática de usar pontuação de crédito em contratações e promoções cria um perigoso ciclo de pobreza. Se, por conta de seu histórico de crédito, você não conseguir um emprego, sem fonte de renda, muito provavelmente esse registro ficará pior, tornando-se ainda mais difícil conseguir trabalho. Trata-se de uma espiral descendente que empurra esses indivíduos para um ciclo de pobreza difícil de romper.

Não é diferente do problema que jovens enfrentam quando procuram o primeiro emprego e são desqualificados por falta de experiência. Ou a situação dos desempregados de longa data, que deixam de receber proposta porque estão sem emprego a demasiado tempo.

O argumento dos empregadores é que o bom histórico de crédito é um proxy (um indicador) de uma pessoa responsável, o perfil que buscam contratar.

No entanto, associar o histórico de dívida de uma pessoa a uma espécie de indicador moral (sobre o indivíduo ser ou não responsável) é um erro. Isso porque muitas pessoas trabalhadoras e confiáveis perdem seus empregos à medida que as empresas falem, cortam custos ou se reestruturam.

Esses números também sobem durante as recessões, como a de 2008 no Estados Unidos. E muitos dos recém-desempregados se veem sem seguro saúde, que, corriqueiramente, é pago pelo empregador nos EUA. [272]

Seguindo o raciocínio, bastaria um acidente ou uma doença para que esses indivíduos perdessem o controle sobre suas finanças. Mesmo com o *Affordable Care Act* tendo reduzido o número de pessoas sem seguro médico, as despesas dessa natureza permanecem sendo a maior causa de falências nos Estados Unidos. [273]

Pessoas que tinham economias guardadas, é claro, poderiam manter seus créditos intactos durante tempos difíceis. Os que viviam de salário em salário, não. Consequentemente, uma classificação de crédito não é apenas uma proxy (uma variável

[271] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 170.
[272] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 176.
[273] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 176.

que substitui outra – um indicador) para responsabilidade e decisões inteligentes. É, também, um proxy para a riqueza. E a riqueza é altamente correlacionada à raça.

O'Neil[274] expõe, nesse sentido, que em 2015, as famílias brancas detinham, em média, cerca de dez vezes mais dinheiro e propriedades que famílias negras e hispânicas. E, enquanto apenas quinze por cento dos brancos detinham um patrimônio líquido negativo ou igual a zero, mais de um terço das famílias negras e hispânicas não detinham qualquer economia.

O quadro piora na medida em que se verifica que a diferença de riqueza aumenta com a idade. Aos sessenta, os brancos são onze vezes mais ricos que os afro-americanos. Diante desses números, não é difícil argumentar que a armadilha da pobreza criada pelo empregador por meio de verificações de crédito afeta a sociedade de forma desigual e ao longo de fileiras raciais. [275]

Enquanto a autora escrevia sua obra, dez estados aprovaram legislação para proibir o uso de pontuação de crédito na contratação. Ao bani-los, o governo da cidade de Nova York declarou que o uso de verificações de crédito "afeta desproporcionalmente requerentes de baixa renda e requerentes de cor". Ainda assim, a prática continua legal em quarenta estados. Isso não quer dizer que os departamentos de pessoal em toda a América estão intencionalmente construindo uma armadilha. Eles sem dúvida acreditam que os relatórios de crédito contêm fatos relevantes que os ajudam a tomar decisões importantes. Afinal, "quanto mais dados, melhor". Esse é o princípio orientador da Era da Informação. No entanto, em nome da justiça e equidade, alguns desses dados devem permanecer não conhecidos.[276]

4.1.4. O caso do H1N1 e da COVID-19

Apesar das duras e relevantes críticas desenvolvidas nas sessões anteriores, nem tudo que ocorre na utilização dos algoritmos e outras técnicas das tecnologias de informação levam à violação de direitos ou à iniquidade. Não raras vezes, os algoritmos desempenham um papel fundamental em áreas estratégicas da vida humana.

---

[274] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 177.
[275] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 177.
[276] O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 177.

Um exemplo latente disso teve como plano de fundo o uso de sistemas informáticos no monitoramento e controle dos casos de H1N1 nos Estados Unidos.

No ano de 2009, uma variante do vírus da gripe avocou a atenção de todo o mundo. A nova cepa de vírus, à época, apresentava altas taxas de mortalidade e transmissão e as informações sobre a existência de novos casos chegava aos Centros de Controle e Prevenção de Doenças (CDC), sempre com uma ou duas semanas de atraso.[277]

Isso dificultava uma estratégia atempada e eficaz no controle dos casos. No entanto, pouco tempo antes do H1N1 ganhar as manchetes, engenheiros da Google, publicaram um notável artigo na revista *Nature*[278] explicando como a empresa poderia "predizer" a disseminação de uma gripe de inverno nos Estados Unidos, não só nacionalmente, mas em regiões específicas ou mesmo em estados. [279]

A companhia poderia realizar tal feito analisando o que as pessoas buscavam na Internet. A partir do momento em que o mecanismo de buscas recebe mais de três bilhões de requisições de pesquisas todos os dias e as armazena, tem-se uma imensidão de dados possíveis de serem trabalhados.[280]

Para cumprir seu objetivo, inicialmente, o Google utilizou os 50 milhões de termos de pesquisa mais comuns digitados pelos americanos e os comparou com os dados do CDC relativos à disseminação de gripes sazonais no mesmo período. Frases como "remédio para tosse e febre", e outras sequências de palavras foram testadas. No total, 450 milhões de diferentes modelos matemáticos foram experimentados e comparados aos dados de casos de gripe entre 2007 e 2008. Assim, a companhia pôde lapidar uma combinação de cerca de 45 termos de pesquisas que, quando usados conjuntamente a um modelo matemático, entregavam uma estreita correlação entre as predições matemáticas e os dados oficiais de doentes catalogados pelo CDC.[281]

Desse modo, quando a crise do H1N1 emergiu, o sistema da Google pôde prover um importante e atual indicador estatístico às autoridades Americanas.

---

[277] MAYER-SCHÖNBERGER; Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. New York: Mariner Book, 2014, p. 1-2.
[278] Ver: GINSBERG, J., MOHEBBI, M., PATEL, R. et al. Detecting influenza epidemics using search engine query data. **Nature** n. 457, p. 1012–1014, 2009. Disponível em: https://doi.org/10.1038/nature07634. Acesso em: 10 jan. 2021.
[279] MAYER-SCHÖNBERGER; Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. New York: Mariner Book, 2014, p. 1-2.
[280] MAYER-SCHÖNBERGER; Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. New York: Mariner Book, 2014, p. 1-2.
[281] MAYER-SCHÖNBERGER; Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. New York: Mariner Book, 2014, p. 1-2.

Situação parecida ocorreu recentemente, em que a coleta de dados e a monitoração das linhas de contágio mostraram-se importantes ferramentas de enfrentamento à pandemia do novo coronavírus (SARS-CoV-2). As tecnologias digitais ofereceram um enorme avanço na precisão, amplitude, confiabilidade e velocidade das informações de contato, rastreamento e demais medidas de vigilância em saúde pública.[282]

Conforme sistematiza a literatura especializada[283], os principais usos das tecnologias na saúde pública durante o enfrentamento da pandemia dividiram-se em 5 áreas principais: a) vigilância epidemiológica, b) identificação de casos, c) interrupção de linhas de contágio, d) comunicação pública e e) cuidados clínicos, catalogados na tabela seguinte:

Tabela 1- Tecnologias digitais utilizadas no combate à pandemia da COVID-19[284].

Necessidade de saúde pública	Ferramenta digital ou tecnologia	Exemplos de uso	Referências[285]
Vigilância epidemiológica Digital	Aprendizagem de Máquina	Ferramentas de inteligência epidêmica baseadas na Web e vigilância sindrômica on-line	Ferramentas de inteligência epidêmicas baseadas na Web: 20–23, 25[286] Com base em mídias sociais ou dados de pesquisa online: 30–33[287]
	Pesquisas aplicativos e websites	Declarações de sintomas	37, 38, 48, 49[288]

[282] Ver: VENKATASUBRAMANIAN, Akarsh. The Human Rights Challenges to Digital COVID-19 Surveillance. **Health and Human Rights Journal**, vol. 22, n. 2, December 2020, p. 79-84. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/harhrj22&i=505. Acesso em: 20 fev. 2022.
[283] BUDD, J., MILLER, B.S., MANNING, E.M. et al. Digital technologies in the public-health response to COVID-19. **Nature Medicine**, n. 26, ago. p. 1183–1192, 2020. Disponível em: https://doi.org/10.1038/s41591-020-1011-4. Acesso em: 25 fev. 2022.
[284] Adaptado de: BUDD, J., MILLER, B.S., MANNING, E.M. et al. Digital technologies in the public-health response to COVID-19. **Nature Medicine**, n. 26, ago. p. 1183–1192, 2020, p. 1184. Disponível em: https://doi.org/10.1038/s41591-020-1011-4. Acesso em: 25 fev. 2022.
[285] As referências dizem respeito ao trabalho original e serão reproduzidas para facilitar a pesquisa do leitor.
[286] 20. ProMED. ProMED-mail. https://promedmail.org/coronavirus/ (2020). 53; 21. Government of Canada. About GPHIN. https://gphin.canada.ca/cepr/aboutgphin-rmispenbref.jsp?language=en_CA. (2020); 22. HealthMap. COVID-19. https://www.healthmap.org/covid-19/ (accessed 29 June 2020) 54; 23. World Health Organization. Epidemic intelligence from open sources (EIOS). https://www.who.int/eios (2020); 25. World Health Organization. EPI-BRAIN. https://www.epi-brain.com/ (2020).
[287] 30. Sun, K., Chen, J. & Viboud, C. Early epidemiological analysis of the coronavirus disease 2019 outbreak based on crowdsourced data: a population-level observational study. Lancet Digit Health 2, e201–e208 (2020); 31. Qin, L. et al. Prediction of number of cases of 2019 novel coronavirus (COVID-19) using social media search index. Int. J. Environ. Res. Public Health 17, 2365 (2020); 32. Lu, Y. & Zhang, L. Social media WeChat infers the development trend of COVID-19. J. Infect. 81, e82–e83 (2020); 33. Lampos, V. et al. Tracking COVID-19 using online search. Preprint at https://arxiv.org/abs/2003.08086 (2020).
[288] 37. COVID Near You. https://www.covidnearyou.org/ (2020); 38. Menni, C. et al. Real-time tracking of self-reported symptoms to predict potential COVID-19. Nat. Med. 26, 1037–1040 (2020); 48. Singapore COVID-19 Symptom Checker. https://sgcovidcheck.gov.sg/ (2020); 49. NHS 111 online. https://111.nhs.uk/covid-19/ (2020).

	Extração de dados e visualização	Data dashboard (quadros de visualização de dados)	39–45[289]
Rápida identificação de casos	Dispositivos de diagnóstico conectados	Diagnóstico já no pronto atendimento	58[290]
	Sensores, incluindo dispositivos wearables	Checagem de sintomas febris	51–53[291]
	Aprendizagem de máquina	Análise de imagens médicas	65, 66[292]
Interrupção da transmissão comunitária	Aplicativos de smartphone, tecnologia Bluetooth de baixa potência	Rastreamento digital de contatos	Artigo científico: 71[293] Aplicativos: 76–79[294] Quadro geral: 81–83[295]

[289] 39. Ministry of Health Singapore. Updates on COVID-19 (coronavirus disease 2019) local situation. https://www.moh.gov.sg/covid-19/ (2020); 40. Centre for Health Protection, Department of Health. Latest situation of novel coronavirus infection in Hong Kong. The Government of the Hong Kong Special Administrative Region https://chp-dashboard.geodata.gov.hk/ covid-19/en.html (accessed 25 April 2020); 41. Nextstrain team. Genomic epidemiology of novel coronavirus—global subsampling. https://nextstrain.org/ncov/global (accessed 25 April 2020); 42. Covid19 SG. Dashboard of the COVID-19 virus outbreak in Singapore. https://co.vid19.sg/singapore/dashboard (accessed 25 April 2020); 43. Thorlund, K. et al. A real-time dashboard of clinical trials for COVID-19. Lancet Digit. Heal. 2, e286–e287 (2020); 44. The World Bank. World Bank Education and COVID-19. https://www. worldbank.org/en/data/interactive/2020/03/24/ world-bank-education-and-covid-19 (accessed 25 April 2020); 45. COVID-19 Mobility Data Network. Movement trends. https://visualization. covid19mobility.org/ (accessed 25 April 2020).

[290] 58. FIND. SARS-CoV-2 diagnostic pipeline. https://www.finddx.org/covid-19/ pipeline/ (accessed 15 June 2020).

[291] 51. Gostic, K., Gomez, A. C. R., Mummah, R. O., Kucharski, A. J. & Lloyd-Smith, J. O. Estimated effectiveness of symptom and risk screening to prevent the spread of COVID-19. eLife 9, e55570 (2020); 52. Quilty, B. J., Clifford, S., Flasche, S. & Eggo, R. M. Effectiveness of airport screening at detecting travellers infected with novel coronavirus (2019-nCoV). Eur. Surveill. 25, 2000080 (2020); 53. Armitage, H. Stanford Medicine scientists hope to use data from wearable devices to predict illness, including COVID-19. Stanford Medicine News Center http://med.stanford.edu/news/all-news/ 2020/04/ wearable-devices-for-predicting-illness-.html (2020).

[292] 65. Mei, X. et al. Artificial intelligence-enabled rapid diagnosis of patients with COVID-19. Nat. Med. https://doi.org/10.1038/s41591-020-0931-3 (2020); 66. Wang, S. et al. A deep learning algorithm using CT images to screen for coronavirus disease (COVID-19). Preprint at medRxiv https://doi. org/10.1101/2020.02.14.20023028 (2020).

[293] 71. Ferretti, L. et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science 368, eabb6936 (2020).

[294] 76. Ministry of Health. HaMagen - the Ministry of Health app for fighting the spread of coronavirus. https://govextra.gov.il/ministry-of- health/ hamagen-app/download-en/ (2020); 77. Australian Government Department of Health. COVIDSafe app. https:// www.health.gov.au/resources/ apps-and-tools/covidsafe-app (2020); 78. Government of India. Aarogya Setu mobile app. https://www.mygov.in/aarogya-setu-app/ (2020); 79. Together we can fight coronavirus – Smittestopp temporarily deactivated. Helsenorge.no https://helsenorge.no/coronavirus/smittestopp (accessed 26 April 2020).

[295] 81. DP-3T/documents: decentralized privacy-preserving proximity tracing–documents. The DP-3T Project https://github.com/DP-3T/documents (accessed 26 April 2020); 82. PEPP-PT. High-level pverview: pan-European privacy-preserving proximity tracing. https://github.com/pepp-pt/pepp-pt-documentation/blob/master/PEPP-PT-high-level-overview.pdf (accessed 27 July 2020); 83. Apple. Apple and Google partner on COVID-19 contact tracing technology. https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/ (2020).

	Dados de localização geográfica de smartphones	Análise de padrão de mobilidade	Análises: 84, 87–89, 93[296] Conjunto de dados: 86, 90, 91, 122[297]
Comunicação pública	Plataformas de redes sociais	Comunicação direcionada	104, 107[298]
	Mecanismos on-line de pesquisas	Priorização de informações	105[299]
	Robôs de bate-papo	Informações personalizadas	110[300]
Cuidados clínicos	Teleconferência	Telemedicina, encaminhamento	50[301]

Resumo das tecnologias digitais implantadas em intervenções de saúde pública para o surto de COVID-19, mostrando as principais publicações, exemplos e recursos. Tradução do autor. Adaptado do original.

Especificamente no controle às cadeias de transmissão da COVID-19, o levantamento feito por O'Neill, Ryan-Mosley e Johnson, publicado na MIT Technology Review,[302] trouxe importante contribuição a respeito das medidas tecnológicas utilizadas no enfrentamento da COVID-19.

A tabela apresentada no Anexo I demonstra a difusão de uma multiplicidade de tecnologias utilizadas no controle da pandemia. Esses mecanismos, no entanto, apesar de bastante úteis, engendraram a preocupação acerca da proteção dos direitos humanos e fundamentais de seus usuários, no que atine à privacidade, à transparência, ao *accountability*, à equidade, à não discriminação e à proteção de dados, sobretudo, contra

[296] 84. Jia, J. S. et al. Population flow drives spatio-temporal distribution of COVID-19 in China. Nature 582, 389–394 (2020); 87. Chinazzi, M. et al. The effect of travel restrictions on the spread of the 2019 novel coronavirus (COVID-19) outbreak. Science 368, 395–400 (2020); 88. Kraemer, M. U. G. et al. The effect of human mobility and control measures on the COVID-19 epidemic in China. Science 368, 493–497 (2020); 89. Pepe, E. et al. COVID-19 outbreak response: a first assessment of mobility changes in Italy following national lockdown. Preprint at medRxiv https://doi.org/10.1101/2020.03.22.20039933 (2020); 93. Zhang, J. et al. Changes in contact patterns shape the dynamics of the COVID-19 outbreak in China. Science 368, 1481–1486 (2020).

[297] 86. China Data Lab. Baidu mobility data. Harvard Dataverse https://doi.org/10.7910/DVN/FAEZIO (2020); 90. Google. COVID-19 Community Mobility Reports. https://www.google.com/covid19/mobility/ (accessed 27 April 2020); 91. Apple. COVID-19 - Mobility Trends Reports. https://www.apple.com/covid19/mobility (accessed 27 April 2020); 122. Microsoft. Bing-COVID-19-Data. GitHub https://github.com/microsoft/ Bing-COVID-19-Data (2020).

[298] 104. World Health Organization. Coronavirus Disease (COVID-19) Situation Reports Report no. 13 https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf?sfvrsn=195f4010_6 (2020); 107. Sesagiri Raamkumar, A., Tan, S. G. & Wee, H.-L. Measuring the outreach efforts of public health authorities and the public response on facebook during the COVID-19 pandemic in early 2020: cross-country comparison. J. Med. Internet Res. 22, e19334 (2020).

[299] 105. Google. SOS alerts help. https://support.google.com/sosalerts/?hl=en (accessed 8 May 2020).

[300] 110. WhatsApp. How WhatsApp can help you stay connected during the coronavirus (COVID-19) pandemic. https://www.whatsapp.com/ coronavirus (2020).

[301] 50. Greenhalgh, T., Koh, G. C. H. & Car, J. Covid-19: a remote assessment in primary care. Br. Med. J. 368, m1182 (2020).

[302] O'NEILL, Patrick Howell; RYAN-MOSLEY, Tate; JOHNSON, Bobbie. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. MIT Technology Review. (maio), 2020. Disponível em: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. Acesso em: 05 mar. 2022.

vazamentos.[303] Algumas dessas aplicações incluem, a utilização de tecnologias Bluetooth e de Geolocalização para rastreamento de cadeias de transmissão, havendo na tabela elaborada pelo MIT[304] (visível no Anexo I) a catalogação dessas tecnologias e os principais riscos apresentados, como a falta de transparência, suspeitas de vazamento e sérias preocupações relativas à privacidade dos usuários.

Além do uso relacionado à excepcional situação do COVID-19, o emprego das tecnologias de informação e comunicação tem um amplo prospecto nas ciências médicas: desde a utilização da inteligência artificial e do aprendizado de máquina para sequenciamento genético, possibilitando uma medicina de precisão, até a análise automatizada de imagens por computadores, capazes de identificar padrões e desvios improváveis de serem percebidos pelo olho humano.

É o que aponta o professor da Universidade de Coimbra, André Gonçalo Dias Pereira[305]:

> Contemporaneamente, a medicina tem vindo a ser confrontada com uma nova exigência que não a de aliviar a dor e o sofrimento, antes a de responder a desejos pessoais (as técnicas de procriação medicamente assistida, a medicina do envelhecimento etc.). Do ponto de vista bioético, lê-se o sintoma de uma medicina do conforto.
> (...).
> O paradigma dominante deixou de ser a resposta a um problema localizado para passar a ser o da reconstrução dos seres humanos com a justificação de que, desse modo, serão melhorados! Estamos a assistir ao melhoramento cognitivo farmacológico (em muitos ambientes escolares), na disputa em torno do *dopping* no desporto e na aurora de tempos da terapia génica de melhoramento? À interação Homem/Inteligência Artificial... construindo o *Homo Deus* de *Harari*? O pós-humano de Fukuyama? Estaremos a caminho de um distópico "Admirável Mundo Novo? De Huxley?

Para o autor:[306]

---

[303] Para um panorama sobre o assunto ver: VENKATASUBRAMANIAN, Akarsh. The Human Rights Challenges to Digital COVID-19 Surveillance. **Health and Human Rights Journal**, vol. 22, n. 2, December 2020, p. 79-84. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/harhrj22&i=505. Acesso em: 20 fev. 2022.

[304] Tradução do autor. Adaptado de: O'NEILL, Patrick Howell; RYAN-MOSLEY, Tate; JOHNSON, Bobbie. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. MIT Technology Review. (maio), 2020. Disponível em: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. Acesso em: 05 mar. 2022.

[305] PEREIRA, André Gonçalo Dias. Inteligência Artificial, Saúde e Direito: Considerações jurídicas em torno medicina de conforto e da medicina transparente. In: Julgar: Lisboa, n. 45, p. 235-262, 2021, p. 236.

[306] PEREIRA, André Gonçalo Dias. Inteligência Artificial, Saúde e Direito: Considerações jurídicas em torno medicina de conforto e da medicina transparente. In: Julgar: Lisboa, n. 45, p. 235-262, 2021, p. 237.

> A medicina é intensamente desafiada pelas ciências da computação e pela economia digital. Identificam-se várias áreas como determinantes da medicina do futuro. Destacam[-se] os temas relativos à IA, ao processo clínico eletrónico, aos medicamentos personalizados, à cirurgia robótica, ao atendimento personalizado e à medicina preditiva. A interação entre a genética, os *big data* e a inteligência artificial afigura-se colossal e irá transformar o mundo da prestação de cuidados de saúde. São os principais tópicos de pesquisa científica e investimento financeiro nos últimos anos, beneficiando de grandes investimentos das grandes indústrias da informática, não só por razões de crescimento de mercado, mas mesmo com base em pressupostos filosóficos. Falamos das doutrinas que advogam uma radical transformação, denominadas de transumanismo ou pós-humanismo.
> O envelhecimento da população, associado ao processamento de grandes conjuntos de dados no campo da saúde, está a contribuir para esta transformação. O investimento em novas tecnologias é apresentado como um fator-chave para assegurar a sustentabilidade a médio prazo, especialmente na União Europeia onde aumento dos custos de saúde de envelhecimento da população está em franco crescimento. Deletar risco para a saúde dos pacientes, não apenas numa base individual, mas de toda a população, é a nova ambição das políticas públicas, com vista a usar os recursos de saúde de forma mais inteligente e com um custo menor.

Dias Pereira destaca que a combinação de técnicas permitirá, em pouco tempo, uma medicina personalizada à nível genético, possibilitando medicamentos customizados, tratamentos e intervenções preventivas (com base em riscos e predisposições genéticas), além de diagnósticos muito mais precisos e personalizados:[307]

> Por seu turno, a medicina personalizada traduz-se na implementação do um modelo de apoio médico personalizado e adaptado a cada individuo, possível graças aos avanços biotecnológicos, especialmente ao nível da sequenciação genômica. Quando ainda não haja doença, a partir do conhecimento da predisposição individual do sujeito para a doença, procede-se à escolha das medidas preventivas e de promoção da saúde que melhor se adaptem ao individuo. Quando já haja doença diagnosticada, a medicina personalizada permite otimizar a escolha da terapêutica medicamentosa que apresente uma maior eficácia ou menores reações adversas. Assim se pretende: (1) identificar doenças mais cedo (diagnóstico precoce). (2) reduzir os encargos do tratamento e (3) adequar o tratamento ao doente (farmacogenômica) e assim afastarmo-nos do tempo atual, da "imprecisão na terapêutica", em que se estima que em elevadas percentagens os medicamentos não produzam os efeitos desejados aquando da prescrição.
> Ora, a IA assume nesta nova medicina personalizada uma extrema importância, pois a capacidade e rapidez de análise da IA supera – de longe – a capacidade humana. Com efeito, [trata-se d]a medicina dos 4 Ps (preventiva, preditiva personalizada e proativa) que tem na IA uma força motriz.

[307] PEREIRA, André Gonçalo Dias. Inteligência Artificial, Saúde e Direito: Considerações jurídicas em torno medicina de conforto e da medicina transparente. In: Julgar: Lisboa, n. 45, p. 235-262, 2021, p. 238.

Esses ganhos expressivos na confiabilidade, previsibilidade e eficiência do tratamento, no entanto, não é indene de riscos. Nas palavras de Dias Pereira:[308]

> Um dos riscos relevantes é de uma limitação da autonomia e de um total olvido do princípio da justiça. O risco da limitação da autonomia vai exigir um reforço do consentimento informado e uma forte regulação da proteção de dados pessoais na área da saúde. O risco do oblívio do princípio da justiça exige maior participação democrática, reforço dos sistemas de saúde de acesso universal e equitativo e uma maior consciencialização para os riscos ambientais e os imperativos sanitários.
> Estas transformações inserem-se na "Quarta Revolução Industrial" (Klaus Schwab), que aponta para "mudanças radicais e desafios resultantes das tecnologias emergentes (novas biotecnologias, inteligência artificial, computação quântica, etc.) e as suas consequências sociais e políticas." (...) e receia que «sistemas facciosos venham acentuas as desigualdades a pôr em causa os direitos das pessoas de todos os países". Como veremos, o princípio bioético da justiça (Beaumont Report) é severamente ameaçado por este conjunto de transformações radicais em curso (genômica, IA, digitalização, cyborgs, etc.), sendo a IA o fator-chave em toda esta transformação. A justiça (no sentido de alocação equitativa dos recursos) pode ser ameaçada, pois as intervenções digitais na área da saúde têm o potencial de desviar recursos das áreas mais carenciadas, como já em 2019 a OMS alertava. (...)
> Encontrámos, nesta breve introdução, já dois problemas jurídico-sociais: (1) a potencial violação do princípio da equidade e da justiça na alocação de recursos na saúde e (2) a crise da relação médico-paciente, que se subdivide nos seguintes desafios: (i) a proteção do laço social, (ii) a proteção de dados pessoais e (iii) a privacidade, incluindo das informações genéticas, bem como (iv) o direito de manter uma interface humana em situações de vulnerabilidade relacionadas com a doença, (v) a autonomia do doente face à possibilidade de ser tratado por um robô, e (vi) a própria autonomia do médico no âmbito que uma recente submissão quase acrítica aos resultados informáticos.

A tônica das relações com as tecnologias parece sempre indicar um benefício muito propagado, quase sempre atrelado a riscos ocultos ou abrandados. Embora os potenciais tecnológicos sejam incríveis, há sempre um grau de preocupação das repercussões dessas técnicas nas mais diversas áreas da vida em sociedade.

[308] PEREIRA, André Gonçalo Dias. Inteligência Artificial, Saúde e Direito: Considerações jurídicas em torno medicina de conforto e da medicina transparente. In: Julgar: Lisboa, n. 45, p. 235-262, 2021, p. 238-240.

E essa é uma marca da sociedade do risco,[309] para a qual dedicaremos algumas últimas palavras que encerrem as discussões sobre as diversas aplicações das tecnologias de informação e comunicação, seus perigos e potenciais.

O último tópico tratará de forma direta os riscos envolvendo fraudes que se utilizam dos dados pessoais vazados ou coletados ilicitamente.

4.1.5. As fraudes envolvendo o uso de dados pessoais

Como derradeiro tópico envolvendo os riscos associados à utilização das novas tecnologias, serão exploradas diversas modalidades de engodos, relacionados à captura e utilização de dados pessoais.

O ponto de partida da discussão não poderia ser outro senão o trabalho do sociólogo alemão Ulrich Beck,[310] que diagnostica um aumento e complexificação significativos dos riscos a que estamos submetidos nas sociedades contemporâneas, vindo a nomear as sociedades atuais de sociedades de ricos. Não é preciso muito esforço para se notar esse conjunto de perigos, que aos poucos passamos a experimentar na sociedade da informação, onde tudo, ou quase tudo, está à distância de um click, inclusive, as ameaças.[311]

Esses riscos, conexos ao fenômeno na digitalização, espraiam-se por todas as áreas, inclusive, pelas relações de empregos, ou, às pretensas relações. E é nesse cenário que nascem as modalidades de fraude que serão abordadas, o *jobfish*, a engenharia social e fraudes correlatas.

O termo *jobfishing*, cunhado em língua inglesa, é utilizado em alusão à expressão *catfish*, também da língua inglesa, empregada para designar as situações nas quais uma pessoa se faz passar por outra (real ou não), buscando enganar o interlocutor. Trata-se de uma prática que tem lugar em ambientes virtuais, especialmente em redes sociais ou aplicativos de relacionamento.[312]

---

[309] BECK, Ulrich. **Sociedade de Risco**. NASCIMENTO, Sebastião (trad.). São Paulo: Editora 34, 2010, p. 20.

[310] BECK, Ulrich. **Sociedade de Risco**. NASCIMENTO, Sebastião (trad.). São Paulo: Editora 34, 2010, p. 20.

[311] *Cf.*: ALENCAR, Antônio Raul Veloso de; LEAL, Carla Reita Faria. "Jobfishing": a expansão dos riscos aos candidatos a empregos na sociedade da informação. O livre. Disponível em: https://olivre.com.br/jobfishing-a-expansao-dos-riscos-aos-candidatos-a-empregos-na-sociedade-da-informacao. Acesso em: 12 maio 2022.

[312] CAMBRIDGE DICTIONARY. *Catfish*. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/catfish. Acesso em: 12 maio 2022.

A expressão *jobfishing*, por outro lado, designa, sob o ponto de vista do candidato a emprego, as falsas promessas de trabalho que têm crescido de forma abrupta durante a pandemia.[313] O termo está atrelado a uma espécie de logro, geralmente virtual, no qual vítimas desavisadas respondem a anúncios de falsos empregos e acabam trabalhando em empresas inexistentes, às vezes durante meses, sob a promessa de uma remuneração que nunca chega.

É o caso recentemente narrado pela BBC do Reino Unido,[314] da empresa "Madbird". Supostamente sediada em Londres, os responsáveis pela empresa enganaram mais de 50 pessoas a aceitarem empregos falsos em diversas funções, como designers, vendedores e gerentes.

Conforme relata a reportagem (com adaptações)[315]:

> O nome da agência (...) "Madbird" e o seu proprietário, Ali Ayad, era dinâmico e inspirador. Seu criador queria que todos na empresa fossem pessoas ativas e ambiciosas como ele. Mas quem participava das reuniões com as câmeras ligadas não sabia que alguns dos participantes listados da reunião não eram pessoas reais.
> Muitos dos funcionários do alto escalação que estavam listados nas chamadas de vídeo eram fictícios. Alguns até tinham contas de e-mail e perfis no LinkedIn, mas seus nomes eram inventados e suas imagens, de outras pessoas. Tudo aquilo era falso e os funcionários reais haviam caído no golpe do falso emprego.

A BBC passou um ano investigando o que teria acontecido e como as vítimas foram enganadas. Tudo foi construído de forma a se crer que a empresa era real. Com executivos experientes, alguns, em tese, ligados a grandes empresas, com seus rostos à mostra e perfis ativos e funcionais.

Validava a experiência o fato de que o diretor da empresa aparecia em diversas interações nas redes sociais e nas chamadas de vídeo em grupo com a equipe. Ele figurava, até mesmo, em campanhas publicitárias para marcas conhecidas em suas redes sociais, as quais se descobriu, mais tarde, serem fabricadas.

Assim, sob o pretexto de uma remuneração por comissão que seria paga logo após a finalização dos acordos em que participassem, algumas vítimas chegaram a trabalhar por até seis meses, antes de saberem que tudo era falso. Muitas dessas pessoas

[313] BBC. Jobfished: the con that tricked dozens into working for a fake design agency. Disponível em: https://www.bbc.com/news/uk-60387324. Acesso em: 12 maio 2022.
[314] BBC. Jobfished: the con that tricked dozens into working for a fake design agency. Disponível em: https://www.bbc.com/news/uk-60387324. Acesso em: 12 maio 2022.
[315] BBC. Como 52 pessoas foram enganadas para trabalhar em agência falsa de design. Disponível em: https://www.bbc.com/portuguese/internacional-60477755. Acesso em: 12 maio 2022.

acabaram drenando todas suas economias e vivendo com cartões de crédito na espera por pagamentos que nunca chegariam.

O caso da "Madbird" não é isolado. Tal como acontece com a maioria dos golpes praticados com auxílio da internet, este é um problema global. O aumento do trabalho remoto, o mercado de trabalho flutuante e a crescente popularidade das entrevistas de emprego por meio de plataformas de vídeo contribuíram para um aumento significativo dessas práticas.

De acordo os dados da *Better Business Bureau* (BBB),[316] por ano, os golpes de emprego atingem cerca de 14 milhões de vítimas, com US$ 2 bilhões em perdas diretas decorrentes do trabalho não remunerado prestado a empregadores fraudulentos. Nos EUA, as perdas relatadas ao Centro de Reclamações de Crimes na Internet do FBI sobre golpes de emprego aumentaram 27% entre 2018 e 2020, enquanto as reclamações ao Centro Canadense Antifraude quase dobraram em 2020, se comparadas com o ano anterior.

No Reino Unido, uma campanha do *Disclosure and Barring Service* (DBS)[317] alertou aqueles que procuram emprego a tomarem cuidado com o conteúdo questionável em anúncios de emprego, como endereços de e-mail ou empresas duvidosas, cópia mal escrita e salários irreais. Isso porque o governo britânico detectou que, em 2020, os golpes sazonais de emprego cresceram 88% em relação ao ano anterior.

O grande cenário de incertezas decorrente da pandemia vulnerou sobremaneira os candidatos a emprego que, desprovidos de qualquer segurança em diversos aspectos da vida (seja segurança alimentar, habitacional ou remuneratória), encontraram-se especialmente sujeitos às pressões do pretenso empregador e mais vulneráveis a serem vítimas de golpes como os narrados.

Foi justamente essa a situação de uma mulher em St. Louis (EUA) que perdeu o emprego durante a pandemia e foi recrutada através de um site de busca de emprego para atuar como assistente remota de uma grande empresa. O "empregador" depositou um cheque de US$ 2.400 em sua conta bancária para que a assistente comprasse equipamentos de um fornecedor terceirizado, depois, pediu que ela comprasse outros US$

[316] BBB. Better Business Bureau. BBB **Study: Looking for a job? Be careful! Job scams increased during pandemic**. Disponível em: https://www.bbb.org/article/investigations/24596-bbb-investigation-job-scams. Acesso em: 12 maio 2022.
[317] CASE, Tony. WTF is jobfishing (and how to avoid it). *Worklife*. Disponível em: https://www.worklife.news/talent/wtf-is-jobfishing-and-how-to-avoid-it/. Acesso em: 12 maio 2022.

2.400 em cartões-presente da Home Depot e enviasse uma mensagem de texto com os números no verso.

Cumpridas as tarefas, ela não teve mais notícias do empregador. Seu banco, no entanto, informou que o cheque depositado em sua conta era fraudulento.[318]

O caso é ilustrativo da situação. O relatório de 2020 do Instituto sobre golpes de emprego do BBB[319] descobriu que os golpes desse tipo vitimaram mais comumente os jovens (pessoas com idades entre 25 e 34 anos), sendo que as mulheres (mais propensas a perderem o emprego) representaram 67% das reclamações. A perda financeira mediana relatada por essas vítimas foi de US$ 1.000; e, frequentemente, foi relatada a perda de tempo útil, já que 32% das vítimas nunca foram pagas pelo trabalho que fizeram para um empregador que acabou se mostrando golpista.

E essa não é uma realidade apenas estrangeira, após a reportagem da BBC sobre a empresa *Madbird* relatada acima, um brasileiro procurou a BBC Brasil relatando ter sofrido um golpe semelhante.

A grande preocupação com todos esses tipos de fraudes, no entanto, não se esgota nos prejuízos diretos causado às vítimas. Frequentemente associada às falsas propostas de emprego encontra-se o roubo de identidade.

No contexto de segurança da informação, convencionou-se chamar-se de engenharia social as técnicas que visam à manipulação psicológica de pessoas para a execução de ações ou para a divulgação de informações confidenciais, muito comumente relacionada à obtenção de dados pessoais para realização de fraudes bancárias.

A engenharia social está usualmente associada ao *jobfishing* como aponta o Better Business Bureau (BBB):[320]

---

[318] BBB. Better Business Bureau. **BBB Study**: Looking for a job? Be careful! Job scams increased during pandemic. Disponível em: https://www.bbb.org/article/investigations/24596-bbb-investigation-job-scams. Acesso em: 12 maio 2022.

[319] BBB. Better Business Bureau. BBB **Study: Looking for a job? Be careful! Job scams increased during pandemic**. Disponível em: https://www.bbb.org/article/investigations/24596-bbb-investigation-job-scams. Acesso em: 12 maio 2022.

[320] Tradução do autor. No original: "Identity theft is a common outcome of job scams, as scammers often steal job seekers' personal information to open bank accounts to further their fraud. BBB found 34% of victims provided their driver's license number and 25% provided their Social Security or Social Insurance number. Fake checks also frequently accompany job scams, and they continue to grow. This new BBB study finds that 36% of job scam complaints to BBB involved a fake check, with fake check complaints to the Federal Trade Commission (FTC) increasing by 65% between 2015 and 2020. In the two years since BBB issued an investigative study on fake check fraud, losses absorbed by banks themselves due to fake checks went up 40% to reach $1.3 billion. Common fraudulent job offers involving fake checks include mystery shopping or secret shopper jobs, car wrap jobs, nanny or caregiver jobs, and small business jobs such as photography or painting houses". BBB. Better Business Bureau. BBB *Study: Looking for a job? Be careful! Job scams increased during pandemic*. Disponível em: https://www.bbb.org/article/investigations/24596-bbb-investigation-job-scams. Acesso em: 12 maio 2022.

> O roubo de identidade é um resultado comum de golpes de emprego, pois os golpistas geralmente roubam as informações pessoais dos candidatos a emprego para abrir contas bancárias e promover sua fraude. A BBB descobriu que 34% das vítimas forneceram o número da carteira de motorista e 25% forneceram o número do Seguro Social ou do Seguro Social. (...)
> Cheques falsos também costumam acompanhar golpes de emprego e continuam a crescer. Este novo estudo do BBB descobriu que 36% das reclamações de golpes de emprego ao BBB envolveram um cheque falso, com as reclamações de cheques falsos à Federal Trade Commission (FTC) aumentando 65% entre 2015 e 2020. Nos dois anos desde que o BBB emitiu estudos investigativos em fraudes de cheques falsos, as perdas absorvidas pelos próprios bancos devido a cheques falsos aumentaram 40%, chegando a US$ 1,3 bilhão. As ofertas de emprego fraudulentas comuns que envolvem cheques falsos incluem compras misteriosas ou empregos secretos, trabalhos de envelopamento de carros, trabalhos de babá ou cuidador e trabalhos em pequenas empresas, como fotografia ou pintura de casas.

Outros casos de engenharia social envolvem falsos telefonemas de bancos, e-mail fraudulentos, anúncios mal-intencionados e outros golpes similares, perpetrados com a finalidade de se obter informações confidenciais das vítimas, causando-lhes prejuízos das mais diversas ordens.

Todo esse cenário demonstra os diversos riscos a que estamos expostos, nas mais diversas áreas de nossas vidas.

Assim, a presente seção cumpre a finalidade de expor a miríade de riscos a que estamos expostos e a necessidade de alguma regulação, especialmente por parte do Estado, objetivando a atenuação desses mesmos riscos.

Destarte, tratada a base fática ou material da pesquisa, passa-se à abordagem das estruturas de regulação até então existentes na seara da proteção de dados pessoais.

PARTE II – ESTRUTURAS REGULATÓRIAS EM MATÉRIA DE PRICAVIDADE E PROTEÇÃO DE DADOS PESSOAIS

Abordada a necessidade de regulação diante dos diversos riscos que lhe cabem equacionar (sem a pretensão de esgotá-los, mas de ilustrar a sua variedade e a dificuldade da tarefa posta), esta seção buscará expor os contornos regulatórios em matéria de privacidade e proteção de dados pessoais que se tem notícia.

Na presente seção buscaremos entender o estado da arte da matéria e as particularidades da regulação no cyberespaço. Enquanto no primeiro capítulo avaliamos os impactos da evolução tecnológica nos sistemas produtivos e a regulação dessas atividades, agora voltaremos os olhos para os serviços e plataformas disponíveis no ciberespaço, se é possível regulá-los e de que forma?

1. O ciberespaço e a regulação

O ciberespaço foi originariamente concebido para ser um território que pudesse proporcionar certa autonomia e liberdade a seus usuários. No entanto, a percepção de que este não deveria ser um local isento de regulação ganhou força nas últimas décadas.[321] A miríade de riscos, como a tomada de decisões automatizadas com potencial discriminatório;[322] o roubo de identidade, as fraudes bancárias e os casos de engenharia social;[323] a disseminação de *fake news* fabricadas e direcionada à medida, com o intuito de influir a percepção de um grupo de indivíduos sobre determinado assunto – condicionando, em especial, seu sentido de voto em eleições futuras;[324] além dos notórios casos de vazamento de dados, com potencial danoso ainda incerto em toda sua extensão,

[321] Cf. SOMBRA, Thiago Luís Santos. Fundamentos da regulação da privacidade e proteção de dados pessoais. São Paulo: Thomson Reuters Brasil, 2019. KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 26.

[322] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Revista Direito Público**, Brasília, v. 16, n. 90, p. 39–64, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em: 2 maio 2021.

[323] CASE, Tony. WTF is jobfishing (and how to avoid it). **Worklife**. [s.l.], 2022. Disponível em: https://www.worklife.news/talent/wtf-is-jobfishing-and-how-to-avoid-it/. Acesso em: 25 jun. 2022.

[324] MARS, Amanda. Como a desinformação influenciou nas eleições presidenciais? **El País**. Nova York, 2018. Disponível em: https://brasil.elpais.com/brasil/2018/02/24/internacional/1519484655_450950.html. Acesso em: 25 jun. 2022. CADWALLADR, Carole. The great British Brexit robbery: how our democracy was hijacked. **The Guardian**, 7 mai. 2017. Disponível em: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy. Acesso em: 14 set. 2022.

a exemplo do episódio envolvendo a empresa *Cambridge Analytica*,[325] os dois casos de vazamentos de dados admitidos *a posteriori* pelo Yahoo[326] e pela Uber,[327] comprometendo os dados de 500 milhões e 25 milhões de indivíduos, respectivamente, sem contar os dois megavazamentos de dados que atingiram 223 e 100 milhões de brasileiros no ano de 2021;[328] são apenas alguns indicativos da necessidade e relevância desse processo regulatório.

Nas linhas seguintes analisaremos os fatores que impulsionaram as principais vertentes regulatórias do ciberespaço e sua conexão com os modelos regulatórios específicos da privacidade e proteção de dados, de forma a se compreender como cada um pretendia apresentar respostas aos novos desafios impostos pelo uso da tecnologia.

Antes, porém, considerando que muito se tem dito sobre a regulação, dedicaremos algumas palavras a entender o que vem a ser o termo, para os fins aqui propostos.

a) Regulação

Em regra, quando falamos em regulação, nos referimos à regulação pública nacional (ou seja, àquela institucionalizada pelo Estado-nação). Dentro dessa perspectiva, a regulação deve ser entendida como a atividade eminentemente estatal, exercida a partir de um conjunto de comandos e regras vinculantes a serem aplicadas e controladas por uma autoridade pública.

Esse é o sentido tradicional de regulação, embora ela assuma diferentes propósitos discursivos, teoréticos e analíticos, em diferentes áreas do conhecimento,

[325] CONFESSORE, Nicholas. Cambridge Analytica and Facebook: the scandal and the fallout so far. **The New York Times**. New York, 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 05 maio 2021. ALVES, Paulo. Facebook e Cambridge Analytica: sete fatos que você precisa saber. **TechTudo**. São Paulo, 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/03/facebook-e-cambridge-analytica-sete-fatos-que-voce-precisa-saber.ghtml. Acesso em 05 maio 2021.

[326] ROHR, Altieres. Vazamento de dados do Yahoo: Veja o que você precisa saber. **G1**, São Paulo, 2016. Disponível em: https://g1.globo.com/tecnologia/blog/seguranca-digital/post/vazamento-de-dados-do-yahoo-veja-o-que-voce-precisa-saber.html. Acesso em: 14 nov. 2022.

[327] NAPOL, Igor. Dados de 57 milhões de usuários da Uber foram acessados por hackers. **Tecmundo**, São Paulo, 2017. Disponível em: https://www.tecmundo.com.br/seguranca/124408-uber-omitiu-ciberataque-expos-dados-57-milhoes-pessoas.htm. Acesso em: 14 nov. 2018.

[328] CORACCINI, Raphael. Fotos e até salários estão entre os dados vazados de 223 milhões de brasileiros. **CNN Brasil**. São Paulo, 2021. Disponível em: https://www.cnnbrasil.com.br/business/2021/01/27/fotos-e-ate-salarios-estao-entre-os-dados-vazados-de-223-milhoes-de-brasileiros. Acesso em: 05 maio 2021. SAMBRANA, Carlos. Exclusivo: Novo vazamento expõe mais de 100 milhões de contas de celular. **NEOFeed**. São Paulo, 2021. Disponível em: https://neofeed.com.br/blog/home/exclusivo-novo-vazamento-expoe-mais-de-100-milhoes-de-contas-de-celular/. Acesso em: 5 maio 2021.

como direito, economia, ciências políticas e políticas públicas, sociologia, história, psicologia, geografia, antropologia, gestão e administração social. Como aponta Levi-Faur, até mesmo as tradições e culturas jurídicas moldam significados diferentes do termo regulação.[329]

É por essa precisa circunstância que é necessário eleger um referencial teórico capaz de nortear o leitor a respeito do que se quer dizer quando nos referimos à regulação. Para tanto, abordaremos alguns significados propostos pela literatura especializada.

O primeiro desses referenciais é abordado no livro escrito por Robert Baldwin, Martin Cave e Martin Lodge[330] (um advogado, um economista e um cientista político) que assinalam ser a regulação frequentemente apontada como um modo discreto e identificável de atividade governamental, que pode ser definido, ao menos, das seguintes maneiras:

> - *Como um conjunto específico de comandos* – nos quais a regulação envolve a promulgação de um conjunto obrigatório de regras a serem aplicadas por um órgão dedicado a esse propósito. Um exemplo seria a legislação de saúde e segurança no trabalho aplicada pela Agência Executiva de Saúde e Segurança.
> - *Como uma influência estatal deliberada* – na qual a regulação tem um sentido mais abrangente e cobre todas as ações estatais destinadas a influenciar os negócios ou o comportamento social. Logo, regimes baseados em comando entrariam nesse uso, assim como uma série de outros modos de influência – por exemplo, aqueles baseados no uso de

[329] Sobre os múltiplos sentidos de regulação, consultar: LEVI-FAUR, David. Regulation & Regulatory Governance. **Jerusalem Papers in Regulation & Governance**. Working Paper n. 1, 2010. O autor faz uma ampla sistematização dos sentidos do conceito, sob diferentes matizes e perspectivas.

[330] Tradução do autor. No original: "*As a specific set of commands* – where regulation involves the promulgation of a binding set of rules to be applied by a body devoted to this purpose. An example would be the health and safety at work legislation as applied by the Health and Safety Executive.
As deliberate state influence – where regulation has a more broad sense and covers all state actions that are designed to influence business or social behaviour. Thus, command-based regimes would come within this usage, but so also would a range of other modes of influence – for instance, those based on the use of economic incentives (e.g., taxes or subsidies); contractual powers; deployment of resources; franchises; the supply of information, or other techniques.
As all forms of social or economic influence – where all mechanisms affecting behaviour – whether these be state-based or from other sources (e.g., markets)– are deemed regulatory. One of the great contributions of the theory of 'smart regulation' has been to point out that regulation may be carried out not merely by state institutions but by a host of other bodies, including corporations, self-regulators, professional or trade bodies, and voluntary organizations. According to this third, broad usage of the term 'regulation', there is no requirement that the regulatory effects of a mechanism are deliberate or designed, rather than merely incidental to other objectives.
As a final comment on the concept of regulation, it should be noted that regulation is often thought of as an activity that restricts behaviour and prevents the occurrence of certain undesirable activities (a 'red light' concept). The broader view is, however, that the influence of regulation may also be enabling or facilitative ('green light') as, for example, where the airwaves are regulated so as to allow broadcasting operations to be conducted in an ordered fashion, rather than left to the potential chaos of an uncontrolled market". BALDWIN, Robert, CAVE, Martin e LODGE, Martin. **Understanding Regulation**, 2a ed. Oxford: Oxford University Press, 2012, p. 3-4.

> incentivos econômicos (por exemplo, impostos ou subsídios); poderes contratuais; implantação de recursos; franquias; o fornecimento de informações ou outras técnicas.
> - *Como quaisquer formas de influência social ou econômica* – na qual todos os mecanismos que afetam o comportamento – sejam eles estatais ou de outras fontes (por exemplo, dos mercados) – são consideradas regulatórios. Uma das grandes contribuições da teoria da "regulação inteligente" foi apontar que a regulação pode ser realizada não apenas por instituições estatais, mas por uma série de outros órgãos, incluindo corporações, autorreguladores, órgãos profissionais ou comerciais e organizações voluntárias. De acordo com esse terceiro uso mais amplo do termo "regulação", não é exigido que os efeitos regulatórios de um mecanismo sejam deliberados ou planejados, ao invés de meramente incidentais a outros objetivos iniciais.
> Como comentário final sobre o conceito de regulação, deve-se notar que esta é muitas vezes pensada como uma atividade que restringe o comportamento e previne a ocorrência de certas atividades indesejáveis (um conceito de regulação como um "sinal vermelho"). Uma visão mais aberta, no entanto, é de que a influência da regulação também pode ser habilitante ou facilitadora ("sinal verde"), como, por exemplo, nos locais onde as ondas de rádio são reguladas permite-se que as operações de radiodifusão sejam conduzidas de maneira ordenada, ao invés de se deixar instaurar um caos em potencial de um mercado descontrolado.

Julia Black[331] adota semelhante entendimento, segundo o qual a regulação assume, pelo menos, três sentidos:

> No primeiro deles, a regulação consiste na promulgação de regras acompanhadas de mecanismos de monitoramento e execução. A presunção usual é de que o governo atua como o legislador, fiscalizador e executor, geralmente por meio de uma agência pública. A segunda definição mantém o governo como regulador, mas amplia as técnicas que podem ser descritas como "regulação" para incluir toda forma de intervenção direta do Estado na economia, seja qual for a forma que essa intervenção assuma. Na terceira definição regulação inclui todos os mecanismos de controle social ou influência afetando o comportamento de qualquer fonte, seja intencional ou não.

Assim, a primeira concepção denota o monopólio estatal para intervenção na esfera privada, sendo entendidas como regulação todas as formas por intermédio das quais o Estado protagoniza as atividades de produção normativa, seguida de monitoramento e

[331] Tradução do autor. No original: "In the first, regulation is the promulgation of rules accompanied by mechanisms for monitoring and enforcement. The usual assumption is that government is the rule-maker, monitor, and enforcer, usually operating through a public agency. The second definition keeps to the government as the 'regulator' but broadens the techniques that may be described as 'regulation' to include any form of direct state intervention in the economy, whatever form that intervention might take. In the third definition, regulation includes all mechanisms of social control or influence affecting behaviour from whatever source, whether intentional or not". BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 129.

de fiscalização, sendo estas atividades, geralmente, executadas por uma agência pública. A segunda conotação, mais ampla, mantém o Estado na posição de principal agente, mas flexibiliza a forma como este intervém na economia, admitindo outras formas de ação além da normativa. Por fim, a terceira concepção afasta a ideia de regulação do monopólio do Estado, referindo-se a qualquer forma de influência comportamental, seja ela protagonizada por agentes públicos ou privados, de forma intencional ou não.[332]

Nesse sentido, um importante aspecto na tentativa de delimitar o conceito de regulação é a sua íntima relação com a atuação das autoridades reguladoras. Como afirma Levi-Faur[333] a regra e seu processo de criação estão fortemente conectados. Essa ênfase se sobressai em uma das definições mais consagradas de regulação, segundo a qual esta assumiria a roupagem de "um controle sustentado e focado exercido por uma agência pública sobre atividades que são valorizadas pela comunidade".[334]

Essa definição não apenas inclui uma referência explícita à existência de uma agência pública, como também enfatiza a natureza sustentada e focada da regulação. A regulação, nesse sentido, envolve uma ação contínua de monitoramento, avaliação e refinamento das regras, ao invés de uma operação *ad hoc*.

Implícita nesta definição está também a expectativa de que as regras *ex ante* serão a forma dominante de controle regulatório. A definição é adequada também no sentido de reconhecer que muitas regulações não são exercidas por "agências reguladoras", mas por uma ampla variedade de órgãos executivos (agências públicas).[335]

Não obstante, o conceito falha ao reconhecer a regulamentação apenas como atividade pública praticada por "agências públicas", excluindo a regulamentação *business-to-business*, bem como a regulamentação *civil*. Também não esclarece quais tipos de controle direcionado o órgão público aplica (se apenas a criação de regras ou também outras formas de controle?); e, ainda, limita desnecessariamente a regulamentação àquelas ações que são valorizadas pela comunidade, quando, em verdade,

---

[332] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 26.

[333] LEVI-FAUR, David. Regulation & Regulatory Governance. **Jerusalem Papers in Regulation & Governance**. Working Paper n. 1, 2010, p. 7.

[334] Tradução do autor. No original: "sustained and focused control exercised by a public agency over activities that are valued by the community". SELZNICK, Phillip. Focusing Organizational Research on Regulation. In: NOLL, Richard. **Regulatory Policy and Social Sciences**. Bereley; Los Angeels: University of California, 1985, p. 363-67

[335] LEVI-FAUR, David. Regulation & Regulatory Governance. **Jerusalem Papers in Regulation & Governance**. Working Paper n. 1, 2010, p. 7.

pode haver outras necessidades a serem reguladas que não necessariamente contem com a estima da sociedade.[336]

Assim, ao buscar por um conceito mais abrangente de regulação, Levi-Faur[337] sugere aquele apresento por Scott, [338] segundo o qual:

> Para os propósitos de uma análise que considere todo o arranjo de instrumentos alternativos para o alcance dos objetivos de política pública, podemos pensar na regulação como qualquer processo ou conjunto de processos pelos quais normas são estabelecidas; o comportamento daqueles sujeitos a essas normas é monitorado ou retornado ao regime; e para os quais há mecanismos para manter o comportamento dos atores regulados dentro dos limites aceitáveis do regime (seja por medidas forçosas de cumprimento, seja por outros mecanismos). A definição de regulação pode ser um pouco limitada ao se pensar que ela é um instrumento de governança que tem foco em sua implantação por uma autoridade. A metáfora do "espaço regulatório" chama a atenção para o fato de que os conceitos de "autoridade regulatória" e "responsabilidade" são frequentemente dispersos entre diversas organizações, públicas e privadas, e essa autoridade não é a única fonte de poder dentro de um domínio regulado. A abordagem do espaço regulatório é "holística" no sentido de que ela olha para as interações de cada um dos atores no espaço e pode reconhecer uma pluralidade de sistemas de autoridade e recursos, assim como um arranjo complexo de interesses e ações.

Assim, segundo o autor, a regulação traduziria qualquer processo ou conjunto de processos que resulte no estabelecimento de uma norma de conduta, acompanhado do monitoramento daqueles que se sujeitam a essa norma, somado à existência de mecanismos que possam realizar a aderência dos atores regulados aos limites adequados do regime criado.

---

[336] LEVI-FAUR, David. Regulation & Regulatory Governance. **Jerusalem Papers in Regulation & Governance**. Working Paper n. 1, 2010, p. 7.

[337] LEVI-FAUR, David. Regulation & Regulatory Governance. **Jerusalem Papers in Regulation & Governance**. Working Paper n. 1, 2010, p. 7.

[338] Tradução do autor. No original: "For purposes of analysis which considers the full range of alternative instruments for achieving public policy objectives, we can think of regulation as any process or set of processes by which norms are established, the behaviour of those subject to the norms monitored or fed-back into the regime, and for which there are mechanisms for holding the behaviour of regulated actors within the acceptable limits of the regime (whether by enforcement action or by some other mechanism). The definition of regulation can be narrowed somewhat by thinking of it is an instrument of governance which takes as its focus the deployment of authority. The 'regulatory space' metaphor draws attention to the fact that regulatory authority and responsibility is frequently dispersed between a number of organisations, public and private, and that authority is not the only source of power within a regulated domain. The regulatory space approach is 'holistic' in the sense that it looks at the interactions of each of the players in the space and can recognise plural systems of authority and of other resources and a complex of interests and actions". SCOTT, Colin. Analyzing Regulatory Space: Fragmented Resouces and Instituional Design. **Public Law** (Summer), p. 283-305, 2001, p. 287.

Essa definição, mais larga, permite retirar a centralidade do Estado para reconhecer novas manifestações regulatórias. Segundo Levi-Faur[339] essas "abordagens decentralizadas da regulação enfatizam a complexidade, fragmentação, interdependência e falhas relacionadas à regulação pelo Estado, e sugerem os limites das distinções entre público e privado, e entre global e nacional".

Esses aspectos serão abordados mais à frente, contrapondo-se à ideia de uma regulação tipicamente estatal (fundada, em geral, em políticas de comando-e-controle), à luz do consistente ensaio de Julia Black.[340]

Aqui, importa saber que a atividade reguladora tem como principal objetivo influenciar o comportamento dos sujeitos regulados. Contudo, os meios como essa influência ocorre podem ser distintos. De um lado, a regulação pode ocorrer por meio de imposição de sanções aflitivas – típicas de uma regulação por comando-e-controle – e, de outro, pode se utilizar do contexto fático para tentar moldar a conduta dos regulados, "segundo incentivos presentes no código de conduta próprio ao ambiente regulado".[341] Em outras palavras, a regulação pode se valer tanto da coerção externa quanto da coerção interna.[342]

O conceito trazido por Scott ainda se alinha à agenda de pesquisas a respeito da regulação e governança,[343] sobretudo a ideia de "nova governança" trazida por Orly

---

339 Tradução do autor. No original: "Decentered approaches to regulation emphasize complexity, fragmentation, interdependencies, and government failures, and suggest the limits of the distinctions between the public and the private and between the global and the national (Black 2001; Scott 2004; Parker 2003; Gunningham 2009)". LEVI-FAUR, David. Regulation & Regulatory Governance. **Jerusalem Papers in Regulation & Governance**. Working Paper n. 1, 2010, p. 7.

340 BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 129.

341 ARANHA, Márcio Iorio. ***Compliance*, governança e regulação**. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 437-452, p. 442.

342 BIANCHI, José Flavio. **A ICANN entre governança e Regulação: análise da atuação regulatória da ICANN nos programas de expansão dos gTLDs no Sistema de Nomes de Domínio (DNS) da Internet**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade Nacional de Brasília, p. 300. 2018, p. 128.

343 Para uma distinção entre regulação e governança, consultar: BIANCHI, José Flavio. **A ICANN entre governança e Regulação: análise da atuação regulatória da ICANN nos programas de expansão dos gTLDs no Sistema de Nomes de Domínio (DNS) da Internet**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade Nacional de Brasília, p. 300. 2018, p. 124-ss. e KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 26-29, 71-ss. Para uma diferenciação que abranja, ainda, o termo *compliance* ver: *ARANHA*, Márcio Iorio. ***Compliance*, governança e regulação**. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 437-452.

Lobel[344], dos modelos híbridos de regulação abordados em alguma medida por David Trubek e Louise Trubek[345] e da ideia de regulação responsiva trazida por Braithwaite,[346] em sua obra "*Regulatory Capitalism: How it Works, Ideas for Making it Work Better*".

Alguns desses conceitos retornarão ao centro da análise, no entanto, para o momento, seguiremos na abordagem das teorias regulatórias do ciberespaço.

1.1. Entendendo as teorias do ciberespaço

Keller[347] aponta que a natureza técnica da Internet se define a partir da convivência de uma série de tecnologias diferentes, que formam um ecossistema único. Os fenômenos da disrupção[348], da convergência[349] e da digitalização[350] parecem ter emancipado esse ecossistema em um fórum dinâmico de interação entre os indivíduos: o ciberespaço.[351]

---

[344] LOBEL, O. The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought. **Minnesota Law Review**, v. 89, p. 342-370, 2004.

[345] TRUBEK, David M.; TRUBEK, Louise G. Hard and Soft Law in the Construction of Social Europe: The Role of the Open Method Co-Ordination. **European Law Journal**, v. 11, n. 3, p. 343- 64, 2005.

[346] BRAITHWAITE, J. **Regulatory Capitalism: How it Works, Ideas for Making it Work Better**. Cheltenham: Edward Elgar, 2008.

[347] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 2

[348] Conceito abordado por Bower e Christensen para designar inovações tecnológicas com potencial disruptivo, isto é: de inaugurar um novo seguimento de produto ou tecnologia aptos a colocar fim a modelos e seguimentos pretéritos. Assim, nem toda inovação tecnológica é disruptiva, mas, apenas aquela com potencial de substituir, na competição de marcado, modelos e opções do passado. BOWER, Joseph L; CHRISTENSEN, Clayton M. Disruptive Technologies: Catching the Wave. **Harvard Business Review (HBR)**, 1995. Disponível em: https://hbr.org/1995/01/disruptive-technologies-catching-the-wave. Acesso em: 25 out. 2022.

[349] A convergência é frequentemente definida, em termo gerais e simplificados, como um processo pelo qual as telecomunicações, as tecnologias da informação e as mídias em geral, setores que originalmente operam largamente de forma independente uns dos outros, passam a se desenvolver conjuntamente. Isso tem ocorrido em níveis diferentes, por exemplo, nas infraestruturas, nos dispositivos destinados aos usuários finais ou em serviços. Segundo Stobbe e Just, podemos definir convergência como um processo de mudança qualitativa que conecta dois ou mais mercados existentes, anteriormente distintos. A força motriz desse processo seria o desenvolvimento de uma nova tecnologia ou a integração de diversas tecnologias que permitem infraestruturas, dispositivos destinados a usuários finais ou serviços adquirirem novas funcionalidades. Outra importante fonte de convergência de mercado, para os autores, é a mudança nas características de um produto resultando em novas tecnologias (convergência do produto). STOBBE, Antje; JUST, Tobias. The dawn of technological convergence. Economics 56. **Deutsche Bank Research**. Frankfurt a.M., may 3, 2006, p. 3.

[350] Digitalização é o processo de transformar um documento físico para o formato digital, através de dispositivos e instrumentos apropriados. É um termo genérico utilizado para descrever a transformação digital da sociedade e da economia, também chamado de desmaterialização.

[351] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 27.

Como forma de compreender as características evolutivas da regulação do ciberespaço, a abordagem escolhida partirá das principais correntes teóricas sobre o tema, tratando dos ciberlibertários e excepcionalistas; dos ciberpaternalistas e da regulação pelo código.

1.1.1. Os ciberlibertários e excepecionalistas e a rejeição à regulação estatal

A expansão da Internet para o uso civil, a partir dos anos 90, foi acompanhada de um movimento teórico que, por diferentes razões, entendia pela impossibilidade de a Internet ser regulada.

Desde a criação da World Wide Web em 1989 por Tim Berners-Lee, a rede se expandiu em funcionalidades e sistemas de comunicação cada vez maiores e mais abrangentes. Em meio a esse novo ambiente, os usuários foram influenciados pela possibilidade de interação em tempo real por e-mails, *chats*, redes sociais, aplicativos e plataformas, ainda que carregados com impressões e sinais do mundo físico.[352]

Esse ambiente virtual até então enigmático, com alcance global, e no qual, num primeiro momento, ainda reinava o mito do anonimato, a possibilidade de implementação do direito tradicional, seja por meio da lei ou do cumprimento de decisões judiciais, ainda era um ponto de incerteza. De tal forma que, em um primeiro momento, a literatura especializada se debruçou sobre a viabilidade ou não de se regular a Internet. [353]

Nesse sentido, os ciberlibertários e excepcionalistas foram os primeiros a considerar de algum modo a regulação do ciberespaço, porém com o propósito de refutá-la. Esses autores defendiam, em última instância, que as características únicas da Internet impediriam a aderência das formas tradicionais do direito.

Para uma breve contextualização histórica do tema, nessa primeira fase do debate em torno da regulação do ciberespaço, John Perry Barlow, um dos fundadores da *Eletronic Frontier Foundation*, teve um papel fundamental. Conhecido por ter declarado a independência do ciberespaço, em 1996, numa reunião do Fórum Econômico Mundial,

---

[352] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 45. O autor ainda aponta como características desse período: "As perspectivas do mercado on-line também afetaram de forma incisiva a economia compartilhada e a forma como as empresas e os governos têm sido redesenhados, notadamente porque a gestão estratégica de dados se transformou numa *commodity* valiosa."

[353] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 2

Barlow[354] foi o responsável pela defesa veemente de que o ciberespaço era um nicho de interação social que deveria permanecer isolado da influência dos atores estatais.[355] [356]

Pautado por um considerável idealismo em torno da perspectiva de que a internet era capaz de proporcionar melhores condições de interação, *accountability* e maior autonomia aos indivíduos, Barlow acreditava que o ciberespaço deveria ser um local de emancipação dos indivíduos, livre das influências do mundo físico, com ampla liberdade de expressão e exercício de direitos.[357]

O Ciberespaço era sentido como uma força democratizante, descentralizada, sem limites territoriais e imune ao controle institucional. Barlow recusava, até mesmo, a legitimidade dos governos em exercer qualquer controle sobre aquele que considerava um novo espaço, o qual deveria ser organizado a partir da autodeterminação da própria comunica virtual. Ao defender que a Internet não seria suscetível à regulação pelo direito dos Estados, tal visão – comum a muitos técnicos e acadêmicos que participaram ativamente dos primeiros anos de implementação da Internet e da Rede Mundial de Computadores – alimentou a percepção de parte da academia de que esse novo mundo seria impossível de controlar.[358] [359]

Essas ideias deram origem a duas correntes ideológicas distintas o ciberlibertarismo e o excepcionalismo. Embora seja possível encontrar referências aos mesmos autores como ciberlibertários ou excepcionalistas, isso ocorre porque, apesar da

---

[354] COHN, Cindy. **John Perry Barlow, Internet Pioneer, 1947-2018**. Disponível em: https://www.eff.org/deeplinks/2018/02/john-perry-barlow-internet-pioneer-1947-2018. acesso em: 21 set. 2022.

[355] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 45-47.

[356] BARLOW, John Perry. **A Declaration of the Independence of Cyberspace**. Disponível em: https://www.eff.org/cyberspace-independence. Acesso em: 21 set. 2022.

[357] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 14.

[358] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 127.

[359] "(...) a ideia geral de que a Internet era difícil ou impossível de se regular era, na época, um lugar-comum político, jornalístico e acadêmico, dado como certo. Por exemplo, refletindo sua época, em 1998 o presidente Clinton fez um discurso sobre os esforços da China para controlar a Internet. "Agora, não há dúvida de que a China está tentando reprimir a Internet – boa sorte", disse ele. "É como tentar pregar gelatina na parede." Tradução do autor. No original: "(...) but the general idea that the Internet was difficult or impossible to regulate was, at the time, a political, journalistic and academic commonplace, taken for granted. For example, reflecting his times, in 1998 President Clinton gave a speech about China's efforts to control the Internet. "Now, there's no question China has been trying to crack down on the Internet—good luck" he said. "That's sort of like trying to nail Jello to the wall". WU, Tim. **Is Internet Exceptionalism Dead?**. In: SZOKA, Berin; MARCUS, Adam (ed.). The Next Digital Decade: Essays on the Future of the Internet. Washington, D.C: TechFreedom, 2010, p. 180. Para mais, ver: GOLDSMITH, Jack L; WU, Tim. **Who controls the internet?: illusions of a borderless world**. New York: Oxford University Press, 2006.

origem comum, fundada na idade de impossibilidade de regulação da Internet, os fenômenos tiveram evoluções distintas. Conforme registra Keller:[360]

> Enquanto o ciberlibertarismo seria definido pela convicção de que a Internet não pode ou não deve ser regulada, o excepcionalismo se basearia, essencialmente, no seu tratamento como algo único, extraordinário. A impossibilidade ou impertinência da regulação poderia figurar como consequência dessa excepcionalidade, mas também seriam possíveis outros cenários, em que o tratamento excepcional geraria não a ausência total de regulação, mas sim a necessidade de uma regulação exclusiva, customizada.

Essa diferença semântica contribui para uma sobrevida maior das ideias excepcionalistas, diante da maior flexibilidade de seu discurso.

São expoentes dessas correntes, John Perry Barlow,[361] David Clark[362] – ambos refutando a própria legitimidade dos governos em regular o ciberespaço, propondo uma espécie de autorregulação pela própria comunidade –, David Post e David Johnson[363] - os dois apregoando a impossibilidade de regular a Internet, em maior parte, em razão de seu alcance global, o que demandaria um marco regulatório independente das doutrinas vinculadas às jurisdições territoriais.

Essas ideias, entretanto, não se sustentaram por longo período. Conforme destaca Sombra:[364]

> À medida que a expansão do ciberespaço proporcionou o surgimento de novas funcionalidades, com outras interfaces, camadas e conexões, essas características o levaram a extrapolar os seus propósitos iniciais, os quais passaram a demandar maior intervenção estatal sob pena de se transformar numa arena anárquica. Barlow não estava sozinho na defesa do ciberespaço como um lugar isolado, despido de associações com o mundo físico, no qual os agentes reguladores não teriam condições de meramente transpor conceitos e teorias. Autores como

---

360 KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 127.

361 COHN, Cindy. **John Perry Barlow, Internet Pioneer, 1947-2018**. Disponível em: https://www.eff.org/deeplinks/2018/02/john-perry-barlow-internet-pioneer-1947-2018. acesso em: 21 set. 2022.

362 SALTZER, Jerome H.; REED, David Patrick; CLARK, David D. End-To-End Arguments in System Design. M.I.T. Laboratory for Computer Science. **ACM Transactions on Computer Systems**, v. 2, n. 4, nov. 1984, p. 277-288. Disponível em: https://groups.csail.mit.edu/ana/Publications/PubPDFs/End-to-End%20Arguments%20in%20System%20Design.pdf. Acesso em: 12 ago. 2022.

363 JOHNSON, David. R, POST, David. Law & Borders: The Rise of Law in Cyberspace, Stanford Law Review, n. 48, p. 1.367-1.403, 1996, p. 1370 e CRAWFORD, Susan P. The Internet and the Project of Communications Law, **UCLA Law Review**, n. 55, pp. 360-393, 2007, p. 379

364 SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 45-47.

> Post e Johnson e ativistas como Julien Assange também foram ferrenhos defensores do ciberlibertarismo e da perspectiva da impossibilidade de delimitação de jurisdição, território e soberania, com argumentos ainda mais contundentes do que os apresentados por Barlow. A despeito da posterior constatação das manifestações de poder das grandes corporações e do poder de vigilância estatal, Post, Johnson e Assange não reviram suas posições históricas iniciais para indicar a necessidade de alguma espécie de regulação.

O ponto crucial à época, e que até hoje levanta controvérsia, envolve a forma como a regulação seria concebida, diante da inexistência de fronteiras físicas que pudessem delimitar a rede de conexões e controlar a arquitetura desses sistemas, sobretudo do ponto de vista dos Estados e de sua soberania.

Conforme destaca Sombra, ainda hoje: [365]

> (...) essa questão representa uma incógnita, embora a regulação tenha aos poucos se tornado um fenômeno necessário e factível para que o ciberespaço pudesse prover tudo aquilo que dele se esperava. Um desses fatores de incompreensão é a proteção dos dados e privacidade que, como observam Post e Johnson, seriam incapazes de delimitação territorial em termos de fluxo transnacional de dados. É sob esse pano de fundo que Baldwin indica que um conjunto descentralizado de comunicações de proporções globais somente poderia funcionar se houver padrões mínimos de interoperabilidade:
> "It is undisputed that the Internet was only able to grow into a global network because it had met the critical operational requirements which any decentralised set of communications systems must meet in order to function as a single cohesive system. These requirements are compatibility, identification, and interconnectivity."[366]
> O surgimento de fenômenos semelhantes aos do mundo físico fez com que os tribunais apreciassem temas relacionados ao ciberespaço não como algo além e contraposto a ele, mas a partir de uma metáfora nele pautada na qual o consideravam um lugar próprio e específico, uma arena, e não um simples protocolo ou a peça de um código, como criticam Dan Hunter[367] e Mark Lemley[368]. Com o surgimento das ameaças a direitos, aos poucos as respostas dos ciberlibertários tornaram-se insuficientes e ilusórias para lidar com os crimes cibernéticos como a pedofilia, os furtos de dados pessoais e corporativos, a vigilância em massa, o ciberterrorismo, a pornografia de vingança e o discurso de ódio.

---

[365] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 45-47.

[366] Tradução do autor: "É indiscutível que a Internet só foi capaz de se transformar em uma rede global porque atendeu aos requisitos operacionais críticos que qualquer conjunto descentralizado de sistemas de comunicação deve atender para funcionar como um sistema único e coeso. Esses requisitos são compatibilidade, identificação e interconectividade".

[367] HUNTER, Dan. **Cyberspace as Place, and the Tragedy of the Digital Anticommons**. SSRN. Disponível em: https://dx.doi.org/10.2139/ssrn.306662. Acesso em: 15 jul. 2022.

[368] LEMLEY, Mark A. **Place and Cyberspace**. Disponível em: http://dx.doi.org/10.2139/ssrn.349760. Acesso em 20 jul. 2022.

> (...)
> O ápice da derrocada do movimento ciberlibertário ocorreu após países como China, Arábia Saudita e Coréia do Norte implementarem medidas de bloqueio ao acesso da internet em seus territórios, o que se repetiu durante as manifestações sociais na Primavera Árabe. Isso demonstrou que a inexistência de fronteiras, território e soberania não eram aspectos decisivos para a regulação do ciberespaço, visto que poderiam facilmente superar essas barreiras com o emprego de leis extraterritoriais como a General Data Protection Regulation (GDPR), o Marco Civil da Internet (MCI) e a Lei Geral de Proteção de Dados Pessoais (LGPD). A conjugação de todos esses aspectos contribuiu sobremaneira para que um novo movimento teórico, conhecido como ciberpaternalismo, apresentasse soluções alternativas para o ciberespaço.

O movimento ciberlibertário guarda expressiva correlação com o modelo de autorregulação de proteção da privacidade e dados pessoais a ser analisado. No entanto, a premissa imposta no ideário coletivo de que a rede não poderia ser regulada, parece ter caído por terra.

1.1.1.2. As influências excepcionalistas na regulação do ciberespaço

Eric Goldman, [369]em contribuição à obra "*The Next Digital Decade: Essays on the Future of the Internet*", verifica três ondas de influência das ideias excepcionalistas sobre a formulação de políticas públicas direcionadas à Internet.

A primeira delas, identificada como *Utopismo da Internet (Internet utopianism)*, descreve o período próximo à metade da década de 1990, no qual se fantasiava sobre uma "utopia" da Internet que superaria os problemas inerentes a outras mídias sociais. Alguns reguladores, temendo o rompimento dessa possível utopia, procuraram tratar a Internet de forma mais favorável do que outras mídias. É exemplo disso, uma lei nos EUA que imunizava categoricamente os provedores *on-line* da responsabilidade pela publicação da maioria dos tipos de conteúdo de terceiros. Essa norma foi promulgada (em parte) "para preservar o vibrante e competitivo mercado livre que existe atualmente para a Internet e outros serviços interativos de computador, sem restrições por regulamentação federal ou estadual". [370] O estatuto era claramente excepcionalista porque trava provedores *on-line*

[369] GOLDMAN, Eric. **The Third Wave of Internet Exceptionalism**. In: SZOKA, Berin; MARCUS, Adam (ed.). The Next Digital Decade: Essays on the Future of the Internet. Washington, D.C: TechFreedom, 2010, p. 165.

[370] Tradução do autor, com adaptações. No original: "In the mid-1990s, some people fantasized about an Internet "utopia" that would overcome the problems inherent in other media. Some regulators, fearing disruption of this possible utopia, sought to treat the Internet more favorably than other media.

de modo mais favoráveis do que editores *off-line* – mesmo quando publicavam conteúdo idêntico.

Mais tarde, na década de 1990, o pêndulo regulatório oscilou na outra direção. Na segunda onda regulatória, conhecida como *Paranoia da Internet (Internet Paranoia)*, os reguladores ainda adotavam o excepcionalismo da Internet, mas, em vez de favorecer a Internet, os reguladores trataram a Internet com mais severidade do que a atividade *off-line* análoga.

Por exemplo, em 2005 um site do Texas chamado *Live-shot.com* anunciou que ofereceria "caça pela Internet". O site permitia que os clientes pagantes controlassem, via Internet, uma arma em sua fazenda de jogos. Um funcionário monitorava manualmente a arma e podia ignorar as instruções do cliente. O site queria dar às pessoas que de outra forma não poderiam caçar, como paraplégicos, a oportunidade de aproveitar a experiência de caça.[371]

A reação regulatória à caçada na Internet foi rápida e severa. Mais de três dúzias de estados proibiram a caça pela Internet nos Estados Unidos. A Califórnia proibiu também a pesca pela Internet para já se garantir. No entanto, os reguladores nunca explicaram como a caça na Internet é mais censurável do que a caça no espaço físico.[372]

Por exemplo, a senadora da Califórnia, Debra Bowen, criticou a caça na Internet porque "não é caça; é um videogame pay-per-view desumano e exagerado que usa animais vivos para praticar tiro ao alvo. Atirar em animais vivos pela Internet exige absolutamente nenhuma habilidade de caça e deve ser ofensivo para todo caçador

---

47 U.S.C. § 230 ("Section 230"—a law still on the books) is a flagship example of mid-1990s efforts to preserve Internet utopianism. The statute categorically immunizes online providers from liability for publishing most types of third party content. It was enacted (in part) "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."2 The statute is clearly exceptionalist because it treats online providers more favorably than offline publishers—even when they publish identical content". GOLDMAN, Eric. **The Third Wave of Internet Exceptionalism**. In: SZOKA, Berin; MARCUS, Adam (ed.). The Next Digital Decade: Essays on the Future of the Internet. Washington, D.C: TechFreedom, 2010, p. 165.

[371] Tradução do autor, com adaptações. No original: "For example, in 2005, a Texas website called Live-shot.com announced that it would offer "Internet hunting." The website allowed paying customers to control, via the Internet, a gun on its game farm. An employee manually monitored the gun and could override the customer's instructions. The website wanted to give people who could not otherwise hunt, such as paraplegics, the opportunity to enjoy the hunting experience". GOLDMAN, Eric. **The Third Wave of Internet Exceptionalism**. In: SZOKA, Berin; MARCUS, Adam (ed.). The Next Digital Decade: Essays on the Future of the Internet. Washington, D.C: TechFreedom, 2010, p. 165-166.

[372] Tradução do autor, com adaptações. No original: "The regulatory reaction to Internet hunting was swift and severe. Over three-dozen states banned Internet hunting. California also banned Internet fishing for good measure. However, regulators never explained how Internet hunting is more objectionable than physical space hunting". GOLDMAN, Eric. **The Third Wave of Internet Exceptionalism**. In: SZOKA, Berin; MARCUS, Adam (ed.). The Next Digital Decade: Essays on the Future of the Internet. Washington, D.C: TechFreedom, 2010, p. 166.

legítimo". As observações da senadora Bowen refletem inúmeras assunções sobre a natureza da caça e o que constitui um jogo justo. No final, no entanto, "caçar" pode ser apenas caçar, caso em que a resposta à caça na Internet pode ser apenas um exemplo típico de excepcionalismo adverso da Internet. [373]

Keller[374] ainda identifica nessa fase o caso das tecnologias de filtro de conteúdo, conhecidas por implementar mecanismos de censura privada com restrições desproporcionais à liberdade de expressão.

Por fim, a terceira onda regulatória seria a *Proliferação do Excepcionalismo (Exceptionalism Proliferation)*, quando o surgimento de cada nova tecnologia baseada na Internet inspirou regulações específicas a ela direcionadas. Aqui, o autor identifica um movimento de multiplicação de quadros regulatórios específicos a determinados serviços e enquadra as regulações direcionadas, por exemplo, a sites de redes sociais, que recebem tratamento próprio.[375]

Conforme destaca: "os reguladores ainda estão engajados no excepcionalismo da Internet, mas cada novo avanço na tecnologia da Internet gerou regulamentações excepcionalistas para essa tecnologia". [376] Por exemplo, o surgimento de blogs e mundos virtuais ajudou a iniciar um impulso em direção a uma regulamentação específica para blogs e mundos virtuais. Com efeito, o excepcionalismo da Internet dividiu-se em bolsões de iniciativas excepcionalistas menores.

As respostas regulatórias a sites de redes sociais como Facebook e MySpace são um excelente exemplo da fragmentação do excepcionalismo da Internet. Em vez de regular esses sites como outros sites, os reguladores buscaram leis específicas para sites

---

[373] Tradução do autor, com adaptações. No original: "For example, California Sen. Debra Bowen criticized Internet hunting because it "isn't hunting; it's an inhumane, over the top, pay-per-view video game using live animals for target practice .... Shooting live animals over the Internet takes absolutely zero hunting skills, and it ought to be offensive to every legitimate hunter. Sen. Bowen's remarks reflect numerous unexpressed assumptions about the nature of "hunting" and what constitutes fair play. In the end, however, hunting may just be "hunting," in which case the response to Internet hunting may just be a typical example of adverse Internet exceptionalism.". GOLDMAN, Eric. **The Third Wave of Internet Exceptionalism**. In: SZOKA, Berin; MARCUS, Adam (ed.). The Next Digital Decade: Essays on the Future of the Internet. Washington, D.C: TechFreedom, 2010, p. 166.

[374] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 2

[375] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 2

[376] Tradução do autor, com adaptações. No original: "Regulators are still engaged in Internet exceptionalism, but each new advance in Internet technology has prompted exceptionalist regulations towards that technology". GOLDMAN, Eric. **The Third Wave of Internet Exceptionalism**. In: SZOKA, Berin; MARCUS, Adam (ed.). The Next Digital Decade: Essays on the Future of the Internet. Washington, D.C: TechFreedom, 2010, p. 166.

de redes sociais, como requisitos para verificar a idade dos usuários, combater predadores sexuais e suprimir conteúdo que promova a violência. O resultado é que a regulamentação de sites de redes sociais difere não apenas das empresas off-line, mas também de outros sites.[377]

Essa abordagem dá a ideia da plasticidade do excepcionalismo, que o levou a ter uma sobrevida maior que o ciberlibertarismo. A ideia de rejeitar a regulação pura e simplesmente por eventual restrição à liberdade ou à ilegitimidade de governos, acabou por ser refutada pela própria prática. De um lado, a falta de regulação dos momentos iniciais da internet defendida pelos dois grupos levou a uma gama de problemas que a liberdade conferida aos membros das comunidades virtuais não poderiam equacionar por si sós, e, de outro, o recurso à extraterritorialidade da lei demonstrou a possibilidade de aplicação além-mar do direito tradicional.

O recurso à extraterritorialidade levou, inclusive, à aplicação de multas severas por parte da União Europeia (e seus estados-membros) a empresas como o Google e o Facebook, seja pela aplicação da legislação em matéria de privacidade e proteção de dados pessoais, seja em matéria antitruste.[378]

De outro lado, a plasticidade dos conceitos exepcionalistas permitiram sua adaptação teórica a diferentes momentos, refletindo em uma duração maior de suas ideias.

No entanto, como diagnostica Keller,[379] apesar da diferença semântica fazer do excepcionalismo um recurso teórico mais complexo e diverso, a sua essência não é pacificada na literatura. Isto é, também a ideia de que a Internet constituiria algo único, sujeita a tratamento especial (ainda que isso não seja sinônimo de um "não tratamento"), também é contestada.

---

[377] Tradução do autor, com adaptações. No original: "Regulatory responses to social networking sites like Facebook and MySpace are a prime example of Internet exceptionalism splintering. Rather than regulating these sites like other websites, regulators have sought social networking site-specific laws, such as requirements to verify users' age, combat sexual predators and suppress content that promotes violence. The result is that the regulation of social networking sites differs not only from offline enterprises but from other websites as well". GOLDMAN, Eric. **The Third Wave of Internet Exceptionalism**. In: SZOKA, Berin; MARCUS, Adam (ed.). The Next Digital Decade: Essays on the Future of the Internet. Washington, D.C: TechFreedom, 2010, p. 167.

[378] Veja sobre a aplicação de leis concorrenciais em: HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Rio de Janeiro: Forense, 2021, p. 98-ss.

[379] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 129-130.

São exemplos disso os trabalhos de Lessig,[380] Yochai Benkler,[381] Sustein[382] e de Tim Wu,[383] que serão tratados mais à frente.

1.1.2. Os Ciberpaternalistas e o protótipo da arquitetura

Depois dos excepcionlistas e, com muito mais intensidade,[384] os ciberlibertários, terem declarado o ciberespaço como o território das liberdades, insuscetível de controle estatal em termos de fronteiras e soberania, os ciberpaternalistas apresentaram uma outra visão do processo de regulação, cuja análise envolvia o controle, a filtragem e a *blacklist* de sítios eletrônicos e softwares de acesso proibido.[385] [386]

E isso se deve, em parte à miríade de riscos nascentes nesse espaço de ampla liberdade. Ilustram esses problemas a indagação de Sombra quanto ao dogma ciberlibertário:[387]

> Se os ciberlibertários estavam corretos em sua perspectiva, como os Estados deveriam lidar com o anonimato na internet, os crimes praticados por meio da *deep web – Dot Onion/Tor –*, a pornografia infantil, o *ciberbullying*, a lavagem de dinheiro e os furtos, as fraudes, os hackers e as extorsões? Como os Estados iriam regular o empreendedorismo evasivo, as novas plataformas disruptivas como o Uber e o AirBnB, a criptografia e os contratos de empréstimo por meio de sistemas peer-to-peer (P2P)? De fato, o ciberespaço seria inconcebível enquanto arena democrática sem alguma forma de regulação, uma vez que não seria possível identificar o papel dos atores

[380] Em sua obra Code e sua atualização Code 2.0: LESSIG, Lawrence. **Code: And Other Laws of Cyberspace, Version 2.0**. New York: Basic Books, 2006.
[381] BENKLER, Yochai. **The Wealth of Networks: How Social Production Transforms Markets and Freedom**. New Haven: Yale University Press, 2006. Disponível em: http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf. Acesso em: 25 set. 2022.
[382] SUNSTEIN, Cass. **Republic.com**. Princeton: Princeton University Press, 2002.
[383] WU, Tim. **Is Internet Exceptionalism Dead?**. In: SZOKA, Berin; MARCUS, Adam (ed.). The Next Digital Decade: Essays on the Future of the Internet. Washington, D.C: TechFreedom, 2010, p. 180. Para mais, ver: GOLDSMITH, Jack L; WU, Tim. **Who controls the internet?: illusions of a borderless world**. New York: Oxford University Press, 2006.
[384] Lembre-se da plasticidade da concepção excepcionalista, que permitiu-lhe se amoldar a diferentes fases regulatórias.
[385] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 48.
[386] Veja-se que a França e a Austrália, por exemplo, aprovaram leis que admitem a filtragem e a lista negra de controle e vigilância com o objetivo de proteger os direitos autorais. O AirBnB promoveu mudanças na política sobre *home sharing* depois que a França e o Reino Unido adaptaram suas leis para tributar os serviços por eles prestados. Ou seja, em comum, todos esses exemplos evidenciam que não há uma esfera de interação social infensa à regulação estatal, ainda que ela ocorra em menor intensidade ou com uma momentânea tolerância. SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 49.
[387] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 48.

> envolvidos, quem representa e quem atua em nome da sociedade. Nesse contexto, a representação política e a *accountability* seriam apenas dois dos elementos político-democráticos cuja identificação e consolidação no ciberespaço constituiriam um desafio da ausência de regulação, em especial porque a deliberação e o processo decisório ainda se revelam pouco maduros.

Essa mudança no paradigma conceitual a respeito da possibilidade de regulação do ciberespaço foi acompanhada de intensa produção dogmática:

1.1.2.1. Joel Reidenberg e a Lex Informatica

O primeiro autor a criticar as falhas do modelo libertário foi Joel Reidenberg,[388] ainda que em parte concordasse com Post e Johnson acerca das fronteiras imaginárias e o processo de desintegração das referências territoriais. Enquanto fundador da corrente ciberpaternalista, Reidenberg estabeleceu uma aproximação entre a teoria do direito no ciberespaço e a *Lex Mercatoria*,[389] processo a que ele denominou de *Lex Informatica*.[390]

O ciberespaço, na visão de Reidenberg, não era imune a intervenções regulatórias; o problema residia, no entanto, na correta identificação dos atores responsáveis por essa regulação. Em sua obra eles os identificou a partir de duas fronteiras de elaboração do processo decisório, os quais envolviam o Estado e o setor privado (os técnicos e os cidadãos). [391]

Reidenberg acreditava que o modelo de regulação estatal ou compreensivo, não era condizente com as características do ciberespaço, pois demandava também a participação dos técnicos e dos cidadãos. Para Reidenberg esse processo de interação tinha alguns componentes e regras especiais pelo fato de serem baseados em acordos

---

[388] REINDENBERG, Joel R. Lex Informatica: The Formulation of Information Policy Rules Through Technology. **Texas Law Review**, v. 76, n. 3, 1998, p. 553-584. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/tlr76&i=571. Acesso em: 24 out. 2021.

[389] Conforme destaca Sombra: "Ao longo de sua história, que remonta ao merchant law medieval, a Lex Mercatoria 188 tornou-se uma das mais exitosas formas de expressão de modelos jurídicos autônomos e racionais189. Baseada em práticas comerciais usuais do comércio internacional - contratos, costumes, códigos de conduta etc. -, ela desempenha papel semelhante ao de normas elaboradas pelos Estados-nações, de modo que deles independe para atuar190. As corporações comerciais atuavam como verdadeiros Estados e as manifestações de poder impediam que as interações sociais ocorressem de forma paritária. Aquele que detivesse maior influência comercial, seja pela detenção de maior acesso a matérias-primas e produtos, detinha melhores condições de se impor sobre os demais". SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 77.

[390] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 50.

[391] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 50.

contratuais entre provedores de serviço de internet (ISPs-Internet Service Providers) e a arquitetura da rede, o que representava o soerguimento de novas fronteiras controladas pela sociedade, conforme pontua Sombra.[392]

Foi Reidenberg que introduziu a ideia de *regulação por arquitetura* (no caso, arquitetura de sistemas), entendendo que, no tocante à Internet, leis e governos não seriam a única fonte de regulamentação das relações jurídicas. Uma vez que as capacidades tecnológicas e a forma como os sistemas são desenhados impõem regras aos seus usuários, a criação e implementação de políticas de informação seriam inerentes ao desenho das redes e suas configurações. Para o autor, o conjunto de regras que determina o fluxo de comunicação nessas redes de comunicação forma o que ele chamou de *Lex Informatica*. Esta seria uma forma específica de direito posto, com base na arquitetura de sistemas, e que deveria ser não apenas entendida pelos governantes, mas conscientemente reconhecida e até encorajada.[393]

Nas palavras de Sombra:[394]

> A *Lex Informatica* seria, então, o novo modelo de governança do ciberespaço, mediante o qual os tomadores de decisão atuariam pautados pelos processos de regulação desenvolvidos tanto pelos atores estatais, quanto pelos técnicos e as normas sociais, ou seja, um modelo mais próximo da corregulação (...). A regulação mediante intervenções normativas seria apenas uma das formas de interferir nas relações sociais ocorridas no ciberespaço. Reidenberg defendia que a principal atividade regulatória seria realizada por outras fontes primárias: as normas sociais e os desenvolvedores de tecnologia. A posição de Reidenberg era mais consistente do que a dos ciberlibertários, em especial quanto à função das interações sociais no ciberespaço e o poder dos desenvolvedores de tecnologia em enviar "mensagens regulatórias" ao mesmo tempo em que promovem mudanças na arquitetura da rede. Reidenberg teve a capacidade de compreender que valores democráticos e o bem comum são fatores diretamente dependentes de algum tipo de controle da rede, que pode ser efetivado por diferentes atores.

As ideias de Reidenberg foram precursoras de uma regulação mais aberta e participativa, no entanto, ele acreditava que uma abordagem estatal tradicional se tornaria

---

[392] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 48.
[393] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 26.
[394] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 48.

menos efetiva com o passar do tempo, prevendo um caminho não só de abertura, mas possivelmente de substituição dos modelos tradicionais de regulação, para aqueles baseados na arquitetura de sistemas.[395] Assinala o autor em suas conclusões que: "As novas instituições e mecanismos não serão os da regulação governamental tradicional" denotando um possível distanciamento, no futuro, da regulação estatal".[396] [397]

A teoria contrapõe-se a ideia de Sustein[398] de que a Internet não poderia, nem deveria, ser imune ao direito tradicionalmente estabelecido. Foi o que se confirmou na atualidade para a maior parte dos contextos regulatórios. Não obstante, tanto Sustein quanto Lessig[399] demonstraram limitações regulatórias do modelo ciberpaternalista.

1.1.2.2. Lawrence Lessig e a regulação pelo Código

Lessig[400] adotou como ponto de partida para o desenvolvimento do seu marco regulatório a contribuição teórica de Reidenberg, adaptando-a, entretanto, a partir de uma percepção importante: as pessoas não deixam de cometer crimes simplesmente porque a lei os proíbe. Se assim o fosse, a imposição de sanções pela lei seria totalmente desnecessária. Em outras palavras, Lessig demonstra que a regulação é a capacidade do Estado de delimitar comportamentos segundo os seus próprios objetivos, o que, no

[395] Reindenberg afirma que: "a abordagem legal tradicional, como as decisões emitidas pelo governo, será menos eficaz na obtenção dos resultados desejados da política de informação do que uma abordagem tecnológica, como a promoção e o desenvolvimento de sistemas flexíveis e personalizáveis. Padrões técnicos e mecanismos de definição de padrões adquirem características políticas importantes. Para o desenvolvimento de regras de política de informação na Lex Informatica, os formuladores de políticas devem usar estratégias e mecanismos diferentes das abordagens regulatórias tradicionais". Tradução do autor. No original: "the traditional law approach, such as government-issued decisions, will be less effective in achieving desired information policy results than a technological approach, such as the promotion and development of flexible, customizable systems. Technical standards and standard-setting mechanisms acquire important political characteristics. For the development of information policy rules in Lex Informatica, policymakers must use strategies and mechanisms that are different from traditional regulatory approaches". REINDENBERG, Joel R. Lex Informatica: The Formulation of Information Policy Rules Through Technology. **Texas Law Review**, v. 76, n. 3, 1998, p. 553-584, p. 556. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/tlr76&i=571. Acesso em: 24 out. 2021.

[396] Tradução do autor. No original: "The new institutions and mechanisms will not be those of traditional government regulation". REINDENBERG, Joel R. Lex Informatica: The Formulation of Information Policy Rules Through Technology. **Texas Law Review**, v. 76, n. 3, 1998, p. 553-584, p. 593. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/tlr76&i=571. Acesso em: 24 out. 2021.

[397] Veja-se que Reidenberg identificou dois tipos de sistemas regulatórios privados: (1) regimes baseados em acordos contratuais - aqueles entre provedores de internet e clientes; e (2) regimes baseados na arquitetura de rede - os padrões técnicos promulgados por órgãos como a IETF (Internet Engineering Task Force).

[398] SUNSTEIN, Cass. **Republic.com**. Princeton: Princeton University Press, 2002.

[399] LESSIG, Lawrence. **Code: And Other Laws of Cyberspace, Version 2.0**. New York: Basic Books, 2006.

[400] LESSIG, Lawrence. **Code: And Other Laws of Cyberspace, Version 2.0**. New York: Basic Books, 2006.

contexto do ciberespaço, significa a habilidade dos atores estatais de controlar a conduta dos seus cidadãos (como visto ao nos referirmos ao conceito de regulação). Lessig observou que quatro fatores de constrangimento influenciam o comportamento dos indivíduos: a lei, as normas sociais, o mercado e a arquitetura. [401]

No entanto, o autor atribuiu uma eficácia maior à regulação da arquitetura através do código. Isso porque, as leis e normas sociais teriam menor aderência (podendo ser desrespeitadas) sendo, por conseguinte, menos executáveis; já os mercados teriam a tendência de ser mais voláteis no ambiente virtual, surgindo e desaparecendo com maior velocidade e frequência. A arquitetura, por meio do código, ao contrário, seria a maneira mais eficaz de todas de estimular ou prevenir comportamentos, na medida em que poderia determinar esses comportamentos antes mesmo de se concretizarem.

Conforme expõe Keller:[402]

> Lessig consignou uma contribuição fundamental para este debate, que se expressa na constatação de que a Internet é um ambiente regulado em si mesmo, através dos códigos e critérios que estabelecem seus limites físicos e virtuais. O que esses códigos permitem ou não permitem que as pessoas façam no ambiente online já constitui uma forma de regulação inerente ao sistema, que funciona de forma similar à arquitetura no mundo físico. Neste sentido, é possível dizer que o código funciona como a "lei" do ciberespaço, determinando que tipo de comportamentos serão aceitos e quais não. Na altamente difundida expressão cunhada pelo autor: *code is law*.[403]

A premissa essencial de Lessig para a construção da base do seu modelo teórico em torno do código envolve a percepção de que a lei é incapaz, enquanto fonte direta, de regular de forma dinâmica os avanços ocorridos no ciberespaço. Por essa razão, o papel regulatório desempenhado pela lei seria complementado pelo código, pelo mercado e

---

[401] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 48.

[402] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 26.

[403] "Há regulamentação de comportamento na Internet e no ciberespaço, mas essa regulamentação é imposta principalmente por meio de códigos. As diferenças nas regulamentações efetuadas por meio de código distinguem diferentes partes da Internet e do ciberespaço. Em alguns lugares, a vida é razoavelmente livre; em outros lugares, é mais controlada. E a diferença entre esses espaços é simplesmente uma diferença nas arquiteturas de controle - ou seja, uma diferença no código". Tradução do autor. No original: "There is regulation of behavior on the Internet and in cyberspace, but that regulation is imposed primarily through code. The differences in the regulations effected through code distinguish different parts of the Internet and cyberspace. In some places, life is fairly free; in other places, it is more controlled. And the difference between these spaces is simply a difference in the architectures of control--that is, a difference in code". LESSIG, Lawrence. **Code: And Other Laws of Cyberspace, Version 2.0**. New York: Basic Books, 2006.

pelas normas sociais. Sombra[404] avalia que Lessig seria claramente um adepto do modelo de corregulação, o que fica ainda mais evidente pela defesa que faz do código e do papel dos atores privados.

O autor ainda explica que: [405]

> Apesar de ambos serem considerados ciberpaternalistas, uma das particularidades entre as posições de Reidenberg e Lessig está no fato de que este adotou o setor privado como um dos mecanismos regulatórios, porém o subdividiu em duas categorias: o mercado e as normas sociais. A influência da arquitetura é um ponto comum entre ambos os autores, que acreditam na sua capacidade de promover alterações estruturais no ciberespaço. Lessig destaca, entretanto, uma diferença crucial entre a lei e o código: a lei permite que os indivíduos sejam previamente conscientes e responsáveis pelos seus atos, ao passo que o código impõe ajustes aos comportamentos sociais a partir de influências externas.
> Essas diferenças se tornam evidentes quando refletimos sobre as nossas ações no mundo físico, no qual temos consciência da escolha entre furtar ou não um objeto, isto é, a realidade nos dá a faculdade de obedecer ou não a lei, respeitar ou não o direito à proteção de dados e privacidade. A arquitetura, por sua vez, nem sempre assegura a mesma liberdade de escolhas. Se por um lado é possível decidir entre caminhar no meio de uma rodovia sem calçadas, por outro a simples [in]existência de uma porta na entrada de uma casa impede ou dificulta o acesso a ela. Esse exemplo ilustra como o código é capaz de modificar a arquitetura da rede para reproduzir elementos do mundo físico, tal como fronteiras, barreiras, jurisdição e obstáculos.

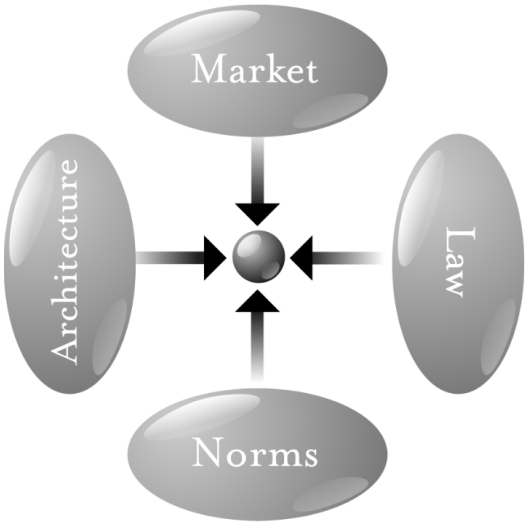
O fato de a tecnologia permitir e estimular que o código e a arquitetura sejam recriados e reconfigurados a todo momento, acaba promovendo um efeito regulatório incessante sobre comportamentos em massa.[406]

O modelo regulatório de Lessig pode ser ilustrado por meio daquilo que ele denomina de *pathetic dot*, isto é, uma representação do modo como o indivíduo é governado, simultaneamente, pela lei, pelo mercado, pelas normas sociais e pela arquitetura, mediante uma força centrípeta e unidirecional, contra a qual pouco pode influir (Figura 1). Esse controle, conforme destaca Sombra,[407] não será realizado apenas pelos atores estatais e pelos tribunais, mas também por atores privados, o que significa

[404] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 52-54.
[405] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 52-55.
[406] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 52-56.
[407] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 58.

que a liberdade se torna a característica mais suscetível de remodelação e de influência no ciberespaço.

Figura 1 - Modelo regulatório de Lawrence Lessig (pathetic dot)



Fonte: LESSIG, Lawrence. **Code and the others laws of cyberspace, version 2.0**. Basic Books, 2006, p.123.

Embora a análise de Lessig tenha sido inovadora, ao menos três aspectos importantes deixaram de ser tratados,[408] alguns deles identificados por David Post[409] e por Viktor Mayer-Schönberger.[410] O primeiro deles é a capacidade recíproca dos indivíduos de influenciar a arquitetura e de ser por ela influenciado, de modo que o *pathetic dot* não seria apenas um ponto perdido no ciberespaço, sujeito à influência de outros atores, mas sem exercer qualquer influência no meio em que vive.[411]

A segunda crítica dirigida ao autor circunscreve-se ao fato de não ter dimensionado de forma apropriada que a legitimidade e a *enforceability* regulatória no ciberespaço são construídas a partir de fronteiras virtuais, com valores sociais e atores

[408] Na avaliação de Thiago Sombra a qual acompanhamos. SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 58.
[409] POST, David G. What Larry doesn't get: code, law, and liberty in cyberspace. **Stanford Law Review**. v. 52. n. 5, p. 1439–1459, 2000, p. 1454–1456.
[410] MAYER-SCHÖNBERGER, Viktor. Demystifying Lessig. **Wisconsin Law Review**. v. 4., p. 713-746, 2008.
[411] Conforme destaca Sombra, não é raro encontrar situações nas quais um único indivíduo é capaz de influenciar massivamente comportamentos, ideias e preferências, sem se valer de mecanismos políticos, de expressão de poder econômico ou de procedimentos deliberativos. Um dos exemplos utilizados pelo autor é o de Shawn Fanning criador do Napster, que teve grande impacto na transformação sofrida pela indústria da música. SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 58.

variados, capazes de influenciar escolhas e comportamentos sob a perspectiva transnacional e em diferentes lugares. Conforme adverte Sombra[412] em um mundo globalizado, a regulação não se limita a um código binário proibir-permitir como supõe grande parte dos agentes reguladores, tampouco é prerrogativa de atores estatais, por mais que os limites estabelecidos pela lei e pelas fronteiras sejam inflexíveis e expressivos. O processo de tomada de decisões no ciberespaço é significativamente plural, assimétrico, policontextual, marcado por decisões cujos parâmetros axiomáticos nem sempre são previamente conhecidos.

Contudo, tal como Post[413] observou, o processo de tomada de decisões no ciberespaço nem sempre tem a característica de escolha coletiva ou de ação política, seja para promover a inovação seja para resguardar direitos como a privacidade e a proteção de dados:

> Não tenho objeções contra a noção de que os códigos/arquiteturas do ciberespaço incorporam valores fundamentais, e não tenho dúvida de que cada um de nós, confrontando o *design* desses novos ciberlugares, enfrenta uma escolha entre diferentes valores. Realmente importa, como apontado por Lessig, se o código de um ciberlugar nos permite ser anônimos ou não, rastreia os rastros de nossos mouses ou não, nos aloca um nome virtual ou dez, nos permite reunir em grupos de 20 ou 50 ou 500, ou nos expõe a muitos ou nenhum encontro aleatório.
> Mas realmente discordo da noção de que as escolhas a serem feitas entre arquiteturas carregadas de valor são, portanto, decisões "políticas" que devem necessariamente estar sujeitas a um processo de tomada de decisão "coletivo". Considere, a título de contraexemplo, o original, e provavelmente o mais poderoso e carregado de valores código/arquitetura de todos: o idioma. As estruturas semânticas e sintáticas do inglês (e de todas as línguas naturais) são restrições arquitetônicas profundas em nossa vida social, como os críticos (e, de fato, o próprio Lessig) gostam de apontar (e, como deve ser notado com justiça, os antropólogos já sabem há algum tempo).
> A linguagem não é apenas "uma forma de comunicar proposições sobre o mundo", é "uma atividade social construtiva", um meio pelo qual e dentro do qual "construímos a realidade social". Como os protocolos de rede com os quais eles se parecem tanto, essas estruturas semânticas e sintáticas incorporam valores importantes e frequentemente fundamentais. Cada um de nós, portanto, tem escolhas a fazer, escolhas sobre como nossas próprias arquiteturas pessoais de realidade social serão constituídas.

[412] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 58.
[413] POST, David G. What Larry doesn't get: code, law, and liberty in cyberspace. **Stanford Law Review**. v. 52. n. 5, p. 1439–1459, 2000, p. 1456–1457.

A última crítica ao marco regulatório de Lessig decorre do fato de ter sido construído com base na experiência de países do sistema *common law*, muitas vezes ignorando as particularidades do sistema continental europeu ou da *civil law*, no qual mesmo as normas sociais, o mercado e a arquitetura atuam segundo parâmetros legais. [414]

Embora as grandes corporações de tecnologia tenham políticas globais de atuação, a pouca dinamicidade do legislador associada à pouca efetividade dos órgãos de fiscalização e controle, têm demonstrado que nos países de sistema *civil law* o Poder Legislativo não é capaz de acompanhar com a mesma velocidade e percepção as inovações no ciberespaço. Um claro exemplo disso é a Lei Geral de Proteção de Dados Pessoais (LGPD), que somente após oito anos de tramitação foi aprovada no Congresso Nacional, e a GDPR (*General Data Protection Regulation* – Regulamento Geral de Proteção de Dados Pessoais – RGPD – Regulation (EU) 2016/679), que teve os seus trabalhos preparatórios iniciados em 2012, só foi aprovado em 2016. [415]

Desse modo, ao contrário do que defendia Lessig, é impossível ignorar o papel desempenhado pelos tribunais e pelo Poder Legislativo nos países de *civil law*. [416]

Por fim, reconhecida que a programação por código determina um número incontável de condutas individuais e coletivas no mundo virtual, com efeitos mais ou menos abrangentes, cabe-nos algumas palavras a respeito dos atores envolvidos nessa intrincada rede regulatória.[417]

É que, conforme expresso por Laura DeNardis, as características da internet fazem das tecnologias que a compõem instâncias de tensão política e cultural, configurando verdadeiros arranjos de poder, construídos a partir de "decisões de *design* que moldam estruturas econômicas e sociais, variando de liberdades civis individuais até políticas de inovação global".[418] Ilustrando a assertiva, Keller,[419] aponta que tanto o exercício individual de liberdade de expressão (condicionado por aquilo que as interfaces

[414] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 58.
[415] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 58.
[416] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 58.
[417] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 26.
[418] DENARDIS, Laura. **The Global War for Internet Governance**. New Haven: Yale University Press. 2014, p. 7.
[419] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 26.

permitem que seja publicado), quanto a possibilidade de disponibilização para o público de determinados serviços virtuais (que precisam obedecer a protocolos de interoperabilidade) dependem do cumprimento de requisitos pré-determinados e materializados através de códigos (veja-se que o bloqueio por região e outras espécies de controle de conteúdo refletem essa marca de controle).[420]

Para Keller,[421] essa condição inerente à forma como a Internet funciona e as suas implicações constitucionais e regulatórias levou parte da doutrina a identificar a inerência de uma "regulação privada" no mundo virtual, expressa nessa influência de atores privados nos comportamentos individuais e coletivos.

Para acessar a Internet, os usuários dependem da intermediação de um conjunto de agentes econômicos, que exercem atividades comerciais distintas. Nela, usa-se navegadores privados para acessar uma rede, que por sua vez é operada por um provedor de serviço privado, para mandar mensagens que viajam por roteadores de propriedade igualmente privada, para acessar websites ou aplicativos onde uma empresa privada presta um determinado serviço. Em cada camada que compõe o acesso virtual (seja ela de infraestrutura física, lógica ou de conteúdo),[422] a conduta de cada agente estaria condicionada às interações permitidas ou não por uma determinada arquitetura de sistemas. Isso implica, no entanto, um problema já diagnosticado por Lessig:[423] "No final, o maior problema será reconhecer essas 'soberanias concorrente', pois cada uma delas influencia o espaço com seus próprios e distintos valores".

Sombra[424] acrescenta, ainda que:

> O código representa, mesmo que de forma ambígua, um novo conceito de liberdade e restrição no ciberespaço, afinal, por meio dele é possível construir, arquitetar ou codificar de modo a proteger os valores que uma sociedade considera fundamental ou até fazê-los desaparecer em dado

[420] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 67.
[421] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 67.
[422] De forma simplificada, a Internet pode ser subdividida em três camadas que representam a cadeia de valor do acesso à rede. A primeira, Camada de Infraestrutura, corresponde a toda parte técnica da Internet -inclui basilarmente o Serviço de telecomunicações. Além dessa, há a Camada lógica, que envolve os Serviços de Conexão à Internet. E, por fim, a camada de conteúdo, que corresponde às aplicações, cujo espaço os usuários têm acesso e utilizam do serviço de informações, inclusive os nomes de domínio.
[423] Tradução do autor. No original: "In the end the hardest problem will be to reckon these 'competing sovereigns', as they each act to mark this space with their own distinctive values". LESSIG, Lawrence. **Code: And Other Laws of Cyberspace, Version 2.0**. New York: Basic Books, 2006.
[424] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 58.

> contexto (...). Um desses pontos sensíveis envolve a utilização do código para a mudança da arquitetura enquanto mecanismo de controle e proteção dados. Ambos desempenham papéis decisivos e cada vez mais o farão, conforme se constata a partir do caso Max Schrems contra o Facebook, no qual a Corte Europeia de Justiça declarou a invalidade do Safe Harbor Agreement entre União Europeia e Estados Unidos, pertinente à transferência intercontinental de dados de cidadãos e empresas americanas e europeias.[425]

A influência dos dois tipos de atores (públicos e provados) é fundamental ao sistema, de modo que uma não pode suplantar a outra.

Veja-se que, de um lado, existe uma cadeia produtiva, de natureza privada, composta por uma série de empresas cujas atividades implicam a influência de comportamentos. A ausência de requisitos legais de legitimidade, como participação, transparência e *accountability*, torna a regulação através dessas tecnologias suscetíveis às críticas que a associam a práticas antidemocráticas ou até ilegais. Contudo, a sua associação a um caráter exclusivamente privado corre o risco de ofuscar a manipulação do código por atores estatais, que também tem o potencial de restringir direitos e liberdades individuais de forma altamente prejudicial.

A capacidade estatal de controlar o comportamento dos cidadãos na Internet já é conhecida. De forma geral, as ferramentas prediletas dos governos são os filtros e bloqueios de conteúdos, que podem ser usados em larga escala – como no simbólico caso do governo chinês que mantém um dos mais difundidos e sofisticados sistemas de controle de acesso a conteúdo, conhecido como *Great Firewall of China*.[426]

1.1.2.3. Yochai Benkler e a regulação por camadas

Embora Yochai Benkler[427] também possa ser considerado um ciberpaternalista, seu modelo regulatório, concebido pela superposição de camadas, adota premissas

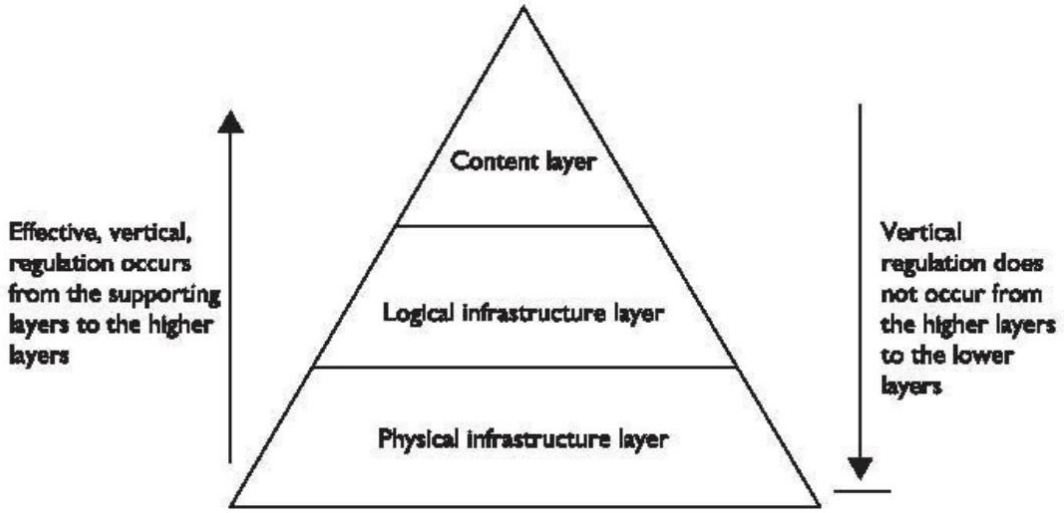
[425] UE. União Europeia. European Court of Justice, Maximillian Schrems v. Data Protection Comissioner (Case 362/2014).

[426] ONI. Open Net Initiative. Country Profiles: China, 2012. Disponível em: https://opennet.net/research/profiles/china-including-hong-kong. Acesso em: 25 out. 2022. 05/01/2018. Uma ampla gama de países também apresentam ferramentas de controle bastante restrito da internet, envolvendo, entre as muitas formas de restrição a aprovação de regulamentações rígidas da mídia doméstica, a possibilidade de responsabilidade delegada por provedores de conteúdo *on-line*, a filtragem *just-in-time* e campanhas de "limpeza" de conteúdos, o bloqueio e listas negras de URLs proibidos, além da limitação de acesso à infraestrutura da rede a pessoas autorizadas, sobretudo pela limitação do governo ao acesso aos provedores de rede. É o caso de países como Rússia, Turquia e Cuba, por exemplo. O perfil de cada país pode ser consultado na *OpenNet Initiative*.

[427] BENKLER, Yochai. **The Wealth of Networks: How Social Production Transforms Markets and Freedom**. New Haven: Yale University Press, 2006.

distintas dos modelos anteriores.[428] Para Benkler, [429] na economia da informação em rede, caracterizada pela descentralização das ações individuais, cada ator exerce um papel relevante e é capaz não apenas de consumir como também de ser um centro de produção. Nesse modelo econômico de produção, a remoção das restrições físicas sobre a efetiva geração de informação tornou a criatividade humana a base do desenvolvimento do ciberespaço.[430] Para explicar o fluxo da informação e como a economia compartilhada funciona, Yochai Benkler desenhou um sistema de comunicação definido em três camadas: física, lógica e de conteúdo.

Figura 2 - Benkler's layers



Fonte: MURRAY, Andrew D..**The Regulation of Cyberspace: Control in the Online Environment**. New York: Taylor e Francisco, 2007, p. 258.

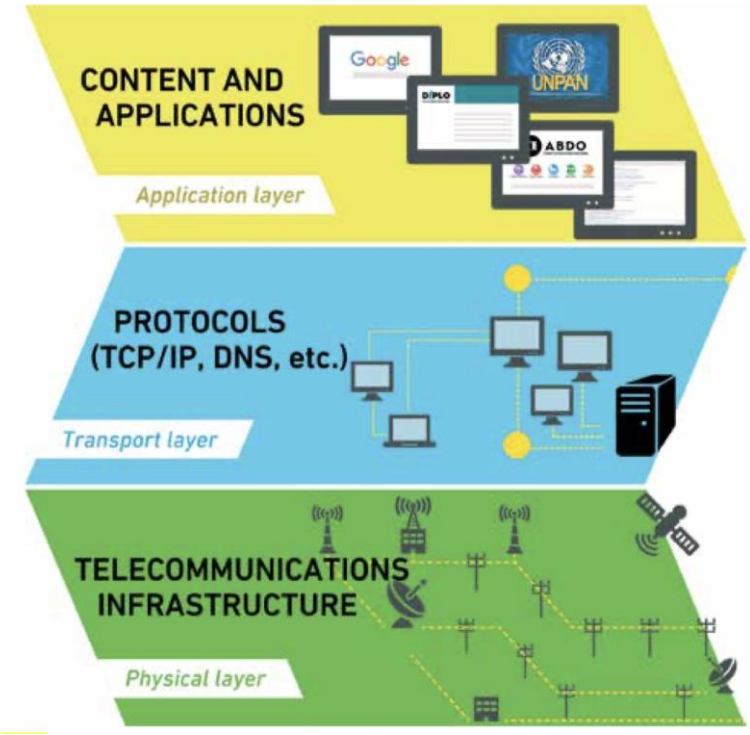
Conforme esclarece Keller[431]:

> A camada física se refere à infraestrutura, incluindo instalações de transmissão (como cabos de fibra óptica e sistemas de telefonia), estruturas e diferentes tipos de hardwares. Nela, destacam-se questões afetas à regulação de infraestrutura física de serviços de comunicações, como interconexão entre provedores de telecomunicações, interoperabilidade e as políticas de expansão da banda larga que

[428] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 60.
[429] BENKLER, Yochai. **The Wealth of Networks: How Social Production Transforms Markets and Freedom**. New Haven: Yale University Press, 2006. BENKLER, Yochai. Freedom in the commons: Towards a political economy of information. **Duke Law Journal**. v. 52, p. 1245-1276, 2002, p. 1248.
[430] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 58.
[431] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 41-42.

permitam universalização do acesso. A camada de código (ou de transporte [ou lógica]) inclui recursos virtuais e padrões técnicos exclusivos da Internet, que se traduzem em recursos críticos para a sua operação – por exemplo, endereços IP, nomes de domínio (junto com o sistema de distribuição dos mesmos conhecido como *Domain Name System* - DNS) e os protocolos padrões da Rede Mundial de Computadores (conhecidos como http – *Hypertext Transfer Protocol* - e html - *Hypertext Markup Language*). Nesse âmbito, os debates de governança orbitam ao redor da definição de protocolos e *design* de *software*, confundindo-se muitas vezes com a atuação dos organismos multisetoriais que definem esses padrões, como a *Internet Corporation for Assigned Names and Numbers* – ICANN e a *Internet Engineering Task Force* – IETF. Por fim, a camada de conteúdo incluiria desde os aplicativos com os quais os usuários finais e os dispositivos interagem diretamente (sendo o mais proeminente deles a própria Rede Mundial de Computadores) até os conteúdos que nele[s] circulam (inclui textos alfanuméricos, áudios, imagens, vídeo e multimídia de todos os tipos). Nela, escolhas de design têm implicações significativas em termos de política pública, que podem se relacionar com áreas tão diversas quanto a privacidade, a imposição de direitos de propriedade intelectual, a proteção dos vulneráveis e os debates que se relacionam de forma geral com liberdade de expressão, censura privada e acesso ao conhecimento (Figura 2)

Figura 3 - Internet Layers



Fonte: KURBALIJA, Jovan. Internet Governance. Malta: DiploFoundation. 7. ed. 2016. Disponível em: https://www.diplomacy.edu/wp-content/uploads/2021/12/AnIntroductiontoIG_7th-edition.pdf. Acesso em: 29 set. 2022.

Sombra[432] pontua que, para Benkler, a comunicação humana no ciberespaço deve seguir as três camadas de regulação para atingir seu propósito, que nada mais é do que o surgimento de capacidades técnicas e práticas em um modelo de não exclusividade de bens, o qual permite o acesso mais econômico à rede, além de evitar o seu controle por uma das partes ou por determinada classe social. Vale destacar, no entanto, que a observância das práticas indicadas pelo autor não transforma o ciberespaço numa arena livre de batalhas entre os atores reguladores sobre a forma como os bens exclusivos, os não exclusivos e as plataformas livres serão facilitados, proibidos ou conjugados de modo a otimizar os benefícios comuns e os individuais.

Benkler parece ter compreendido melhor que Lessig algumas das particularidades das interações sociais no ciberespaço, especialmente pelo paralelo que foi capaz de traçar entre os sistemas de comunicação e cooperação,[433] os quais serão a principal premissa de análise dos *network* comunitaristas, analisados na sequência.

1.1.3. Os Network Comunitaristas e o modelo simbiótico de relação dos atores

Conforme nos expõe Sombra,[434] se por um lado o código e a arquitetura foram as principais características do modelo ciberpaternalista, por outro lado os *network comunitaristas* (comunitarismo em rede), liderados por Andrew Murray, Colin Scott e Paul Bernal, tiveram como foco o fluxo dinâmico da informação no ciberespaço.

As bases teóricas do modelo *network comunitarista* advêm de duas correntes teóricas importantes da sociologia, a Teoria dos Atores em Rede (*Actors Network Theory – ANT*) de Bruno Latour[435] e a Teoria dos Sistemas Sociais (*Social System Theory – SST*),[436] formulada por Niklas Luhmann[437]. A teoria de Lhumann esclarece que o

[432] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 60.
[433] BENKLER, Yochai. **The Penguin and the Leviathan: How Cooperation Triumphs over Self-Interest**. New York: Crown Business, 2011.
[434] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 60.
[435] LATOUR, Bruno. **Reagregando o Social: uma introdução à Teoria do Ator-Rede**. SOUSA, Gilson César Cardoso de (trad.). Salvador/Bauru: Edufba/Edusc, 2012.
[436] MURRAY, Andrew D. Nodes and Gravity in Virtual Space. **Legisprudence**. v. 5. n. 2, oct., 2011, pp. 195-222. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/legisp5&i=195. Acesso em: 29 de set. 2022.
[437] LUHMANN, Niklas. **Introduction to systems theory**. BAECKER, Dirk (ed.). GILGEN, Peter (trad.). Cambridge: Polity Press, 2013.

ciberespaço deve ser compreendido a partir da complexidade do fluxo da informação em sistemas sociais e sua capacidade de afetar toda a organização da sociedade. [438]

Ao contrário dos ciberpaternalistas, os network comunistaristas acreditam que não há um *pathetic dot* estático, incapaz de influenciar e ser influenciado no ciberespaço.[439] Na visão do comunitarismo em rede, o indivíduo não se resume a um ponto amorfo e estático; ele interage de forma ativa, mediante linhas multitudinais de comunicação, dentro de uma rede muito mais ampla do que se supõe.[440] Teubner[441] denomina esse processo de comunicação como "vilas globais", um sistema de pluralismo jurídico formado por diversos atores globais conectados pela informação.[442]

Isso decorre, em parte, da ideia de que a regulação é feita por Atores em Rede (*Actors Network Theory – ANT*)[443] e da Teoria dos Sistemas Sociais (*Social System Theory – SST*)[444], segundo a qual a comunicação, ao possibilitar o acoplamento estrutural entre sistemas sociais diversos, em regra fechados, permite que estes sistemas se comuniquem (através da linguagem), por meio de uma espécie de irritabilidade entre as distintas esferas sociais. Essas teorias permitem enxergar um universo policontextual

---

[438] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 60.

[439] SCOTT, Colin. Regulation in the Age of Governance: the rise of the post-regulatory state In: JORDANA, Jacin; LEVI-FAUR, David. **The Politics of Regulation** – Institutions and Regulatory Reform for the Age of Governance. Cheltenham: Edward Elgar, pp. 145-176, p. 146, 2004. Note-se que o conceito de Estado Pós Regulatório foi precedido pela ideia de um direito pós regulatório, desenvolvida por Gunther Teubner em 1984. Na ocasião, o autor a introduziu como uma resposta à "crise do direito regulatório", expressa principalmente nas deficiências de eficácia e falência institucional do modelo de Bem-Estar Social. Nesse contexto, o autor ofereceu três perspectivas para uma interpretação pós instrumental do direito, capaz de endereçar essas deficiências: a primeira, a partir da sua implementação, demandaria uma revisão das preocupações com resolução de conflitos judiciais em favor de orientação de políticas públicas; a segunda, se refere a processos de desregulação e deslegalização a partir da retirada da intervenção estatal de áreas sociais; já a terceira perspectiva, que chama de controle da autorregulação, se refere à necessidade de adoção de soluções alternativas, que transcendem a distinção entre leis formais e substantivas, favorecendo formas mais abstratas e indiretas de controle pelo direito. Guardadas as particularidades do contexto abordado pelo autor, essas formulações – principalmente a última delas – já apontavam no sentido de uma concepção sobre o papel do Estado deslocada da centralidade do direito hierárquico. TEUBNER, Gunther. After Legal Instrumentalism: Strategic Models of Post-Regulatory Law In: TEUBNER, Gunter (org). **Dilemmas of Law in the Welfare State**. Berlin: De Gruyter, 1986, p. 306.

[440] SCOTT, Colin. Accountability in the Regulatory State. **Journal of Law and Society**. v. 27. n. 1. mar. 2000, p. 38-60. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/jlsocty27&i=46. Acesso em: 27 set. 2022.

[441] TEUBNER, Gunther. **Global Bukowina: Legal Pluralism in the World-Society**. Global Law Without A State. Gunther Teubner (ed.). Dartmouth: Brookfield, 1997, pp. 3-28. SRRN. Disponível em: https://ssrn.com/abstract=896478. Acesso em: 10 set. 2021.

[442] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 60-61.

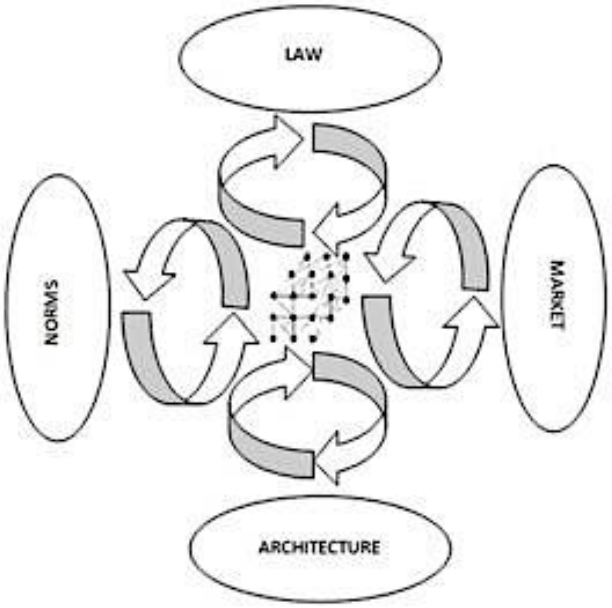
[443] LATOUR, Bruno. **Reagregando o Social: uma introdução à Teoria do Ator-Rede**. SOUSA, Gilson César Cardoso de (trad.). Salvador/Bauru: Edufba/Edusc, 2012.

[444] LUHMANN, Niklas. **Introduction to systems theory**. BAECKER, Dirk (ed.). GILGEN, Peter (trad.). Cambridge: Polity Press, 2013.

(sistemas e atores múltiplos) que, embora isolados, acabam se comunicando em alguns espaços de irritabilidade, por meio de uma estrutura de acoplamento, a linguagem, ou informação.

Os network comunitaristas conseguiram formular um juízo mais interativo do ciberespaço, no qual as normas sociais, a lei, o mercado e a arquitetura podem se influenciar mutuamente e ser influenciados pela comunidade. A percepção estática do *pathetic dot* e a falta de cooperação entre os atores no ciberespaço é talvez a mais interessante contradição dos ciberpaternalistas. A seguir, o esquema proposto pelo network comunitarismo:

Figura 4 - Modelo regulatório de Andrew Murray



Fonte: MURRAY, Andrew D. Nodes and Gravity in Virtual Space. **Legisprudence**. v. 5. n. 2, oct., 2011, pp. 195-222. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/legisp5&i=195. Acesso em: 29 de set. 2022.

Além disso, os *network comunitaristas* não enxergam o ciberespaço como uma arena que demande fatores de constrangimento, mas sim como um lugar em que a regulação pode ser feita por consentimento e outros valores democráticos como a *accountability*,[445] [446] ou seja, o ciberespaço não é um fórum que pertence apenas a agentes

[445] SCOTT, Colin. Accountability in the Regulatory State. **Journal of Law and Society**. v. 27. n. 1. mar. 2000, p. 38-60, p. 48. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/jlsocty27&i=46. Acesso em: 27 set. 2022.
[446] SUNSTEIN, Cass. **Republic.com**. Princeton: Princeton University Press, 2002, p. 74.

reguladores.[447] Isso implica diferentes abordagens regulatórias, sobretudo em modelos híbridos, conforme esclarecem Murray e Scott: [448] [449]

> Da mesma forma, Colin Scott e eu, em nosso artigo *Controlling the New Media*, sugerimos um foco em modelos híbridos de regulação. Nós, como Lessig, sugerimos quatro modalidades de regulação que intitulamos, (1) controle hierárquico, (2) controle baseado na competição, (3) controle baseado na comunidade e (4) controle baseado no *design*. Ao contrário de Lessig, reconhecemos que o desenvolvimento de estruturas regulatórias é frequentemente de natureza orgânica, embora imaginemos que órgãos reguladores, por meio do emprego de controles hierárquicos, moldando a estrutura de tais sistemas organicamente desenvolvidos. Assim, neste artigo, apoiamos o consenso de que os reguladores projetam sistemas regulatórios. Logo, todos esses modelos compartilham uma base comum. Todos são modelados com base na crença de que os projetos regulatórios são baseados em escolhas ativas feitas pelos reguladores: eles sugerem um regulador que trabalha dentro de um ambiente estabelecido e que tem tempo para considerar positivamente as decisões políticas.

De certo modo, os network comunitaristas entenderam de forma mais precisa como o ciberespaço realmente funciona, quais forças o governam, que atores o influenciam e, em grande medida, isso se deve ao fato de terem compreendido como a interação ocorre no sistema depois de um processo complexo caracterizado pelo fluxo dinâmico da informação disponível para os tomadores de decisão, a que denominam de *symbiotic web*.[450] Isso os aproxima ainda mais da premissa da policontextualidade de Teubner nas vilas globais, referida anteriormente.

---

[447] BENKLER, Yochai. **The Wealth of Networks: How Social Production Transforms Markets and Freedom**. New Haven: Yale University Press, 2006, p. 42. Disponível em: http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf. Acesso em: 25 set. 2022.

[448] MURRAY, Andrew D.; SCOTT, Colin. Controlling the New Media: Hybrid Responses to New Forms of Power. **The Modern Law Review**. v. 65. n. 4, 2002, pp. 491–516. JSTOR. Disponível em: http://www.jstor.org/stable/1097592. Acesso em: 29 set. 2022.

[449] Tradução do autor. No original: "Similarly, Colin Scott and myself in our paper Controlling the New Media suggest a focus on hybrid models of regulation. We, like Lessig, suggest four modalities of regulation which we title, (1) hierarchical control, (2) competition-based control, (3) community-based control and (4) design-based control. Unlike Lessig, we acknowledge that the development of regulatory structures is often organic in nature, though we imagine regulatory bodies, through the employment of hierarchical controls, fashioning the structure of such organically developed systems. Thus, ultimately in this paper we support the consensus that regulators design regulatory systems. Thus these models all share a common foundation. All are modelled upon the belief that regulatory designs are based upon active choices made by regulators: they suggest a regulator who works within a settled environment and who has time to positively consider policy decisions". MURRAY, Andrew D..**The Regulation of Cyberspace: Control in the Online Environment**. New York: Taylor e Francisco, 2007, p. 29.

[450] MURRAY, Andrew. Symbiotic Regulation. **John Marshall Journal of Computer and Information Law**, vol. 26, no. 2, Winter 2008, pp. 207-228. HeinOnline, Disponível em: https://heinonline.org/HOL/P?h=hein.journals/jmjcila26&i=211. Acesso em: 15 out. 2022.

Apesar disso, algumas críticas feitas aos ciberpaternalistas podem ser dirigidas, também, aos network comunitaristas especialmente o fato de não considerarem as particularidades dos países de sistema continental europeu ou da *civil law*, no qual a lei exerce um papel de extrema relevância no processo regulatório.[451] Como o Poder Legislativo e o Poder Judiciário nem sempre estão preparados para conduzir a vanguarda dos debates em relação aos temas do ciberespaço, à sociedade é concedida uma larga margem de atuação para modelá-lo por meio da arquitetura e do código, do mercado e das normas sociais, tal como ocorre nos países de sistema *common law*.[452]

2. Os direitos à privacidade e à proteção de dados pessoais

Analisada as vertentes regulatórias do ciberespaço, abordaremos nas próximas seções os modelos regulatórios específicos da privacidade e da proteção de dados, de modo a se compreender de que forma cada um pretendia apresentar respostas aos novos desafios impostos pelo uso da tecnologia.

Para dar conta dessa análise, no entanto, iniciaremos a abordagem nos recordando do alvorecer dos direitos relacionados à privacidade e, mais especificamente, a proteção de dados pessoais, para, depois, conceituarmos os arranjos regulatórios atuais.

2.1. Introito: algumas notas sobre o Direito, a Privacidade e a Tecnologia

A tecnologia sempre teve uma relação conflituosa com a privacidade. O famoso ensaio de Warren e Brandeis[453] acerca da privacidade colocava em perspectiva os avanços técnicos de sua época, especialmente o desenvolvimento da imprensa e da fotografia instantânea. A privacidade, ainda vista como o direito a ser deixado só (*the right to be let alone*), foi concebida como uma reação do homem à possibilidade de invasão de sua vida particular propiciada pela tecnologia.

---

[451] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 65.
[452] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 65.
[453] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, 1890, p. 195.

O caso precursor da matéria, na Inglaterra, foi a publicação não autorizada das correspondência entre Alexander Pope e Jonathan Swift[454]; também nas cortes inglesas marcou o advento de uma noção de privacidade a discussão envolvendo a reprodução gráfica e a venda de objetos da coleção privada do Príncipe Albert e da Rainha Vitória.[455]

Do outro lado do Canal da Mancha, o primeiro caso abordando uma noção primária de privacidade envolveu a atriz francesa Elisa Rachel Félix[456] cujos retratos em seu leito de morte tiveram ampla divulgação pela mídia. E, na Itália, entre os primeiros julgados que envolveram o direito à privacidade, acham-se a exibição de um filme retratando aspectos da vida íntima do cantor Enrico Caruso[457] e as frequentes discussões nos tribunais italianos envolvendo a divulgação de detalhes da vida amorosa do ditador Benito Mussolini e sua amante Clara Petacci.[458]

Os casos são ilustrativos de que a tutela da privacidade, desde seu alvorecer,[459] relaciona-se com as Tecnologias de Informação e Comunicação (TIC's), sobretudo o desenvolvimento da fotografia, da reprodução gráfica, do cinema, do sistema de correspondência, da rede de telégrafos do século XIX,[460] mais tarde, do telefone e da internet. Essa relação, muitas vezes conturbada, marcou os séculos XVIII e XIV.

Algumas teorias relacionadas ao desenvolvimento de nossa linguagem trazem certa luz a essa conflitualidade existe entre a privacidade e as Tecnologia de Informação e Comunicação. A teoria de Robin Dunbar,[461] por exemplo, ao apontar que o

---

[454] Pope v. Curl, 26 Eng. Rep. 608 (1741). No caso, um editor publicou sem autorização a correspondência privada entre ambos, o que originou uma sentença a favor de Alexander Pope reconhecendo-lhe o direito de propriedade sobre suas próprias, na qualidade de autor. William Blackstone. **Commentaries on the Laws of England**. Oxford: Clarendon Press, 1765, p. 407.

[455] Prince Albert v. Stange 64 ER 293 (1848). Discutiu-se a reprodução gráfica e venda de objetos da coleção privada do príncipe. A sentença, outra vez, reconheceu a existência de um direito de propriedade que impediria essa reprodução. CASEMINE. **Prince Albert v. Stange 64 ER 293 (1848)**. Disponível em: https://www.casemine.com/judgement/uk/5a8ff8d260d03e7f57ecdced#. Acesso em: 10 jul. 2022.

[456] Tribunal civil *de la Seine* (16 de junho de 1858, D.P., 1858.3.62). Após sua morte, retratos de Rachel no leito de morte foram amplamente publicados, o que fez com que sua irmã solicitasse ao Tribunal a cessação destas publicações. O tribunal o fez, em respeito à dor da família. Raymond Lindon. **Une création prétorienne**: Les droits de la personnalité. Paris: Dalloz, 1974, p. 11.

[457] Tribunal de Roma, sentença de 14 de setembro de 1953. Um filme, *Leggenda di una voce*, expôs aspectos da vida íntima de Enrico Caruso, motivando reclamações por parte de seus familiares. O Tribunal romano reconheceu em sentença a inadequação da exposição de alguns desses aspectos da vida do retratado que, na percepção de De Cupis, marcou o início do reconhecimento do *diritto alla riservatezza* na Itália. Adriano De Cupis, "Il diritto alla riservatezza esiste", in: Foro Italiano, IV, 1954, pp. 90-97.

[458] Tribunal de Milão, 24 de setembro de 1953, in: Foro Italiano, 1953, parte I, p, 1341, cf. Tommaso Amedeo Auletta. **Riservatezza e tutela della personalità**. Milano: Giuffrè, 1978, pp. 63-64.

[459] Ainda como um conceito relacionado ao direito de propriedade.

[460] STANDAGE, Tom. **The Victorian Internet**: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers. New York: Berkley Books, 1999.

[461] DUNBAR, Robin. **Grooming, Gossip, and the Evolution of Language**. Cambridge: Harvard University Press, 1998.

desenvolvimento de nossa linguagem com toda sua complexidade e singularidade, estaria relacionada à confluência de alguns mecanismos de convivência social, em especial, a fofoca, poderia explicar com alguma racionalidade o fato de que o desenvolvimento de novas tecnologias de comunicação e informação sempre acarretarem um risco à esfera privada dos indivíduos.

Veja-se que o simples fato de haver meios de divulgação de informações não explicaria por inteiro as razões desses mesmos meios serem utilizados como forma de acesso e divulgação a fatos da vida privada de outros indivíduos em sociedade, ainda que simplifiquem o acesso e distribuição da informação.

A teoria de Dubar parece apontar para uma estratégia evolutiva que se incorporou como um hábito residual – uma espécie de órgão vestigial – persistente ao longo de nossa evolução. Em uma breve reflexão sobre o assunto, Yuval Noah Harari destaque que:[462]

> (...) nossa linguagem singular evoluiu como um meio de partilhar informações sobre o mundo. Mas as informações mais importantes que precisavam ser comunicadas eram sobre humanos, e não sobre leões e bisões. Nossa linguagem evoluiu como uma forma de fofoca. De acordo com essa teoria, o *Homo sapiens* é antes de mais nada um animal social. A cooperação social é essencial para a sobrevivência e a reprodução. Não é suficiente que homens e mulheres conheçam o paradeiro de leões e bisões. É muito mais importante para eles saber quem em seu bando odeia quem, quem está dormindo com quem, quem é honesto e quem é trapaceiro.
>
> A quantidade de informações que é preciso obter e armazenar a fim de rastrear as relações sempre cambiantes até mesmo de umas poucas dezenas de indivíduos é assombrosa. (Em um bando de cinquenta indivíduos, há 1.225 relações de um para um, e incontáveis combinações sociais mais complexas.) Todos os macacos mostram um ávido interesse por tais informações sociais, mas eles têm dificuldade para fofocar de fato. Os neandertais e os *Homo sapiens* arcaicos provavelmente também tiveram dificuldade para falar pelas costas uns dos outros – uma habilidade muito difamada que, na verdade, é essencial para a cooperação em grande número. As novas habilidades linguísticas que os *sapiens* modernos adquiriram há cerca de 70 milênios permitiram que fofocassem por horas a fio. Graças a informações precisas sobre quem era digno de confiança, pequenos grupos puderam se expandir para bandos maiores, e os *sapiens* puderam desenvolver tipos de cooperação mais sólidos e mais sofisticados.

[462] Em apoio à teoria de Dunbar. HARARI, Yuval Noah. **Sapiens**: uma breve história da humanidade. Tradução de Janaína Marcoantonio. 1. ed. Porto Alegre: L&PM, 2015, p. 29.

A hipótese proposta por Robin Dunbar e abordada por Harari apoia-se no fato de nossa linguagem ser adaptada para contar histórias. A teoria do autor indica que nossa preparação vocal teria evoluído gradualmente para uma linguagem vocal, inicialmente na forma de "fofoca". O fato de as estruturas de linguagem demonstrarem adaptações à função da narração em geral, parece confirmar a teoria de Dunbar, ainda que não imune a críticas.

Isso ajuda a entender, em alguma medida, a razão pela qual, ao longo da história, a difusão de técnicas de comunicação e informação representaram um risco tão grande à vida privada. Se tomarmos como verdadeira a hipótese de Dunbar, as incursões aos domínios sagrados da vida privada seriam resquícios de comportamentos evolutivos que ditaram a sobrevivência de nossa espécie em relação a outras. Tal fato ilustraria, com alguma racionalidade, os motivos de a divulgação de fatos da vida íntima de outros indivíduos mostrar-se uma atividade prazerosa a tantas pessoas, além de negócio lucrativo, ainda que repreensível sob diversos aspectos.

A teoria da comunicação de Dunbar revela, como consequência, uma predisposição do *homo sapiens* à circulação da informação de caráter pessoal, facilitada pelo progresso tecnológico.

Posto isso, passemos a entender os surgimentos dos direitos à privacidade e proteção de dados pessoais.

2.2. O desenvolvimento dos direitos à privacidade e proteção de dados pessoais

Como aponta a Professora Laura Schertel Ferreira Mendes, a discussão sobre o direito à privacidade é consequência do surgimento de novas técnicas e instrumentos tecnológicos que facilitaram o acesso e, portanto, a divulgação de fatos e informações que não eram comumente mostradas ao público.[463] [464]

Essa ideia foi discutida pela primeira vez por Warren e Brandeis,[465] em 1890, quando abordaram como a fotografia, os jornais e outros aparelhos tecnológicos invadiram os domínios sagrados da vida privada e doméstica.

---

[463] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 27.
[464] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 174.
[465] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, 1890, p. 195.

Em seu artigo, os autores trouxeram, a partir da análise da jurisprudência inglesa da *common law*, o conceito de que a privacidade seria o direito a "ser deixado só"[466] [467]. Apregoavam àquela altura uma concepção estritamente negativa de privacidade que não mais encontra paralelo na atualidade.

Atualmente, a privacidade converteu-se em uma garantia de controle pelo indivíduo de suas informações, assumindo uma postura positiva e autônoma, como esperado nos regimes democráticos.[468]

O direito à privacidade, assim, passou a ter relação direta com a inviolabilidade da proteção à personalidade, envolvendo sua autodeterminação informativa e rompendo com a ideia anterior de exclusão, isto é: de ser deixado só. E isso acontece porque a ideia de privacidade enceta um conceito um tanto indeterminado, refletindo, a sociedade e a época que a revelam.[469]

A partir do século XX, as mudanças no papel do Estado, alinhadas à revolução tecnológica, fez com que o conceito do direito em questão cambiasse para revelar essa concepção positiva e includente em relação aos processos digitais em rede, acompanhada de certas garantias, como nos aponta Stefano Rodotà.[470] [471]

Essa evolução será analisada a seguir, sendo extremamente relevantes a narrativa alemã nesse contexto.

2.3. Os direitos à privacidade e proteção de dados pessoais na perspectiva alemã

Alemanha é por muitos reconhecida como a terra natal da proteção de dados[472], existe ali uma rica história por trás do desenvolvimento da noção de defesa do indivíduo contra o uso indesejado e ilegal das informações que lhe dizem respeito.[473]

---

[466] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, 1890, p. 195.
[467] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 27.
[468] DONEDA, Danilo. **A proteção da privacidade e de dados pessoais no Brasil**. Observatório Itaú Cultural: Direito, Tecnologia e Sociedade, Rio de Janeiro, ed. 16, p. 136-149, jan/jun 2014.
[469] DI FELLICE, Massimo; LEMOS, Ronaldo. **A Vida em Rede**. São Paulo: Paprius, 2014.
[470] RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Trad. Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.
[471] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 29.
[472] ALBRECHT, Jan Philipp. **Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung**. Überblich und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog. CR, 2016 p. 89.
[473] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em:

Essa tradição implica reconhecer que para melhor se compreender o estado atual de coisas, deve-se atravessar a compreensão dos caminhos traçados pela Alemanha na consagração dessa espécie de direito.

Pois bem. Primeiro de tudo, é indispensável notar que a proteção de dados pressupõe, fundamentalmente, uma assimetria de poder informacional. O papel desse direito é estabelecer um equilíbrio entre a proteção do indivíduo, na dimensão informacional da sua privacidade e personalidade, e o tratamento legítimo dos seus dados, seja pelo Estado, ou mesmo por particulares. A proteção de dados é uma evolução dogmática que retira os indivíduos de sua posição passiva-negativa, inerente ao direito à privacidade, e o reposiciona sob um *status* ativo-positivo, colocando-o sob o controle de suas informações, dando consentimento para o uso de suas próprias informações ou recusando esse mesmo consentimento, na medida de seu interesse e do grau de participação que deseja ter nos processos informativos digitais.[474]

É importante perceber, contudo, que a proteção dos dados, conquanto estimulada por ambientes informatizados, não depende, necessariamente, da existência de tecnologia ou mesmo de um tratamento automatizado ou eletrônico de informações (embora estes incrementem os riscos associados), mas, tão somente, de situações em que o indivíduo se vê especialmente debilitado em relação à manipulação de seus dados por terceiro, ainda que de forma manual ou mecânica.

Nesse compasso, a primeira grande manifestação de assimetria de poder informacional pode ser remetida ao Estado Moderno, que, por meio de seu aparato, coletava e tratava dados (pessoais ou não), para exercer o poder e o controle sobre seu território.[475]

Essa coleta, no entanto, levantou grandes questões quando regimes totalitários se instalaram na Alemanha. É que, se a utilização de dados pessoais significa poder sobre os indivíduos, o controle da população e, por conseguinte, a manutenção da ordem política dependeria de uma coleta massiva de informações. Essa coleta buscava identificar

---

https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

[474] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

[475] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

"formas de vida degeneradas, grupos de pessoas desleais ao ideário estabelecido, bem como toda e qualquer situação que representasse alguma ameaça à continuidade e exercício do poder".[476]

Por conta disso, é fácil compreender por qual razão os regimes autoritários adotam atividades de vigilância intensa sobre a população. Quanto mais se sabe, melhor se pode subjugar.

Esse assunto, inclusive, ganhou evidência nos últimos tempos diante da massiva coleta de dados pelo Estado Chinês, no contexto da pandemia do novo coronavírus. Texto do filósofo sul-coreano, Byung-Chul Han[477] discute a possibilidade de alastramento do Estado policial chinês, como "um modelo de sucesso" contra a pandemia. Em suas palavras:

> A China exibirá a superioridade de seu sistema ainda mais orgulhosamente. (...) O vírus não pode substituir a razão. É possível que chegue até ao Ocidente o Estado policial digital ao estilo chinês. Com já disse Naomi Klein, a comoção é um momento propício que permite estabelecer um novo sistema de Governo. Também a instauração do neoliberalismo veio precedida frequentemente de crises que causaram comoções. É o que aconteceu na Coreia e na Grécia. Espero que após a comoção causada por esse vírus não chegue à Europa um regime policial digital como o chinês. Se isso ocorrer, como teme Giorgio Agamben, o estado de exceção passaria a ser a situação normal.

Esse estado policialesco refletia-se em diversos regimes totalitários por toda a Europa (na Alemanha, Itália, Espanha e Portugal, por exemplo). Como manifestação concreta dessa vigilância, a burocracia estatal criava órgãos especializados para a realização da tarefa de controle político da população, por meio da coleta e tratamento de seus dados pessoais. Os grandes exemplos que marcaram a história alemã foram a *Geheime Staatspolizei* (Gestapo – Polícia Secreta do Estado) durante o período do Nazismo e a *Staatssicherheitsdienst* (Stasi – Serviço de Segurança do Estado) na Alemanha oriental durante o Governo da *Deutsche Demokratische Republik* (DDR – República Democrática Alemã).[478]

---

[476] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

[477] HAN, Byung-Chul. O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han. **El País**. Disponível em: https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html. Acesso em: 15 nov. 2021.

[478] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em:

O intuito de controlar dissidentes políticos e obter domínio sobre o povo é o que estimulava (e até hoje estimula) regimes autoritários a adotarem atividades de vigilância massiva sobre a população.

As consequências nefastas disso, nem precisam ser relembradas.

Passados alguns anos, com a superação desses regimes e a fundação de um Estado Democrático de Direito na Alemanha, levantou-se a questão central de saber qual o ponto de equilíbrio entre a demanda por dados pessoais para o funcionamento da administração estatal e a proteção dos indivíduos contra abusos. A partir das experiências passadas, estava claro que as atividades de vigilância precisavam ser controladas pelo Direito e, em especial, por meio da Constituição.[479]

A solução proposta na *Grundgesetz* (Lei Fundamental Alemã) de 1949 foi o começo de uma ponderação necessária entre as atividades administrativas e a proteção de dados pessoais, ainda que não tenha sido citado expressamente um direito à proteção de dados.

A proposição engendrada pela Lei Fundamental consistia na separação orgânica entre as atividades de polícia e a atividade de inteligência do Estado; na independência das polícias estaduais perante a polícia federal; e na coleta de dados necessários apenas às finalidades de cada administração.[480]

Esse plano tinha como fundamento o princípio da separação informacional dos poderes (*informationelle Selbstbestimmung*), segundo o qual cada órgão da Administração deveria ter acesso apenas às informações necessárias ao exercício de sua atividade pública.[481]

O princípio, como sugere seu nome, é desdobramento da separação dos poderes e conduz ao fato de que a competência de cada órgão público, prevista em lei, não estabeleceria só a sua atividade, mas, também, quais informações ele poderia ter acesso

---

https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

[479] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

[480] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

[481] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

de forma legítima. Para Gasiola[482] está aí, ainda que de uma forma inacabada, a gênese do princípio da finalidade de tratamento tão discutida no Regulamento Geral sobre a Proteção de Dados europeu.

De outro Norte, o reconhecimento legislativo expresso do direito à proteção de dados somente se deu em 1970, com a Lei de Proteção de Dados do Estado de Hesse (*hessisches Datenschutzgesetz*). Anos mais tarde, veio a Lei Federal de Proteção de Dados (*Bundesdatenschuzgesetz* – BDSG) de 1977, com entrada em vigor em 1979.[483] As regras gerais estabelecidas pela BDSG, no entanto, não excluíam a competência dos estados federados de publicarem suas próprias leis, inclusive para regular a proteção de dados quando o tratamento fosse realizado pela administração estadual ou municipal. Vale notar, como aponta Gasiola:[484]

---

[482] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

[483] Laura Schertel Ferreira Mendes aponta que essas foram a primeira geração das normas de proteção de dados pessoais, as quais surgiram como reação ao processamento eletrônico de dados nas administrações públicas e nas empresas, como à ideia de centralização da informação em enormes bancos de dados nacionais. A autora cita como exemplo de normas dessa primeira geração, no âmbito europeu, as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Nos EUA, foram aprovadas, nesse mesmo período o *Fair Credit Reporting Act* (1970), com foco na regulação dos relatórios dos consumidores, e o *Privacy Act* (1974), aplicável à administração pública. MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 29-30. Nota-se que, no EUA, a origem do direito está tipicamente associada ao consumo, tanto que a primeira normativa sobre proteção de dados revela uma preocupação com os *scores* de crédito e as informações coletadas para sua criação. Para se ter uma ideia da dimensão do problema, em 1967, a *Association of Credit Bureaus of America* (ACBA) já possuía mais de 110 milhões de dossiês de consumidores, emitindo quase 100 milhões de relatórios. Ralph Nader, diante desse quadro, apontou para "a invasão dos dossiês" nos EUA, alertando para os diversos aspetos discriminatórios e de lesão a direitos coletivos que esses dossiês poderiam ocasionar. Na época, Nader (*apud* Zanatta), pontuou o seguinte: "quando você busca um empréstimo de dinheiro, o concedente recebe um arquivo do birô de crédito para estabelecer sua pontuação de crédito. Esse dossiê contém todos os fatos pessoais que o birô de crédito pode reunir – seu emprego, salário, tempo em que está no atual emprego, status marital, uma lista de seus débitos passados e atuais, seu histórico de pagamento, qualquer registro criminal, ações judiciais de qualquer tipo e registros de imóveis em seu nome. O dossiê fornece até mesmo um teste de Q.I. que você fez no ensino médio. Quando o concedente terminar de conversar com o birô de crédito, ele provavelmente saberá mais sobre sua vida pessoal que sua sogra. (...) Birôs de crédito e agências de inspeção são as maiores fontes de informações sobre indivíduos. Mas governos, escolas, empregadores e bancos também são registradores, e algumas vezes fornecedores, de informação". ZANATTA, Rafael. A. F. **Perfilização, Discriminação e Direitos**: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais/download. Acesso em: 21 jun. 2021.

[484] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

> não é por acaso que diversas leis de proteção de dados foram publicadas na Alemanha em um curto período de tempo. Elas são reações a projetos estatais para implementar bancos de dados centralizados sobre a população, em meio à euforia tecnológica que marcou o pós-guerra. O choque entre a recente lembrança (ou presença) dos governos autoritários e a iminência de tais projetos levou ao reconhecimento expresso da proteção de dados perante as pretensões públicas de aumentar seu poder informacional. O objetivo dessas leis era, acima de tudo, estabelecer limites e garantir a transparência na criação de bancos de dados.

Ainda construção do direito alemão, em 1983, seu Tribunal Constitucional (*Bundesverfassungsgericht* – TCA) reconheceu um direito fundamental à autodeterminação informativa (*informationelles Selbstbestimung*), no conhecido julgamento sobre a Lei do Censo[485] (Volkszählungsurteil – 1 BvR 209/83, de 15.02.1983).

Nesse julgamento histórico, o Tribunal radicalizou o conceito do livre controle do indivíduo sobre o fluxo de suas informações na sociedade e decidiu pela inconstitucionalidade parcial da Lei de Recenseamento, argumentando a existência de um direito à "autodeterminação informativa" (*informationelle Selbstbestimmung*) com base nos artigos da Lei Fundamental que protegiam a dignidade humana e o livre desenvolvimento da personalidade, respetivamente, Art. 1 I GG e Art. 2 I GG 9.[486]

O Tribunal reconheceu ali que os dados de um indivíduo constituem uma projeção descentralizada de sua personalidade e que a coleta e tratamento ilimitado desses dados pode configurar uma grave ameaça a sua personalidade, na medida em que possibilitam o armazenamento ilimitado de dados, bem como a sua combinação de modo a formar um retrato completo do indivíduo,[487] sem a sua participação ou conhecimento.[488] [489]

A lei do recenseamento visava a coleta dos dados dos cidadãos referentes à profissão, moradia e local de trabalho, com o intuito de fornecer à administração pública

---

[485] "Lei do Recenseamento de População, Profissão, Moradia e Trabalho de 1982".
[486] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 30-31.
[487] Ver referências à teoria do mosaico à página 19.
[488] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 31.
[489] LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí, v. 14. n. 2, p. 27–53, 2009, p. 29-30. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/1767. Acesso em: 7 mar. 2021. Nas palavras da autora: o cidadão converte-se no denominado "homem de cristal" (Sentença de 15-12-83, do TC Alemão, BCJ, 1984, p. 137).

informações acerca do crescimento populacional, da distribuição espacial da população pelo território e das atividades econômicas realizadas no país. Os dados a serem coletados por pesquisadores estavam listados na lei, que estabelecia também uma multa para o cidadão que se recusasse a responder. Além disso, o §9º da norma determinava que os dados poderiam ser comparados àqueles presentes em registos públicos, com a finalidade de averiguar a veracidade das informações fornecidas e possibilitar a sua transmissão de forma anônima aos órgãos públicos federais.[490]

Diante desse quadro, foram ajuizadas diversas reclamações constitucionais contra a norma, com fundamento na violação direta ao Art. 2 I GG, que protege o livre desenvolvimento da personalidade. O Tribunal conheceu das reclamações e, no mérito, confirmou a constitucionalidade da lei em geral, declarando nulos, entretanto, os dispositivos que determinavam a comparação dos dados coletados, bem como a sua transferência para outros órgãos da administração. A sentença da Corte Constitucional, na sua formulação de um direito à autodeterminação da informação, criou um marco para a teoria da proteção de dados pessoais e para as subsequentes normas nacionais e europeias sobre o tema, ao reconhecer um direito subjetivo fundamental, alçando o indivíduo a protagonista no processo decisório que envolve o tratamento de seus dados.[491]

O grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais se baseia em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado.[492]

É interessante notar, no entanto, que a despeito da importância desse julgamento, o direito à autodeterminação informativa não foi recepcionado em outros países europeus. Na Alemanha, no entanto, o direito à proteção de dados acabou assumindo o papel de opção política (dentre outras) para operacionalizar esse novo direito fundamental de autodeterminação informativa. A proteção de dados, em si, não seria um bem jurídico, mas um instrumento para a realização desses direitos de personalidade. Essa construção doutrinária, no entanto, é ausente em outros países europeus e no RGPD.[493]

---

[490] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 31.
[491] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 31.
[492] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 32.
[493] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha: a tensão entre a demanda estatal por informações e os limites jurídicos impostos**. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021. Em arremate, é digno de nota, que em 2008, outro julgamento do TCA (Tribunal Constitucional Alemão) abordou a temática do uso de tecnologia pela

2.4. As gerações da legislação sobre proteção de dados

A narrativa alemã introduz a primeira fase ou geração das Leis de Proteção de dados, com uma perspectiva de proteção do indivíduo contra os grandes bancos de dados públicos. No entanto, como pontuado na abertura deste capítulo e em *passim* ao longo do trabalho, o direito à privacidade antecede o direito à proteção de dados pessoais, sendo o trabalho de Warren e Brandeis,[494] referido no prólogo, o primeiro indicador dos contornos e limites do referido direito.

Laura Schertel Ferreira Mendes aponta que os autores ao fundamentarem a proteção do direto à privacidade o fazem, pela primeira vez, relacionando-o à proteção da personalidade, "rompendo com a tradição anterior que a associava à proteção da vida privada à propriedade".[495]

No termos narrados Warren e Brandeis [496]: "o princípio que protege escritos pessoais e outras produções pessoais, não contra o furto ou a apropriação física, mas contra toda forma de publicação, não é, na verdade, o princípio da propriedade privada, mas o da inviolabilidade da personalidade".

E ao identificarem esse princípio, os autores também são capazes de identificar seus limites, sintetizados pela Professora Laura Schertel Ferreira Mendes do seguinte modo:[497]

Administração Pública. Na oportunidade, o TCA reconheceu o direito fundamental à garantia da confidencialidade e integridade dos sistemas de informação (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* – IT-Grundrecht, 1 BvR 370/07, de 27.02.2008), consubstanciado na defesa do indivíduo contra intromissão estatal indevida a uma chamada esfera de intimidade digital. Essa proteção se estenderia aos dados e informações pessoais salvas em sistemas de informação, que não poderiam ser acedidos ou alterados pelo Estado, proibindo, assim, uma vigilância massiva e preventiva de computadores para investigação criminal, exceto em casos de perigo concreto, para proteger bens jurídicos relevantes, como a vida ou a liberdade da pessoa. A decisão, no entanto, foi duramente criticada, sobretudo, porque a proteção cunhada já decorreria de outros direitos fundamentais reconhecidos anteriormente, não sendo necessário um novo direito para tutelar a situação GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

[494] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, 1890, p. 195.

[495] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 29.

[496] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, 1890, p. 195.

[497] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 29.

> (a) O direito à privacidade não impede a publicação do que é de interesse geral; (b) o direito à privacidade não veda a comunicação de tudo que é privado, pois se isso acontecer sob a guarda da lei, como, por exemplo, em um Tribunal ou em uma Assembleia Legislativa, não há violação desse direito; (c) a reparação não será exigível se a intromissão for gerada por uma revelação verbal que não cause danos; (d) o consentimento do afetado exclui a violação do direito; (e) a alegação de veracidade da informação pelo agressor não exclui a violação do direito; e (f) a ausência de dolo também não exclui a violação desse direito.

O direito à privacidade, assim, parte de uma análise eminentemente individualista, como direito a ser deixado só, externando suas características, à época, de um direito negativo, com a exigência de absoluta abstenção do Estado na esfera privada/individual para a sua garantia. [498]

Somente no século XX é que "de um direito com uma dimensão estritamente negativa e com uma conotação quase egoísta, passou a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático", conforme avalia a Professora Laura Schertel Ferreira Mendes.[499]

Isso culminou em um "processo de inexorável reinvenção da privacidade", conforme destaca Rodotà.[500] De um lado, impingiu-se um caráter positivo a esse direito, que passou a ser reconhecido até mesmo no âmbito internacional. De outro, o direito à privacidade transformou-se para fazer emergir a dimensão de proteção de dados pessoais, em virtude dos novos desafios que efervesceram no ordenamento jurídico a partir do tratamento informatizado dos dados.[501]

Logo, a partir da década de 1970, vislumbrou-se a edição de diferentes legislações ao redor do globo, o surgimento de decisões judiciais em diversos países e a celebração de diferentes acordos internacionais em variados níveis consagrando o direito à proteção de dados, de modo a se poder fazer referência a diferentes gerações de normas.[502]

---

[498] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 29.
[499] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 29.
[500] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Trad. Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 15.
[501] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 174-ss.
[502] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 29.

Nesse passo, a primeira geração de regulamentos de privacidade de dados surgiu como uma resposta ao processamento eletrônico de informações por governos e empresas privadas, bem como à tendência de criação de bases de dados centralizadas em uma única base, gerenciada pelos governos nacionais.[503]

São exemplos de normas da primeira geração, no âmbito europeu, as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Nos EUA, foram aprovados nesse mesmo período o *Fair Credit Reporting Act* (1970), com foco na regulação dos relatórios de crédito dos consumidores, e o *Privacy Act* (1974), aplicável à administração pública.[504]

Essa primeira fase, portanto, se caracteriza pelo rigor quanto à criação dos arquivos informatizados, sendo a lei do Land Hesse, na Alemanha, a primeira dessa espécie de legislação, inaugurando a proteção dos dados informatizados, em 7/10/70. Esse texto, pioneiro, contemplava somente os arquivos informatizados de titularidade pública. A lei da República Federal Alemã de 27/1/77, que posteriormente a sucedeu é que passou a regular os arquivos de titularidade pública e privada. [505]

A segunda geração, por sua vez, se caracteriza por normas menos rigorosas para criação de arquivos e pela preocupação com relação à tutela dos direitos fundamentais. São exemplos deste período: a lei francesa de 6/1/78, a lei suíça de 1981, a lei da Islândia de 26/5/81 e a de Luxemburgo de 30/3/79. [506] A legislação francesa, por exemplo, aporta uma contribuição importante para o âmbito jurídico de proteção de arquivos informatizados, que é a criação da Agência Nacional para proteção de dados. O objetivo do organismo de controle era garantir a segurança e o resguardo da informação pessoal.[507]

Sob uma perspectiva histórica, foi nesse período que o governo dos Estados Unidos, em 1965, propôs a criação de um Data Center Nacional para administrar o

---

[503] AGREL, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge, **Harvard Journal of Law & Technology**, v. 11, n. 3, Summer 1998, p. 871-880.
[504] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 30.
[505] LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí, v. 14. n. 2, p. 27–53, 2009, p. 36. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/1767. Acesso em: 7 mar. 2021.
[506] LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí, v. 14. n. 2, p. 27–53, 2009, p. 36. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/1767. Acesso em: 7 mar. 2021.
[507] LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí, v. 14. n. 2, p. 27–53, 2009. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/1767. Acesso em: 7 mar. 2021.

orçamento nacional e reduzir custos.[508] A ideia era criar uma central única que eliminasse os investimentos de outras agências em centros de informática e armazenamento de dados. No entanto, esse projeto nunca se concretizou, pois começou-se a temer o "poder" que o governo teria por conta de tal "Centro Nacional". Ressoou a tradição americana do liberalismo a pôr fim a esse projeto.[509]

Não obstante, quando a tecnologia permitiu o armazenamento e processamento de dados, formou-se um vínculo entre privacidade e proteção de dados pessoais. O direito à privacidade começou a mudar, assim como a forma como era apresentado. Passaram a fazer parte da ordem de ideias e da dogmática, *e.g.*, as expressões "privacidade da informação", "proteção de dados pessoais" e "autodeterminação da informação".

Assim, a segunda geração de regulamentos de privacidade de dados surgiu da necessidade de alterar as legislações existentes. Essas legislações buscavam abordar expressamente o direito à privacidade e não apenas em relação ao processamento de dados. O medo de um banco de dados unificado foi substituído pelo medo de bancos de dados diferentes espalhados pelo mundo, conectados entre si e gerenciados por órgãos públicos e empresas privadas.[510]

Nesse contexto, o direito à privacidade passou a ser regulamentado não apenas pela lei ordinária, mas também se tornou um direito constitucional. Exemplo dessa nova abordagem legal são as leis da Áustria, França, Dinamarca e Noruega.[511]

No entanto, a segunda geração de leis trouxe uma nova questão controversa, relacionada com a eficácia do consentimento dos cidadãos e da existência de um exercício real da liberdade de escolha do consumidor, sabendo que a recusa a fornecer os seus dados pode causar a exclusão social de um indivíduo dos processos informacionais.[512]

Esse fato faz aflorar a terceira geração de leis de proteção de dados, marcada pela decisão do Tribunal Constitucional Federal da Alemanha, que interpretou a Lei Federal de Proteção de Dados Alemã em consonância com a Lei Fundamental de Bonn.

---

[508] GARFINKEL, Simson. **Database National: the death of privacy in the 21th century**. California: O'Reilly Media, 2000.
[509] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 174-ss.
[510] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 31. DONEDA, Danilo**. Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 174-ss.
[511] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 31. DONEDA, Danilo**. Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 174-ss.
[512] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 32.

O Tribunal entendeu que todos os cidadãos tinham direito à autodeterminação das informações, com a ideia de que os usuários controlassem seus dados.[513]

A principal diferença entre a segunda e a terceira geração está relacionada com a participação dos cidadãos no tratamento dos dados. Nas leis de terceira geração, o usuário participa de todo o processo, desde a coleta dos dados até seu armazenamento e compartilhamento. [514]

O objetivo dessa terceira fase de desenvolvimento legislativo é a garantia dos direitos e a tentativa de não obstaculizar o desenvolvimento do setor informático. São deste período a lei do Reino Unido de 12/7/84, a nova lei alemã de 20/12/90, a primeira lei de Portugal de 20/4/91, modificada pela de 26/10/98, a lei espanhola de 31/10/92, revogada pela de 13/12/99, bem com a lei italiana de 31/12/96.[515]

Por sua vez, a quarta geração de estatutos normativos procurou solucionar os problemas de consentimento e buscar remédios para os vazamentos de dados.[516] [517]

Em primeiro lugar, essas leis visavam fortalecer a posição dos usuários, possibilitando o autocontrole efetivo sobre seus dados. Como exemplo dessa abordagem, há a compensação sem culpa que trata de reclamações pessoais individuais sobre violação de dados na Alemanha ou Noruega.[518]

Em segundo lugar, removeu-se alguns dados do controle individual, pois o conteúdo desses dados específicos seria tão essencial que deveriam ser extremamente protegidos. Portanto, não poderia estar à disposição de outros indivíduos.[519] Esse tipo de tratamento pode ser visto em relação aos "dados sensíveis", ou seja, todo dado cuja

---

[513] MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005.

[514] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 29.

[515] LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí, v. 14. n. 2, p. 27–53, 2009, p. 36. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/1767. Acesso em: 7 mar. 2021.

[516] CUNHA, Mario Viola de Azevedo. Privacy, Security and the Council Framework Decision 2008/977/JHA. **World Jurist Association Law and Technology Journal**, v. 43, p. 1-18, 2010. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1666140. Acesso em: 14 mar. 2021.

[517] BOTTA, Marco; VIOLA, Mario. La protezione dei dati personali nelle relazioni tra UE e USA: le negoziazioni sui trasferimento dei PNR' (2010), **Diritto dell'informazione e dell'informatica**, v. 26, n. 2, 2010.

[518] MAYER-SCHÖNBERGER, Viktor. **Generational development of data protection in Europe**. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: The MIT Press, 2001.

[519] SIMITIS, Spiros. Revisiting sensitive data: review of the answers to the questionnaire of the consultative committee of the convention for the protection of individuals concerning automatic processing of personal data (ETS 108). Strasbourg, 24-26 November 1999. Available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806845af>. Access on 08 June 2019.

divulgação possa resultar em discriminação, como informações sobre sexualidade, etnia, opiniões políticas, religião, entre outros.

A questão da proteção de dados surge na sociedade da informação como uma alternativa para proteger a personalidade individual contra os riscos decorrentes do tratamento de dados. O objetivo é proteger a pessoa que possui os dados e não os dados em si, como aponta a Professora Laura Schertel Ferreira Mendes.[520]

Com efeito, a descoberta de novas tecnologias que possibilitaram a coleta, registro, cruzamento, organização e transmissão de dados, em um cenário jamais imaginado, também permitiram a coleta de informações valiosas dos cidadãos, facilitando a tomada de decisões econômicas, políticas e sociais.[521] O valor da informação não é apenas uma questão de capacidade de armazenamento de dados, mas principalmente a possibilidade de "criar" novas informações a partir de seu tratamento. Em outras palavras, o processamento de dados previamente armazenados cria novas informações, sem a necessidade de uma nova coleta. Novos dados são criados a partir de dados existentes, independentemente de sua coleta ter ocorrido diretamente junto ao usuário.[522] [523] Exemplo disso são as técnicas de *profiling*, já abordadas.

Nesse cenário, há um *trade-off* entre tecnologia e privacidade, uma vez que a ampliação da tecnologia reduz a privacidade pessoal. Consequentemente, pode-se pensar que a única solução para a conter é impedir o desenvolvimento das tecnologias da informação. No entanto, a maneira mais eficaz de examinar esse problema, conforme assinala a Professora Laura Schertel Ferreira Mendes,[524] foi aquela apontada por Simson Garfinkel.[525] Segundo o autor, a questão deve ser respondida pela concepção de que o desenvolvimento tecnológico deve ser buscado concomitantemente com a preservação da privacidade dos cidadãos. Assim, para aos autores "a melhor forma de se observar a questão não é por meio da dicotomia entre tecnologia e privacidade, mas, sim, a partir da

[520] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 32.
[521] ALCALÁ, Humberto Nogueira. Autodeterminación informativa y hábeas data en Chile e información comparative. **Anuário de Derecho Constitucional Latinoamericano** 2005, t. II, Konrad Adenauer Stiftung.
[522] DE LA CUEVA, Pablo Lucas Murillo. La construcción del derecho a la autodeterminación informative. **Revista de Estudios Políticos**, Madrid, 104, (Nueva Época), Abril/Junio 1999.
[523] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 33.
[524] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 34.
[525] GARFINKEL, Simson. **Database National: the death of privacy in the 21th century**. California: O'Reilly Media, 2000.

concepção de que o desenvolvimento tecnológico deve ser harmonizado com a preservação da privacidade dos cidadãos".[526] [527] No entanto, a "solução" apontada por Garfinkel só é possível se os usuários tiverem a chance de preservar sua privacidade.

Nesse sentido, é fundamental que o debate sobre a proteção de dados pessoais tenha como foco as opções jurídicas e econômicas relativas às funções que a tecnologia deve assumir na sociedade, rejeitando-se a ideia de que ela é a responsável pela perda de privacidade pessoal da sociedade contemporânea. Isto é, não é a tecnologia em si a causa do problema da privacidade, mas as decisões que tomamos em relação à tecnologia, arremata Mendes.[528]

Assim na seção seguinte abordaremos essas decisões, constituídas pelos arranjos institucionais consagrados em matéria de privacidade e proteção de dados.

3. Os arranjos institucionais da regulação em matéria de privacidade e proteção de dados pessoais

Nessa seção analisaremos a implementação da agenda regulatória em matéria de privacidade e proteção de dados pessoais. Em um primeiro momento, avaliaremos as tipologias de regulação, com foco sobre o papel do Estado em cada uma delas, para, depois, contextualizar como estes modelos se desenvolveram na realidade.

Ao analisarmos concretamente esse modelos de proteção de dados faremos um recorte sobre as transferências internacionais de dados pessoais, cuja forma de regulação, propomos abranger também processos internos, aplicáveis, sobretudo, ao Poder Público e às grandes empresas nacionais.

3.1. O sentido da regulação da privacidade e da proteção de dados pessoais

A narrativa que teve início em tópicos anteriores mostra que o paradoxo da modernidade tem indicado um suposto dualismo entre inovação tecnológica e regulação. Em boa medida, parte desse dualismo se deve à percepção de que a modernidade tem

[526] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 34.
[527] GARFINKEL, Simson. **Database National: the death of privacy in the 21th century**. California: O'Reilly Media, 2000.
[528] MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 34.

imposto um *trade-off* entre fomentar a inovação tecnológica, resguardar o direito à privacidade e impor um formato de regulação restritiva, como se necessariamente se excluíssem.

Tradicionalmente, os Estados eram vistos como os atores essenciais do processo de construção, implementação e aplicação das leis, ou seja, os Estados conduziam todo o processo regulatório. Para desempenhar essas atividades, desenvolveram instituições sofisticadas e suficientemente capazes de implementar as leis por meio da força, as agências reguladoras.[529] Como premissa geral, não existia lei fora das fronteiras soberanas do Estado. Por essa razão, o principal desafio imposto pela globalização passou a envolver a definição de instrumentos regulatórios em um ambiente exponencialmente em transformação, com entidades privadas com cada vez mais força política, econômica e social.

No âmbito da privacidade e proteção dos dados pessoais não foi diferente. A globalização foi capaz de criar um cenário de transações instantâneas em âmbito global,

[529] Essas entidades seriam as *independent agencies* e nas *Independent Regulatory Commissions*, criadas nos EUA. Refere João Nuno Calvão da Silva que essas agências "surgem como uma tentativa de o Poder Público controlar os excessos das *corporations* e, sobretudo, de limitar os efeitos perversos da concorrência selvagem. Na verdade, ao contrário do que sucedeu na Europa, onde as ARI [Autoridades Reguladoras Independentes] surgiram num contexto de desmantelamento das barreiras estatais ao livre funcionamento do mercado, na génese das *independent agencies* americanas está a razão inversa: a necessidade de conter os efeitos nefastos derivados da livre concorrência. Nos anos 70/80 do séc. XIX criaram-se diversas *Comissions* regulatórias ao nível estadual, sobretudo no sector ferroviário, onde a livre competição havia conduzido a monopólios e tarifas discriminatórias. Em vários Estado do Oeste, surgiram *comissions* dotadas de amplos poderes regulamentares e de fixação de tarifas (*strong comissions*), enquanto nos Estado do Leste estes organismos se limitavam a competências consultivas (*weak comissions*)". SILVA, João Nuno Galvão da. **Mercados e Estados: serviços de interesse económico geral**. Coimbra: Almedina, 2008, p. 131.
Vital Moreira sustenta que a redução à cópia do modelo estadunidense é, no entanto, empobrecedora da realidade histórica. O autor avalia que, para além da assimilação de um modelo americano, três inspirações europeias podem ser apontadas para o surgimento das agências reguladoras: as *Comissions* da Grã-Bretanha (em atividades regulatórias de mercado, denotando, estas sim, uma clara ligação ao modelo americano); mas, também, as autoridades administrativas independentes francesas (*autorités administratives indépendantes*) que detém funções de proteção a direitos fundamentais; além do banco central alemão (Bundesbank) que desde logo passou a ter autonomia em relação ao governo, estabelecendo taxas de juros e outras diretrizes econômico-financeiras. MOREIRA, Vital. As Entidades Administrativas Independentes e o Provedor de Justiça. In: **O Cidadão, o Provedor de Justiça e as Entidades Administrativas Independentes**. Lisboa: Provedoria de Justiça – Divisão de Documentação, 2012, p. 96-98.
Carlos Blanco de Morais (2001, p. 114 e ss.) também apresenta uma narrativa sobre a evolução dessas entidades na ordem jurídica europeia, bem como a teleologia por trás de sua criação, a qual seria informada por três fatores principais: os escândalos de corrupção (na Itália e França) e arbitrariedade policial (na Espanha); os ideais da doutrina neoliberal que se espraiaram após as crises das décadas de 70 e 80; assim como, em razão da apregoada ideia de ineficiência da administrativa. MORAIS, Carlos Blanco de. As Autoridades Independentes na ordem jurídica portuguesa. In: **Revista da Ordem dos Advogados**. n. 61. p. 101-154, 2001, p. 114-ss. Juliana Ferraz Coutinho, igualmente, menciona a presumida ideia de ineficiência da Administração como uma das razões para se terem criado tais entidades. COUTINHO, Juliana Ferraz. **O público e o privado na organização administrativa: da relevância do sujeito à especialidade da função**. Coimbra: Almedina, 2017, p. 669.

por meio das quais uma expressiva quantidade de dados passa a ser transferida sem a plena consciência, compreensão e consentimento dos usuários da rede.

Para fins de delimitação conceitual, a ideia de regulação aqui adotada, como visto, abrange uma noção alargada, não se limitando ao papel desempenhado pelo Estado, em especial, porque temos visto surgir novas formas de regulação decorrentes da multiplicação de redes e atores não estatais responsáveis pela execução e implementação das diversas camadas da rede.

Também devemos apontar que, para fins metodólogos, considera-se a regulação pela perspectiva da proteção de dados pessoais todas a variedade de instrumentos que visam controlar o processamento de dados e suas consequências. É que, conforme notado Sombra,[530] a rigor, a regulação não envolve apenas o controle estatal e observância a preceitos legais, mas todas as ferramentas capazes de disciplinar comportamentos, restringir e otimizar ações, definindo diretrizes complementares para a execução de políticas públicas.

3.2. Os arquétipos regulatórios à luz do papel do estado

Não é novidade para o direito administrativo a existência de diferentes arranjos institucionais regulatórios. Esses arranjos institucionais, em regra se diferem pelo maior ou menor grau de participação do Estado e/ou órgãos reguladores, bem como em relação ao nível de receptividade da atuação regulatória conjunta de atores privados.

Em geral, tais arranjos podem ser identificados na regulação estatal direta, na corregulação e na autorregulação. Essa é, *v. g.*, a divisão adotada pelo órgão regulador das comunicações do Reino Unido (*Office of Communications – Ofcom*),[531] para o qual a regulação direta acontece quando um órgão criado por lei desenvolve, aplica, monitora e fiscaliza um determinado arcabouço regulatório.[532] Conforme aponta Keller,[533] é a lógica

[530] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 87.
[531] UK. United Kingdom. Office of Comunnications. **Online protection: A survey of consumer, industry and regulatory mechanisms and systems**, [s.l], 2006. Disponível em: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/27586/report.pdf. Acesso em: 20 set. 2022.
[532] É o que Robert Baldwin, Martin Cave e Martin Lodge identificam como tarefas regulatórias, representadas pelo quadro DREAM: Detection, Responding, Enforcing, Assessing, Modifying. , Resposta, Aplicação, Regulatory tasks: the DREAM framework. BALDWIN, Robert, CAVE, Martin e LODGE, Martin. Understanding Regulation, 2. ed. Oxford: Oxford University Press, 2012, p. 227.
[533] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 166.

comumente associada com a estratégia de implementação por comando e controle, o que requer alguma cautela.

De fato, essa forma caracteriza uma parcela relevante da atuação estatal na economia, não sendo, contudo, o único tipo de instrumento de que dispõe a Administração Pública para, sem o uso de agentes intermediários, promover a ação regulatória em determinado setor.[534]

Os arranjos de corregulação, por sua vez, seriam aqueles "fundados na divisão de tarefas e responsabilidades entre Estado, agentes regulados e partes interessadas, cuja concretização se dá, formalmente, por meio de delegação de tarefas por parte do Poder Público, mediante fixação de parâmetros sob controle estatal".[535]

Por fim, os arranjos autorregulatórios seriam aqueles em que um grupo de empresas ou indivíduos exerce controle sobre seus próprios membros por meio de um conjunto de regras estabelecidas pelos próprios participantes, que a elas aderem voluntariamente.[536]

Cada uma dessas três formas guarda um número de variações, mas é no espectro entre a regulação estatal direta, num extremo, e a autorregulação no outro, que se situa a corregulação, onde a diversidade de arranjos institucionais é maior, e por conseguinte, também o é a discordância taxonômica.

3.3. Sintonizando o espectro regulatório: regulação direta, corregulação e autorregulação

Conforme destaca Keller,[537] sob o rótulo da corregulação verifica-se uma gama de organizações diferentes, que têm em comum a implementação de regimes regulatórios

---

[534] Nesse sentido, veja-se aquilo que Gustavo Binenbojm chama de *normas de indução*, utilizadas para a criação de incentivos, operando na fórmula "prescrição-prêmio", ou ainda, o que ele chama de estratégias regulatórias não normativas (que incluiriam políticas públicas de fomento, o uso de sociedades empresariais estatais ou até estruturas alternativas de suporte de acesso a recursos financeiros, conhecidas como project finance). BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 163-171.

[535] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 163-171.

[536] UK. United Kingdom. Office of Comunnications. **Online protection: A survey of consumer, industry and regulatory mechanisms and systems**, [s.l], 2006. Disponível em: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/27586/report.pdf. Acesso em: 20 set. 2022.

[537] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 166.

baseados na interação entre legislação estatal e órgãos autorregulatórios.[538] Hanneke van Schooten e Jonathan Verschuuren[539] distinguem a corregulação pela combinação de diferentes atores não estatais (como empresas, grupos de empresas e organizações sem fins lucrativos) com algum nível de envolvimento estatal. Dentro desse espectro, é possível detectar diferentes composições, que variam a forma, o momento e a intensidade com que se dá o controle estatal.[540] Definidos por essa natureza essencialmente híbrida, sob o ponto de vista instrumental, esses arranjos também são comumente associados aos conceitos de *soft law*[541] e governança,[542] já que, como eles, se referem a formas mistas de influenciar comportamentos (o que não exclui a relevância das leis em sua organização).

A partir dessa caracterização de estruturas descentralizadas e mistas que contam com a presença estatal, é possível verificar a associação da corregulação com os conceitos de governança, que também presumem uma diversidade de agentes envolvidos no processo de regulação, bem como o uso de meios não necessariamente formais de implementação.[543] Essa variedade de regras de governança descreve um modelo institucional que trata de conformidade e negociação, em vez de monopólio da força, que se aproximaria, assim, da corregulação, como uma das formas intermediárias entre a ação da agência reguladora ou qualquer órgão de Estado e outras formas de autorregulamentação.[544]

---

[538] MARSDEN, Christopher T. **Internet Co-regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace**. Cambridge: Cambridge University Press, 2011, p. 46

[539] SCHOOTEN, Hanneke van e VERSCHUUREN, Jonathan (Orgs.). **International Governance and Law: State Regulation and Non-State Law**. Cheltenham: Edward Elgar Publishing, 2008. SSRN. Disponível em: https://ssrn.com/abstract=1291162. Acesso em 12 set. 2022.

[540] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 163-171.

[541] TRUBEK, David M.; TRUBEK, Louise G. Hard and Soft Law in the Construction of Social Europe: The Role of the Open Method Co-Ordination. **European Law Journal**, v. 11, n. 3, p. 343- 64, 2005.

[542] Para uma distinção entre regulação e governança, consultar: BIANCHI, José Flavio. **A ICANN entre governança e Regulação: análise da atuação regulatória da ICANN nos programas de expansão dos gTLDs no Sistema de Nomes de Domínio (DNS) da Internet**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade Nacional de Brasília, p. 300. 2018, p. 124-ss. e KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 26-29, 71-ss. Para uma diferenciação que abranja, ainda, o termo *compliance* ver: *ARANHA*, Márcio Iorio. ***Compliance*, governança e regulação**. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 437-452. A Governança acaba por ser um instrumento de política mais abrangente, que engloba diretrizes empresariais, códigos internos de conduta, entre outros elementos intencionais ou não de influência nas ações dos atores em operação.

[543] MARSDEN, Christopher T. **Internet Co-regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace**. Cambridge: Cambridge University Press, 2011, p. 55.

[544] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 166.

A presença estatal, serve, contudo, para distinguir a corregulação dos arranjos de autorregulação – que, em sentido mais amplo, se referem às operações e iniciativas regulatórias em que o governo não se envolve em nenhum nível de formulação ou implementação.[545] É comum a sua definição como a prática da indústria de tomar a iniciativa de produzir e fazer cumprir regras e códigos de conduta sem envolvimento governamental, apesar de também haver quem enquadre sob seu título atuações estatais limitadas, como por exemplo os de observador ou conselheiro.[546] Não se trata, assim, de uma distinção pacífica, já que a autorregulação, por sua vez, também guarda diferentes acepções.[547]

Julia Black, por exemplo, discute ambas as formas no âmbito da descentralização administrativa, identificando variações entre autorregulação, corregulação e *quasi regulação*.[548] Segundo a autora, a autorregulação também se distingue, além da ausência de governo, pela equiparação das regras não legais e de *soft law* (apesar desta também ser associada à corregulação) e na adoção de regras bilaterais ou multilaterais, navegando pelas distinções entre voluntariedade e mandatoriedade, público e privado, legal e não legal. Pode, assim, ser usada para significar a adoção de instrumentos variados, como regras ou acordos coletivos que não sejam necessariamente fruto de legislação (ou que não envolvam o governo), acordos bilaterais entre empresas e governo ou a adoção unilateral de padrões e arranjos neocorporativistas. [549]

Em outra definição, Gustavo Binenbojm diferencia a corregulação (que presumiria uma partição equilibrada de funções entre Estado e agentes regulados) da ideia de autorregulação regulada, que designaria "o conjunto de arranjos em que a ordenação é exercida predominantemente por entidades privadas, com variações entre si quanto à

[545] BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 116-118.
[546] BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 116.
[547] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 166.
[548] BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 118.
[549] BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 118.

forma, momento e intensidade da regulação estatal".[550] O mesmo esforço é verificado na adoção do Guia de Melhores Práticas Regulatórias da Austrália (*Australian Better Regulation Guide*),[551] que diferencia a corregulação de *quase-regulação* para situar nela:

> os arranjos que, em algum grau, se sustentam em leis, como, por exemplo, quando há delegação legislativa de poder à indústria para regulamentar e impor códigos (esperando ou exigindo que ela assim o faça sem abrir mão da possibilidade de impor um), prescrevendo códigos de conduta da indústria como voluntários ou obrigatórios, estabelecendo padrões mínimos que a indústria pode melhorar ou impondo às empresas o cumprimento de um código.[552]

[550] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 163-171. SCHULZ, Wolfgang, HELD, Thorsten. **Regulated Self-regulation as a modern form of government**. Indiana: John Libbey, 2004. HOFFMANN-RIEM, Wolfgang. **Regulating Media: The Licensing and Supervision of Broadcasting in Six Countries**. New York: Guildford Press, 1996.

[551] AUSTRÁLIA. Office of Regulation Review. **A Guide to Regulation**. 2. ed. Australia, 1998, p. B2. Disponível em: https://www.pc.gov.au/research/supporting/regulation-guide/reguide2.pdf. Acesso em :23 set. 2022.

[552] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 166. A autora ainda aponta que: "A corregulação refere-se a um grau de apoio legislativo de códigos ou normas, e.g., delegação legislativa de poder à indústria para regular e impor códigos, esperando ou exigindo que a indústria tenha um código mas tendo poder legislativo para impor um, prescrevendo códigos da indústria como voluntários ou obrigatórios na legislação, legislação estabelecendo padrões mínimos que a indústria pode melhorar ou obrigar as empresas a cumprir um código." Trecho original em inglês: "Co-regulation refers to a degree of legislative underpinning of codes or standards, e.g. legislative delegation of power to industry to regulate and enforce codes, expecting or requiring industry to have a code but having back-stop legislative power to impose one, prescribing industry codes as voluntary or mandatory in legislation, legislation setting minimum standards which industry can improve upon, or enforcing undertakings to comply with a code". (Office of Regulation Review. A Guide to Regulation, 2th ed. Australia, 1998 p. B2. Disponível em: https://www.pc.gov.au/research/supporting/regulation- guide/reguide2.pdf. Acesso em 14 mar. 2019). Já a quase regulação pode ser entendida como a "gama de regras, arranjos ou padrões que os governos pressionam as empresas a cumprir, mas que não são legalmente vinculantes. A quase-regulação pode incluir códigos de prática da indústria que o governo endossou, mas não é responsável por fazer cumprir, negociar diretamente com a indústria sobre padrões de comportamento acordados ou fazer cumprir tais códigos ou acordos necessários para competir por contratos ou financiamentos do governo. Este tipo de regulação pode ser útil quando é necessária uma solução específica da indústria para um problema." Trecho original em inglês: "Quasi-regulation refers to the range of rules, arrangements or standards which governments pressure businesses to comply with, but which are not legally binding. Quasi-regulation can include industry codes of practice which the government has endorsed but is not responsible for enforcing, negotiating directly with industry on agreed standards of behaviour, or making compliance with such codes or agreements necessary in order to compete for government contracts or funding. This type of regulation may be useful where an industry specific solution to a problem is required". NSW Government. NSW Guide to Better Regulation. Department of Premier & Cabinet: Sydney, 2016. Disponível em: https://www.productivity.nsw.gov.au/sites/default/files/2022-05/TPP19-01_Guide-to-Better-Regulation.pdf. Acesso em: 14 mar. 2019.

Conforme aponta Keller[553] alguns autores também tratam, dentro desse espectro, da ideia de metaregulação, que engloba uma série de interações entre regulação governamental e autorregulação. Contudo, o termo não se confunde com a corregulação, distinguindo-se a partir de uma visão reflexiva sobre a própria regulação, na qual em vez de se impor sobre indivíduos ou atores sociais, o processo de regulação se torna o objeto regulado.[554]

Verifica-se, assim, dentro do espectro da corregulação, um conjunto que pode englobar diversas iniciativas, por exemplo, supervisão sobre órgãos da indústria que exercem autorregulação na sua atividade; criação de órgão autorregulador por lei ou de mecanismos de supervisão e *accountability* (ou dos dois juntos); obrigações atribuídas aos particulares de desenvolver ou dar concretude a um corpo de princípios básicos editados pelo Estado, por meio de lei ou de regulamento, sob a supervisão de um regulador estatal; [555] ou atribuição de prática de um ato de polícia a uma entidade privada específica.[556]

Arremata a autora apontando que na Internet a maior vantagem da corregulação é a garantia de algum grau de segurança jurídica (provida pela base legal) a um espaço interpretativo aberto para desenvolvimento da inovação e abordagens mais flexíveis. Isso

---

[553] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 167.

[554] Keller aponta que se incluem nesse modelo os processos de "regulação dos reguladores, sejam eles agências públicas, corporações privadas autorreguladoras ou terceiros que atuem como gatekeepers" (PARKER, Christine. *The Open Corporation: Effective Self-regulation and Democracy*. Cambridge: Cambridge University Press. 2002, p. 283. Disponível em: https://www.cambridge.org/core/books/open - corporation/3C6D96ADBB3A5912A598F1F4E6759F19. Acesso em: 14 mar. 2019.), podendo se referir tão somente a "interações entre diferentes reguladores ou níveis de regulação" (COGLIANESE, Carry, MENDELSON, Evan. **Meta-Regulation and Self-Regulation**. In: BALDWIN, Robert, CAVE, Martin, LODGE, Martin. The Oxford Handbook of Regulation. Oxford: Oxford University Press, 2010, pp. 146-168, p. 147). A possível confusão entre os conceitos aconteceria quando, dentro do processo em que uma autoridade regulatória supervisiona um sistema de controle ou administração de riscos (ao invés de desempenhar diretamente a regulação), a entidade supervisora é necessariamente pública (e daí, necessariamente, exercendo suas funções a partir de previsão estatutária). KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 168.

[555] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 163-171. SCHULZ, Wolfgang, HELD, Thorsten. **Regulated Self-regulation as a modern form of government**. Indiana: John Libbey, 2004. HOFFMANN-RIEM, Wolfgang. **Regulating Media: The Licensing and Supervision of Broadcasting in Six Countries**. New York: Guildford Press, 1996.

[556] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 163-171. SCHULZ, Wolfgang, HELD, Thorsten. **Regulated Self-regulation as a modern form of government**. Indiana: John Libbey, 2004. HOFFMANN-RIEM, Wolfgang. **Regulating Media: The Licensing and Supervision of Broadcasting in Six Countries**. New York: Guildford Press, 1996.

permite a determinação de critérios e implementação de soluções pensadas pelos agentes regulados, enquanto os princípios da política pública, bem como mecanismos de controle e transparência, são vinculados à legislação primária.[557] Representa, assim, um necessário meio termo para a viabilidade dessas políticas - inclusive as que envolvem proteção da liberdade de expressão e da privacidade, a despeito dos entendimentos sobre sua inaptidão para tais fins.[558]

4. Os principais modelos regulatórios em matéria de proteção de dados pessoais

Na sequência, serão abordados alguns usos desses arranjos nos últimos anos, e como eles podem contribuir para as análises dos modelos institucionais.[559]

Conforme consigna Doneda,[560] as soluções adotadas para a disciplina da proteção de dados, em geral, podem ser agrupadas em modelos que sintetizam uma determinada abordagem do problema. Aqui, serão abordados dois desses modelos, o norte-americano e o europeu, que se apresentam como indutores de soluções adotadas em outros ordenamentos (como o brasileiro, por exemplo).

Como bem discute o autor, há uma tendência à convergência das legislações em tema de proteção de dados, tendo em vista que as características intrínsecas da matéria

---

[557] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 169.

[558] A saber: "A noção de corregulação tem sido usada com algum sucesso no contexto da regulação da Internet por causa do que foi chamado de "uma mudança para o meio" - um papel cada vez maior para intermediários na regulação (Kerr e Gilbert, 2004; Palfrey e Rogoyski, 2006). Também tem sido utilizado na regulação de outras mídias (Instituto Hans Bredow, 2006), bem como em outras áreas, como governança corporativa, responsabilidade social corporativa (Berns et al, 2007) e direito ambiental. Pode ser visto como paradigma geral da governança global no contexto da globalização". Trecho original em inglês: *"The notion of co-regulation has been used with some success in the context of internet regulation because of what was called 'a move to the middle' – an ever-increasing role for intermediaries in regulation (Kerr and Gilbert, 2004; Palfrey and Rogoyski, 2006). It also has been used in regulation of other media (Hans Bredow Institute, 2006), as well as in other areas such as corporate governance, corporate social responsibility (Berns et al, 2007) and environmental law. It may be seen as general paradigm for global governance in the context of globalization*". (FRYDMAN, Benoît, HENNEBEL, Ludovic, LEWKOWICZ, Gregory. Co-regulation and The Rule of Law In: BROUSSEAU, Eric, MARZOUKI, Meryem e MÉADEL, Cécile, *Regulation, Governance and Powers on the Internet*. Cambridge: Cambridge University Press, pp. 133-150, p. 134, 2012). KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 169.

[559] A análise que se seguirá, terá como pressuposto as obras de DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 185-256. e Guilherme Guidi, visível em: GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

[560] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 185-186.

não favorecem a adoção de soluções isoladas em contextos meramente nacionais. Em paralelo a essa convergência, porém, verifica-se uma especial polarização entre esses dois modelos, motivo pelo qual traçaremos o perfil de ambos.[561]

Cada um desses arquétipos se apresenta com características diversas. O europeu,[562] sistemático,[563] estruturou-se, inicialmente, em torno de uma Diretiva (95/46/CE) e, atualmente, encontra-se estruturado em torno de um Regulamento Geral de Proteção de Dados (GDPR, a sua sigla em inglês pela qual é internacionalmente reconhecido) aplicável de maneira direta e uniforme em todos seus Estados-membros. O modelo norte-americano, por outro lado, apresenta-se fracionado (setorial), com disposições legislativas e jurisprudenciais concorrentes em uma complexa estrutura federativa, o que torna sua leitura em chave sistemática – e até mesmo a compreensão geral de seu conjunto – um desafio para os próprios juristas norte-americanos.[564]

---

[561] Doneda explica que: "a diversidade entre os sistemas de *common law* e *civil law* certamente exerceu influência no desenvolvimento de diferentes regimes de proteção de dados pessoais, sendo que uma certa resistência de países da esfera do *common law* em vincular a matéria aos direitos fundamentais ou a modelos como o da tutela da dignidade pode ser mencionada como sintomática da diferença entre enfoques. Ao mesmo tempo, deve-se ter em conta que essa divisão não é taxativa e que países que fazem parte da geografia do *common law*, como a Austrália, a Nova Zelândia e o Canadá, entre outros, apresentam hoje características mistas em suas disciplinas de proteção de dados pessoais, denotando em alguns casos uma aproximação real de elementos do modelo europeu – além do caso do Reino Unido que, mesmo após sua saída da União Europeia, deverá continuar sob o efeito direto da normativa europeia". DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 186-187

[562] Antes de mais nada, é importante esclarecer a natureza jurídica das normas da União Europeia. Os atos jurídicos normativos da União Europeia estão descritos no artigo 288 do Tratado sobre o Funcionamento da União Europeia (TFUE). O TFUE resultou da alteração do Tratado de Roma, de 1957, que estabeleceu a Comunidade Europeia, pelo Tratado de Lisboa assinado em 2007, que reforma os tratados base da União e reorganiza suas instituições. Conforme apontado pela normativa, são 5 as modalidades legislativas europeias, os Regulamentos, as Diretivas, as Decisões, as Recomendações e os Pareceres. Os Regulamentos são normas vinculativas diretamente aplicáveis a todos os países, incluindo-se aí seus cidadãos e pessoas jurídicas, valendo como se direito nacional fosse. As Diretivas são normas adotadas pela Comissão e pelo Parlamento Europeu que fixam um objetivo que todos os Estados-Membros devem alcançar, cabendo a cada um decidir os meios exatos para tal, respeitando os preceitos básicos da norma supranacional. As Decisões são atos vinculativos apenas para partes específicas, sejam elas Estados ou empresas, sendo diretamente aplicáveis para os envolvidos. As Recomendações e Pareceres são atos não vinculativos e podem ser emitidos por diversas instituições europeias, contendo normalmente a recomendação de se adotar ou evitar certa posição ou comportamento, ou a declaração de uma posição quanto à determinada questão. UE. União Europeia. **Tipos de legislação**. Disponível em: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt. Acesso em: 25 jun. 2021.

[563] Fala-se em sistema pois o modo de interrelação entre as diversas Diretivas, Regulamentos, Decisões vinculantes regionais e suas contrapartes nacionais enquadram-se no conceito de Norberto Bobbio, que assim define sistema: "Diz-se que um ordenamento jurídico constitui um sistema porque não podem coexistir nele normas incompatíveis. Aqui, "sistema" equivale à validade do princípio que exclui a incompatibilidade das normas. Se num ordenamento vêm a existir normas incompatíveis, uma das duas ou ambas devem ser eliminadas. Se isso é verdade, quer dizer que as normas de um ordenamento têm um certo relacionamento entre si, e esse relacionamento é o relacionamento de compatibilidade, que implica a exclusão da incompatibilidade." BOBBIO, Norberto. **Teoria do ordenamento jurídico**. São Paulo: Polis, 1989. p. 80.

[564] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 185-186.

Da parte europeia, a complexidade também não é pouca. O modelo europeu passou a existir com a uniformidade de hoje apenas muito recentemente, com a entrada em vigor do GDPR em maio 2018. Até então ele não havia chegado ainda a assumir uma forma “pura" – por minuciosa que tenha sido a normativa anterior, a Diretiva 95/46/CE, a sua aplicabilidade direta ocorria apenas em via de exceção, já que a lei efetivamente aplicada aos casos concretos era a lei nacional, resultado da transposição da diretiva por cada estado-membro. Como notou Pietro Perlingieri[565] a respeito do ordenamento comunitário europeu, a relação entre os sistemas de fontes da União Europeia teve como consequência que não existisse propriamente um sistema comunitário, porém tantos sistemas quanto resultassem da integração das normas comunitárias com as de cada país.[566]

Essa espécie de fragmentação foi diagnosticada como um dos motivos principais que justificaram a atualização da normativa europeia justamente sob a forma de um regulamento, com aplicabilidade direta em todos os países-membros da União Europeia.[567] Outra justificativa relevante foi a necessidade de atualização da disciplina de proteção de dados em diversos pontos, por conta do desenvolvimento dos sistemas de tratamento de dados pessoais e a sua integração com dinâmicas como a do Mercado Comum Digital. [568]

A aplicação direta do GDPR aos países-membros não exclui, no entanto, que coexistam legislações nacionais sobre o tema nos diversos países-membros da União Europeia. Estas, que perdem a centralidade por não serem mais a fonte direta referente à matéria em seus respectivos países (eis que não há mais a necessidade de transposição da norma europeia), passam a cobrir, no entanto, aspectos de natureza operacional ou espaços deixados explicitamente pelo GDPR para que a legislação nacional possa realizar a integração com a normativa comunitária. [569]

4.1. O modelo europeu

[565] Pietro Perlingieri. **Normativa comunitaria e ordinamento interno**. In: I giuristi e l'Europa. Luigi Moccia (org.). Laterza: Bari, 1997, p. 110.
[566] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 185-186.
[567] O detalhamento quanto às espécies normativas europeias será feito na sequência, quando estudado o modelo em si.
[568] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 185-186.
[569] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 185-186.

Como se pôde perceber da evolução histórica relacionada à proteção de dados pessoais, a União Europeia sempre esteve na vanguarda da proteção de dados pessoais. A Convenção nº 108 do Conselho Europeu, chamada de Convenção de Estrasburgo, inaugurou,[570] em 1981, as iniciativas para um modelo robusto de tutela, que hoje é referência em todo o mundo.

b) Estrutura normativa e de tutela

O sistema atualmente vigente de proteção de dados pessoais europeu é composto por regulamentos, diretivas, decisões vinculantes e orientações de diversos níveis hierárquicos, criando um quadro normativo de diversas camadas, que partem sempre de orientações gerais e estabelecem normas cada vez mais específicas sobre os direitos e obrigações relativas aos dados pessoais.[571]

Até pouco tempo, a Diretiva 95/46/CE era o texto legal central no sistema europeu de proteção de dados pessoais. A Diretiva concentrava os principais conceitos no campo da proteção dos dados pessoais na União Europeia, trazia os princípios básicos da tutela dos dados pessoais, tanto na coleta, quanto na manipulação e tratamento de tais dados pelos interessados e por terceiros; elencava os direitos básicos dos titulares dos dados tratados; estabelecia os padrões para as transferências internacionais de dados; e criava, ainda, um aparato de supervisão que servia como fiscal, árbitro e legislador, nas funções que a Diretiva lhe atribuía.[572]

A Diretiva, no entanto, necessitava ser transposta pelos Estados-membros, ensejando um quadro normativo desigual e dificultoso para os propósitos da implantação do Mercado Único Digital,[573] tendo sido, em 2018, substituída pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à

[570] Isso sem contar ainda algumas leis anteriores de países daquele continente, por vezes de alcance nacional e por outras regional. Alguns exemplos são a Bundesdatenschutzgesetz, de 1977 do Land de Hesse, na Alemanhã, e a Loy Informatique et Libertés, de 1978, da França.
[571] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[572] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[573] UE. União Europeia. **Mercado Único Digital**. Disponível em: https://www.consilium.europa.eu/pt/policies/digital-single-market/. Acesso em: 30 jun. 2021.

proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.[574]

Além dessas normas centrais, outras de caráter complementar também foram criadas, buscando a transposição dos princípios do Regulamento para outras áreas de controle, antes não abrangidas pelo sistema, são exemplos o Regulamento nº 1725/18,[575] a Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho[576] e a Diretiva 2016/680, do Parlamento Europeu e do Conselho.[577]

Abaixo das diretivas e regulamentos, encontramos, ainda, algumas decisões da Comissão Europeia que ajudam a complementar o quadro regulatório. Essas decisões, não sendo produto de deliberações generalizadas[578] – como no caso dos regulamentos e diretivas sobre o assunto, que precisam ser aprovadas pelo Parlamento Europeu –, são,

[574] UE. União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial** L 119/1, 04 de maio de 2016.

[575] Norma autoaplicável que vincula as instituições e órgãos da União Europeia a um sistema baseado no Regulamento (UE) 2016/679, para a proteção de dados, ainda que de modo mais detalhado decorrente da necessidade de aplicação direta da norma. UE. União Europeia. Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE. **Jornal Oficial** L. 295/39, 21 de novembro de 2018.

[576] Posteriormente complementada e atualizada pelas Diretivas 2006/24/CE e 2009/136/CE, ela rege o tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrônicas. A diretiva aborda questões específicas e sensíveis como a conservação de dados de conexão para fins de faturamento dos serviços de conexão prestados, o envio de mensagens eletrônicas não solicitadas (spam), a utilização de dados pessoais em listagens públicas (como listas telefônicas), e a utilização dos chamados "testemunhos de conexão" ou cookies. UE. União Europeia. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas. **Jornal Oficial** L. 201, 31 de julho de 2002.

[577] UE. União Europeia. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial** L. 119/89, 4 de maio de 2016.

[578] Segundo o artigo 16, 2 do TFUE, o Parlamento Europeu e o Conselho da União Europeia devem adotar o processo legislativo ordinário para dispor sobre a proteção dos cidadãos quanto ao tratamento de seus dados pessoais. Por tal procedimento, de acordo com os artigos 289 e 294 do mesmo tratado, a proposta de normativa (regulamento, diretiva ou decisão) é introduzida pela Comissão Europeia e encaminhada para análise do Parlamento e do Conselho, que proferem ao fim uma decisão conjunta. Em alguns casos, no entanto, a Comissão pode emitir decisões únicas, quando assim autorizado por norma não obstada pelo Parlamento ou pelo Conselho, conforme o artigo 290 do TFUE. No caso, o próprio Regulamento (UE) 2016/679 delega à Comissão a regulamentação de alguns pontos específicos através de decisões únicas, como é o caso dos artigos 13, f) e 14, f), 45 e 46, relativos à decisão de adequação para viabilizar transferências internacionais de dados pessoais.

assim, mais facilmente revistas e atualizadas, característica que permite um detalhamento ainda maior em suas provisões. [579]

Ainda no quadro da Diretiva 95/46/CE, uma das mais notórias dessas decisões trata-se da Decisão da Comissão 2000/520/EC, datada de 26 de julho de 2000, que dizia respeito ao programa de "porto seguro" (*Safe Harbour*), criado em conjunto com o Departamento de Comércio dos Estados Unidos da América,[580] para facilitar as transferências de dados pessoais entre as duas partes, através do estabelecimento de padrões mínimos de segurança e sigilo. Entre as razões para sua concretização, estava o fato de que a União Europeia via com grande preocupação o cenário legislativo norte-americano no que tocava a proteção de dados pessoais, eis que, sendo os Estados Unidos um grande polo empresarial e, sobretudo, no oferecimento de produtos e serviços em um ambiente online, havia a legítima preocupação sobre o destino dos dados de cidadãos europeus eventualmente transferidos a empresas localizadas naquele país.

O programa "Safe Harbor", no entanto, foi encerrado em outubro de 2015, quando a Corte de Justiça da União Europeia, diante das denúncias sobre violações generalizadas de privacidade pelo governo estadunidense feitas pelo ex-agente da Agência de Segurança Nacional norte-americana (NSA), Edward Snowden,[581], julgou inválida a Decisão 2000/520/CE.

Na sequência dessa decisão, entabularam-se novas discussões entre Estados Unidos e União Europeia, com a finalidade de se criar um programa para garantir o intercâmbio de informações. O resultado desses esforços foi a Decisão de Execução 2016/1250/CE,[582] que estabeleceu o agora conhecido "Privacy Shield", que aprimorou o modelo anterior.[583] O programa, no geral, exige que as empresas afiliadas garantam certos

---

[579] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

[580] UE. União Europeia. Comissão Europeia. Decisão 2000/520/CE. Decisão da Comissão de 26 de julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de "porto seguro" e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América. **Jornal Oficial** L 215, 25 de agosto de 2000.

[581] GREENWALD, Glenn; MACASKILL, Ewen. NSA Prism program taps into user data of Apple, Google and others. **The Guardian Online**, June 7, 2013. Disponível em: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em: 30.11.16.

[582] UE. União Europeia. Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. **Jornal Oficial** L. 207/1, 01 de agosto de 2016.

[583] A adesão ao programa Privacy Shield é voluntária, apesar de ser requisito para transferências de dados que envolvam a União Europeia. Uma vez feita a adesão ao programa, no entanto, o atendimento a seus requisitos é obrigatório e exigível pela lei local norte-americana. Confira-se: https://www.privacyshield.gov/.

direitos aos indivíduos cujos dados são transferidos, como informações básicas, acesso a mecanismos simples e gratuitos de resolução de disputas, além de exigir o cumprimento de alguns princípios básicos de proteção, sigilo e segurança dos dados, bem como de transparência em seu tratamento.

Também assume especial importância a Decisão da Comissão 2021/914/CE, datada de 4 de junho de 2021,[584] que fornece aos interessados em transferir dados pessoais para destinos externos à União Europeia cláusulas-tipo que apresentam garantias suficientes, nos termos do Regulamento (UE) 2016/679, para a preservação dos direitos concedidos pelo Regulamento aos titulares dos dados a serem transferidos.

O sistema europeu, introduzido pela Diretiva no 95/46/CE, sofreu grandes alterações com a entrada em vigor do Regulamento (UE) 2016/679, o Regulamento Geral de Proteção de Dados (RGPD), ou *General Data Protection Regulation* (GDPR).[585]

Entre as principais alterações trazidas pelo GDPR, temos três mais relevantes, divididas de acordo com sua finalidade: alterações para reforçar direitos dos usuários; alterações para reforçar as competências das Autoridades de Proteção de Dados; e alterações para induzir e incentivar certos comportamentos por parte dos responsáveis pelo tratamento.[586]

Em primeiro lugar, no que diz respeito ao reforço aos direitos individuais, a forma de expressão do consentimento e a relevância do adjetivo "informado" foram robustecidos, exigindo-se que o titular dos dados tenha acesso facilitado às informações sobre o tratamento, expressas de modo simplificado (ao invés da linguagem geralmente hermética dos contratos), e que seu consentimento seja expresso de modo destacado, com igual facilidade para sua revogação. No mesmo sentido, os direitos de acesso e de eliminação de dados (na forma do "direito ao esquecimento") são reelaborados e expandidos, dando maior segurança ao titular e ao mercado.[587]

---

[584] UE. Comissão Europeia. Decisão de Execução (UE) 2021/914 da Comissão de 4 de junho de 2021 relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (Texto relevante para efeitos do EEE). Jornal Oficial L 99/31, 7 de junho de 2001.

[585] UE. União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial** L 119/1, 04 de maio de 2016.

[586] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

[587] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

No que concerne ao reforço das Autoridades de Proteção de Dados, podemos citar a especificação de sanções que podem ser impostas aos responsáveis por tratamentos de dados que não respeitem as regras do GDPR, a responsabilização também do agente processador dos dados e a nova obrigação de notificação de violações de segurança de dados. Assim, empresas que sofrerem ataques relacionados ao roubo de dados ou que tiverem dados pessoais de seus clientes vazados, por exemplo, deverão notificar os titulares dos dados e a Autoridade de Proteção de dados sobre tal fato.[588]

Ainda nessa esteira, o novo Regulamento cria diversas regras sobre procedimentos de avaliação de impacto em privacidade, os chamados *Privacy Impact Assessments*, ou simplesmente PIAs. Apesar de não haver uma obrigação de registro de tratamentos de dados, em certos casos é exigido do controlador ou responsável que elabore tal estudo, de modo a reduzir os riscos à privacidade dos titulares dos dados, podendo submetê-lo à aprovação da Autoridade de Controle.[589]

Por fim, o Regulamento também traz algumas práticas que servem como incentivo ao responsável pelo tratamento dos dados pessoais, para que este zele pelo cumprimento do regulamento e pela garantia da privacidade dos titulares dos dados.

A primeira mudança nesse sentido vem pela consolidação dos conceitos de *privacy by default* e *privacy by design* como obrigações do responsável pelo tratamento de dados pessoais, de forma que deve sempre construir seus produtos, serviços e processos tendo em mente a preservação da privacidade e os princípios gerais da matéria, além de utilizar como padrão de operação a escolha pela preservação da privacidade em detrimento da publicidade, na ausência de um posicionamento expresso do titular dos dados.[590]

A segunda mudança, de igual importância, vem pela reafirmação dos programas de incentivo ao cumprimento do Regulamento pela criação de selos e sistemas de certificação relacionados ao grau de zelo da empresa com a privacidade de seus usuários,

---

[588] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[589] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[590] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

além de códigos de condutas e listas de infratores, os quais serão objeto de nossos estudos à frente.[591]

c) Tutela em camadas, indução de comportamentos e fiscalização multinível

O que se nota pelo panorama traçado é um sistema de proteção construído em camadas: partimos de garantias fundamentais de grande amplitude, passando a normas ainda bastante gerais que especificam tais princípios e preveem tanto exceções quanto possíveis conflitos com outros princípios, e em seguida outras normas ainda mais específicas que abordam questões setoriais, chegando, por fim, a decisões e normativas de grande detalhamento, mas que contam com grande flexibilidade em sua criação e atualização (decisões, por exemplo).[592]

Nessa estrutura piramidal os valores essenciais estão contidos no topo, em normas gerais de pouca aplicabilidade prática e direta, crescendo os instrumentos legais em número, especificidade e flexibilidade conforme avançam para a base da estrutura.[593]

Essa configuração é de imensa importância diante das dificuldades inerentes à regulação de um setor tão influenciado pelo desenvolvimento tecnológico, como é o caso dos dados pessoais.[594] O importante, a essa altura, é perceber que tal estrutura hierarquizada de valores, princípios e regras é essencial para uma sincronia entre a lei e a realidade social. Em um campo fático de rápida evolução, é importante que a lei mantenha um patamar mínimo de aplicabilidade e seja, no mais, envidado esforços para a constante atualização das normas, de modo que elas possam acompanhar – ainda que a certa distância – o desenvolvimento tecnológico.[595]

Estruturadas da forma com que se encontram, as normas comunitárias básicas sobre a proteção de dados fornecem uma estrutura na qual (i) os valores fundantes – cuja

[591] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[592] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[593] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[594] MOSES, Lyria Bennett. How to think about law, regulation and technology: problems with technology as a regulatory target. **Law, Innovation and Technology**, n. 5, v. 1, 2013.
[595] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

atualização não precisa seguir o ritmo da tecnologia – estão bem fixados em normas gerais, que costumam apresentar também maiores dificuldades para sua alteração; (ii) os princípios e subprincípios em que se traduzem tais valores são bem desenhados e fixados em normas ainda de caráter geral, mas tecnologicamente neutras – o que garante que possam ser aplicadas ainda que com mudanças razoáveis no campo tecnológico; e (iii) regras específicas criadas pelo sopesamento e fixação legal desses princípios são construídas em normas de caráter específico e sujeitas a um procedimento simplificado de produção e atualização – permitindo que, ainda que não absolutamente tecnologicamente neutras, sigam a curta distância o desenvolvimento tecnológico.[596]

Do ponto de vista regulatório, a garantia de certos direitos e a condução dos atores envolvidos a um "comportamento ideal" é buscada por vias diferentes, que se complementam. Por um lado, temos princípios gerais e normas de conduta que impõem certos deveres. Por outro, temos o recurso a práticas de mercado, como a autorregulação e a criação de sistemas que premiam o cumprimento da lei, mais que simplesmente punir sua violação.[597]

Ainda, no modelo europeu temos a figura das Autoridades de Proteção de Dados, cujas atribuições extrapolam o de uma simples agência reguladora, mas caracterizam um órgão que agrega funções fiscalizatórias, normativas e jurisdicionais, ainda que em instância administrativa, permitindo que os titulares de dados possam acompanhar de perto o que é feito de seus dados e tenham um canal efetivo e especializado para a resolução de controvérsias que possam surgir, incentivando assim que o próprio usuário seja um fiscal ativo de seus direitos. [598]

4.2. O modelo norte-americano

O segundo modelo regulatório a ser examinado é o vigente nos Estados Unidos. O modelo norte-americano é o segundo mais influente do mundo, sendo que a maioria dos estudiosos define que, na atualidade, geralmente a lei de proteção de dados pessoais

[596] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[597] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[598] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

recentemente adotada (ou a tutela dos dados em sua ausência) tem grande chance de adotar um dos dois sistemas (o europeu ou o estadunidense), ou neles se inspirar.[599]

a) Estrutura normativa e de tutela

Os Estados Unidos não possuem uma lei geral de proteção de dados pessoais no âmbito federal. Ao invés de tratar a disciplina da coleta e do uso dos dados pessoais de uma maneira uniforme, optou por dar um tratamento setorial à matéria. Assim, no âmbito federal os Estados Unidos da América possuem leis federais que disciplinam a proteção e o uso de dados pessoais de crianças e adolescentes; os dados médicos ou de saúde; os dados financeiros; os dados pessoais inseridos no contexto das comunicações eletrônicas; entre outros setores específicos, mas não dispõem de uma lei central que defina princípios e regras comuns, ou que estabeleça direitos unificados aos cidadãos.

Alguns estados também possuem legislação específica sobre privacidade e proteção de dados, destacando-se o exemplo da Califórnia, que é referência no país sobre o tema.[600]

Nesses aspectos, no âmbito federal, chama a atenção o *Electronic Communications Privacy Act* de 1986,[601] constituído pelo *Wiretap Act*, pelo o *Stored Communications Act* e pelo *Pen Register Act.*

O *Wiretap Act* proíbe a interceptação, uso ou revelação de qualquer tipo de comunicação telefônica, oral ou eletrônica, aplicando-se tanto ao setor privado quanto ao público (salvo as exceções em caso de investigação criminal, por exemplo). Note-se que a referência aqui é a comunicação *em fluxo*, o que se extrai do próprio termo *interceptação*. Os dados referentes a comunicações armazenadas, que já foram recebidas

[599] Tradução do autor. "Os Estados Unidos, que por muito tempo apoiaram soluções baseadas no mercado, rejeitaram a legitimidade da legislação da UE, alimentando o primeiro conflito comercial da era da informação. (...) Contra as objeções dos EUA, as regras europeias se tornaram o padrão internacional da realidade (*de facto*), com mais de trinta países seguindo a abordagem europeia". No original: "The United States, which long supported market-based solutions, rejected the legitimacy of the EU's legislation, stoking the first trade conflict of the information age. (...) Against U.S. objections, European rules became the *de facto* international standard with more than thirty countries following the European approach". NEWMAN, Abraham. L. Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive. **International Organization**. Cambridge: Cambridge University Press, n. 62, ed. 1, p. 103–130. Confira-se também: CASTETS-RENARD, Céline. **Droit de l'internet: droit français et européen**. 2. ed. Paris: Montchrestien, 2012. p. 26.

[600] SOTTO, L.J.; SIMPSON, A.P. United States In: **Data Protection & Privacy 2015**, Londres: Law Business Research, 2015, pp. 208-209.

[601] ESTADOS UNIDOS DA AMÉRICA. Electronic Communications Privacy Act, 18 U.S.C. §2510 e ss., **Public Law**, Washinton D.C., 21 out. 1986.

ou enviadas e não se encontram mais em fluxo, são protegidos, por sua vez, pelo *Stored Communications Act*, que diz respeito aos dados de comunicação e de cadastro (como nome, endereço etc.) armazenados por provedores de serviço. O *Pen Register Act*, por sua vez, regula a utilização pelo governo (e a proibição ao público em geral) das *pens registers* e outros dispositivos de rastreamento de chamadas. Esses dispositivos servem para identificar os terminais em uma determinada comunicação (geralmente telefônica), mas não tem capacidade para interceptar ou acessar o conteúdo da comunicação em si. [602]

Ainda no âmbito federal, o COPPA, acrônimo para *Children's Online Privacy Protection Act*,[603] de 1998, cria salvaguardas para a interação de crianças com menos de 13 (treze) anos com a Internet em geral e no que diz respeito à sua privacidade. A Lei traz um mecanismo interessante de *safe harbor*, diferente do projeto internacional entre Estados Unidos e União Europeia. Por tal mecanismo, associações setoriais de empresas podem submeter à *Federal Trade Comission* (FTC) códigos de autorregulação que serão então avaliados e eventualmente homologados, tornando-se vinculantes para as empresas associadas.[604]

O diferencial aqui diz respeito ao fato de que tais códigos geralmente preveem mecanismos de resolução de disputas entre as empresas associadas e seus consumidores e/ou mecanismos internos de disciplina das empresas envolvidas em possíveis violações de privacidade. Com tais provisões, uma vez aprovado o código, empresas em violação do COPPA estariam primeiro sujeitas aos procedimentos disciplinares setoriais, e só depois, em certos casos, poderia ser submetida à investigação da FTC.[605]

No setor da saúde, de outra banda, vige o *Health Insurance Portability and Accountability Act* de 1996, mais conhecido por *HIPAA*, que traz regras federais setoriais de privacidade e proteção de dados médicos.[606] Tal norma traz disposições padrões de segurança física e técnica, para dados relacionados à saúde em formatos eletrônicos; a

---

[602] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[603] ESTADOS UNIDOS DA AMÉRICA. Children's Online Privacy Protection Act, 15 U.S.C. §6501-6506., **Public Law**, Washinton D.C., 21 out. 1998.
[604] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[605] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[606] ESTADOS UNIDOS DA AMÉRICA. Health Insurance Portability and Accountability Act, 110 Stat. 1936, **Public Law**, Washinton D.C., 21 ago. 1996.

obrigação de notificar os titulares dos dados, e muitas vezes a Secretaria de Saúde[607] e a mídia local[608] no caso de vazamento ou violações de dados pessoais; as condições básicas para o tratamento justo e legal dos dados pessoais e as situações em que o consentimento do titular é ou não necessário; direitos básicos de acesso aos dados e informação sobre o tratamento e as medidas cabíveis de segurança e sigilo; além de diretrizes específicas sobre a responsabilidade das entidades abrangida pela lei e por seus funcionários, incluindo-se aí treinamentos, questões de política interna de privacidade e de disciplina.[609]

O *Privacy Act* de 1974,[610] por fim, é a lei federal vigente que estabelece os princípios e regras para a coleta, armazenamento, uso e comunicação de dados pessoais no seio das atividades estatais conduzidas pelas agências federais.

A lei traz regras sobre a revelação de dados pessoais a outras agências ou terceiros – geralmente mediante o consentimento do titular ou diante de alguma circunstância de interesse público – no exercício da administração pública ou em atividades particulares com fins estatísticos, histórico, negocial, entre outros; garante direitos de acesso; limitações quanto à finalidade, quantidade e qualidade dos dados tratados; diretrizes para garantir a segurança, sigilo e a transparência dos tratamentos; diretrizes sobre as políticas internas de segurança e tratamento de dados; a obrigatoriedade de registro dos bancos de dados federais submetidos ao *Privacy Act*, entre tantos outros assuntos menores.[611]

O sistema estadunidense não possui uma Autoridade de Proteção de Dados nos moldes europeus, isto é: um órgão técnico, independente e dedicado unicamente à matéria da privacidade e da proteção de dados pessoais. Em seu lugar, certos órgãos já existentes e não exclusivos do governo atuam como agências reguladoras, sendo responsáveis pelo *enforcement* das leis vigentes. Por haver uma certa separação por setores ou atividades econômicas, essa atuação nem sempre é homogênea, como também não são as posições

[607] U.S. Department of Health and Human Services.
[608] Quando o número de indivíduos afetados superar 500 (quinhentos) em um mesmo estado.
[609] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[610] ESTADOS UNIDOS DA AMÉRICA. Privacy Act, 88 Stat. 1896, **Public Law**, Washinton D.C., 31 dez. 1974.
[611] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

desses agentes reguladores em relação às controvérsias que possam surgir sobre este ou aquele conceito.[612]

Assim, a *Federal Trade Commission* é responsável, por exemplo, por fiscalizar a aplicação do COPPA e das regras relativas à proteção do consumidor, segundo seu próprio estatuto,[613] que podem incluir abusos na coleta e utilização de dados dos consumidores. Já o *Department of Health and Human Services*, é responsável pela supervisão do cumprimento do HIPAA. No setor financeiro, por sua vez, temos o *Consumer Financial Protection Bureau*.[614]

Tais agências geralmente têm competências fiscalizatórias, sancionatórias e normativas, podendo complementar as regras setoriais de que cuidam, mas o Poder Judiciário ainda exerce um importante papel no sistema de tutela. Isso porque, até mesmo as próprias agências e escritórios geralmente precisam recorrer ao Judiciário para executar suas decisões ou buscar o cumprimento de certas obrigações, o que demonstra a posição central do processo judicial no sistema americano. Se isso não bastasse, na ausência de leis mais amplas de proteção de dados, os princípios e regras gerais necessários para um modelo mais completo de tutela geralmente têm que ser deduzidos dos precedentes judiciais, reafirmando sua importância.[615]

b) Descentralização, contratualismo e judicialização

O modelo regulatório dos Estados Unidos é singular na medida em que apresenta uma abordagem bastante heterodoxa no que diz respeito às limitações à proteção de dados pessoais. Há, de fato, o reconhecimento de que os dados pessoais têm alguma ligação com a privacidade do indivíduo e com o controle que ele exerce sobre sua vida

[612] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[613] ESTADOS UNIDOS DA AMÉRICA. Federal Trade Comission Act, 15 U.S.C. §41-58., **Public Law**, Washinton D.C., 1914.
[614] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[615] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

particular.[616] Tal "direito à tutela", no entanto, dificilmente é autoaplicável ou diretamente exigível pelo titular dos dados daquele que os coleta e os trata.[617]

A norma de direito mais próxima do indivíduo é, pois, o contrato que rege sua relação com a empresa que coleta e utiliza seus dados pessoais. Talvez por conta da alta estima que o preceito liberdade têm naquele sistema jurídico, o legislador parece ter deixado à liberdade das partes de contratar a definição do que é razoável e possível. [618]

O instituto central do modelo norte-americano pode ser apontado, pois, como o *consentimento*. As condições e características desse consentimento variam de acordo com o setor de mercado e com a corte competente, mas é bastante claro que o consentimento possui, naquele contexto valor muito mais elevado que o a ele atribuído nos demais modelos regulatórios, pois não se trata aqui de um *consentimento informado*, livre ou expresso, resultado da consideração do indivíduo sobre o que se pretende com seus dados e o sopesamento entre benefícios e malefícios. O consentimento, na tradição norte-americana, parece ter maior ligação com a *venda* de informações do que com o estabelecimento de uma relação entre o usuário e o responsável pelo tratamento, dando-se ao contrato o tom de uma transação comercial, ao invés de uma cessão temporária de direitos sobre os dados em questão.[619] [620]

O contrato, no entanto, não serve sempre como substituto à garantia de certos direitos abrangentes, principalmente em situações em que uma das partes é uma grande empresa e a outra um indivíduo que deseja usufruir de um serviço seu – ao qual não terá acesso caso não aceite o contrato padrão provedor do serviço. O usuário vê-se forçado a aceitar termos impostos pelo provedor, não importa quão injustos. Esse desequilíbrio contratual, resultado da disparidade de força das partes, gera situações abusivas que não

---

[616] WESTIN, Alan. Privacy and Freedom, New York: Atheneum, 1970 *apud* PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. 1. ed. 6. imp, Curitiba: Juruá, 2011, p. 128.

[617] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

[618] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

[619] "Em contraste com outras áreas do mundo, como os Estados Unidos, onde as informações pessoais são amplamente comercializadas como um bem convencional, as regras europeias limitaram a mercantilização de dados individuais". Tradução do autor. No original: "In contrast to other areas of the world such as the United States, where personal information is widely traded like a conventional good, European rule limited the commodification of individual data". NEWMAN, Abraham. L. Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive. **International Organization**. Cambridge: Cambridge University Press, n. 62, ed. 1, p. 103–130.

[620] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

são tuteladas pela lei e, pela massificação dos negócios digitais,[621] acarretando, por sua vez, ações judiciais, individuais ou coletivas, como única solução. [622]

A judicialização de conflitos, ampliada pela ausência de uma norma geral ou mesmo de um órgão regulador específico, tem diversas consequências, tanto para a efetividade dos direitos garantidos quanto para a condução dos negócios em si. [623]

Ademais, como pontua Guilherme Guidi, relegar ao judiciário a garantia de direitos, sem criar outros mecanismos que os assegurem ou que busquem incentivar a adoção de certas práticas recomendáveis no tratamento da privacidade dos indivíduos, instala no empreendedor e nas empresas em geral a ideia de que a garantia da privacidade de seus clientes ou futuros clientes é apenas um fator na análise de rentabilidade e viabilidade de um modelo de negócios, e não um valor que deve ser preservado. [624]

Do ponto de vista geral, essa abordagem privilegia a livre iniciativa e a inovação, permitindo que usos novos e não regulados da informação sejam descobertos e utilizados para gerar valor aos consumidores. Do ponto de vista da proteção de dados pessoais, no entanto, trata-se, na visão de Guidi um modelo ineficaz de regulação, que recorre apenas a um viés regulatório jurídico, ao invés de avaliar a conduta regulada em termos econômicos, sociais e de "arquitetura", como queria Lessig.[625] Nesse ponto, vale considerar se a via adotada pelos juristas estadunidenses é a mais efetiva para a realização dos dois propósitos aparentemente contraditórios: proteção de dados/privacidade e inovação. [626]

---

[621] Confira-se, por exemplo: BARRETT, Brian. Spotify clears up its controversial Privacy Policy. **Wired Online**. 2015. Disponível em: https://www.wired.com/2015/08/spotify-clears-up-its-privacy-policy/. Acesso em: 25 out. 2022. PAUL, Ian. Instagram updates Privacy Policy, inspiring backlash. **PC World.** 2012. Disponível em: https://www.pcworld.com/article/456103/instagram-updates-privacy-policy-inspiring-backlash.html. Acesso em: 26 set. 2022.

[622] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

[623] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

[624] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

[625] LESSIG, Lawrence. **Code: And Other Laws of Cyberspace, Version 2.0**. New York: Basic Books, 2006.

[626] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109. A resposta, indicada por Garfinkel e Mendes no item 2.4 do trabalho, segundo a qual a melhor forma de se observar a questão não é por meio da dicotomia entre tecnologia e privacidade, mas, sim, a partir da concepção de que o desenvolvimento tecnológico deve ser harmonizado com a preservação da privacidade dos cidadãos, parece ir de encontro com as estruturas apregoadas pelo sistema americano. Não obstante, como assinala Hoffmann-Riem, o sistema europeu parece estar passando por uma espécie de

5. Outros modelos regulatórios em matéria de proteção de dados pessoais

Além dos modelos europeu e norte-americano, abordaremos, ainda, alguns outros modelo de proteção. O primeiro deles, tratando-se de uma formulação de proteção de dados pessoais bastante peculiar: o modelo uruguaio.

O arquétipo do país latino-americano é o mais centralizador e de intervenção Estatal a ser analisado, traduzindo um modelo de intervenção que chega a lembrar o extinto modelo europeu de análises *ex ante* abordado na antiga Diretiva 95/46/CE.

É que, com o surgimento do RGPD, ao mesmo tempo em que foram previstos poderes regulatórios mais abrangentes às Autoridades de Controle Independentes, estimulou-se a atuação de operadores e controladores de dados. O modelo europeu cambiou, assim, de um controle preventivo da Administração (*ex ante*), em que muitas matérias precisavam de prévia autorização da entidade reguladora, a uma fiscalização a posteriori (*ex post*), baseada no risco.[627]

A direção que caminhou o RGPD foi a de garantir uma maior independência aos *Stakeholders* a partir da concentração na figura do encarregado de proteção de dados (*Data Protection Officer*) de uma série de controles prévios, que antes eram incumbidos à Administração Pública. Como aponta Filipa Urbano Calvão:[628]

> O delegado [controlador] assume em boa medida as funções de controle prévio e sucessivo que tradicionalmente eram da competência da autoridade administrativa (cf. artigo 37.º), constituindo a obrigação

setorização, como revela a abordagem de normativas específicas para diversas áreas e atividades, como a Inteligência Artificial*; algorithmic trading*; condução autônoma; plataformas digitais, entre outras. Contudo, sem perder o marco de ser um sistema centralizador, por meio de um regulamento geral e fortes autoridades reguladoras. HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Rio de Janeiro: Forense, 2021, p. 34-35.

[627] Maria João Carvalho e Paulo Simões Lopes ressaltam entre as mudanças promovidas pelo RGPD: - O reconhecimento da importância em proteger os dados pessoais; - O alargamento do conceito de dados pessoais que passa a incluir quaisquer dados suscetíveis de identificar, mesmo que de forma indireta, o indivíduo; - O Reforço dos direitos dos titulares (direito ao esquecimento e a portabilidade); - Alteração do modelo de regulação, uma vez que passa de um modelo de hétero-regulação (pelo Estado) para o modelo de autorregulação [publicamente regulada, isto é: sob a supervisão estatal – o que para nós corresponderia a um modelo de corregulação, com certo protagonismo de atores privados]; - A Introdução de um quadro sancionatório; - A obrigatoriedade de reporte à Autoridade de Controle (CNPD) de incidentes que envolvam o comprometimento de dados pessoais. CARVALHO, Maria João; LOPES, Paulo Simões. **Da Privacidade à Proteção de Dados**, 2019. Disponível em: URL: https://www.uc.pt/protecao-de-dados/protecao-de-dados-pessoais/privacidade-e-protecao-dados/. Acesso em: 17 set. 2022.

[628] CALVÃO, Filipa Calvão. **O modelo de supervisão de tratamentos de dados pessoais na União Europeia: da atual diretiva ao futuro regulamento**, 2015. In: Revista Fórum de Proteção de Dados. n.1, p. 36-48, p. 42. Disponível em: https://www.cnpd.pt/media/owgnsrp2/forum_1_af_web_low.pdf. Acesso em: 15 nov. 2022.

> legal da sua criação uma expressiva manifestação da transferência do poder de controle da autoridade administrativa para o próprio responsável pelo tratamento, que, noutros planos, tem vindo a ser institucionalizado (como sucede no domínio do direito do ambiente).

Esse movimento, pode ser visto como um recrudescimento do modelo intervencionista estatal, para uma lógica de mercado, de regulação. No entanto, o fenômeno em si, não se confunde com uma desregulamentação. Isso porque, os poderes Administrativos, embora alternado no momento de seu exercício, continuam a existir e, até mesmo, em maior grau.

Assim, o modelo Uruguaio, como se verá, se aproxima bastante da Diretiva 95/46/CE adotando uma postura bastante defensiva muito provavelmente por razões históricas relacionadas ao momento em que se estabeleceu o sistemas de proteção de dados naquele país.

5.1. O modelo uruguaio

Conforme destaca Guilherme Guidi,[629] o modelo regulatório uruguaio é de especial interesse, pois, a preocupação com a privacidade de dados dos cidadãos naquele país teve origem semelhante à brasileira, na medida em que ambas foram resultado de uma tradição sul-americana de reafirmação e expansão de direitos fundamentais, após regimes ditatoriais que tiveram na compilação de dados sobre seus cidadãos, nomeadamente daqueles com ideais incompatíveis com tais regimes, uma importante arma na repressão de movimentos democráticos.[630]

A estrutura fechada do regime antevê uma preocupação com a assimetria de informação entre Estado e cidadãos, bem como a preocupação em se assegurar o novo regime democrático, e os direitos fundamentais a ele inerentes.

---

[629] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

[630] "Sinteticamente, apontamos o fato de que um instituto do gênero tenha uma especial razão de ser em sociedades recém-saídas de regimes militares, como em diversos países latino-americanos na década de 1980 em diante, em cuja sociedade civil persistia o trauma pelo uso autoritário da informação. Em um momento posterior ao fim desses regimes, um instrumento para a requisição das informações pessoais em mãos do poder público era tanto desejado quanto necessário, seja para a tutela dos direitos fundamentais envolvidos, como também pelo seu importante papel na formação de uma cultura democrática; para tal foi concebido o habeas data – para proporcionar ao cidadão um instrumento para conhecer diretamente e, se necessário, retificar as informações sobre sua própria pessoa armazenadas em bancos de dados". DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 55-62.

a) Estrutura normativa e de tutela

A principal lei uruguaia sobre o tema é a Lei no 18.331 de 2008 que trata da "Proteção de dados pessoais e da ação de 'Habeas Data'"[631], representando o ponto central do sistema de tutela daquele país. A referida lei traz as disposições gerais aplicáveis a todos os contextos em que dados pessoais possam ser coletados, tratados e utilizados. Especificamente, a lei traz disposições sobre princípios gerais da proteção de dados; os direitos de informação, acesso, retificação, supressão de dados, proteções especiais para categorias de dados consideradas sensíveis; algumas disposições específicas sobre a utilização de dados pessoais em setores como publicidade, bancos de dados de consumo e telecomunicações; regras para transferências internacionais de dados; registro obrigatório de bancos de dados; a criação do Órgão de Controle, a "*Unidad Reguladora y de Control de Datos Personales*", que consiste, basicamente, em uma Autoridade de Proteção de Dados; e disposições específicas sobre a ação de "Habeas Data", um dos elementos centrais do modelo regulatório.[632]

A citada norma foi regulamentada pelo Decreto nº 414 de 2009,[633] que trata com maior minúcia alguns temas da Lei de Proteção de Dados. Entre esses temas, podemos citar as especificações sobre a comunicação do consentimento para tratamento de dados; as medidas técnicas e administrativas de segurança; além de detalhes sobre o exercício dos direitos de acesso, retificação e eliminação ou supressão de dados. O decreto não elabora a atribuição normativa do Órgão de Controle, deixando aberto os temas a serem objeto de tais orientações ou mesmo o valor jurídico desses documentos. [634]

Algumas outras normativas tratam da coleta e tratamento de dados pessoais em certos setores, como o Decreto nº 396 de 2003, que trata dos dados pessoais referentes à saúde do indivíduo, e o Decreto nº 249 de 2007, que regula a identificação de pessoas por meios informáticos. Por fim, a própria *Unidad Reguladora y de Control de Datos*

[631] URUGUAI. Lei nº 18.331 de 2008 sobre a Proteção de dados pessoais e a ação de 'Habeas Data'. **Diario Oficial**, Montevideo, 18 ago. 2008.
[632] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[633] URUGUAI. Decreto nº 414 de 2009. **Diario Oficial**, Montevideo, 31 ago. 2009.
[634] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

Personales tem emitido normativas de caráter particular, interpretando e integrando as regras contidas na legislação vigente sobre Proteção de Dados. [635]

b) Descentralização, contratualismo e judicialização

O modelo uruguaio de regulação e proteção de dados pessoais guarda semelhanças com o modelo europeu, mesmo considerando que sua lei geral de proteção tomou por inspiração a Diretiva 95/46/CE da União Europeia, modelo hoje praticamente ultrapassado, tanto pelo desenvolvimento do sistema uruguaio quanto do próprio sistema europeu, com sua recente reforma.[636]

Não obstante, algumas diferenças são fundamentais, tanto na adoção inicial quanto nos caminhos adotados em um e noutro contexto.

À semelhança do modelo europeu de proteção de dados, o Uruguai conta com um arcabouço normativo diversificado e estratificado, ainda que não chegue ao nível de complexidade das normas que têm como referência.[637]

Lá, encontramos uma lei geral, cujos pontos mais importantes são desenvolvidos com mais detalhes em decretos regulamentadores. Encontramos também normativas emitidas pela Autoridade de Proteção de Dados criada pela lei geral e que regula assuntos específicos e muitas vezes técnicos, como cláusulas contratuais para transferência internacional de dados pessoais,[638] monitoramento de ambientes por vídeo,[639] dentre outros assuntos. Ainda, paralelamente, temos o incentivo para a adoção de códigos de conduta, que complementam a legislação estatal com a autorregulação dentro dos princípios gerais já estabelecidos.[640]

O tom das normas em vigor, no entanto, não deixa dúvida de que a legislação uruguaia tem forte tendência à centralização de competências. As normativas baseiam-

[635] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[636] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[637] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[638] Confira-se Dictamen no 003/2009 da Unidad Reguladora y de Control de Datos Personales.
[639] Confira-se Dictamen no 014/2011 da Unidad Reguladora y de Control de Datos Personales.
[640] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

se, antes de tudo, em direitos de acesso, retificação e eliminação de dados, garantidos de forma muito abrangente, combinado com o registro obrigatório de bases de dados.[641]

Essa configuração permite que a Autoridade de Proteção de Dados realize um controle prévio do tratamento previsto, através da análise de informações como os procedimentos de coleta e tratamento de dados, medidas de segurança e descrição técnica da base de dados, destino dos dados em caso de comunicação, entre outras. A Autoridade pode também, seja através de denúncias, inspeções ou solicitação de informações, fiscalizar o cumprimento da lei, podendo aplicar as sanções administrativas permitidas, quais sejam, advertência, multa ou suspensão de bases de dados.[642]

Uma última característica da Autoridade de Proteção de Dados uruguaia é que esta não possui competência jurisdicional ou de resolução de conflitos. Ao contrário de modelos como o europeu, a Autoridade uruguaia não tem poder decisório para determinar certa conduta a um ente, público ou privado, que entre em conflito com um cidadão. Ao invés disso, a Autoridade deve informar ao cidadão que a procure os meios judiciais a sua disposição para buscar a tutela adequada de seus direitos.[643]

Não há, pois, uma instância administrativa dedicada a questões relacionadas a proteção de dados, sendo tais casos direcionados ao Poder Judiciário em geral, que pode ser acionado exclusivamente pelo titular dos dados.[644]

Por fim, é necessário notar que o modelo regulatório uruguaio promove a judicialização de conflitos sobre dados pessoais, contando o sistema com um remédio específico, o Habeas Data. Essa ação visa especificamente permitir ao cidadão "tomar conhecimento de dados referentes a sua pessoa, e sua finalidade e usos, que constem em bancos de dados público ou privados" podendo exigir, segundo o caso, sua retificação, inclusão ou supressão.[645]

---

641 GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

642 GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

643 GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

644 GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

645 GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

Na ausência de meios administrativos de solução de controvérsias, salvo a negociação direta com o responsável pelo tratamento ou pela pressão exercida por sanções administrativas da Autoridade de Proteção de Dados em casos coletivos, resta ao cidadão buscar o Poder Judiciário (o Estado).

5.2. O modelo brasileiro de inspiração europeia

O modelo regulatório nacional estrutura-se em volta da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018, ou LGPD) e traz uma necessária organicidade ao arcabouço legal brasileiro. A LGPD tenta unificar os mais de 40 diferentes estatutos que atualmente governam os dados pessoais, *on-line* e *off-line*, no Brasil, substituindo certas regulações e suplementando outras.

Essa unificação de regulamentos, frequentemente díspares e contraditórios, é somente uma das similaridades que compartilha com o Regulamento Geral sobre a Proteção de Dados (GDPR) do qual retira clara inspiração.

Conforme nos expõe Sombra: [646]

> Além de ter sido uma das últimas democracias da América Latina a ter um marco regulatório de proteção de dados pessoas, a legislação brasileira pode ser praticamente considerada como um transplante legal da GDPR, na medida em que muitos dos seus pontos são frutos de inspiração do modelo europeu, dada a pressão comercial pela manutenção das relações com aquele bloco. Um claro exemplo disso advém da comparação dos qualificadores acrescidos ao consentimento, que bem demonstra o quanto o Brasil foi incapaz de olhar para outros modelos regulatórios e suas experiências positivas, conforme se observa na tabela abaixo:

[646] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 132.

Figura 5 - Similaridade entre o consentimento na LGDP e no GDPR

GDPR	LGPD
Consentimento deve ser: • Prévio • Livre • Informado • Específico • Indicação inequívoca por declaração ou ação afirmativa Se para dados sensíveis, também deve ser: • Explícito Consentimento pode ser revogado a qualquer tempo. Consentimento deve ser manifestado de maneira apartada de outros termos.	Consentimento deve ser: • Prévio • Livre • Informado • Para uma finalidade determinada • Inequívoco • Por escrito ou outro meio que demonstre a vontade do titular Se para dados sensíveis, também deve ser: • Específico • Em destaque Consentimento pode ser revogado a qualquer tempo. Consentimento deve ser manifestado de maneira apartada de outros termos.

Fonte: SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 132

As similaridades entre as duas normativas não param por aí, havendo um ressonância entre elas naquilo que se entender por dados pessoais e dados pessoais sensíveis; nos direitos garantidos aos titulares de dados pessoais;[647] nas exigências para a transferência de dados internacionais; e nos poderes sancionatórios conferidos à autoridade de controle.

De outro lado, talvez a mais significativa diferença entre a LGPD e o Regulamento europeu recaia sobre aquilo que se qualifica como bases legais para o

[647] O artigo 18 da LGPD prevê nove direitos fundamentais que titulares de dados possuem: (a) Confirmação da existência de tratamento; (b) Acesso aos dados; (c) Correção de dados incompletos, inexatos ou desatualizados; (d) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei; (e) Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (f) Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no artigo 16 da lei; (g) Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (h) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; (i) Revogação do consentimento, nos termos do parágrafo 5º do artigo 8º da lei.
Ainda que o GDPR só tenha garantido oito direitos fundamentais, eles são essencialmente os mesmos direitos que a LGPD menciona. Aparentemente a LGPD especificou "o direito a ser informado, pelo controlador, sobre com quais entidades públicas ou privadas ele compartilhou seus dados" da disposição mais geral da GDPR sobre o "direito de ser informado", para torná-lo mais explícito.

tratamento de dados. Enquanto o GDPR tem seis bases legais para o processamento, e o controlador de dados deve escolher uma delas para justificar a utilização de dados do titular, a LGPD, em seu artigo 7º, lista dez bases. São eles: (a) diante do fornecimento de consentimento pelo titular; (b) para o cumprimento de obrigação legal ou regulatória pelo controlador; (c) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do capítulo IV da Lei; (d) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (e) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; (f) para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); (g) para a proteção da vida ou da incolumidade física do titular ou de terceiro; (h) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (i) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; e, (j) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Apesar disso, substancialmente, a Lei Geral se assemelha ao Regulamento. A inclusão de uma base legal relacionada ao crédito parece se alinhar às discussões decorrentes de nossa tradição jurídica que já tinham nos escores de crédito um ponto de questionamento, inclusive, no Poder Judiciário.

Em relação às transferências internacionais de dados, o alinhamento da LGPD com o GDPR pode ser explicado, sobretudo, pela preocupação e interesse em manter o contínuo fluxo comercial do Brasil com a União Europeia. Argumenta-se que se o modelo brasileiro de transferência internacional discrepasse das condições e requisitos do GDPR, possivelmente o Brasil permaneceria sem o reconhecimento da adequação da União Europeia e as transferências somente poderiam ser realizadas mediante a adoção de salvaguardas pelas empresas (como BCRs – *Binding Corporate Rules*, ou regras corporativas vinculadas –, cláusulas-padrão, contratos-tipo, certificações e códigos de conduta), o que impactaria no custo das operações.[648]

[648] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 132.

A rigor, a LGPD inovou apenas naquilo que considerou possível ou particular à realidade do país, ou seja, o tratamento de dados realizado pelo poder público, que administra as bases de dados mais relevantes dos cidadãos.[649]

O capítulo de transferência internacionais da LGPD revela uma especial atenção do legislador. Tal preocupação pode ser explicada pelo fato de que, caso os dados pessoais de um titular sejam coletados no Brasil, transferidos e tratados em outra jurisdição, os referidos dados se sujeitarão a outras legislações – as quais poderão ser mais brandas e menos protetivas dos direitos dos titulares dos dados, se comparadas à legislação brasileira. Nesse ponto, a LGPD em muito se aproximou do modelo europeu, na medida em que replica o uso da extraterritorialidade para ver tutelado os interesses de seus cidadãos, ainda que fora do espaço nacional de sua soberania.[650]

Outra explicação para o cuidado da LGPD com as transferências internacionais envolve as questões de territorialidade (*data localization* ou *data residency request*) e seus impactos no *enforcement* pelas autoridades de segurança pública, que acreditam que os dados pessoais deveriam sempre ser armazenados no país de origem para viabilizar o acesso nos casos de investigações criminais e assegurar a imposição de sanções.[651]

Como forma de tentar equilibrar esse debate, a LGPD optou por adotar o regime da extraterritorialidade ampla da sua aplicabilidade ao invés de se ocupar de exigências territoriais que se mostrariam incapazes de apresentar soluções plausíveis para regular as empresas de tecnologia.

Assim, operações de tratamento de dados realizadas dentro do território brasileiro estão invariavelmente sujeitas à aplicação da LGDP. Além de operações realizadas dentro do país, quando o tratamento tiver por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no território brasileiro, a lei também será aplicável, ainda que a organização responsável por essa atividade esteja sediada ou localizada fora do país. Desse modo, o local onde os dados são tratados não é requisito único ou preponderante para aplicação da lei, sendo também importante identificar a localização do indivíduo cujos dados serão coletados.[652]

---

649 SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 132.
650 SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 132.
651 SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 132.
652 SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 132.

É evidente, portanto, a reprodução dos mecanismos de transferências internacionais de dados da GDPR por parte da LGPD e a adoção do *geographically-based approach*. Para não se mencionar que o modelo brasileiro é uma cópia fiel da GDPR, cumpre esclarecer que em dois pontos relevantes deixou-se de seguir a legislação europeia. Primeiro, o Brasil não coloca como obrigatória a designação de um representante no Brasil quando o responsável pelo tratamento dos dados (controlador) aqui não esteja estabelecido, o que representa um sério risco à efetiva fiscalização e imposição das sanções previstas na lei. Segundo, ao contrário da GDPR, o Brasil não previu derrogações ao regime legal de transferência de dados, como aquelas pertinentes às transferências não reiteradas, massivas ou estruturais, ou realizadas mediante o consentimento, conclusão ou execução de um contrato ou exercício de defesa em processos judiciais.[653]

5.3. Algumas ponderações sobre os modelos de proteção de dados analisados

Para melhor entendermos as nuances entre os três modelos apontados (subsumindo-se o brasileiro ao modelo europeu), buscaremos enquadrá-los em três facetas da estratégia regulatória: o papel do Estado, o papel do mercado e o papel da tecnologia. [654]

Em relação ao papel do Estado incluímos não só seu papel normativo, mas também fiscalizatório com a atuação das Autoridades de Proteção de Dados e órgãos semelhantes, e jurisdicional, com a atuação do Poder Judiciário.

Os três modelos analisados utilizam-se, de alguma forma, desses poderes para tutelar a proteção de dados, mas o fizeram de modos diferentes.

Nesse sentido, o modelo norte-americano utiliza-se de normas setoriais para criar princípios e regras sobre proteção de dados em determinados contextos, mas opta por não disciplinar uma normativa forte e centralizadora, genérica, para garantir um direito geral à proteção de dados.[655]

---

[653] SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019, p. 132.
[654] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[655] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

Nesse modelo, há alguma atuação das autoridades fiscalizatórias, em geral, também setoriais, mas com ênfase em seu papel fiscalizador/sancionatório e normativo. De modo geral, o papel do Estado no modelo estadunidense é reduzido, e mesmo a legislação existente sobre o tema remete muitos assuntos à autorregulação, conforme aponta Guilherme Guidi.[656] O Poder Judiciário aparece como recurso final para a resolução dos conflitos eventualmente surgidos durante a relação entre titular de dados e responsável pelo tratamento, mas tem grande importância para o modelo, dada a ausência de alternativas mais especializadas para a resolução de controvérsias.

O modelo uruguaio, por sua vez, tem uma abordagem diferente, na medida em que possui normas centrais, abrangentes e generalistas sobre proteção de dados, que reúnem os princípios básicos que devem informar as demais regras do sistema, qualquer que seja sua natureza. Mesmo os códigos de autorregulação são homologados com sua inserção no campo legislativo estatal, por normativa da respectiva Autoridade de Proteção de Dados. Talvez o ponto de maior interesse aqui seja o modelo fiscalizatório, baseado sobretudo no cadastramento prévio de bancos de dados, a cargo da Autoridade de Proteção, tratando-se de um caso singular em nossa análise e de Guidi.[657]

Na ausência de competência específica para solucionar contendas entre titulares e responsáveis pelo tratamento de dados,[658] resta ao Judiciário solucionar os casos relativos à proteção de dados pessoais. Um aspecto interessante desse modelo é o remédio de *Habeas Data*, que foi adaptado e expandido, de modo a servir como ferramenta universal para execução específica de certas obrigações.[659]

O modelo europeu (ao qual se filia o brasileiro), por seu turno, apesar de ter um grande número de normas centrais sobre proteção de dados pessoais, delega grande parte da competência legislativa – no que toca os aspectos técnicos e outros assuntos de grande especificidade – à Autoridade de Proteção de Dados. A recente reforma legislativa que representou o Regulamento, concedeu à Autoridade de Controle ainda mais e maiores

---

656 GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

657 GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

658 Lembrando que a APD uruguaia pode, diante da denúncia do descumprimento de um direito de acesso, por exemplo, aplicar uma sanção (advertência, multa ou suspensão do banco de dados), mas não tem meios específicos para exigir o cumprimento da obrigação para com o titular dos dados.

659 GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

poderes fiscalizatórios e sancionatórios, permitindo a ela maior espaço de manobra. É de imenso interesse o papel central das Autoridades de Controle Independentes no modelo europeu pois, além de suas competências normais, atuam também na resolução de conflitos diretamente entre as partes, em uma esfera administrativa, evitando-se assim a judicialização de inúmeros conflitos.[660]

No que atine ao papel do mercado, o modelo estadunidense talvez seja o que mais nele se fia, porquanto sua regulação esparsa exige que grande parte da prática comum e aceitável seja definida pelos próprios agentes econômicos, seja por meio da prática contratual (sujeita a eventual inspeção judicial), seja pela autorregulação. Em um modelo onde a liberdade contratual é um dos fundamentos básicos da matéria, é de se esperar que a garantia de direitos venha através de incentivos econômicos para isso. Assim, ainda que nem sempre no interesse do consumidor ou do titular dos dados, há uma abertura para que a privacidade do consumidor seja definida pelo retorno esperado.[661]

O modelo uruguaio é, dentre os modelos analisados, o que menos recorre ao mercado para tentar moldar comportamentos. O modelo de tutela impositivo, como descrito anteriormente, ignora parcialmente o valor dos mecanismos econômicos e seu impacto regulatório, fazendo mera referência a códigos de conduta (um tanto esquecidos), sem outros pontos de contato interessantes entre Direito e Economia [662]

O modelo europeu, de outra banda, apesar de não trazer a definição exata da coleta e do tratamento de dados na lei, apresenta uma abordagem interessante sobre o papel do mercado em um modelo regulatório. Em suma, a União Europeia utiliza mecanismos de mercado para incentivar a adesão a padrões de tutela já definidos nas normas sobre proteção de dados. Tais mecanismos geralmente funcionam em uma base de troca, sendo que os agentes que optarem por aderir a tais regras, em tese, poderiam receber benefícios competitivos por isso.

O exemplo mais óbvio dessa política é justamente o sistema de certificação criado pelo GDPR, que permite às empresas utilizarem certos certificados e selos de qualidade quando seja constatado o cumprimento substancial das normas em vigor. No

[660] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[661] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.
[662] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

contexto atual, em que a privacidade ganha importância para o cidadão comum, a vantagem competitiva expectável acaba por criar interesses convergentes das duas pontas da transação: proteger a privacidade do usuário deixaria de ser um custo para se tornar um diferencial competitivo e uma fonte de receitas.[663]

Por fim, a tecnologia em si tem um papel nos modelos regulatórios. Enquanto todos recomendam certas medidas de segurança e sigilo (como a adoção da criptografia e do processo de anonimização), o modelo europeu possui um diferencial de nota na matéria. Com o especial reforço na recente reforma legislativa, os conceitos de *privacy by design and by defaut* e de *privacy enhancing technologies*, surgiram e ganharam espaço para incentivar alterações na "arquitetura normal" – o modo e o que a tecnologia permite em razão do modo como é construída – para fazer com que o próprio valor da privacidade tenha lugar na concepção inicial de qualquer serviço ou produto. Essa característica, no entanto, na visão de Guidi é arriscada na medida em diminui a neutralidade tecnológica do texto e arrisca torná-lo obsoleto mais cedo do que seria esperado.[664]

Posto isso tudo, passaremos a avaliar as estratégias regulatórias e modelos de regulação esperados e incentivados ao contexto nacional, trazendo nossa proposta de intervenção para a diminuição dos riscos relacionados ao contexto de tratamento de dados brasileiro.[665]

A análise do próximo capítulo trará a construção e expansão de um modelo regulatório baseado na integração entre mecanismos regulatórios típicos da corregulação, visando incrementar-se o cenário de proteção, diante dos riscos já explorados associados às novas tecnologias.

---

[663] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

[664] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

[665] Especificamente em relação ao modelo brasileiro, de inspiração europeia, temos que, apesar deste também ser fundar em uma lei geral que tutele a matéria, com diversas atribuições elencadas à Autoridade de Controle, o modelo brasileiro se distanciou um pouco do europeu ao mitigar a independência dessa Autoridade de Controle (que somente recentemente tem ganhado a autonomia devida), aliado à diminuição, também, da garantia de se pedir a revisão, por um humano, das decisões automatizadas. Outro ponto que deve ser apontado é nossa cultura de litígio, expectando-se um forte papel do judiciário na concretização das salvaguardas disciplinadas pela Lei Geral de Proteção de Dados Pessoais, não obstante a atuação da Autoridade Reguladora esteja em expansão.

PARTE III – MECANISMOS HÍBRIDOS DE REGULAÇÃO COMO INCENTIVO À ADOÇÃO DE PRÁTICAS DE CONFORMIDADE

A terceira parte do trabalho dedica-se a estudar as limitações de um modelo regulatório tipicamente estatal, acenando para espécies híbridas de regulação, por meio da utilização de códigos de conduta, selos, processos de certificação e listagens.

Em nosso sentir, a utilização desses mecanismos, de forma associativa, poderia gerar um substancial incremento na capacidade das políticas públicas de promover a segurança no tratamento de dados pessoais, diminuindo os riscos associados às novas e muito diversas tecnologias.

A terceira parte considera as limitações estatais e propõe um cenário de acoplamento estrutural (como abordado Luhmann)[666] por meio do diálogo entre diferentes estratégias regulatórias e atores, capazes de mitigar fatores de risco relacionados às tecnologias de comunicação e informação (TICs).

1. As limitações do Estado como agente regulador

Se a tônica da primeira seção do trabalho foi o cenário de exploração humana proporcionado pela força disruptiva da tecnologia, tendente a escapar de qualquer espécie de regulação estatal,[667] aqui traremos um outro ponto vista, representado pelas abordagens das limitações do Estado como agente regulador.

1.1. As tarefas de regular

A aplicação de controles regulatórios envolve a realização de uma série de tarefas. Mesmo que se suponha que os objetivos regulatórios tenham sido estabelecidos com clareza, ainda há uma série de tarefas a serem realizadas.

---

[666] LUHMANN, Niklas. **Introduction to systems theory**. BAECKER, Dirk (ed.). GILGEN, Peter (trad.). Cambridge: Polity Press, 2013.

[667] Embora a assertiva tenha sido redigida de forma neutra, não ignoramos o fato de que a fuga à regulação estatal é, muitas vezes, um objetivo direto de certos *stakeholder*. Apontamos essa conclusão na primeira parte do trabalho quando abordamos o *dumping* social e outras formas de se furtar à legislação trabalhista, como forma de reduzir custos e se aumentar vantagem competitiva.

Conforme discorrem Baldwin, Cave e Lodge[668] todo processo regulatório deve levar em conta, ao menos, cinco etapas, expressas pela sigla DREAM (*Detection, Responding, Enforcing, Assessing, Modifying*), conforme quadro a seguir, elaborado pelos dos autores:

Figura 6 - Regulatory tasks: the DREAM framework

1.	**DETECTING**	The gaining of information on undesirable and non-compliant behaviour.
2.	**RESPONDING**	The developing of policies, rules, and tools to deal with the problems discovered.
3.	**ENFORCING**	The application of policies, rules, and tools on the ground.
4.	**ASSESSING**	The measuring of success or failure in enforcement activities.
5.	**MODIFYING**	Adjusting tools and strategies in order to improve compliance and address problematic behaviour.

Fonte: BALDWIN, Robert, CAVE, Martin e LODGE, Martin. **Understanding Regulation**, 2. ed. Oxford: Oxford University Press, 2012, p. 227.

Segundo avaliam os autores,[669] o ciclo regulatório envolve ao menos as seguintes tarefas: a coleta de informações sobre possíveis riscos e potenciais problemas sobre os quais se pretende intervir (comportamentos indesejáveis ou desconformes); a formulação de regras, políticas e ferramentais de respostas para lidar com esses problemas; a aplicação ou implementação dessas regras, políticas e ferramentas em campo; a fiscalização quanto ao sucesso das medidas projetadas (monitoramento); e, por fim, a adoção de correções ou ajuste nas estratégias regulatórias projetadas, visando aprimorar as soluções endereçada aos problemas.

Cada uma dessas atividades compreende diferentes técnicas e ferramentas de intervenção, agrupadas pela literatura,[670] em, ao menos, sete formas de intervenção, cada uma delas associadas a um conjunto de vantagens de desvantagens (identificadas na Tabela 4, visível no Anexo II), são elas: 1. Comando e controle (*Command & Control)*; 2. Incentivos (*Incentives*); 3. Controles de aproveitamento de marcado (*Market-harnessing controls*), como: (a) Leis concorrenciais (*Competition laws*), (b) Franquias

[668] BALDWIN, Robert, CAVE, Martin e LODGE, Martin. **Understanding Regulation**, 2. ed. Oxford: Oxford University Press, 2012, p. 227.
[669] BALDWIN, Robert, CAVE, Martin e LODGE, Martin. **Understanding Regulation**, 2. ed. Oxford: Oxford University Press, 2012, p. 227.
[670] BALDWIN, Robert, CAVE, Martin e LODGE, Martin. **Understanding Regulation**, 2. ed. Oxford: Oxford University Press, 2012, p. 134.

(*Franchising*), (c) Contratações (*Contracting*) e (d) Permissões negociáveis (*Tradable permits*); 4. Divulgação (*Disclosure*); 5. Ações diretas e soluções de designe (*Direct action and design solutions*), como: (a) Intervenções diretas (*Direct interventions*) e (b) Estratégias de "Nudge" ('*Nudge' strategies*); 6. Legislações de direitos e responsabilidades (*Rights and liabilities laws*); e 7. Compensações públicas/segurança social (*Public compensation / social insurance*).

Os autores[671] descrevem essas sete estratégias como a aplicação das "capacidades ou recursos básicos que os governos possuem e que podem utilizar para influenciar a atividade industrial, econômica ou social". Assim, o governo pode (a) usar sua autoridade legal e a força da lei para perseguir objetivos políticos, ou pode (b) empregar riqueza por meio de contratos, empréstimos, doações, subsídios ou outros incentivos para influenciar determinada conduta, (c) aproveitar mercados canalizando forças competitivas para fins específicos, (d) distribuir informações estrategicamente para desencadear ações programadas, (e) agir diretamente adotando ações materiais próprias, ou, ainda, (f) conferir proteção para criar incentivos de ação.[672]

Baldwin, Cave e Lodge[673] apontam, ainda, que o governo pode influenciar o resultado de qualquer situação aplicando uma mistura de incentivos e controles para alcançar o resultado desejado. Essa mistura de incentivos também é apregoada por Murray e Scott, [674] propondo um modelo híbrido de regulação, diante das peculiaridades desse novo ambiente regulatório que é a internet.

---

[671] BALDWIN, Robert, CAVE, Martin e LODGE, Martin. **Understanding Regulation**, 2. ed. Oxford: Oxford University Press, 2012, p. 227.

[672] MURRAY, Andrew D..**The Regulation of Cyberspace: Control in the Online Environment**. New York: Taylor e Francisco, 2007, p. 29.

[673] BALDWIN, Robert, CAVE, Martin e LODGE, Martin. **Understanding Regulation**, 2. ed. Oxford: Oxford University Press, 2012, p. 227.

[674] "Da mesma forma, Colin Scott e eu, em nosso artigo Controlling the New Media, sugerimos um foco em modelos híbridos de regulação. Nós, como Lessig, sugerimos quatro modalidades de regulação que intitulamos, (1) controle hierárquico, (2) controle baseado na competição, (3) controle baseado na comunidade e (4) controle baseado no design. Ao contrário de Lessig, reconhecemos que o desenvolvimento de estruturas regulatórias é frequentemente de natureza orgânica, embora imaginemos que órgãos reguladores, por meio do emprego de controles hierárquicos, moldando a estrutura de tais sistemas organicamente desenvolvidos. Assim, neste artigo, apoiamos o consenso de que os reguladores projetam sistemas regulatórios. Logo, todos esses modelos compartilham uma base comum. Todos são modelados com base na crença de que os projetos regulatórios são baseados em escolhas ativas feitas pelos reguladores: eles sugerem um regulador que trabalha dentro de um ambiente estabelecido e que tem tempo para considerar positivamente as decisões políticas". Tradução do autor. No original: "Similarly, Colin Scott and myself in our paper Controlling the New Media suggest a focus on hybrid models of regulation. We, like Lessig, suggest four modalities of regulation which we title, (1) hierarchical control, (2) competition-based control, (3) community-based control and (4) design-based control. Unlike Lessig, we acknowledge that the development of regulatory structures is often organic in nature, though we imagine regulatory bodies, through the employment of hierarchical controls, fashioning the structure of such organically developed systems. Thus, ultimately in this paper we support the consensus that regulators

Os autores, utilizando-se das teorias de Lessing[675] – que enxerga quatro fatores de constrangimento que influenciam o comportamento dos indivíduos no cyberespaço: a lei, as normas sociais, o mercado e a arquitetura – propõem um quadro de regulação baseado em quadro elementos de controle: (1) controle hierárquico, (2) controle baseado na competição, (3) controle baseado na comunidade e (4) controle baseado no designe, conforme tabela a seguir:

Tabela 2 - Elements of Control Systems.

Element of a Control System	Hierarchical Control	Community-Based Control	Competition-Based Control	Design-Based Control
Standard Setting	Law or Other Formalised Rules	Social Norms	Price/Quality Ratio (and equivalents with non-market decisions)	Inbuilt design features and social and administrative systems
Information Gathering	Monitoring (by agencies or third parties)	Social Interaction	Monitoring by dispersed buyers, clients, etc	Interaction of design features with environment
Behaviour Modification	Enforcement	Social Sanctions (eg ostracism, disapproval)	Aggregate of decisions by buyers, clients, etc on purchase, take-up, location etc	As for information gathering (self-executing)

Fonte: MURRAY, Andrew D..**The Regulation of Cyberspace: Control in the Online Environment**. New York: Taylor e Francisco, 2007, p. 29.

Essa abordagem surge da noção de que o ciberespaço por suas especiais características, demandam uma ação peculiar de respostas aos diversificados problemas que enfrentam. Nas palavras de Murray e Scott[676]:

design regulatory systems. Thus, these models all share a common foundation. All are modelled upon the belief that regulatory designs are based upon active choices made by regulators: they suggest a regulator who works within a settled environment and who has time to positively consider policy decisions". MURRAY, Andrew D..**The Regulation of Cyberspace: Control in the Online Environment**. New York: Taylor e Francisco, 2007, p. 29.

[675] LESSIG, Lawrence. **Code: And Other Laws of Cyberspace, Version 2.0**. New York: Basic Books, 2006.

[676] Tradução do autor. No original: "The emergence and identification of the new media, premised upon the development and application of digital technologies, has created new sources and locations of power, many not fully documented or understood. Those new configurations of power which have been identified have stimulated distinctive literatures about the most appropriate mechanisms of control. With much of the literature classical or 'command and control' regulation is held either to be undesirable or unfeasible in the face of the new policy challenges. For one school of thought the changing market structures associated with the new media indicate a reduced role for classical regulation and its virtually total displacement by

> A emergência e identificação das novas mídias, tendo como premissa o desenvolvimento e aplicação de tecnologias digitais, criou fontes e locais de poder, muitos não totalmente documentados ou compreendidos. Essas novas configurações de poder que foram identificadas estimularam distintos estudos sobre os mecanismos mais apropriados de controle. Em grande parte da literatura, a regulação clássica ou de "comando e controle" é mantida mesmo que seja indesejável ou inviável diante dos novos desafios políticos. Para outras escolas de pensamento, no entanto, as mudanças nas estruturas de mercado associadas às novas mídias indicam um papel reduzido para a regulação clássica e seu deslocamento quase total pelo direito concorrencial. Para outra escola, o surgimento da Internet apresenta problemas insuperáveis para a regulação e mecanismos alternativos de controle baseados em autorregulação e arquitetura são mais prováveis de serem eficazes.

Murray e Scott,[677] de outra banda, partindo para uma perspectiva estreita sobre a regulação das novas mídias digitais, avalia que o cenário regulatório está sujeito a quatro problemas essenciais: problemas de arbitragem regulatória, anonimato e escassez de recursos.

Julia Balck,[678] por sua vez, expõe de forma minuciosa as falhas e contradições de um modelo regulatórios tipicamente estatal, baseados em estruturas de comando e controle, propondo um modelo descentralizado de regulação.

A autora argumenta que a regulamentação de Comando e Controle postula um papel particular para o Estado contra o qual a análise da "descentralização" é contraposta. Nesse modelo centralizado de intervenção assume-se que o Estado tem total capacidade de comandar e controlar, e de ser potencialmente eficaz nessa tarefa.

Presume-se uma abordagem unilateral (o Estado comandando e os demais atores obedecendo), baseado em simples relações de causa e efeito, e em uma pressuposta progressão linear dessas políticas desde sua formulação até implementação.

As falhas desse modelo são identificadas pela autora de várias maneiras como, por exemplo, o fato de que os instrumentos usados (leis respaldadas por sanções) sejam

---

competition law.1 For another school the emergence of the Internet presents insuperable problems for classical regulation and alternative mechanisms of control based on self-regulation and architecture are more likely to be effective". MURRAY, Andrew D.; SCOTT, Colin. Controlling the New Media: Hybrid Responses to New Forms of Power. **The Modern Law Review**. v. 65. n. 4, 2002, pp. 491–516. JSTOR. Disponível em: http://www.jstor.org/stable/1097592. Acesso em: 29 set. 2022.

[677] MURRAY, Andrew D.; SCOTT, Colin. Controlling the New Media: Hybrid Responses to New Forms of Power. **The Modern Law Review**. v. 65. n. 4, 2002, pp. 491–516. JSTOR. Disponível em: http://www.jstor.org/stable/1097592. Acesso em: 29 set. 2022.

[678] BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 116.

inadequados e pouco sofisticados (falha de instrumento); que o governo não tem conhecimento suficiente para ser capaz de identificar as causas dos problemas, para projetar soluções que sejam apropriadas, e identificar seu não cumprimento (falha de informação); que a implementação das regras projetada seja inadequada (falha de implementação); e/ou que os regulados não estejam suficientemente inclinados a cumprir as políticas projetadas (falha de motivação).

1.2. Um modelo descentralizado de regulação

No cenário atual, não é precipitado cogitar-se da insuficiência dos mecanismos de formulação e implementação de políticas públicas pelo Estado-regulador diante deste ambiente tecnológico e dinâmico. Muitos autores situam a discussão sobre regulação da das novas tecnologias dentro de um debate maior sobre funções, modos e estratégias relevantes para a regulação de ambientes globalizados, complexos e altamente caracterizados pela incerteza de conhecimento.

A compreensão descentralizada da regulação é baseada em diagnósticos ligeiramente diferentes de falha regulatória, diagnósticos que se baseiam e dão origem a uma compreensão alterada da natureza da sociedade, do governo e da relação entre eles.

A partir disso, Black[679] oferece um conjunto de características que diferenciam e explicam a necessidade de modelos descentralizados de atuação.

O primeiro aspecto apontado pela autora é a complexidade. Ela refere-se tanto à complexidade causal quanto à complexidade das interações entre os atores da sociedade (ou sistemas, para os adeptos à teoria dos sistemas). Há um reconhecimento de que os problemas sociais são o resultado de vários fatores atuantes, dos quais nem todos podem ser conhecidos, cuja natureza e relevância mudam ao longo do tempo, e a interação entre eles será apenas imperfeitamente compreendida por um único ator. A atenção também é chamada, em escritos mais conceituais, para as interações dinâmicas entre atores e/ou sistemas e para as operações de forças que produzem uma tensão constante entre estabilidade e mudança dentro de um sistema vagamente definido. Essas interações são em si complexas e intrincadas, e os atores são diversos em seus objetivos, intenções, propósitos, normas e poderes.

[679] BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 106-1-7.

O segundo aspecto de influência é a fragmentação e a construção do conhecimento na atualidade. Essa característica às vezes é referida simplesmente como a assimetria de informação entre o regulador e o regulado: o governo não pode saber tanto sobre a indústria quanto a indústria sabe sobre si mesma. Formulado nesses termos, o problema é familiar e bem reconhecido. A partir de uma teoria descentralizada da regulação, no entanto, o problema da informação é ainda mais complexo, pois diferentemente da análise tradicional, ela não pressupõe que qualquer ator tenha todas as informações necessárias para resolver os problemas sociais: não se trata, simplesmente, de uma questão de a indústria ter conhecimento e o governo dele precisar. Ao contrário disso, a descentralização reconhece que nenhum ator individual possui todo o conhecimento necessário para resolver problemas complexos, diversos e dinâmicos, e nenhum ator isoladamente possui a visão geral necessária para empregar todos os instrumentos necessários para tornar a regulamentação eficaz.

O problema pode ser enquadrado de forma mais radical; isto é, não apenas o conhecimento é fragmentado, mas também a informação é construída socialmente: não existem coisas como verdades sociais "objetivas". Conforme anota Black,[680] chega-se a essa conclusão por meio de várias rotas teóricas, a mais influente nos escritos regulatórios tem sido a autopoiese. Subsistemas autopoieticamente fechados, como política, administração e direito, constroem suas imagens de outros subsistemas apenas por meio das lentes distorcidas de seu próprio aparato perceptivo, ou seja, por meio de experiências de seu ambiente e em termos de uma manifestação entre oposições binárias (é/não é; sim/não). Assim, a informação que os sistemas possuem sobre outros sistemas é simplesmente aquela que eles próprios construíram de acordo com seus próprios critérios. (geralmente por contraste e oposição a seu próprio conhecimento).[681] Black[682] ressalta que essa mesma conclusão também é alcançada por meio da hermenêutica, ou por meio de várias vertentes do novo institucionalismo, bem como de algumas vertentes da teoria cultural e de algumas teorias de tomada de decisão, a saber: os tomadores de decisão,

[680] BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 107.

[681] Ajuda a compreender, avaliar que, sendo homem e me identificando como tal, consigo perceber que o oposto (a mulher) é diferente de mim. A partir do meu sistema de informações, eu seria capaz de identificar proposições binárias (entre ser e não ser), muito embora, por não fazer parte daquele grupo, jamais poderia compreender o que é ser mulher e as implicações de pertencer àquele grupo.

[682] BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 107.

organizações, etc., constroem imagens de seu ambiente em sua própria imagem ou por meio de seus próprios quadros cognitivos.[683]

O terceiro aspecto é a fragmentação do exercício do poder e do controle. Este é o reconhecimento de que o governo não detém o monopólio do exercício do poder e do controle, fragmentado entre os atores sociais e entre estes e o Estado. Os sistemas regulatórios existentes nas esferas sociais são tão importantes para a ordenação social, se não mais, quanto a ordem formal do Estado. A regulamentação ocorre em muitos locais, em muitos fóruns e espaços.

A fragmentação do exercício do poder e do controle acarreta o quarto aspecto da compreensão descentrada da regulação: o reconhecimento da autonomia dos atores sociais. A autonomia não é aqui usada no sentido de liberdade da interferência do governo, mas no sentido de que os atores continuarão a se desenvolver ou agir à sua maneira na ausência de intervenção. A regulação, portanto, não pode tomar como constante o comportamento dos regulados.

Segundo destaca Black[684]: "Regulação é, como Foucault disse sobre governança, a 'conduta da conduta', ou conforme reformulado por Rose, 'agir sobre a ação'."

Isso tem várias implicações práticas, a mais óbvia delas que a regulação produzirá mudanças no comportamento e resultados que não são intencionais (embora não necessariamente adversos); e que sua forma pode ter de variar dependendo da atitude do regulado em relação à adequação, atitude que ele mesmo pode afetar e que a autonomia do ator regulado irá, até certo ponto, torná-lo insuscetível à regulação externa.

Além disso, nenhum ator isolado pode esperar dominar o processo regulatório unilateralmente, pois todos os atores podem ser severamente restringidos em alcançar seus próprios objetivos, não apenas por limitações em seu próprio conhecimento, mas também pela autonomia de outros. Se isso acontece por conta da capacidade dos atores de empregar poderes e recursos direcionados às suas ações, ou por causa das características inerentes do sistema, ou por qualquer outro motivo, ainda é um ponto de debate.

---

[683] Para uma discussão geral, ver: BLACK, Julia. New Institutionalism and Naturalism in Socio-Legal Analysis: Institutionalist Approaches to Regulatory Decision Making. **Law & Policy**, v. 19, n. 1, January 1997, p. 51-94. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/lawpol19&i=61. Acesso em: 25 nov. 2022.

[684] Tradução do autor. No original: "Regulation is, as Foucault said of governance, the 'conduct of conduct', or as rephrased by Rose, 'to act upon action'". BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 109.

Black[685] avalia, nesse sentido, que a teoria da autopoiese tem a análise mais radical da autonomia. Os autopoeticistas divergem sobre o significado de autonomia, mas amplamente se referem à autorregularão, autoprodução e auto-organização de sistemas que são normativamente fechados, mas cognitivamente abertos. A consequência disso é que nenhum sistema pode agir diretamente sobre o outro, e as tentativas de fazê-lo resultarão no trilema regulatório de Teubner: a indiferença do sistema "alvo" à intervenção, a destruição do próprio sistema "alvo" ou a destruição do sistema interveniente.[686]

O quinto aspecto da compreensão descentralizada da regulação é a existência e a complexidade das interações e interdependências entre os atores sociais e o governo no processo de regulação. Esta é uma reivindicação tanto descritiva quanto normativa. Descritivamente, observa-se que a regulação é um processo de mão dupla, ou de três ou quatro vias, entre todos os envolvidos no processo regulatório, e particularmente entre regulador e regulado na implementação da regulação. Nos termos de Offe,[687] a regulação é "coproduzida". Em parte, isso é expresso no argumento do "espaço regulatório", mas o argumento agrupa tantas variáveis que afetam a formação e implementação de políticas públicas que tende mais a obscurecer mais do aclarar a ideia.

A dinâmica da relação adotada no novo entendimento da regulação formulado por Black[688] é que existem interdependências e interações entre o governo e os atores sociais. Além disso, ela não se reduz ao simples caso de que a sociedade tem necessidades (problemas) e o governo capacidades (soluções). Ao contrário, cada ator deve ser visto como detentor de problemas (necessidades) e soluções (capacidades), sendo mutuamente dependentes um do outro para sua resolução e usos. Não se deve presumir, entretanto, que essas intervenções e interdependências estejam contidas dentro das fronteiras territoriais nacionais, as análises sobre a globalização enfatizam que elas podem se estender muito além delas.

---

685 BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 109.

686 BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 109.

687 OFFE, Claus. Contradictions of the Welfare State. London: Hutchinson & Co. (Publishers) Ltd, 1984.p 310.

688 BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 110.

A ideia de que a governança e a regulação são o produto de interações e interdependências leva a um sexto aspecto da compreensão descentralizada da regulação, que é o colapso da distinção público/privado em termos sociopolíticos e um repensar do papel da autoridade formal na governança e na regulamentação.

No entendimento descentralizado da regulação, a regulação ocorre na ausência de sanção legal formal – ela é o produto de interações, não do exercício da autoridade governamental formal e constitucionalmente reconhecida. O colapso da distinção público/privado como uma ferramenta útil para a análise da governança e da regulação se manifesta na identificação de organizações ou redes "híbridas" que combinam atores governamentais e não governamentais em uma variedade de maneiras. Black[689]consigna que para as alternativas de governo burocráticos (hierarquias) e de mercados foram adicionadas associações - os "governos de interesse privado" identificados por Streeck e Schmitter como o novo corporativismo.

Para a autora[690] o conceito de autoridade ainda desempenha seu papel, no entanto, para esses modelos compartilhados, por meio da autoridade do estado de fazer e impor decisões obrigatórias. Adições mais recentes são as redes de influências, nas quais dentro das interações de uma gama de atores, o Estado é apenas mais um. Conforme observado acima, governança e regulamentação são vistas como o resultado da interação entre ações de redes ou, alternativamente, "teias de influência" que operam na ausência de um governo formal ou de sanções legais. Na noção descentralizada da regulação, portanto, a autoridade formal *de lege* desempenha um papel ambíguo.

Dessa forma, a complexidade; a fragmentação e construção do conhecimento; a fragmentação do exercício do poder e do controle; a autonomia; as interações e interdependências dos atores; e o colapso da distinção público/privado: são os elementos do que compõem a "noção descentralizada da regulação". Juntos, eles sugerem um diagnóstico de falha regulatória que se baseia na dinamicidade, complexidade e diversidade da vida econômica e social assim como na dificuldade de aderência dos métodos tradicionais de regulação.

---

689 BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 110.

690 BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 110.

As marcas das estratégias regulatórias defendidas por essa corrente são híbridas (combinam atores governamentais e não governamentais), multifacetadas (utilizam várias estratégias diferentes simultânea ou sequencialmente) e indiretas.

Nesse contexto, as dificuldades de aderência dos meios tradicionais podem ser identificadas como um fenômeno comum subjacente às novas tecnologias, do qual decorrem diferentes consequências teóricas e empíricas, expressas a partir de diferentes terminologias.[691] São teorias distintas, que se expressam em campos do direito distintos, mas que têm em comum o esforço de interpretar esse cenário de insuficiência. Muitas dessas teorias foram desenvolvidas em momentos anteriores ou concomitantes aos debates sobre regulação da Internet, sem se referenciar ou condicionar necessariamente por eles, refletindo o que Gunther Teubner chama de "uma rápida proliferação de esferas regulatórias que estabelecem regimes específicos que, tendo alcance global, frustram a autonomia local ou regional do estado nação e do território".[692] Desse aspecto subjetivo fragmentado e necessariamente descentralizado do Estado, decorre a adoção de instrumentos de *soft law* (de forma exclusiva ou combinada com a *hard law* tradicional), "aptos a orientar políticas públicas ou a recomendar a implementação de mudanças institucionais"[693] de Estados membros, ou a constituir políticas organizacionais internas, como diretrizes, princípios gerais, recomendações ou políticas de uso.

Com efeito, essas teorias resultantes desse esforço de compreensão e conformação pela literatura acadêmica de um contexto de globalização econômica e cultural em curso, podem ser expressos nas ideias de *Estado Pós-Regulatório*, *Descentralização Administrativa*, *Direito Administrativo Global* e de *Constitucionalismo Global*.

1.3. Considerações sobre o *Estado Pós-Regulatório, Descentralização Administrativa, Direito Administrativo Global e Constitucionalismo Global*.

691 GRAFENSTEIN, Maximilian von. **The Principle of Purpose Limitation in Data Protection Laws**. The Risk- Based Approach, Principles, and Private Standards as Elements for Regulating Innovation. Baden-Baden: Nomos, 2018, p. 4.
692 TEUBNER, Gunther. **Constitutional Fragments: Societal Constitutionalism and Globalization**. Oxford: Oxford University Press, 2012, p. 52.
693 BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 52.

Considerando as diferentes correntes teóricas sobre uma mesma tendência global de pluralismo jurídico, dedicaremos algumas palavras a explicá-las.

Conforme nos expõe Keller,[694] a ideia de *Estado Pós Regulatório* é desenvolvida por Colin Scott[695] para tratar de um novo modelo de atuação estatal, após a transição do modelo de Bem-Estar Social (que apregoava ideias como a propriedade pública dos meios de produção, intervenção estatal direta e integração entre formulação de políticas públicas e funções operacionais) para o Estado Regulatório.

Ao contrário do paradigma que o precedeu, o Estado Regulatório diluiu a intervenção estatal direta na economia, estabelecendo um modelo caracterizado sobretudo, pela separação das atividades operacionais e de regulação. Nesse modelo, a regulação incorpora a concepção da subsidiariedade, o que importa reconhecer os princípios gerais da livre iniciativa e da livre empresa, reservando-se ao Estado o instrumento da regulação como meio de orientar a atuação dos particulares à realização de valores fundamentais. [696] [697]

Segundo Scott, o estágio seguinte – o Estado Pós-Regulatório – seria caracterizado por tendências teóricas e empíricas que "desafiam a ideia de que a regulação seria orientada para as capacidades do Estado", cuja principal característica são as fronteiras antes distintas, ora borradas, entre os Estados e os mercados, entre o que é público e o que é privado. [698] Assim, o autor identifica, dentre as características marcantes deste modelo: a variedade de normas, expressa na pluralidade de atores com competência para produção de regras formais, na adoção de instrumentos de *soft law* e de direito privado (ao passo que o Estado Regulador se baseia em normas primárias e secundárias);[699] a variedade de mecanismos de controle, que antes eram estruturados na

[694] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 166.
[695] SCOTT, Colin. Regulation in the Age of Governance: the rise of the post-regulatory state In: JORDANA, Jacin; LEVI-FAUR, David. **The Politics of Regulation** – Institutions and Regulatory Reform for the Age of Governance. Cheltenham: Edward Elgar, pp. 145-176, 2004, p. 146.
[696] SCOTT, Colin. Regulation in the Age of Governance: the rise of the post-regulatory state In: JORDANA, Jacin; LEVI-FAUR, David. **The Politics of Regulation** – Institutions and Regulatory Reform for the Age of Governance. Cheltenham: Edward Elgar, pp. 145-176, 2004, p. 147.
[697] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 166.
[698] SCOTT, Colin. Regulation in the Age of Governance: the rise of the post-regulatory state In: JORDANA, Jacin; LEVI-FAUR, David. **The Politics of Regulation** – Institutions and Regulatory Reform for the Age of Governance. Cheltenham: Edward Elgar, pp. 145-176, p. 146, 2004
[699] SCOTT, Colin. Regulation in the Age of Governance: the rise of the post-regulatory state In: JORDANA, Jacin; LEVI-FAUR, David. **The Politics of Regulation** – Institutions and Regulatory Reform for the Age of Governance. Cheltenham: Edward Elgar, pp. 145-176, 2004, p. 161.

hierarquia normativa do Estado e agora se realizam por caminhos diversos (um ponto que o autor ilustra com a ideia de Lessig sobre a ação conformadora de normas sociais, mercados, direito e arquitetura);[700] a variedade de controladores, a partir dos quais além do Estado Nação, a legitimidade tem referência em níveis supranacional, em uma gama de organizações governamentais, supragovernamentais e não governamentais;[701] e, por fim, a variedade de controlados, de forma que os negócios deixam de ser os únicos destinatários do controle, a partir do reconhecimento de que importa para a ordem social e econômica o comportamento de uma variedade de atores e contextos.[702] [703]

Numa abordagem referenciada nos agentes, Julia Black descreve o mesmo fenômeno como descentralização, para caracterizar um momento em que a regulação passa a se concretizar através de estratégias indiretas. A autora associa o movimento pós-regulatório à ampliação do entendimento sobre o conceito de "regulação", de forma a englobar técnicas híbridas e indiretas, além da produção normativa descentralizada, mas sob algum controle do Estado:[704] [705]

> A literatura sobre estratégias regulatórias (ou pós-regulatórias) indiretas é extensa e, embora ofereça muitos projetos inovadores para técnicas de regulação, não é o objetivo de revisá-las aqui. Para os propósitos desta discussão, é suficiente notar que a autorregulação, como um elemento de fechamento autopoiético, é central para a análise descentralizada. Ele fornece seu principal diagnóstico de falha regulatória e é considerado normativamente como a chave para o

[700] SCOTT, Colin. Regulation in the Age of Governance: the rise of the post-regulatory state In: JORDANA, Jacin; LEVI-FAUR, David. **The Politics of Regulation** – Institutions and Regulatory Reform for the Age of Governance. Cheltenham: Edward Elgar, pp. 145-176, 2004, p. 164.
[701] SCOTT, Colin. Regulation in the Age of Governance: the rise of the post-regulatory state In: JORDANA, Jacin; LEVI-FAUR, David. **The Politics of Regulation** – Institutions and Regulatory Reform for the Age of Governance. Cheltenham: Edward Elgar, pp. 145-176, 2004, p. 165.
[702] SCOTT, Colin. Regulation in the Age of Governance: the rise of the post-regulatory state In: JORDANA, Jacin; LEVI-FAUR, David. **The Politics of Regulation** – Institutions and Regulatory Reform for the Age of Governance. Cheltenham: Edward Elgar, pp. 145-176, 2004, p. 166.
[703] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 106.
[704] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 106.
[705] Tradução do autor. No original: "The literature on indirect regulatory (or post-regulatory) strategies is extensive, and whilst it offers many innovative designs for techniques of regulation, it is not the aim to review those here. For the purposes of this discussion it is sufficient to note that self-regulation, as an element of autopoietic closure, is central to the decentring analysis. It provides its principal diagnosis of regulatory failure, and is posited normatively as the key to regulatory success. The task of regulation has been redefined: it is to regulate self- regulation. However, it is to do so indirectly, in a 'post-regulatory' way". BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001, p. 128.

> sucesso regulatório. A tarefa da regulação foi redefinida: é regular a autoregulação. No entanto, é fazê-lo indiretamente, de uma maneira "pós-regulatória".

Apesar de reconhecer a sua conformidade com diferentes significados, importa aqui a referência que a autora faz às técnicas de "regulação descentralizada", que chama de regulação em diversos espaços. Elas refletem a ideia de que a atividade regulatória, considerada como influência de comportamento da coletividade por um determinado agente, público ou privado, pode afastar-se do Estado e ser exercida de forma descentralizada por uma série de atores sociais de natureza jurídica diversa, tais como organizações privadas, associações coletivas, comitês técnicos, profissões, e até agentes privados de mercado.[706]

Por sua vez, a existência de um direito administrativo global já foi constatada e problematizada por diferentes autores,[707] e tem como componente distintivo a criação de regras de direito administrativo de alcance global por uma rede de agentes públicos e privados que não se confundem com a figura do Estado.[708] Em seu âmbito, é possível identificar uma disputa pelos meios de implementação do direito administrativo, já que essas entidades exercem suas políticas através de instrumentos que fogem da normatividade típica dos ordenamentos (administrativos) internos, sendo desprovidos de vinculação e obrigatoriedade. Na definição de Patrícia Ferreira Baptista e Leonardo Coelho, o direito administrativo global poderia ser entendido como um "direito paralelo, forjado em foros de negociação internacional, cunhado em agências estatais e não estatais, com o objetivo de atender às necessidades [dos] setores econômicos que atuam no espaço global".[709]

---

[706] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 106.

[707] *Cf.* DIMITROPOULOS, Georgios. Global Administrative Law as 'Enabling Law': How to Monitor and Evaluate Indicator-Based Performance of Global Actors, 2012. **IRPA**. SSRN. Disponível em: http://dx.doi.org/10.2139/ssrn.2167405. Acesso em: 26 out. 2022.; VERMEULE, Adrian. Local and Global Knowledge in the Administrative State, 2012. Public Law & Legal Theory Working Paper Series Paper No. 13-01. **Harvard Law School**. Disponível em: http://dx.doi.org/10.2139/ssrn.2169939. Acesso em: 14 out. 2022.; ANTUNES, Luís Filipe Colaço. **O direito administrativo sem estado: crise ou fim de um paradigma?** Coimbra: Coimbra Editora, 2008; Administração Estado, ver: OTERO, Paulo. **Manual de Direito Administrativo** - vol. 1. Coimbra: Almedina, 2013, p. 513.

[708] DIMITROPOULOS, Georgios. Global Administrative Law as 'Enabling Law': How to Monitor and Evaluate Indicator-Based Performance of Global Actors, 2012. **IRPA**. SSRN. Disponível em: http://dx.doi.org/10.2139/ssrn.2167405. Acesso em: 26 out. 2022.

[709] BAPTISTA, Patrícia Ferreira; RIBEIRO, Leonardo Coelho. Direito administrativo global: uma nova ótica para a regulação financeira de investimentos. *In:* RIBEIRO, Marilda Rosado Sá. Direito internacional dos investimentos. Rio de Janeiro: Renovar, 2014. p. 803.

Por sua vez, Gustavo Binenbojm atribui a sua relevância a uma demanda por um direito administrativo desterritorializado, resultante da "febril desterritorialização da economia globalizada",[710] além de já identificar a sua influência sobre o desenho regulatório institucional, interagindo com as fontes normativas primárias e condicionando a interpretação jurídica da *hard law* (como o agir das Administrações Públicas nacionais, tornando-se importante componente da juridicidade administrativa):[711]

> (...) [e] como demanda a ela correspondente, o surgimento de um direito administrativo desterritorializado, forjado no hiato entre os direitos domésticos e o clássico direito internacional. Tal fenômeno revela também o desenvolvimento de uma certa transculturalidade administrativa, tanto ao nível regional como no âmbito mundial, como uma identidade partilhada entre povos, agentes econômicos e operadores do direito público, que transcende as fronteiras nacionais.
> Quanto ao ponto, é importante ressaltar que a globalização, a rigor, não representa um esfacelamento do Estado, mas essencialmente uma força propulsora de reformas institucionais que, embora fragilizem, em algum grau, a soberania interna dos países e, em última análise, a concepção tradicional de legalidade administrativa, estimula a redefinição de estratégias regulatórias para adaptação a uma nova realidade internacional que traz consigo atores adicionais produtores de normas e novas fontes do direito administrativo.

Expressões deste paradigma são igualmente encontradas no âmbito do Direito Constitucional, no qual as reflexões orbitam ao redor da aplicação de estruturas constitucionais a arranjos híbridos (como organizações internacionais com presença ou representação estatal voltadas à discussão e desenvolvimento de políticas em temas determinados – como a Organização Mundial do Comércio - OMC e a Organização para a Cooperação e Desenvolvimento Econômico - OCDE) e até exclusivamente não estatais com caráter transnacional (como a ICANN - Internet Corporation for Assigned Names and Numbers), ganhando relevância a aplicação de princípios materiais antes centrados no ideal de um Estado de Direito – como o direito ao contraditório e à ampla defesa – a código e regulações híbridas, numa espécie Constitucionalismo Global.[712]

---

[710] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 335.
[711] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 335-345.
[712] TEUBNER, Gunther. **Self-Constitutionalizing TNCs? On the Linkage of "Private" and "Public" Corporate Codes of Conduct**, Indiana Journal of Global Legal Studies, Vol. 18, pp. 617-638, 2011. Disponível em: https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1457&context=ijgls Acesso em: 12 nov. 2022.

Para ilustrar alguns desse fóruns de regulação global Gustavo Binenbojm[713] aponta a experiência de alguns deles, conforme se vê:

> Em termos históricos, o impulso fundamental à disseminação do fenômeno de normatividade administrativa transnacional pode ser atribuído e se confunde, ao mesmo tempo, com a criação, por iniciativa conjunta de múltiplos países, de inúmeras organizações internacionais voltadas à discussão de temas de interesse comum com relevância global. Isto é, a partir da segunda metade do século XX, observa-se a institucionalização e a consolidação de organizações internacionais – supraestatais e não estatais – com propósitos de estabelecimento de diretrizes normativas consensuais a respeito de assuntos específicos, notadamente com a predominância de temas econômicos.
> Tais organizações escapam, com frequência, ao modelo tradicional de organizações constituídas e compostas por Estados Nacionais. Veja-se, e.g., o Comitê da Basileia de Bancos Centrais, que congrega reguladores domésticos no plano da burocracia administrativa. Há casos de reguladores privados transnacionais, como a *International Standard Association* (ISO) e a Agência Mundial Anti-Doping (WADA). Existem, ainda, entidades híbridas, formadas por Estados e entes privados, como é o caso da Comissão *Codex Alimentarius*, criada pela Organização das Nações Unidas para a Alimentação e a Agricultura (FAO) e pela Organização Mundial da Saúde (OMS) para a elaboração de um código contendo standards para a harmonização das regulações nacionais relativas a alimentos, com vistas à proteção dos consumidores. Tal Comissão é composta tanto por órgãos ou entidades estatais, como por entidades privadas, representativas de produtores e de consumidores.

O autor prossegue analisando que: [714]

> O fenômeno não se limita, todavia, a organizações transnacionais estatais ou híbridas (envolvendo entes públicos e entidades privadas), abarcando ainda o exercício de governança administrativa por entidades privadas, destituídas ou não de fins lucrativos. Interessante destacar o caso da ICANN – *Internet Corporation for Assigned Names and Numbers*, fundada em 1998. Trata-se de um modelo de gestão privada da internet à escala global, sem fins lucrativos, constituído sob as leis do Estado da Califórnia, que coordena a alocação e designação de identificadores exclusivos (v.g., endereços de IP), credencia registradores de nomes de domínio de primeiro nível genérico e ajuda a dar voz a voluntários de todo o mundo dedicados a manter a internet segura, estável e operável.

[713] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 336-337.
[714] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 336-337.

Ainda, para ilustrar o assunto, Gustavo Binenbojm descreve como algumas dessas entidades atuam, com destaque para a ICANN, em razão de nosso objeto de estudo:[715]

> A ICANN desenvolve sua atividade regulatória por meio de uma vasta rede de contratos celebrados com entes públicos, associações e empresas mundo afora, que, por sua vez, também subcontratam parcela de suas atividades com terceiros, constituindo-se uma ampla rede de relações que ultrapassa as fronteiras dos Estados nacionais, tal como a própria internet. Como destaca Suzana Tavares da Silva, trata-se de um modelo de governança de interesses das populações, que não é mediado pelo Estado segundo objetivos políticos, mas sim por entidades privadas, segundo critérios predominantemente técnicos, e cuja forma de deliberação não reside em discussões presenciais, mas sim em processos de formação de decisão *bottom up* – simples, informais e a distância – sendo, por essa razão, apontado como um embrião do direito administrativo global.
>
> Tais organizações transnacionais deram ensejo à criação de ambientes internos de deliberação ou fóruns de discussão voltados a debater pautas mínimas de convergência ou concertação entre os respectivos membros, utilizando-se, essencialmente, de instrumentos de *soft law*, aptos a orientar políticas públicas ou a recomendar a implementação de mudanças institucionais aos países delas integrantes, geralmente pela edição estruturada, por tema de interesse, de *guidelines* (diretrizes), *list of general principles* (princípios gerais) ou *recommendations* (recomendações).
>
> Paralelamente, é possível notar, na experiência internacional, dois fenômenos institucionais de extrema relevância para compreender os efeitos do funcionamento continuado das organizações internacionais ao longo do tempo, quais sejam: (i) a interação constante entre organizações internacionais com objetivos institucionais comuns tem gerado arranjos informais de relacionamento mútuo entre elas, chamados de "redes globais de governo" (*global networks*), com predominância de algumas em relação a outras, a depender dos objetivos institucionais perseguidos e da reputação internacional conquistada ("redes de redes globais de governo"), e (ii) a ocorrência de um processo mais lento de harmonização de sistemas jurídicos com tendência à homogeneização normativa, baseado na troca de experiências, equalização e difusão de informações entre os participantes, que tem gerado, a partir de deliberações com ampla participação procedimental, documentos consensuais com diretrizes regulatórias compartilháveis, dotados de grau considerável de eficácia persuasiva.

[715] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 337-338.

Nesse passo, o autor[716] identifica que a constituição e a consolidação de redes globais de governança – envolvendo entidades privadas e, às vezes, autoridades estatais, em diferentes arranjos institucionais – têm cada vez mais propiciado a coordenação de esforços institucionais em prol da edição de instrumentos normativos de *soft law*, com graus variados de eficácia, a depender de como os sistemas jurídicos nacionais e instituições políticas domésticas os recebem ou interpretam, inclusive a Administração Pública. Ele destaca que o ambiente deliberativo relativamente mais flexível e participativo desses fóruns tem facilitado a definição tempestiva de diretrizes regulatórias com potencialidade de aplicação em escala global.

A partir desse quadro Binenbojm[717] assevera que o uso disseminado da *soft law* transnacional já tem impactado a forma de pensar a legalidade administrativa sob o aspecto institucional, diante da força persuasiva das diretrizes regulatórias internacionalmente estipuladas, sobretudo, em deliberações consensuais, que tem vindo a servir de critério internacional de julgamento do desempenho de países e instituições políticas. Ademais, no âmbito do funcionamento regulatório da Administração Pública contemporânea tem-se visto uma tendência de aderência e de adaptação institucional dos entes e órgãos administrativos domésticos aos padrões aceitos internacionalmente, incluindo-se a influência sobre o conteúdo da regulação.

Essa situação tem revelado uma força vinculativa impressionante e impensável décadas atrás, desse conjunto de diretrizes internacionais, o que tem feito diversos estudiosos do direito a cogitar de um incipiente direito administrativo global.

Em algumas palavras, o Binenbojm sintetiza o fenômeno de natureza empírica, e ilustra a situação com alguns exemplos, veja-se:[718]

> Com efeito, diante das evidências empíricas, percebe-se que esse direito administrativo global, ainda que permeado de maior informalidade e dotado de graus distintos de vinculatividade, tem: (i) afetado o desenho regulatório institucional dos países, (ii) interagido de diversas maneiras com fontes normativas primárias ou *hard law*, independentemente de integração normativa formal, (iii) servido de critério de interpretação

[716] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 338-339.
[717] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 338-339.
[718] BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016, p. 338-339.

jurídica do *hard law* e, em última análise, (iv) condicionado o agir das Administrações Públicas nacionais, tornando-se importante componente da juridicidade administrativa.

A título ilustrativo, o exemplo mais evidente de *soft l*aw transnacional com impacto profundo no Direito Administrativo brasileiro tem sido a adesão continuada, pelo Conselho Monetário Nacional (CMN), órgão do Ministério da Fazenda, e pelo Banco Central do Brasil (BACEN), autarquia federal vinculada ao Ministério da Fazenda, às diretrizes e princípios contidos nos documentos conhecidos como "Acordos de Basileia", que resultam de deliberações internacionais efetuadas no âmbito do Comitê de Supervisão Bancária da Basileia (CSBB), instituído no âmbito do Banco de Compensações Internacionais (BIS), destinados a estabelecer diretrizes técnicas ou princípios básicos para uma regulação financeira prudencial de riscos mais eficaz (*guidelines and supervisory standards*).

Nesse sentido, ainda que se perceba uma tendência de integração normativa do *soft law* produzido no CSBB, com as devidas adaptações e de forma gradual, por intermédio da edição formal de Resoluções e Circulares, os reguladores financeiros brasileiros participam e observam toda a atividade do Comitê ao longo do ano e respeitam as recomendações internacionalmente estipuladas, além de se submeter, periodicamente, a inspeções internacionais para a verificação da adequação do Brasil aos padrões regulatórios internacionais.

Outra instituição que desempenha atividade intensa na edição de diretrizes (*guidelines*) e recomendações com repercussão no Direito Administrativo regulatório é a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que possui um plano institucional bem amplo de atuação. Exemplificativamente, dentro do contexto político de empreendimento de esforços direcionados a adotar medidas de poder de polícia mais eficientes no combate à corrupção, o país tem se engajado em Grupos de Trabalho específicos da OCDE instituídos para avaliar a implementação, no país, da Convenção Anticorrupção da OCDE (*Anti-Bribery Convention*), tendo sido recentemente avaliado pela instituição, que apontou evoluções positivas, como a edição da Lei Anticorrupção (Lei no 12.846/2013). Além disso, a OCDE expede recomendações que podem servir como fonte relevante de informações para ajustes nas políticas públicas brasileiras, evidenciando, por vezes, possibilidades regulatórias que passam despercebidas devido à ausência de cultura institucional no país sobre esse tipo específico de regulação anticorrupção.[719]

[719] Aqui, não poderíamos deixar de acrescentar o papel da OCDE e da OMC no estabelecimento de recomendações em matéria de Contratos Públicos que servem de parâmetro normativo-interpretativo, nas políticas públicas nacionais voltadas à contratação pública. CATOZZZO, Franceslly. **Estudo da OCDE sugere políticas públicas para compras voltadas ao desenvolvimento de uma Conduta Empresarial Responsável**, 2022. Disponível em: https://sollicita.com.br/Noticia/?p_idNoticia=18969&n=estudo-da-ocde-sugere-pol%C3%ADticas-p%C3%BAblicas-para-compras. Acesso em: 15 nov. 2022. Até mesmo relatórios do Banco Mundial (BM) – especialmente à época de austeridade financeira – serviram de parâmetro interventivo em políticas públicas (como educação) nacionais durante a crise financeira de 2016. SILVA, Renata Valério; MOREIRA, Jani Alves da Silva. A educação, reformas curriculares e as propostas do banco mundial no contexto pós-golpe (2016-2018). **Colloquium Humanarum**, [S. l.], v. 16, n. 1, p. 145–162, 2019. Disponível em: https://journal.unoeste.br/index.php/ch/article/view/2975. Acesso em: 12 nov. 2022.

No âmbito particular às tecnologias, isso se expressa na atual difusão da ideia de constitucionalismo digital, que se refere à constelação de iniciativas que procuraram articular um conjunto de direitos políticos, normas e limites de governança sobre o exercício de poder no âmbito da Internet. [720]

Muito embora o aprofundamento teórico em cada uma dessas teorias refuja ao escopo deste trabalho, é essencial o seu reconhecimento como um *background* literário nas discussões ora tratadas. Isso porque elas ilustram as reações a ambientes regulatórios complexos como o da rede mundial de computados, ao mesmo tempo em que oferecem uma perspectiva própria sobre o Estado e suas funções, servindo de alicerces para a busca de soluções eficazes.

Importa notar que a relevância desse marco teórico não implica na proposição de critérios autorregulatórios, isso porque, como visto na introdução e na primeira parte da pesquisa, o Estado cumpre um papel importante na regulação da privacidade e da proteção de dados, de tal modo que o seu total afastamento não se mostra de forma algum eficiente como se pôde constatar pela gama de riscos autopoiéticos que emergiram de um espaço não regulado. Isso demonstra que a regulação da matéria é um desafio particularmente complexo para os governos, e que não pode ser inteiramente deixado para uma indústria que amadureceu rapidamente e, muitas vezes, sem supervisão.

Assim, o marco teórico do trabalho é a adoção e expansão de modelos conciliatórios de regulação, expressos por regulações híbrida ou corregulatórias. Conquanto se assuma que o Estado desempenha um importante papel, está sujeito, tal como os demais agentes atuantes no mercado, a fatores como a complexidade e a fragmentação (do poder e do conhecimento), interdependência entre atores e contextos, bem como às falhas regulatórias.

Dessa forma, somente uma teoria capaz de amalgamar as capacidades dos diversos atores sociais, mitigando suas falhas intrínsecas, seria capaz de conferir uma maior efetividade e, consequentemente, uma maior sobrevida a um sistema regulatório.

Nesse aspecto, além de tudo que foi aqui trazido, o Estado ainda sofre com um outro problema, mencionado, em parte, por Murray e Scott,:[721] a escassez de recursos.

---

[720] KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018, p. 106.

[721] Parcial porque os autores apenas enxergam o fenômeno da escassez relacionada à existência limitada de recursos naturais ou fabricados pelo homem, enquanto para nós, a escassez terá uma conotação mais abrangente, envolvendo os recursos, atividades humanas e toda a gama de operações relacionadas à regulação. Veja-se: "All new media sectors draw heavily on limited resources, whether these be natural

Embora o emprego da expressão pelos autores se dê em referência à escassez de recursos naturais e tecnológicos, ao falarmos em regulação pelo Estado, não podemos ignorar as diferentes políticas públicas sob seu encargo, bem como a finitude de recursos disponíveis para a realização de todos seus fins político-sociais.

Sunstein e Holmes[722] apontam, nesse sentido, que para que os indivíduos desfruem de seus direitos, em um sentido legal (em oposição a uma percepção moral), é necessário um conjunto de estruturas estatais que os garanta e os promova. Este simples fato ajuda a perceber que todos os direitos legalmente impostos (e não apenas os direitos sociais como a doutrina clássica costumava apontar) convocam recursos para a sua realização, seja em maior ou menor grau.

Os autores[723] avaliam que os direitos são caros porque também os remédios para assegurá-los o são, isto é: sua aplicação é cara, especialmente uma aplicação uniforme e justa; e os direitos se tornam vazios na medida em que não são cumpridos. Em outras palavras: quase todo direito implica um dever correlato, e os deveres só são levados a sério quando sua negligência é punida pelo poder público, drenando recursos do erário, seja através das estruturas administrativas (poder de polícia e fiscalização), seja do Poder Judiciário.

Traduzindo essa relação de forma bastante sinóptica, Harisson Leite[724] assinala que o orçamento público lida, inevitavelmente, com recursos limitados para atender

---

resources such as spectrum for the telecommunications or broadcasting sectors or man-made resources such as domain names in relation to Cyberspace". "Todo o setor das novas mídias drena uma quantidade muito grande de recursos limitados, seja recursos naturais como os espectros para comunicação ou setores de difusão [como a radiodifusão], seja recursos fabricados pelo homem, como os nomes de domínio em relação ao ciberespaço". Tradução do autor. MURRAY, Andrew D.; SCOTT, Colin. Controlling the New Media: Hybrid Responses to New Forms of Power. **The Modern Law Review**. v. 65. n. 4, 2002, pp. 491–516. JSTOR. Disponível em: http://www.jstor.org/stable/1097592. Acesso em: 29 set. 2022.

[722] Cass Sunstein e Stephen Holmes relatam que até mesmo direitos de defesa dependem de uma estrutura estatal que os assegure, demandando recursos do Estado para efetivá-los. Logo, seria evidente que todo direito pressupõe uma atuação do Estado, seja mediante provocação (através do Poder Judiciário, por exemplo), seja espontaneamente (através da atuação do poder de polícia, ou das instituições administrativas), demandando recursos do erário. No original: "'Where there is a right, there is a remedy' is a classical legal maxim. Individuals enjoy rights, in a legal as opposed to a moral sense, only if the wrongs they suffer are fairly and predictably redressed by their government. This simple point goes a long way toward disclosing the inadequacy of the negative rights/positive rights distinction. What it shows is that all legally enforced rights are necessarily positive rights. Rights are costly because remedies are costly. Enforcement is expensive, especially uniform and fair enforcement; and legal rights are hollow to the extent that they remain unenforced. Formulated differently, almost every right implies a correlative duty, and duties are taken seriously only when dereliction is punished by the public power drawing on the public purse.". HOLMES, Stephen; SUNSTEIN, Cass. **The cost of rights: why liberty depends on taxes**. New York: W.W. Norton & Company, 1999, p. 43.

[723] HOLMES, Stephen; SUNSTEIN, Cass. **The cost of rights: why liberty depends on taxes**. New York: W.W. Norton & Company, 1999, p. 43.

[724] LEITE, Harisson. **Manual de direito financeiro**. 5. ed. Salvador: JusPODIVM, 2016, p. 49-52.

demandas cada vez maiores, decorrente de sociedades cada vez mais complexas e plurais. Isso impele que ao se buscar regular direitos e deveres se tenha em mente, ainda, os custos envolvidos nessa implementação.

Nessa ordem de ideias, todos os esforços regulatórios (decomposto em um ciclo de tarefas e atividade), bem como os recursos por eles convocados (e.g., humanos, financeiro e temporais) são fatores que não podem ser ignorados.

2. Conciliando teorias regulatórias: um modelo regulatório aberto

Como visto, o reconhecimento da força regulatória de uma rede de agentes e instituições privadas já não pode ser ignorada pelo Direito.

Ao mesmo tempo, todas as vezes que se viu um afastamento do Estado na regulação de temas relacionados aos sistemas produtivos, como se dá atualmente na economia de dados, viu-se a recondução das estruturas de poder a cenários de exploração humana, especialmente de extratos mais vulneráveis da sociedade. O fato de as plataformas digitais reconduzirem trabalhadores a um estado de absoluta carência de amparo socioassistencial, deixa isso bem claro.

Se por um lado a "mão invisível"[725] do mercado não é capaz de equacionar o quadro de exploração social, e, até mesmo, as próprias antinomias do mercado,[726] de outro o Estado também não é capaz de, isoladamente, apresentar respostas satisfatórias aos muitos problemas que é chamado a atuar.

Por essas razões, edificados nas ideias de *Estado Pós-Regulatório*, *Descentralização Administrativa*, *Direito Administrativo Global* e de *Constitucionalismo Global*, propomos um modelo de regulação sistemático-dialógico (*systematic-dialogical regulation - SDR*) baseado na ideia de formação de um sistema aberto de interação entre atores estatais e não estatais, possível por meio da produção de códigos de conduta (setoriais ou não), integrados por mecanismos de estímulo à *compliance* (*e.g.* selos e processos de certificações – *stamps and certification processes*) e de desestímulo a condutas incompatíveis com o sistema regulatório (*e.g.* listas-sujas – *black lists*).

Embora todos esses instrumentos sejam previstos de algum modo no modelo regulatório brasileiro, não são vistos de modo integrado, possuindo uma restrita aplicação

[725] SMITH, Adam (27 de agosto de 2010). The Wealth of Nations: An Inquiry into the Nature and Causes of the Wealth of Nations (em inglês). Smith (1776)
[726] Como se constatou com a crise de 1929 e, mais recentemente, com a bolha especulativa de 2008.

aos casos de transferências internacionais de dados, não obstante, seu potencial de aplicação abranger também os atores internos, como reconhece a União Europeia em suas Diretrizes nº 1/2019 relativas aos Códigos de Conduta e Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679.

Demais disso, até mesmo na experiência europeia, mais desenvolvida, os códigos de conduta elaborados com a participação do Estado ainda se encontram em fase embrionária (face a mudança de marco regulatório da Diretiva 95/46/CE para o Regulamento (UE) 2016/679), de modo que as discussões, ainda pioneiras, poderão trazer benefícios regulatórios ainda pouco dimensionados pela literatura.[727]

Assim, o modelo proposto (SDR – *systematic-dialogical regulation*), inspirado nas citadas teorias, assemelha-se, ao *The Renew Deal*, construído por Orly Lobel,[728] à medida que procura conciliar ideias aparentemente antagônicas, a partir da utilização de uma hibridização integradora.

Como aponta o autor, referindo-se ao "The new deal": [729]

> O modelo de governança adota uma ecologia mista. A força central do Renew Deal é que ele explicitamente e engenhosamente adota uma hibridização teórica, reunindo elementos de escolas de pensamento rivais. Em seu espírito e estilo, o Renew Deal é integrativo, acolhedor e otimista. Defende a proliferação de métodos e estruturas de aceitação pragmática de cada um. Ao oferecer uma grande tenda [um grande espaço de acomodação], pode responder às exigências de acomodação flexível à nova economia e às variadas condições locais, bem como à permanente necessidade de ação pública. A hibridização permite que o pensamento jurídico contemporâneo conviva com o paradoxo. Por exemplo, a manutenção obsessiva das fronteiras tradicionais – incluindo as de público e privado, lucrativo e sem fins lucrativos, formal e informal, teoria e prática, secular e religiosa, esquerda e direita – não é mais uma grande preocupação com a mudança para o paradigma do Renew Deal. Pelo contrário, o modelo de governança visa ir além dessas dicotomias generalizadas em busca de estruturas sustentáveis. Seu objetivo não é policiar fronteiras, mas sim buscar e promover estruturas que facilitem horizontes imaginativos mais amplos. Além disso, o modelo se sente à vontade para estabelecer vínculos entre os níveis local, regional, nacional e global, com múltiplas autoridades sobrepostas. Como será discutido na seção seguinte, o modelo aceita uma rica definição de democracia, combinando aspectos diretos, representativos, associativos, participativos e deliberativos.

[727] Diante da ausência de estudos empíricos que analisem a eficiência de um sistema já estabelecido, voltado à proteção da privacidade e dos dados pessoais dos titulares.
[728] LOBEL, Orly. The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought. **Minnesota Law Review**, v. 89, p. 342-370, 2004.
[729] LOBEL, Orly. The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought. **Minnesota Law Review**, v. 89, p. 342-370, 2004.

> O modelo de governança deve, portanto, ser entendido como uma tentativa de vislumbrar uma terceira via entre a regulamentação "top-down" [ou verticalizada], baseada no Estado, e uma dependência obstinada em normas baseadas no mercado; entre a regulação centralizada de comando-e-controle e o livre contrato individual. Visa transcender as dicotomias conceituais de regulação e desregulamentação; de diretriz legal e comportamento espontâneo do mercado. A invenção de práticas administrativas flexíveis e responsivas pode ser a única alternativa para grandes burocracias já desbotadas, de um lado, e mecanismos de mercado privado, por outro.
> Uma promessa fundamental do Renew Deal é a sugestão explícita de que a eficiência econômica e a legitimidade democrática podem, sob certas condições, apontar na mesma direção. Os princípios de governança podem aumentar a eficácia e a responsabilidade, restaurando assim a legitimidade do regime legal. A governança é eficiente porque abrange múltiplas arenas e mecanismos para aprender, adaptar e melhorar. É democrático porque incentiva a participação de mais cidadãos e a atenção a mais interesses nos processos legislativos. Além disso, a visão do Renew Deal reconcilia a tensão contínua entre o medo de um governo dilatado e a necessidade de uma resposta pública aos desafios sociais. A descentralização coordenada atende à expectativa dos americanos de que a política do governo reflita seus valores morais e senso de justiça, mas "de forma eficiente, deixando o maior controle possível nas mãos daqueles que estão mais próximos dos problemas".[730]

[730] No original: "The governance model fosters a mixed ecology. A central strength of the Renew Deal is that it explicitly and ingeniously embraces theoretical hybridization, drawing together elements from rival schools of thought. In its spirit and style, the Renew Deal is integrative, accommodating, and optimistic. It advocates the proliferation of methods and structures pragmatic acceptance of each. By offering a big tent, it can respond to demands for flexible accommodation in the new economy and varied local conditions, as well as to the ongoing need for public action. Hybridization enables contemporary legal thought to live with paradox. For example, the obsessive maintenance of traditional boundaries –including those of public and private, profit and nonprofit, formal and informal, theory and practice, secular and religious, left and right – is no longer a major concern with the shift to the Renew Deal paradigm. On the contrary, the governance model aims to move beyond these pervasive dichotomies in search of sustainable structures. Its objective is not to police boundaries, but rather to seek out and open structures that will facilitate wider imaginative horizons. Furthermore, the model is comfortable making links among the local, regional, national, and global levels, as multiple overlapping authorities. As will be argued in the succeeding section, the model accepts a rich definition of democracy, combining direct, representative, associative, participatory, and deliberative aspects.
The governance model should thus be understood as an attempt to envision a third way between state-based, top-down regulation and a single-minded reliance on market-based norms; between centralized command-and-control regulation and individual free contract. It aims to transcend the conceptual dichotomies of regulation and deregulation; of legal directive and spontaneous market behavior. Inventing flexible, responsive administrative practices may be the only alternative to big, blunt bureaucracies on the one hand, and private market mechanisms on the other.
A key promise of the Renew Deal is its explicit suggestion that economic efficiency and democratic legitimacy can, under certain conditions, point in the same direction. Governance principles can increase both efficacy and accountability, thereby restoring the legitimacy of the legal regime. Governance is efficient because it encompasses multiple arenas and mechanisms by which to learn, adapt, and improve. It is democratic because it encourages the participation of more citizens and attention to more interests in legal processes. Moreover, the Renew Deal vision reconciles the ongoing tension between the fear of big government and the need for a public response to social challenges. Coordinated decentralization addresses the expectation of Americans that government policy will reflect their moral values and sense of fairness, but "efficiently, leaving the greatest possible amount of control in the hands of those closest to the problems". LOBEL, Orly. The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought. **Minnesota Law Review**, v. 89, p. 342-370, 2004.

O modelo regulatório proposto tem o mesmo espírito conciliatório, buscando uma espécie de arranjo entre as múltiplas arenas decisórias que possibilitem mecanismos de aprendizado, adaptação e melhoria entre esses fóruns de debates, incentivando a participação de mais atores sociais e mais interesses nos processos decisórios. Além disso, reconcilia a tensão contínua entre um Estado dilatado e a necessidade de uma resposta pública aos desafios sociais. A descentralização, de forma coordenada, atende à expectativa de que as políticas públicas reflitam valores sociais de forma justa e democrática, deixando o maior controle possível nas mãos daqueles com maior aptidão para enfrentar cada problema.

Essa, se pensarmos melhor, já é uma maneira de atuar do Regulamento europeu, que trabalha com a gestão de riscos, deixando, um extenso leque de atividades sob a incumbência do controlador de dados. No entanto, a nosso ver ainda falta a criação de um sistema integrado entre os diversos mecanismos disponíveis para utilização, de forma que se complementem em buscas dos resultados propostos: a adequada proteção da privacidade e dos dados pessoais.

Como terceira via, o paradigma do SDR surge em um momento em que há literatura em abundância no mundo jurídico sobre o fracasso tanto da regulação governamental quanto da não regulação, deixada nas mãos do mercado.

As falhas regulatórias têm estado no centro do estudo jurídico por várias décadas. A regulação pelo Estado (intervenção direta) já foi descrita como tendo se tornado "a Stalingrado da guerra política doméstica".[731] Dentre as deficiências regulatórias apontadas a esse modelo incluem-se a rigidez, o desperdício de recursos, a tendência à uniformidade e a supressão à inovação. Schuck ainda aponta as seguintes deficiências: "competição reprimida, grosseira ineficiência, hostilidade à participação social nos processos decisórios, frustração da inovação, caos administrativo e atraso, sigilo, ausência de planejamento de longo prazo e indiferença a objetivos sociais concorrentes". [732]

Na fase de concepção, a regulação é muitas vezes baseada em poucas informações e análises de políticas que simplificam por demais os problemas. As agências governamentais muitas vezes carecem de recursos para monitorar a implementação,

[731] SCHUCK, Peter Apud LOBEL, Orly. The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought. **Minnesota Law Review**, v. 89, p. 342-370, 2004, 344, 444.
[732] LOBEL, Orly. The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought. **Minnesota Law Review**, v. 89, p. 342-370, 2004, p. 444.

muito menos para determinar adequadamente as relações de causa e efeito observadas. Elas estão suscetíveis à busca de renda e à captura pelo particular, por meio da qual poderosos grupos de interesse controlam e afetam desproporcionalmente as decisões regulatórias. Assim, abundam exemplos de comportamentos desviantes de agências governamentais por toda o globo. [733]

Por outro lado, as falhas de mercado também são numerosas e incluem desigualdades distributivas, externalidades não previstas, falhas de ação coletiva e problemas de carona (*free rider*), assimetrias de informação, vieses cognitivos, e ineficiências de escala. Certos mercados, como aqueles de recursos escassos e monopólios naturais, são particularmente vulneráveis a falhas regulatórias. Ademais, frequentemente, os mercados também carecem de espaços adequados para a troca pública de ideias.

Como aponta Lobel:[734]

> Algumas avaliações de falhas regulatórias e de mercado baseiam-se em distinções factuais entre as capacidades do mercado e a ação pública. Nesses casos, a escolha da ação pública ou privada é empírica e instrumental. Dado um certo objetivo compartilhado, como a redução da poluição industrial, a questão é qual arranjo institucional alcançará melhor os resultados desejados. Outras preocupações são baseadas em avaliações normativas das diferenças entre várias esferas – política, econômica e cívica. Em tais contextos, pode haver um valor intrínseco em privatizar ou divulgar uma função social, independentemente de qual fórum está melhor situado instrumentalmente para atingir certos objetivos.

O acúmulo de percepções sobre as falhas regulatórias e de mercado revela a importância de ir além dos padrões existentes de legislação, por isso, nossa preocupação nessa seção de abordar as dificuldades estatais em relação à regulação, em contraste ao primeiro capítulo em que avaliamos o cenário de exploração e de perigos que se desenvolve sem a intervenção do Estado.

A propositura de um regime conciliatório, busca, assim, promover adaptações necessárias para amalgamar diferentes riscos regulatórios, na busca de se promover o

---

[733] SCHUCK, Peter Apud LOBEL, Orly. The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought. **Minnesota Law Review**, v. 89, p. 342-370, 2004, 344, 444.
[734] LOBEL, Orly. The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought. **Minnesota Law Review**, v. 89, p. 342-370, 2004. O autor aponta desvios e "maus comportamentos" que variam desde falhas da *Food and Drug Administration* ao controle de energia nuclear americana. Na ausência de uma abordagem abrangente, a regulação corre mais riscos de retroceder.

aprendizado, adaptação e melhoria entre os diversos mecanismos de intervenção e arenas de debates.

3. Mecanismos híbridos de regulação: proposição

Passada a análise sobre as razões factuais (capítulo I) e teóricas (capítulos I, II e III) que fundamentam a proposta regulatória sob exame, é chegado o momento de esmiuçar seu funcionamento.

Em verdade, o modelo de regulação que propomos, a que intitulamos de modelo regulatório sistemático-dialógico (*systematic-dialogical regulation - SDR*), consiste na integração e extensão do uso de diversos mecanismos de diálogo previstos no regime regulatório europeu, à realidade brasileira, com as devidas adaptações. Isso somente é possível porque, como visto, nosso modelo de regulação em matéria de privacidade e proteção de dados teve clara inspiração no modelo europeu, contando com alguns desses instrumentos, ainda que de forma reduzida (muito provavelmente por se tratar de nosso primeiro marco regulatório dedicado, com exclusividade, à proteção de dados pessoais).

Aqui, serão tratadas as formas de interação entre os mecanismos propostos, sua base legal, além de aspectos sobre seu funcionamento.

Para todos os casos, buscaremos abordar exemplos de sua aplicação em concreto, ainda que por analogia, utilizando da *expertise* de outras áreas do direito que os empregam, tendo em vista que muitos deles ainda não se desenvolveram suficientemente no âmbito da proteção de dados pessoais.

3.1. Códigos de Conduta

Inicialmente, estudaremos como os Códigos de Conduta se desenvolvem no âmbito europeu, tendo como base as Diretrizes nº 1/2019 e 04/2022 relativas aos Códigos de Conduta e aos Organismos de Supervisão, ao abrigo do Regulamento (UE) 2016/679.

A primeira diretriz refere-se à utilização dos Códigos de Conduta como instrumento de *compliance*, em conformidade com o artigo 40º, nº 1 e considerando 98 do RGPD;[735] enquanto a diretriz 04/2022, refere-se à utilização dos códigos de conduta

[735] Art. 40.º, n.º 1: "Os Estados-Membros, as autoridades de controle, o Comité e a Comissão promovem a elaboração de códigos de conduta destinados a contribuir para a correta aplicação do presente regulamento, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das

como instrumento para a transferência internacional de dados, nos termos do artigo 40.º, n.º 3, do RGPD[736]

3.1.1. Códigos de Conduta como instrumento de aplicação e *compliance* do Regulamento Geral de Proteção de Dados Pessoais, segundo as Diretrizes n.º 1/2019 do Comitê Europeu para a Proteção de Dados[737]

a) Introdução

Um dos principais objetivos do RGPD é assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno.[738] O RGPD introduz igualmente o princípio da responsabilidade, segundo o qual o responsável pelo tratamento dos dados é responsável pelo cumprimento do regulamento e tem de poder comprová-lo.[739]

Nos termos da diretriz, as disposições dos artigos 40.º e 41.º do RGPD relativas aos códigos de conduta : "representam um método prático, significativo e potencialmente eficaz em termos de custos para assegurar níveis de coerência mais elevados no que respeita aos direitos à proteção de dados".[740] Os códigos podem ser utilizados como um

micro, pequenas e médias empresas". Somada ao considerando nº 98, segundo o qual: "As associações ou outras entidades que representem categorias de responsáveis pelo tratamento ou de subcontratantes deverão ser incentivadas a elaborar códigos de conduta, no respeito do presente regulamento, **com vista a facilitar a sua aplicação efetiva**, tendo em conta as características específicas do tratamento efetuado em determinados setores e as necessidades específicas das micro, pequenas e médias empresas. Esses códigos de conduta poderão nomeadamente regular as obrigações dos responsáveis pelo tratamento e dos subcontratantes, tendo em conta o risco que poderá resultar do tratamento dos dados no que diz respeito aos direitos e às liberdades das pessoas singulares".

[736] Art. 40.º, n.º 3: "Além dos responsáveis pelo tratamento ou dos subcontratantes sujeitos ao presente regulamento, também os responsáveis pelo tratamento ou subcontratantes que não estão sujeitos ao presente regulamento por força do artigo 3.º **podem cumprir códigos de conduta aprovados em conformidade com o n.º 5 do presente artigo** e de aplicabilidade geral por força do n.º 9 do presente artigo, d**e modo a fornecer garantias apropriadas no quadro das transferências dos dados pessoais para países terceiros ou organizações internacionais nos termos referidos no artigo 46.º, n.º 2, alínea e)**. Os responsáveis pelo tratamento ou os subcontratantes assumem compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias apropriadas, inclusivamente em relação aos direitos dos titulares dos dados".

[737] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022. A análise apresentada terá por substrato as citadas diretrizes.

[738] Ver considerando 13 do RGPD.

[739] Ver artigo 5.º, n.º 2, do RGPD.

[740] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**.

procedimento para demonstrar o cumprimento das disposições do RGPD.[741] Designadamente, podem ajudar a colmatar as lacunas de harmonização que possam existir entre os Estados-Membros na aplicação da legislação em matéria de proteção de dados.[742] Constituem igualmente uma oportunidade para setores específicos refletirem sobre atividades comuns de tratamento de dados e aprovarem regras de proteção de dados específicas e práticas, que satisfaçam as necessidades do setor e os requisitos do RGPD.[743]

Os Estados-Membros, as Autoridades de Controle, o Comitê Europeu para a Proteção de Dados e a Comissão Europeia são obrigados a promover a elaboração de códigos destinados a contribuir para a correta aplicação do regulamento.[744] As diretrizes, que ora se discute, cumprem o papel de apoiar os titulares e facilitar a sua tarefa durante o processo de elaboração de códigos, ou em caso de alteração ou aditamento.

b) Disclaimer

Antes de prosseguir com a análise dos Códigos de Conduta, cumpre apontar que a presente seção é construída com base nas diretrizes n.º 1/2019[745] que têm como objetivo formular orientações práticas e ajudar à interpretação relativamente à aplicação dos artigos 40.º e 41.º do Regulamento Geral de Proteção de Dados Pessoais (o RGPD). As diretrizes destinam-se a ajudar a clarificar os procedimentos e regras envolvidos na

Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

[741] Ver, por exemplo, o artigo 24.º, n.º 3, o artigo 28.º, n.º 5, e o artigo 32.º, n.º 3, do RGPD. Os subcontratantes também podem utilizar um código de conduta para demonstrar garantias suficientes de que o seu tratamento de dados cumpre as disposições do RGPD (ver o artigo 28.º, n.º 5).

[742] Ver considerandos 77, 81, 98, 99, 148, 168 e artigos 24.º, 28º, 35º, 40º, 41º, 46º, 57º, 64º e 70º do RGPD. É este o caso, em especial, quando um código diz respeito a atividades de tratamento em vários Estados-Membros.

[743] Os códigos não devem necessariamente ser circunscritos ou limitados a um setor específico. Por exemplo, um código poderia ser utilizado em setores distintos que partilham, todavia, uma atividade de tratamento com as mesmas características e necessidades em matéria de tratamento. No caso em que um código seja de aplicação intersetorial, podem ser nomeados vários organismos de supervisão relativamente a esse código. No entanto, nesse caso, o âmbito das funções do organismo de supervisão deve ser claramente precisado para este código; por outras palavras, é conveniente precisar os setores em que cada organismo de supervisão exercerá as suas funções nos termos do artigo 41.º e os mecanismos de supervisão de que dispõe cada um destes organismos de supervisão. A este respeito, as secções pertinentes das presentes diretrizes, que definem as responsabilidades, obrigações e exigências em matéria de acreditação em relação aos organismos de supervisão aplicam-se individualmente a cada um desses organismos designados para o código em causa.

[744] Artigo 40.º, n.º 1, do RGPD.

[745] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

apresentação, aprovação e publicação dos citados códigos, a nível nacional (nos Estados-Membros) e europeu.

Pretendem estabelecer os critérios mínimos exigidos por uma Autoridade de Controle competente para a aceitação da realização de uma revisão e avaliação exaustivas de um código.[746] Além disso, pretendem estabelecer os fatores relacionados com o conteúdo que devem ser tidos em conta ao avaliar se um determinado código assegura e contribui para a correta e efetiva aplicação[747] do RGPD.

Por último, pretendem estabelecer os requisitos para uma supervisão efetiva de conformidade com um código.[748] Tais diretrizes devem também proporcionar um quadro claro que permita a todas as Autoridades de Controle competentes, ao Comitê e à Comissão proceder à avaliação dos códigos de forma coerente e simplificar os procedimentos envolvidos no processo de avaliação. Esse quadro também deve assegurar uma maior transparência, garantindo que os titulares de códigos que pretendam obter aprovação para uma norma compreendam não só o processo de aprovação como também os requisitos formais e os limites adequados aplicáveis.

Ademais, para efeitos das orientações que serão discutidas, são aplicáveis as seguintes definições:

«*Acreditação*»: a confirmação de que o organismo de supervisão proposto satisfaz os requisitos estabelecidos no artigo 41.º do RGPD para proceder à supervisão de conformidade com um código de conduta. Esta verificação é efetuada pela Autoridade de Controle sempre que o código é apresentado para aprovação (artigo 41.º, n.º 1). A acreditação de um organismo de supervisão só se aplica a um código específico.[749]

«*Titulares de códigos*»: associações ou outros organismos que elaboram e apresentam o seu código.[750] Beneficiarão de um estatuto jurídico apropriado, conforme exigido pelo código e de acordo com o direito nacional.

«*Autoridade de Controle competente*»: a Autoridade de Controle competente, nos termos do artigo 55.º do RGPD.

«*Organismo de supervisão*»: um organismo/comitê ou vários organismos/comitês (internos ou externos à organização dos titulares de códigos)[751] que

[746] Ver artigo 40.º, n.º 5, artigo 55.º, n.º 1, e considerando 122 do RGPD.
[747] Ver artigo 40.º, n.º 1, e considerando 98 do RGPD.
[748] Ver, por exemplo, artigo 41.º, n.º 2 e n.º 3, do RGPD.
[749] No entanto, um organismo de supervisão pode ser acreditado para mais de um código desde que satisfaça os requisitos de acreditação.
[750] Em conformidade com o considerando 98 do RGPD.
[751] Ver igualmente os pontos 64 e 67 infra.

exercem uma função de supervisão com vista a verificar e assegurar a conformidade do código com os requisitos do artigo 41.º.

«*Autoridades de Controle interessadas*»: entendidas como aquelas referidas no artigo 4.º, n.º 22, do RGPD.

«*Código nacional*»: um código que abrange as atividades de tratamento realizadas em um Estado-Membro.

«*Código transnacional*»: um código que abrange as atividades de tratamento realizadas em mais do que um Estado-Membro.

c) O que são códigos?

No âmbito do RGPD, os códigos de conduta constituem instrumentos de responsabilização voluntários que estabelecem regras específicas em matéria de proteção de dados para categorias de responsáveis pelo tratamento de dados e de subcontratantes. Conforme assinalam as diretrizes,[752] podem ser um instrumento de responsabilização útil e eficaz, e apresentam uma descrição circunstanciada do que é o conjunto de comportamentos mais adequado, lícito e ético de um setor.

Do ponto de vista da proteção de dados, os códigos podem funcionar como um conjunto de regras destinadas aos responsáveis pelo tratamento e aos subcontratantes que projetam e executam atividades de tratamento de dados conformes com os requisitos do RGPD, conferindo um significado operacional aos princípios de proteção de dados estabelecidos no direito nacional e europeu.

As associações comerciais ou os organismos que representam um setor podem criar códigos para ajudar esse setor a cumprir as disposições do RGPD de forma eficiente e potencialmente eficaz em termos de custos.

Tal como previsto na lista não exaustiva constante do artigo 40.º, n.º 2, do RGPD, os códigos de conduta podem abranger, designadamente, temas como: a) o tratamento equitativo e transparente; b) os legítimos interesses dos responsáveis pelo tratamento em contextos específicos; c) a recolha de dados pessoais; d) a pseudonimização dos dados pessoais; e) a informação prestada às pessoas e o exercício dos direitos das pessoas; f) as informações prestadas às crianças e a sua proteção (incluindo procedimentos para obter

[752] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

o consentimento dos pais); g) as medidas técnicas e organizativas, incluindo a proteção de dados e medidas de segurança; h) a notificação de violações; i) a transferência de dados para países terceiros; ou j) os procedimentos de resolução de litígios.

Ao revogar a anterior Diretiva relativa à proteção de dados (95/46/CE), o RGPD previu disposições mais específicas e pormenorizadas aplicáveis aos códigos de conduta, bem como os requisitos que deviam ser cumpridos e os procedimentos envolvidos na obtenção de sua aprovação. Previu-se ainda o registo, a publicação e a promoção desses códigos, uma vez aprovados.

Essas disposições, em conjunto com as diretrizes n.º 1/2019, [753] têm a aptidão de incentivar os titulares de códigos a contribuir diretamente para a criação de normas e regras de proteção de dados para os seus setores de tratamento.

Importa referir que os códigos são um dos vários instrumentos voluntários que podem ser utilizados de um conjunto de instrumentos de responsabilização em matéria de proteção de dados previsto pelo RGPD, tais como as avaliações do impacto sobre a proteção de dados[754] e a certificação.[755] Constituem, assim, procedimentos que podem ser utilizados para ajudar as organizações a demonstrar o cumprimento quanto às disposições do RGPD.[756]

d) Quais as vantagens dos códigos segundo as diretrizes n.º 1/2019?

Os códigos representam uma oportunidade para estabelecer um conjunto de regras que contribuam para a correta aplicação do RGPD, de uma forma prática, transparente e potencialmente eficaz em termos de custos, e refletem as nuances de um determinado setor e/ou das suas atividades de tratamento.

Podem ser elaborados para os responsáveis pelo tratamento e para os subcontratantes, tendo em conta as características específicas do tratamento efetuado em

[753] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

[754] Os códigos de conduta e a certificação são instrumentos de responsabilização voluntários, enquanto uma avaliação do impacto sobre a proteção de dados será obrigatória em determinadas circunstâncias. Para mais informações sobre outros instrumentos de responsabilização, consultar a página Web de orientação geral do CEPD (www.edpb.europa.eu).

[755] Ver artigo 42.o do RGPD e as Diretrizes CEPD n.º 1/2018 sobre a certificação e identificação de critérios de certificação de acordo com os artigos 42.o e 43.o do RGPD.

[756] A observância de um código, por si só, não garante a conformidade com o RGPD nem imunidade para os responsáveis pelo tratamento/subcontratantes quanto a sanções ou responsabilidades previstas no RGPD.

determinados setores e as necessidades específicas das micro, pequenas e médias empresas.[757] Podem constituir um instrumento especialmente importante e benéfico para as PME (pequenas e médias empresas) e as microempresas,[758] facultando um procedimento que lhes permita assegurar o cumprimento dos requisitos em matéria de proteção de dados de uma forma mais rentável.[759]

Os códigos podem ajudar, também, os responsáveis pelo tratamento e os subcontratantes a cumprir os requisitos do RGPD, regulando domínios como o tratamento equitativo e transparente, os legítimos interesses, as medidas em matéria de segurança e de proteção de dados desde a concepção e por padrão, bem como as obrigações do responsável pelo tratamento. [760] Podem ser utilizados por todos os setores de tratamento e podem ser redigidos de forma restrita ou ampla de modo a adaptarem-se a um setor específico,[761] desde que contribuam para a aplicação correta e efetiva do RGPD.[762]

Os códigos podem proporcionar um grau de corregulação aos responsáveis pelo tratamento e aos subcontratantes e diminuir o nível de dependência que, por vezes, sentem

[757] Ver considerando 98 do RGPD no que respeita ao artigo 40.º, n.º 1. Por exemplo, um código poderia ser adaptado de forma adequada para satisfazer os requisitos aplicáveis às micro organizações, além dos aplicáveis às pequenas e médias empresas.

[758] O artigo 40.º, n.º 1, do RGPD, em particular, identifica os códigos como uma solução para responder às necessidades dessas empresas.

[759] As diretrizes n.º 1/2019 fornecem o seguinte exemplo: "Por exemplo, as microempresas envolvidas em atividades de investigação semelhantes no domínio da saúde podem reunir-se através das suas associações relevantes e desenvolver em conjunto um código que diga respeito aos seus procedimentos de recolha e de tratamento de dados de saúde, em vez de tentarem realizar por si próprias essa análise abrangente do ponto de vista da proteção de dados. Os códigos também beneficiarão as autoridades de controle, proporcionando-lhes um melhor entendimento e conhecimento das atividades de tratamento de dados de uma profissão ou indústria específica ou de outro setor específico". UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

[760] As diretrizes n.º 1/2019 fornecem o seguinte exemplo: "Por exemplo, pode ser solicitada aprovação para um conjunto de regras respeitantes à forma como um setor caritativo específico garante que os seus acordos de tratamento são equitativos e transparentes. Em alternativa, o setor caritativo específico pode decidir elaborar um código que incorpore e aplique adequadamente várias disposições diferentes no âmbito do RGPD a fim de abranger todas as suas atividades de tratamento, desde o quadro jurídico para a recolha de dados pessoais até à notificação de violações de dados pessoais.". UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

[761] O artigo 40.º, n.º 2, do RGPD faz referência a códigos elaborados por organizações representantes de «categorias de responsáveis pelo tratamento ou de subcontratantes». Por conseguinte, tal poderia incluir códigos intersetoriais, desde que os critérios de representatividade sejam respeitados.

[762] Um código que incida em matérias restritas deve deixar suficientemente claro para os titulares dos dados (e de forma satisfatória para uma autoridade de controle competente) que a observância do código por parte dos responsáveis pelo tratamento/subcontratantes não assegura necessariamente a conformidade com toda a legislação. Neste caso, uma garantia adequada poderia ser assegurar uma transparência adequada quanto ao âmbito de aplicação limitado do código para aqueles que tenham aderido ao código e para os titulares dos dados.

em relação às Autoridades de Controle da proteção de dados, no sentido de estas elaborarem orientações mais exaustivas para as suas atividades de tratamento específicas.

Eles podem proporcionar um grau de autonomia e controle aos responsáveis pelo tratamento e aos subcontratantes na elaboração e aprovação de regras em matéria de boas práticas para os seus setores. Podem constituir uma oportunidade para consolidar melhores práticas para as operações de tratamento em domínios específicos. E podem, igualmente, tornar-se um recurso vital no qual as empresas podem confiar para resolver problemas críticos nos seus procedimentos de tratamento, para garantir uma observância mais eficaz das normas de proteção de dados.

Esses instrumentos têm aptidão de proporcionar aos responsáveis pelo tratamento e aos subcontratantes a tão necessária confiança e segurança jurídica, disponibilizando soluções práticas para os problemas identificados por setores específicos em relação às atividades comuns de tratamento, incentivando o desenvolvimento de uma abordagem coletiva e coerente às necessidades em matéria de tratamento de dados de um setor específico.

Os códigos podem ser um instrumento eficaz para conquistar a confiança dos titulares de dados, abordando uma variedade de questões, muitas das quais poderão ter sido suscitadas por preocupações do público em geral ou até mesmo por preocupações existentes no próprio setor, e, como tal, constituírem um instrumento que reforça a transparência para as pessoas em causa, no que diz respeito ao tratamento de seus dados pessoais.[763]

Os códigos podem, igualmente, demonstrar ser um procedimento útil e importante no domínio das transferências internacionais de dados. As novas disposições

[763] Lembrar, nesse sentido, a lista não exaustiva constante do artigo 40.º, n.º 2, do RGPD. Ademais, as próprias diretrizes ilustram o seguinte caso: "Por exemplo, no contexto do tratamento de dados de saúde para fins de investigação, as preocupações quanto às medidas apropriadas a serem adotadas para promover o cumprimento das regras aplicáveis ao tratamento de informações de saúde sensíveis poderiam ser atenuadas pela existência de um código aprovado e circunstanciado. Esse código poderia descrever de forma equitativa e transparente os seguintes aspetos:

- as garantias relevantes a aplicar às informações a fornecer aos titulares de dados;
- as garantias relevantes a aplicar aos dados recolhidos de terceiros;
- a comunicação ou a divulgação dos dados;
- os critérios a aplicar para garantir o respeito do princípio da minimização dos dados;
- as medidas de segurança específicas;
- os sistemas de conservação de dados apropriados; e
- os procedimentos para gerir os dados em resultado do exercício dos direitos dos titulares dos dados (nos termos dos artigos 32.º e 89.º do RGPD). UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

do RGPD permitem que terceiros cheguem a um acordo quanto à observância de códigos aprovados, de modo a satisfazer os requisitos legais para fornecer garantias apropriadas em relação às transferências internacionais de dados pessoais para países terceiros (não integrantes da União Europeia).[764]

Além disso, os códigos aprovados deste tipo podem resultar na promoção e no desenvolvimento do nível de proteção que o RGPD proporciona à comunidade internacional em geral, ao mesmo tempo que permitem transferências internacionais de dados pessoais de forma sustentável e conformes às disposições legais.

Ademais, apontam as diretrizes n.º 1/2019[765] que os códigos aprovados podem funcionar como instrumentos de responsabilização eficazes dos responsáveis pelo tratamento e dos subcontratantes. Tal como referido no considerando 77 e no artigo 24.º, n.º 3, do RGPD, a observância a um código de conduta aprovado está prevista, entre outros, como um método adequado para demonstrar o cumprimento de partes ou princípios específicos do Regulamento ou das disposições do Regulamento, no seu conjunto, por parte de um responsável pelo tratamento de dados ou de um subcontratante.[766]

As Autoridades de Controle devem também ter em conta a observância de um código de conduta aprovado: aquando da avaliação das características específicas do tratamento de dados, como os aspectos de segurança[767]; na avaliação dos efeitos do tratamento no âmbito de uma avaliação de impacto sobre a proteção de dados[768]; ou da aplicação de uma multa.[769] Em caso de violação de uma das disposições do regulamento, a observância a um código de conduta aprovado pode igualmente indicar em que medida é necessária a intervenção da Autoridade de Controle, através de uma multa que seja efetiva, proporcionada e dissuasiva ou através de outra medida corretiva.[770]

---

[764] Ver artigo 40.º, n.º 2, alínea j, e n.º 3, do RGPD.

[765] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

[766] Ver também artigo 24.º, n.º 3, e artigo 28.º, n.º 5, do RGPD.

[767] Artigo 32.º, n.º 3, do RGPD.

[768] Artigo 35.º, n.º 8, do RGPD.

[769] Artigo 83.º, n.º 2, alínea j), do RGPD. Importa referir ainda a aplicação de códigos no que respeita às Diretrizes de aplicação e fixação de multas para efeitos do Regulamento (UE) 2016/679 (WP 253/17), adotadas pelo CEPD. UE. União Europeia. Comissão Europeia. **Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253/17)**. Disponível em: https://ec.europa.eu/newsroom/article29/items/611237/en. Acesso em: 19 nov. 2022.

[770] Artigo 83.º, n.º 2, alínea j), do RGPD. Importa referir ainda a aplicação de códigos no que respeita às Diretrizes de aplicação e fixação de multas para efeitos do Regulamento (UE) 2016/679 (WP 253/17), adotadas pelo CEPD. UE. União Europeia. Comissão Europeia. **Guidelines on the application and setting**

e) Critérios de admissibilidade de um projeto de código

As Autoridades de Controle competentes devem cumprir um conjunto de condições antes de avaliar e rever, na íntegra, um código de conduta, para os fins do artigo 40.º, n.º 5, do RGPD. Essas condições visam facilitar uma avaliação eficiente de qualquer projeto de código. Sendo-lhes aplicáveis os critérios seguintes:

i. Exposição de motivos e documentação de apoio

Os projetos de código apresentados para aprovação devem conter uma exposição de motivos clara e concisa, que forneça informações sobre o objetivo do código, o seu âmbito de aplicação[771] e a forma como facilitará a aplicação do regulamento.[772] Essas informações ajudarão a agilizar o processo e a proporcionar a clareza necessária à apresentação do projeto de código, a qual deve também incluir documentação de apoio, quando relevante, para fundamentar o projeto de código e a exposição de motivos[773].

ii. Representante

O código deve ser apresentado por uma associação/consórcio de associações ou outros organismos representantes de categorias de responsáveis pelo tratamento de dados ou de subcontratantes («titulares de códigos»), em conformidade com o artigo 40.º, n.º 2. Uma lista não exaustiva de possíveis titulares de códigos poderia incluir: associações comerciais e representativas, organizações setoriais, instituições universitárias e grupos de interesse.

Os titulares de códigos devem demonstrar às Autoridades de Controle competentes que são um organismo representante eficaz que dispõe de capacidade para

of administrative fines for the purposes of the Regulation 2016/679 (WP 253/17). Disponível em: https://ec.europa.eu/newsroom/article29/items/611237/en. Acesso em: 19 nov. 2022.

[771] Podem ser aplicáveis as seguintes categorias não exaustivas: identificação dos membros, atividade de tratamento, titulares de dados, tipos de dados, jurisdições, autoridades de controle interessadas (artigo 4.º, n.º 22, do RGPD).

[772] Esse documento constitui uma oportunidade para os titulares de códigos exporem as razões subjacentes ao pedido de aprovação do seu código. Disponibiliza uma plataforma para descreverem a adequação das garantias propostas e para demonstrarem que os procedimentos propostos são adequados aos fins a que se destinam.

[773] Os exemplos podem incluir um resumo da consulta, informações sobre os membros ou investigações que demonstrem a necessidade do código.

compreender as necessidades dos seus membros e para definir claramente a atividade ou o setor de tratamento ao qual o código se destina a ser aplicado. Dependendo da definição e dos parâmetros do setor em causa, a representatividade pode ser determinada com base nos seguintes elementos, entre outros: a) Número ou percentagem de membros potenciais do código entre os responsáveis pelo tratamento ou de subcontratantes relevantes desse setor; b) Experiência do organismo representante do setor e das atividades de tratamento respeitantes ao código.

iii. Âmbito de aplicação do tratamento

O projeto de código deve ter um âmbito de aplicação definido que determine de forma clara e precisa as operações de tratamento (ou as características do tratamento) dos dados pessoais nele abrangidos, bem como as categorias de responsáveis pelo tratamento ou de subcontratantes nele regulamentados. Esse âmbito de aplicação incluirá as questões relacionadas com o tratamento às quais pretende dar resposta e para as quais procura apresentar soluções práticas.

iv. Âmbito de aplicação territorial

O projeto de código deve especificar se trata de um código nacional ou transnacional e facultar informações relativas ao âmbito de aplicação territorial, identificando todas as jurisdições relevantes nas quais pretende ser aplicável. No caso de códigos transnacionais (bem como de alterações ou aditamentos a códigos transnacionais), deve ser incluída uma lista de Autoridades de Controle interessadas. O Anexo III, reproduz os critérios elencados nas diretrizes para se estabelecer a distinção entre códigos nacionais e transnacionais, segundo a Diretriz n.º 1/2019.

v. Apresentação às Autoridades de Controle competentes

Os titulares de códigos devem assegurar que a Autoridade de Controle escolhida para avaliar um projeto de código é competente para o exercício das funções que lhe são atribuídas, em conformidade com o artigo 55.º do RGPD.[774] O Anexo IV, reproduz um

[774] O artigo 55.º do RGPD estabelece que as autoridades de controle são competentes para prosseguir as atribuições e exercer os poderes que lhes são conferidos pelo regulamento no território do seu próprio Estado-Membro. Ver também considerando 122 do RGPD.

conjunto de informações adicionais elaboradas no bojo das Diretrizes n.º 1/2019 que podem ajudar os titulares de códigos na escolha de uma Autoridade de Controle competente para a supervisão de um código transnacional. Essa disposição, entretanto, tem uma aplicação muito restrita à realidade do bloco europeu, razão porque deslocamos a informação para um dos anexos do trabalho.

vi. Procedimentos de controle

O projeto de código deve prever procedimentos que permitam efetuar a supervisão do cumprimento das suas disposições pelas partes interessadas que se comprometam a aplicá-lo.[775] Os procedimentos de controle aplicam-se tanto a códigos do setor público como do setor privado.

vii. Organismo de supervisão

Um projeto de código que envolva atividades de tratamento de Autoridades ou organismos privados (não públicos) deve também identificar um organismo de supervisão e conter procedimentos que permitam que esse organismo desempenhe as suas funções de acordo com o artigo 41.º do RGPD.[776] Os organismos de supervisão identificados devem dispor de capacidade adequada para cumprir os requisitos de serem plenamente responsáveis no exercício da sua função.[777] Ademais, os organismos de supervisão devem ser acreditados para a função pela Autoridade de Controle competente, em conformidade com o artigo 41.º, n.º 1, do RGPD.

viii. Consulta

Um projeto de código deve conter informações sobre o alcance da consulta realizada. O considerando 99 do RGPD estabelece que, durante o processo de elaboração de um código de conduta (ou em caso de alteração ou aditamento), deve ser realizada uma

[775] Ver artigo 40.º, n.º 4, do RGPD.
[776] Os códigos que envolvam o setor público devem conter igualmente procedimentos adequados para efetuar a supervisão das suas disposições.
[777] Nos termos do artigo 83.º, n.º 4, alínea c), do RGPD, a violação das disposições do regulamento, no que respeita às obrigações do organismo de supervisão, está sujeita a uma multa.

consulta com as partes interessadas relevantes, incluindo os titulares dos dados, sempre que possível.

Por conseguinte, os titulares de códigos devem confirmar e demonstrar que foi realizada uma consulta das partes interessadas relevantes aquando da apresentação do código para aprovação. Na ocasião, apresentarão especificamente informações sobre outros códigos de conduta aos quais os membros potenciais do código poderiam estar sujeitos e mostrarão de que modo o seu código complementa outros códigos. Devem também descrever o nível e a natureza da consulta realizada aos seus membros, a outras partes interessadas e aos titulares de dados ou às associações/aos organismos que os representam.[778]

Na prática, as diretrizes n.º 1/2019[779] recomendam vivamente a realização de uma consulta aos membros que fazem parte da organização ou do organismo que atua como titular do código e que seja tida em conta a atividade de tratamento de dados de seus clientes.

Nos casos em que não tenha sido realizada qualquer consulta das partes interessadas relevantes e específicas devido à falta de viabilidade, caberá ao titular do código explicar essa situação.

ix. Legislação nacional

Esse requisito também tem uma aplicação mais restrita ao contexto europeu, e quer dizer que os titulares de códigos devem confirmar que o projeto de código cumpre a legislação nacional pertinente, nomeadamente quando o código envolve um setor que é regido por disposições específicas, consagradas no direito nacional, ou diz respeito a operações de tratamento que devem ser avaliadas com base em requisitos específicos e obrigações legais pertinentes, à luz do direito nacional.

x. Língua

[778] Por exemplo, os titulares de códigos podem descrever como avaliaram os contributos recebidos em resposta à consulta.
[779] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

Os titulares de códigos devem cumprir os requisitos linguísticos da Autoridade de Controle competente à qual apresentarão o seu código. Em geral, os códigos devem ser apresentados na língua da Autoridade de Controle competente do Estado-Membro em causa.[780] No que respeita aos códigos transnacionais, estes devem ser apresentados na língua da Autoridade de Controle competente e na língua inglesa.[781] Outro requisito mais próprio ao contexto do bloco europeu ou no âmbito de outros blocos econômicas e acordos transnacionais.

xi. Lista de verificação

Em última análise, caberá à Autoridade de Controle competente escolhida determinar se o projeto de código avança para a próxima etapa de avaliação, ou seja, se é realizada uma avaliação completa do conteúdo em conformidade com os artigos 40.º e 41.º do RGPD e com os procedimentos descritos a seguir. A lista de verificação descrita no Anexo V, constante das diretrizes n.º 1/2019,[782] é indicada como referência para a documentação apresentada a uma Autoridade de Controle competente e para ajudar a enquadrar a apresentação do projeto de código naquele contexto.

f) Critérios para aprovação de códigos

Os titulares de códigos devem poder demonstrar a forma como o seu código contribuirá para a correta aplicação do RGPD, tendo em conta as características específicas dos vários setores de tratamento e as obrigações e os requisitos específicos dos responsáveis pelo tratamento ou dos subcontratantes visados pelo código. Este requisito (abrangente) envolve uma série de aspectos. Os titulares de códigos devem poder demonstrar que o seu projeto de código: a) satisfaz uma necessidade específica do setor ou da atividade de tratamento em questão; b) facilita a aplicação do RGPD; c)

[780] A legislação nacional de alguns Estados-Membros pode exigir a apresentação de um projeto de código na sua língua oficial, pelo que se recomenda aos titulares de códigos a análise desta questão com a autoridade de controle competente antes de apresentarem formalmente o seu projeto de código para aprovação.
[781] A língua inglesa é o idioma de trabalho do CEPD, nos termos da secção 23 do seu Regulamento Interno.
[782] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

especifica a aplicação do RGPD; d) prevê garantias suficientes de proteção;[783] e e) prevê procedimentos efetivos para a supervisão de conformidade com o código.

Esses requisitos serão esmiuçados na sequência:

i. Satisfaz uma necessidade específica

Os titulares de códigos devem demonstrar a necessidade de elaborar um código. Por conseguinte, deve-se abordar, no próprio código, as questões relacionadas com a proteção de dados levantadas para um determinado setor ou atividade de tratamento.[784]

Os titulares de códigos devem poder explicar e definir os problemas que o código procura abordar e apresentar prova da forma como as soluções nele disponibilizadas serão eficazes e benéficas, não apenas para os seus membros, como também para os titulares dos dados.

ii. Facilita a aplicação efetiva do RGPD

De acordo com o considerando 98 do RGPD, para que um código seja aprovado, os seus titulares devem poder demonstrar que ele facilita a aplicação efetiva do RGPD. Nesse sentido, o código deve estipular com clareza a aplicação específica do RGPD ao seu setor e identificar e satisfazer as necessidades específicas desse setor (por exemplo, os enumerados no artigo 40.º, n.º 2, do RGPD). [785]

---

[783] Por exemplo, prevê-se que os setores de «elevado risco», como o tratamento de dados de crianças ou de saúde, disponham de garantias mais sólidas e rigorosas, devido à sensibilidade dos dados pessoais em causa.

[784] As diretrizes n.º 1/2019 fornecem o seguinte exemplo: "Por exemplo, o setor dos sistemas de informação para a detecção de riscos de crédito ao consumidor pode identificar a necessidade de elaborar um código que preveja garantias e procedimentos suficientes para assegurar que os dados recolhidos são pertinentes, exatos e utilizados exclusivamente para a finalidade específica e legítima de proteção do crédito. De modo idêntico, o setor da investigação no domínio da saúde pode identificar a necessidade de elaborar um código que seja coerente na abordagem, estabelecendo normas para cumprir de forma adequada o requisito de consentimento explícito e os requisitos de responsabilidade que o acompanham no âmbito do RGPD". UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

[785] As diretrizes n.º 1/2019 fornecem o seguinte exemplo: "Por exemplo, a apresentação de uma lista de definições específicas do setor e uma abordagem adequada centrada em temas particularmente pertinentes para o setor constituem formas de facilitar a aplicação efetiva do RGPD. A utilização de terminologia específica para descrever de forma circunstanciada a aplicação dos requisitos do RGPD no setor também pode melhorar a compreensão clara das regras pelo setor e, assim, facilitar a aplicação efetiva do RGPD. Os códigos devem ter plenamente em conta os riscos prováveis de uma atividade de tratamento específica a um setor e regular de forma adequada as obrigações conexas dos responsáveis pelo tratamento ou dos subcontratantes abrangidos pelo seu âmbito de aplicação, tendo em conta esses riscos nesse setor específico, ou seja, apresentando exemplos de termos e condições aceitáveis em relação ao uso de dados pessoais em

iii. Especifica a aplicação do RGPD

Os códigos devem especificar a aplicação prática do RGPD e refletir com precisão a natureza da atividade ou do setor de tratamento. Devem poder introduzir melhorias claras e específicas para o setor em termos de cumprimento da legislação em matéria de proteção de dados. Devem estabelecer normas realistas e viáveis para todos os seus membros e ter a qualidade e a coerência interna necessárias para fornecer valor agregado suficiente.[786] Em outras palavras, o projeto de código deve centrar-se de forma adequada em domínios[787] e problemas específicos relativos à proteção de dados no setor específico ao qual se aplica e deve oferecer soluções suficientemente claras e eficazes para esses domínios e problemas.[788]

Um código não pode ser apenas uma reprodução do Regulamento Geral de Proteção de Dados Pessoais (RGPD).[789] Pelo contrário, deve ter como objetivo codificar, de uma forma específica, prática e precisa, o modo como o RGPD deve ser aplicado. As normas e regras aprovadas devem ser inequívocas, concretas, viáveis e executáveis (suscetíveis de serem testadas).

A definição de regras distintas no domínio específico é um método aceitável através do qual um código pode fornecer seu valor. A utilização de uma terminologia única e pertinente para o setor e a apresentação de cenários concretos ou de exemplos específicos de «melhores práticas»[790] podem ajudar a cumprir este requisito.[791]

A exposição dos pilares dos planos para promover o código aprovado com o objetivo de informar as pessoas da sua existência e do seu conteúdo também pode ajudar a cumprir o requisito de «especificar a aplicação do RGPD». É fundamental que os códigos possam conferir um significado operacional aos princípios de proteção de dados, conforme previsto no artigo 5.º do RGPD. Também é fundamental que tenham

---

marketing direto. Em termos de formato, o conteúdo dos códigos também deve ser apresentado de forma a facilitar a sua compreensão e a utilização prática, bem como a aplicação efetiva do RGPD". UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

[786] Esta norma foi aplicada pela primeira vez no documento de trabalho WP 13 DG XV D/5004/98, adotado em 10 de setembro de 1998.

[787] Por exemplo, os enumerados no artigo 40.º, n.º 2, do RGPD.

[788] Este requisito reflete a posição anterior do GT29, conforme descrito no documento de trabalho sobre os códigos de conduta WP 13 DG XV D/5004/98, adotado em 10 de setembro de 1998.

[789] A apresentação de reproduções da legislação em matéria de proteção de dados foi uma característica comum aos projetos de código elaborados de forma incorreta que foram submetidos à aprovação do GT29.

[790] E «práticas inaceitáveis».

[791] Um código deve evitar, sempre que possível, ser excessivamente legalista.

devidamente em conta os pareceres e posições pertinentes publicados ou aprovados pelo Comitê Europeu para a Proteção de Dados (CEPD) sobre um setor específico ou uma atividade de tratamento específica.[792] Por exemplo, os códigos que contenham especificações relativas a atividades de tratamento podem igualmente facilitar a identificação de fundamentos jurídicos adequados para essas atividades de tratamento nos Estados-Membros nos quais esteja prevista a sua aplicação.

iv. Fornece garantias suficientes

Os códigos devem, igualmente, cumprir os requisitos do artigo 40.º, n.º 5 do RGPD. Isso porque, a aprovação só será viabilizada quando for determinado que um projeto de código fornece garantias adequadas e suficientes.[793] Os titulares de códigos devem demonstrar adequadamente à Autoridade de Controle competente que os seus códigos contêm garantias adequadas e eficazes para a atenuação dos riscos relacionados com o tratamento de dados e os riscos para os direitos e liberdades individuais (isto é, para os direitos fundamentais).[794] Caberá aos titulares de códigos apresentar provas claras de que o seu código cumprirá esses requisitos. [795]

v. Prevê procedimentos que permitam uma supervisão efetiva

Nos termos do artigo 40.º, n.º 4, do RGPD, os códigos devem prever procedimentos que garantam a supervisão adequada das suas regras e a aplicação de medidas de execução eficientes e significativas para garantir o pleno cumprimento dessas obrigações. Em especial, os códigos devem identificar e propor estruturas e procedimentos que permitam uma supervisão eficaz e a aplicação de sanções em caso de

[792] Também devem ter plenamente em consideração a jurisprudência nacional e europeia pertinente.
[793] Ver considerando 98 do RGPD.
[794] Também podem ser aplicadas garantias quanto às competências dos organismos de supervisão para o desempenho eficaz das suas funções.
[795] As diretrizes n.º 1/2019 fornecem o seguinte exemplo: "Por exemplo, em atividades de tratamento de «elevado risco», como o tratamento em larga escala de dados de crianças ou de saúde, a criação de perfis ou o controle sistemático, é expectável que os códigos contenham requisitos mais exigentes para os responsáveis pelo tratamento e para os subcontratantes, de modo a refletir um nível adequado de proteção. Além disso, os titulares de códigos podem [se] beneficiar de uma consulta mais aprofundada, conforme previsto no considerando 99 do RGPD, para fundamentar um código que envolva o tratamento de domínios de elevado risco". UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

infração. O projeto de código deve também identificar um organismo adequado que disponha de procedimentos que lhe permitam efetuar, com eficácia, a supervisão de conformidade com o código. Os procedimentos podem incluir requisitos regulares de auditoria e de comunicação, procedimentos claros e transparentes para tratar reclamações e procedimentos de resolução de litígios, sanções e medidas corretivas concretas em caso de violação das disposições do código, bem como políticas para comunicação de violações de suas disposições.

Um projeto de código que envolva atividades de tratamento por autoridades ou organismos privados (não públicos) deve identificar um organismo de supervisão. Essencialmente, um código deve não só considerar o conteúdo das regras aplicáveis à atividade de tratamento desse setor específico como também implementar procedimentos de controle que garantam a aplicação efetiva dessas regras. Um projeto de código que envolva vários organismos de supervisão pode propor com sucesso procedimentos de controle diferentes, com vistas a uma supervisão eficaz. No entanto, todos os procedimentos de controle propostos para realizar a supervisão adequada de um código devem ser claros, adequados, viáveis, eficientes e executáveis (suscetíveis de serem testados).

Os titulares de códigos devem estabelecer os fundamentos e demonstrar a razão pela qual as suas propostas de supervisão são adequadas e operacionalmente viáveis.[796].

g) Apresentação, Admissibilidade e Aprovação para códigos nacionais (incluindo alterações e aditamentos a códigos anteriormente aprovados)

i. <u>Apresentação</u>

Os titulares de códigos devem apresentar formalmente o seu projeto de código em formato eletrônico ou em formato escrito (impresso/suporte papel) à Autoridade de Controle competente.[797] Esta acusará a recepção e procederá a uma análise do projeto de

[796] O documento WP7 do Grupo de Trabalho do Artigo 29 intitulado «Avaliação da autorregulamentação por parte de um setor: em que casos contribui de forma significativa para o nível de proteção dos dados em países terceiros?», adotado em 14 de janeiro de 1998, constitui igualmente um documento informativo que fornece mais informações sobre a avaliação do valor de um código e os fundamentos gerais necessários para que este seja eficaz. Recomenda-se que este documento também seja considerado (quando pertinente) durante a elaboração de um código.

[797] Obviamente, essa autoridade é a autoridade de controle nacional para os membros a quem o código se aplica. Também é importante que os titulares do código indiquem claramente à autoridade de controle competente que estão a apresentar formalmente um projeto de código para aprovação, bem como o seu

código para determinar se este satisfaz os critérios de admissibilidade tal como acima estabelecidos,[798] antes de proceder a uma avaliação completa do seu conteúdo.

ii. Admissibilidade de um código

Se o projeto de código não for aceito com base no descumprimento dos critérios de admissibilidade,[799] a Autoridade de Controle competente notificará do fato os titulares do código por escrito, expondo a fundamentação da sua decisão. O processo terminará nesta fase, e os titulares do código devem apresentar um novo projeto.[800]

Se o projeto de código cumprir os critérios acima definidos, a Autoridade de Controle competente notificará os titulares do código, por escrito, de que prosseguirá com a fase seguinte do processo e avaliará o conteúdo do projeto de código em conformidade com os procedimentos pertinentes previstos no direito nacional aplicável.

iii. Admissibilidade de um código

A menos que o direito nacional defina um prazo específico, a Autoridade de Controle competente deve elaborar um parecer, num período razoável, e deve fornecer informações atualizadas e de forma regular aos titulares do projeto de código, no que concerne ao processo e aos prazos indicativos. O parecer deve fundamentar a sua decisão em conformidade com os critérios de aprovação, conforme descrito acima.[801]

Se a Autoridade de Controle competente decidir recusar a aprovação, o processo será concluído e caberá aos titulares do código analisar as conclusões do parecer e ponderar a revisão do projeto de código a partir dessa base. Caso decidam reapresentá-lo posteriormente, devem proceder à sua atualização e (re)apresentá-lo formalmente.

Se a Autoridade de Controle competente aprovar um projeto de código, deve realizar seu registo e publicação (através do seu sítio Web e/ou de outros meios de

âmbito jurisdicional. Consultar também o Anexo III em relação à distinção entre códigos nacionais e transnacionais.

[798] Consultar também a lista de verificação do Apêndice V.

[799] Consultar também a lista de verificação do Apêndice V.

[800] Importa referir que a recusa, nesta fase do processo de aprovação, será provavelmente baseada em requisitos preliminares gerais ou processuais e não em questões substantivas ou centrais associadas a qualquer disposição do projeto de código.

[801] Para o efeito, a autoridade de controle competente pode formular observações úteis para os titulares de códigos, caso estes decidam rever, corrigir e reapresentar o projeto de código posteriormente.

comunicação adequados).[802] O artigo 40.º, n.º 11, exige, igualmente, que o Comitê disponibilize publicamente todos os códigos aprovados.

h) Apresentação, Admissibilidade e Aprovação para códigos transnacionais, incluindo alterações e aditamentos a códigos anteriormente aprovados

i. Apresentação

Os titulares de códigos devem apresentar formalmente o seu projeto de código em formato eletrônico ou em suporte de papel à Autoridade de Controle competente, que atuará como Autoridade principal para a aprovação do código.[803] A Autoridade de Controle competente acusará a recepção da documentação e procederá a uma análise do projeto de código para determinar se este satisfaz os requisitos acima estabelecidos,[804] antes de proceder a uma avaliação completa do seu conteúdo. A Autoridade de Controle competente notificará o mais rapidamente possível todas as restantes Autoridades de Controle da apresentação de um código e fornecerá as informações importantes que permitirão a sua fácil identificação e referência. Todas as Autoridades de Controle devem confirmar, em resposta, se são Autoridades de Controle interessadas, nos termos do artigo 4.º, n.º 22, alíneas a) e b), do RGPD.[805]

ii. Admissibilidade de um código

Se o projeto de código não for aceito com base no descumprimento dos critérios de admissibilidade definidos, a Autoridade de controle competente notificará do fato os titulares do código, por escrito, expondo a fundamentação da sua decisão. O processo terminará nesta fase, e os titulares do código deverão apresentar um novo projeto.[806] A

[802] Nos termos do artigo 40.º, n.º 6, do RGPD.
[803] Deve ser interpretado no contexto do procedimento descrito abaixo.
[804] Consultar também a lista de verificação do Anexo V.
[805] Esta confirmação é importante, uma vez que se pretende que os coavaliadores do projeto de código sejam autoridades de controle afetadas pelo tratamento de dados pessoais pelo fato de o responsável pelo tratamento ou o subcontratante estar estabelecido no território do Estado-Membro dessa autoridade de controle ou pelo facto de «os titulares de dados que residem no Estado-Membro dessa autoridade de controle serem substancialmente afetados, ou suscetíveis de o ser, pelo tratamento dos dados».
[806] Importa referir que a recusa, nesta fase do processo de aprovação, será provavelmente baseada em requisitos preliminares gerais ou processuais e não em questões substantivas ou centrais associadas a qualquer disposição do projeto de código.

Autoridade de Controle competente também emitirá uma notificação para informar todas as Autoridades de Controle interessadas sobre a sua posição.

Se o projeto de código for aceito com base no cumprimento dos critérios de admissibilidade, a Autoridade de Controle competente deverá notificar os titulares do código, por escrito, de que prosseguirá com a fase seguinte do processo e avaliará o conteúdo do projeto de código. Esta comunicação desencadeará o procedimento de cooperação informal seguinte no que diz respeito à avaliação do código para aprovação.

iii. Cooperação

A Autoridade de Controle competente emitirá uma notificação para informar todas as Autoridades de Controle[807] sobre a sua posição, identificará as Autoridades de Controle interessadas e apresentará um pedido de colaboração voluntária de, no máximo, dois coavaliadores, a fim de a assistir (auxiliar) na avaliação substantiva do projeto de código.

A nomeação dos coavaliadores será efetuada com base na ordem de chegada das respostas ao pedido,[808] e a sua função consistirá em auxiliar a Autoridade de Controle competente na avaliação do projeto de código.

Após a confirmação dos coavaliadores, estes devem apresentar as suas observações sobre o conteúdo do código no prazo de 30 dias a contar da data da confirmação. Essas observações, depois, serão tidas em consideração pela Autoridade de Controle competente ao realizar a avaliação do projeto para aprovação.

Nos termos do artigo 40.º, n.º 7, a Autoridade de Controle competente deve decidir se o projeto de decisão deve ser apresentado ao Comitê Europeu para a Proteção de Dados (CEPD), em conformidade com os artigos 63.º e 64.º do RGPD.[809]

A Autoridade de Controle competente deve ter como objetivo chegar a uma decisão num período razoável e deve informar regularmente os titulares do código sobre os progressos realizados e os prazos indicados. Deve, também, fundamentar a sua decisão

[807] As autoridades de controle interessadas devem ser identificáveis pelo âmbito de aplicação do projeto de código.
[808] Este pedido de colaboração permanecerá em aberto durante dez dias úteis. Enquanto decorrer a identificação dos coavaliadores, a autoridade de controle competente prosseguirá com a avaliação. Regra geral, a autoridade de controle competente consultará dois coavaliadores sempre que sejam afetados pelo código, pelo menos, 14 Estados-Membros. Abaixo deste número, é possível ter um ou dois coavaliadores, dependendo do caso específico.
[809] Esta situação só pode ocorrer se a autoridade de controle competente pretender aprovar o projeto de código. Ver artigo 40.º, n.º 7 e artigo 64.º, n.º 1, do RGPD.

(recusar ou aprovar o código) em consonância com os fundamentos gerais de aprovação e comunicar essa decisão aos titulares do código em tempo útil.

iv. Recusa

Se a Autoridade de Controle competente decidir recusar a apresentação do projeto do código ao Comitê Europeu para a Proteção de Dados (CEPD), o processo será concluído e caberá aos titulares do código analisar as conclusões da decisão e ponderar a revisão do projeto de código. Caso pretendam reapresentar o código posteriormente, devem proceder à sua atualização. A Autoridade de Controle competente deve também notificar todas as Autoridades de Controle interessadas da sua posição, bem como das razões para recusar a aprovação do código.

v. Preparação para apresentação ao Comitê

Se a Autoridade de Controle competente pretender aprovar o projeto de código, deverá apresentar o seu projeto de aprovação a todas as Autoridades de Controle interessadas, antes da apresentação ao Comitê Europeu para a Proteção de Dados (CEPD). Estas disporão de 30 dias para responder, devendo as questões importantes ser apresentadas ao subgrupo pertinente do CEPD para discussão. Caso as Autoridades de Controle interessadas não respondam, o processo de avaliação do código avançará para a fase seguinte.

vi. O Comitê

Se a Autoridade de Controle competente decidir apresentar o assunto ao Comitê Europeu para a Proteção de Dados, em conformidade com o artigo 40.º, n.º 7, do RGPD, comunicará essa decisão a todas as Autoridades de Controle no âmbito do procedimento de controle de coerência (entre os diversos Estados-membros interessados).[810] Deverá, igualmente, apresentar o assunto ao Comitê em consonância com o regulamento interno deste e com o artigo 40.º, n.º 7, do RGPD.

[810] Ver o artigo 64.º, n.º 4, do RGPD, segundo o qual as posições das outras autoridades de controle interessadas devem ser apresentadas juntamente com o projeto de decisão da autoridade de controle competente.

Nos termos do artigo 64.º, o Comitê deve emitir um parecer sobre as questões a que se refere o artigo 40.º, n.º 7, do RGPD.[811] O regulamento interno do Comitê Europeu para a Proteção de Dados (CEPD), juntamente com as disposições do artigo 64.º, será aplicável ao CEPD e à Autoridade de Controle competente aquando da realização de uma avaliação e da comunicação de uma decisão sobre a aprovação de códigos transnacionais.

vii. Aprovação

O parecer do Comitê será transmitido à Autoridade de Controle competente, em conformidade com o artigo 64.º, n.º 5, do RGPD, e caberá a essa Autoridade decidir se tenciona manter ou alterar o projeto de decisão, nos termos do artigo 40.º, n.º 5.[812] O Comitê também poderá apresentar o seu parecer à Comissão Europeia, nos termos do artigo 40.º, nº 8, e deverá recolher todos os códigos de conduta transnacionais aprovados e disponibilizá-los ao público, nos termos do artigo 40.º, n.º 11.

i) Compromisso

Importa referir que o processo de avaliação não deve ser utilizado como uma oportunidade para uma consulta complementar à Autoridade de Controle competente sobre as disposições do código apresentado. Nos termos do artigo 40.º, n.º 5, a Autoridade de Controle competente emite um parecer sobre a conformidade do projeto de código com o RGPD.[813] Nesse sentido, a comunicação prevista entre a Autoridade de Controle competente e os titulares do código durante esta fase do processo servirá essencialmente para fins de clarificar e auxiliar na realização de uma avaliação nos termos dos artigos 40.º e 41.º.

Espera-se que os titulares do código, se for caso disso, contatem as Autoridades de Controle antes de apresentarem o seu projeto de código para aprovação. Em princípio, a fase de aprovação do processo não deve permitir que os titulares do código efetuem uma consulta complementar sobre as disposições específicas do projeto de código nem permitir uma avaliação alargada através da qual sejam continuamente apresentadas

[811] Ver a atribuição do Comitê nos termos do artigo 70.º, n.º 1, alínea x) do RGPD.
[812] Ver artigo 64.º, n.º 7, em especial os procedimentos invocados caso uma autoridade de controle competente discorde do parecer do Comitê, nos termos do artigo 64.º, n.º 8, do RGPD.
[813] A autoridade de controle competente também pode aconselhar e, se for caso disso, formular recomendações aos titulares de códigos sobre o conteúdo e o formato do respetivo projeto de código.

alterações à Autoridade de Controle. É igualmente imperativo que os titulares do código estejam disponíveis para prestar esclarecimentos, num prazo razoável, sobre o seu projeto de código.

É importante, também, que os titulares do código estejam preparados e organizados para esclarecer dúvidas de uma forma eficiente. As diretrizes n.º 1/2019[814] recomendam que seja indicado à Autoridade de Controle competente um ponto de contato único ou dedicado. Caberá à Autoridade de Controle competente decidir se necessita de mais informações antes de tomar uma decisão sobre o projeto de código, bem como determinar a forma de comunicação entre as partes.

A fim de assegurar a continuidade, a Autoridade de Controle competente deve manter-se como ponto de contato principal durante todo o processo de aprovação dos códigos transnacionais.

j) Funções da comissão Europeia

A Comissão Europeia pode, através de um ato de execução, decidir que um código transnacional aprovado será de aplicabilidade geral na União, e deve assegurar a publicidade adequada, caso essa aplicabilidade seja declarada.[815]

k) Supervisão de um código

Para que um código (nacional ou transnacional) seja aprovado, é necessário que um organismo (ou organismos) de supervisão seja(m) identificado(s) no âmbito do código e acreditado(s) pela Autoridade de Controle competente como tendo aptidão/competência para realizar uma supervisão eficaz do código.[816] A Autoridade de Controle competente apresentará ao Comitê Europeu para a Proteção de Dados (CEPD) os projetos de

[814] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

[815] Ver artigo 40.º, n.º 9, e artigo 40.º, n.º 10 do RGPD. Essa decisão deve também permitir que os responsáveis pelo tratamento e os subcontratantes que não estejam sujeitos às disposições do RGPD assumam compromissos vinculativos e com força executiva em relação a um código validado (ver artigo 40.º, n.º 3). Tal permitiria a transferência de dados para países terceiros ou organizações internacionais com base na existência de garantias adequadas e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes [ver também artigo 46.º, n.º 1 e n.º 2, alínea e)].

[816] Artigo 41.º, n.º 1, do RGPD. Importa também referir que o artigo 41.º não se aplica a autoridades ou organismos públicos.

requisitos para a acreditação de um organismo de supervisão, em conformidade com o procedimento de controle da coerência a que se refere o artigo 63.º do RGPD. Uma vez aprovados pelo Comitê, os requisitos podem ser aplicados pela Autoridade de Controle competente para acreditar um organismo de supervisão.

O RGPD não define o termo «acreditação». No entanto, o artigo 41.º, n.º 2, do RGPD enumera requisitos gerais para a acreditação do organismo de supervisão. Existe um conjunto de requisitos que deve ser cumprido de forma satisfatória para que uma Autoridade de Controle competente acredite um organismo de supervisão. Os titulares de códigos devem explicar e demonstrar a forma como o organismo de supervisão que propõem cumpre os requisitos estabelecidos no artigo 41.º, n.º 2, para obter a acreditação.

O RGPD prevê flexibilidade quanto ao tipo e estrutura de um organismo de supervisão para que este seja acreditado ao abrigo do artigo 41.º. Os titulares de códigos podem decidir utilizar organismos de supervisão externos ou internos, desde que, em ambos os casos, o organismo em causa cumpra os requisitos de acreditação do artigo 41.º, n.º 2, conforme indicado nas oito subsecções seguintes.

l) Requisitos de acreditação dos organismos de supervisão

i. <u>Independência</u>

Os titulares de códigos devem demonstrar que o organismo em questão goza da independência e imparcialidade necessárias ao desempenho das suas funções, no que diz respeito aos membros do código e à profissão, à indústria ou ao setor aos quais o código se aplica. Essa independência pode ser demonstrada através do financiamento do organismo de supervisão, da nomeação dos seus membros/pessoal, do seu processo de decisão e, mais genericamente, da sua estrutura organizativa, adiante explicitados pormenorizadamente.

Os titulares de códigos dispõem de dois modelos principais de supervisão que podem se utilizar para cumprir os requisitos aplicáveis aos organismos de supervisão: organismo de supervisão interno ou externo. Existe alguma flexibilidade entre estes dois tipos de abordagem à supervisão, podendo ser propostas diferentes versões que sejam adequadas em função do contexto do código. Os exemplos de organismos de supervisão internos podem incluir um comitê interno *ad hoc* ou um departamento separado e independente na organização do titular do código. Caberá aos titulares dos códigos

explicar a abordagem à gestão dos riscos, no que diz respeito à sua imparcialidade e independência.

Por exemplo, sempre que seja proposto um organismo de supervisão interno, o pessoal, a gestão, a responsabilidade e as funções devem ser separados das restantes áreas da organização. Esta separação pode ser obtida de várias formas, por exemplo, através da utilização de barreiras eficazes em matéria de informação e de estrutura organizativa e de estruturas separadas de gestão da comunicação para a organização e para o organismo de supervisão. À semelhança de um encarregado da proteção de dados, o organismo de supervisão deve poder agir de forma totalmente independente e estar protegido de qualquer tipo de sanção ou interferência (direta ou indireta) pelo fato de exercer as suas funções.

Para demonstrar a independência do organismo de supervisão, poderá ser necessário que um consultor externo ou outra entidade que tenha participado na elaboração do código de conduta demonstre que este dispunha de garantias adequadas e suficientes para a atenuação de um eventual risco para sua independência ou de um conflito de interesses. O organismo de supervisão deve demonstrar a adequação dos instrumentos que identificariam e atenuariam esses riscos de modo satisfatório.[817] O organismo de supervisão deve, também, identificar de forma continuada os riscos para a sua imparcialidade, tais como as suas atividades ou os riscos decorrentes das suas relações pessoais. Caso seja identificado um risco para a imparcialidade, o organismo de supervisão deve demonstrar a forma como elimina ou minimiza esse risco e como utiliza instrumentos adequado para garantir a imparcialidade.

A independência, ademais, pode ser demonstrada através da concessão de plena autonomia em matéria de gestão do orçamento e de outros recursos, mormente nos casos em que o organismo de supervisão seja interno.

O organismo de supervisão também deve poder agir de forma independente na escolha e aplicação de sanções a um responsável pelo tratamento ou a um subcontratante que tenha aderido ao código. Em suma, o organismo de supervisão (interno ou externo), no desempenho das suas funções e no exercício dos poderes que lhe são atribuídos pelo âmbito de aplicação do código, deve agir de forma independente dos titulares e membros do código.

[817] O contexto do código determinará a abordagem a adotar. Por exemplo, pode ser suficiente apresentar uma proposta que contenha uma separação adequada de funções, segundo a qual o pessoal do organismo de supervisão não elabora nem testa o código.

ii. Conflito de interesses[818]

Deve ser demonstrado que o exercício das funções e atribuições do organismo de supervisão não implica um conflito de interesses. Nesse sentido, os titulares de códigos devem demonstrar que o organismo de supervisão proposto se absterá de qualquer ato incompatível com as suas funções e atribuições e que serão dadas garantias de que não exercerá nenhuma atividade que seja incompatível com elas.

De modo idêntico, o organismo de supervisão não deve estar sujeito a influências externas, diretas ou indiretas, e não deve solicitar nem receber instruções de qualquer pessoa, organização ou associação.

O organismo deve dispor do seu próprio pessoal, selecionado por si ou por outro organismo independente do código, que deve ficar sob a sua direção exclusiva. No caso de um organismo de supervisão interno, este deve estar protegido de qualquer tipo de sanção ou interferência (direta ou indireta) por parte do titular do código, de outros órgãos pertinentes[819] ou de membros do código, pelo fato de exercer as suas funções.

iii. Competências especializadas

Os titulares de códigos devem poder demonstrar que o organismo de supervisão tem o nível necessário de competências para desempenhar a sua função com eficácia. Nesse sentido, a apresentação de um código deve incluir informações relativas aos conhecimentos e experiência do organismo sobre a legislação em matéria de proteção de dados, bem como sobre o setor ou a atividade de tratamento em causa. Por exemplo, poder comprovar a experiência anterior no exercício de funções de supervisão em setor específico pode ajudar a cumprir este requisito.

Além disso, dispor de um conhecimento aprofundado de questões relativas à proteção de dados e de conhecimentos especializados das atividades de tratamento específicas que são o objeto do código será uma mais-valia.

O pessoal do organismo de supervisão proposto deve também dispor da experiência operacional e formação adequadas, por exemplo, no domínio de atividades

[818] Imparcialidade no desempenho de funções, ou seja, a capacidade para agir de forma autônoma.
[819] Organismos que representem categorias de responsáveis pelo tratamento dos dados ou de subcontratantes.

de auditoria, acompanhamento ou garantia de qualidade, para efetuar a supervisão do cumprimento das disposições do código.

iv. Estruturas e procedimentos estabelecidos

O organismo de supervisão deve também dispor de procedimentos e estruturas de governança que lhe permitam executar adequadamente as seguintes funções: (a) avaliar a elegibilidade dos responsáveis pelo tratamento e dos subcontratantes em causa para aplicar o código; (b) verificar se estes respeitam as suas disposições; e (c) efetuar revisões do seu funcionamento.

Deve ser criado um conjunto completo de procedimentos de verificação que avalie adequadamente a elegibilidade dos responsáveis pelo tratamento e dos subcontratantes para aderirem ao código e cumpri-lo. Deve, igualmente, ser assegurado que os responsáveis pelo tratamento e os subcontratantes cumprem as disposições do código.

Serão necessários procedimentos e estruturas para a supervisão ativa e eficaz do cumprimento do código pelos seus membros, os quais podem incluir auditorias aleatórias ou não anunciadas, inspeções anuais, relatórios regulares e a utilização de questionários.[820]

Os procedimentos de controle podem ser concebidos de diferentes formas, desde que tenham em conta fatores como os riscos suscitados pelo tratamento de dados no âmbito de aplicação do código, as reclamações apresentadas ou incidentes específicos, o número de membros do código etc. No âmbito de aplicação do código, pode ser ponderada a publicação de relatórios de auditoria, bem como das conclusões de relatórios periódicos dos responsáveis pelo tratamento e dos subcontratantes.

Os titulares de códigos devem também demonstrar que o organismo de supervisão proposto dispõe de recursos e pessoal adequados para desempenhar adequadamente as suas funções. Os recursos devem ser proporcionais ao número e à dimensão previstos dos membros do código, bem como à complexidade ou ao grau de risco do tratamento de dados em causa.

[820] Tal pode igualmente ajudar a evitar uma situação em que uns membros sejam controlados repetidamente e outros não.

v. Estruturas e procedimentos estabelecidos

O organismo de supervisão deve criar procedimentos e estruturas eficazes que possam tratar reclamações de uma forma imparcial e transparente. Nesse sentido, deve dispor de um processo de tratamento de reclamações acessível ao público, com recursos suficientes para gerir as reclamações, e assegurar que as decisões do organismo são tornadas públicas.[821]

Os organismos de supervisão devem dispor de procedimentos eficazes para assegurar o cumprimento do código pelos responsáveis pelo tratamento ou pelos subcontratantes. A título de exemplo, poderiam ser atribuídos ao organismo de supervisão poderes para suspender ou excluir do código um responsável pelo tratamento ou um subcontratante, caso este atue à margem dos termos do código (ou seja, aplicação de medidas corretivas).

Se um membro de um código infringir as regras deste, o organismo de supervisão é obrigado a adotar medidas adequadas imediatas, que terão como objetivo pôr termo à infração e evitar a sua repetição. Essas medidas corretivas e sanções podem incluir atuações que vão desde ações de formação a uma advertência, à denúncia do membro ao Comitê, a um aviso formal a exigir a aplicação de medidas específicas num prazo específico ou à suspensão temporária do membro do código até que sejam tomadas medidas para a exclusão definitiva desse membro do código. As medidas podem ser publicadas pelo organismo de supervisão, em especial, em caso de violações graves do código.

Se for esse o caso, o organismo de supervisão deve informar o membro do código, o titular do código, a Autoridade de Controle competente e todas as Autoridades de Controle interessadas sobre as medidas adotadas e a sua justificação, sem indevida demora.[822] Além disso, no caso de um código transnacional e se for possível identificar

[821] As diretrizes n.º 1/2019 fornecem o seguinte exemplo: "Por exemplo, o processo de tratamento de reclamações pode ser demonstrado através da descrição de um procedimento para receber, avaliar, acompanhar, registar e resolver reclamações. Este procedimento pode ser descrito em orientações sobre o código disponíveis ao público para que o autor da reclamação possa compreender e acompanhar o processo de tratamento de reclamações. Além disso, a separação das funções operacionais e de gestão no organismo de supervisão pode reforçar a independência destes procedimentos". UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

[822] Se a supervisão for realizada por um organismo externo à associação/ao organismo que apresenta o código de conduta, o titular do código também deve ser informado.

uma Autoridade de Controle principal[823] para um dos seus membros, o organismo de supervisão deve também notificar essas medidas a essa autoridade.

vi. Comunicação com as Autoridades de Controle competentes

Deve ser proposto um quadro para os organismos de supervisão que permita à Autoridade de Controle competente e a outras Autoridades de Controle a comunicação eficaz de quaisquer medidas relativas ao código adotadas por um organismo de supervisão. Esse quadro pode incluir decisões relativas às medidas adotadas em caso de violação do código por um dos seus membros, a apresentação de relatórios periódicos sobre o código ou a apresentação de conclusões de auditoria ou análises do código.[824]

Além disso, deve garantir que a Autoridade de Controle não é prejudicada nem impedida de exercer a sua função. Por exemplo, um código que proponha que os seus membros possam, unilateralmente, aprovar, excluir ou suspender um organismo de supervisão sem aviso prévio e sem o acordo da Autoridade de Controle competente estaria violando o artigo 41.º, n.º 5, do RGPD.

vii. Procedimentos de avaliação

Um código deve definir procedimentos de avaliação adequados para garantir que permanece relevante e continua a contribuir para a correta aplicação do RGPD. Deve prever igualmente procedimentos de avaliação que permitam a adaptação a quaisquer alterações na aplicação e na interpretação da lei ou sempre que a evolução tecnológica possa ter impacto no tratamento de dados realizado pelos seus membros ou nas suas disposições.

viii. Estatuto jurídico

O organismo de supervisão proposto (interno ou externo) e as suas estruturas de governança devem ser concebidos de forma a que os titulares de códigos possam demonstrar que o organismo de supervisão dispõe da capacidade adequada para

[823] Nos termos do artigo 56.o do RGPD.
[824] Ver artigo 41.º, n.º 4, do RGPD.

desempenhar as suas funções nos termos do artigo 41.º, n.º 4, e está sujeito à aplicação das multas previstas no artigo 83.º, n.º 4, alínea c), do RGPD.

m) Códigos aprovados

Indubitavelmente, a natureza e o conteúdo do código determinarão as funções das partes interessadas relevantes para assegurar o cumprimento das disposições do código e do RGPD. No entanto, caberá à Autoridade de Controle competente assegurar que o código continua adequado aos fins a que se destina.

Por conseguinte, a Autoridade de Controle competente trabalhará em estreita colaboração com o organismo de supervisão, no que se refere aos requisitos de comunicação decorrentes do código. O organismo de supervisão terá a função de ponto de contacto principal e coordenador para quaisquer questões que possam surgir em relação ao código.

A Autoridade de Controle competente deve aprovar quaisquer alterações ou aditamentos ao código e acreditar os novos organismos de supervisão.[825] Nos termos do artigo 40.º, n.º 5, do RGPD, as alterações ou aditamentos a um código existente terão, ainda, de ser apresentados à Autoridade de Controle competente, em consonância com os procedimentos descritos no presente documento.

n) Revogação de um organismo de supervisão

Sempre que um organismo de supervisão não cumprir as disposições aplicáveis do RGPD, a Autoridade de Controle competente terá poderes para revogar a sua acreditação, nos termos do artigo 41.º, n.º 5, do RGPD.[826] É importante que o titular do código introduza nele disposições adequadas para fazer face a um cenário de revogação.

No entanto, caso se trate do único organismo de supervisão a um código, a revogação da acreditação pode implicar a suspensão ou a exclusão permanente desse

[825] Entre as alterações que requerem a aprovação, por exemplo, poderia incluir-se a adição de uma nova norma ao código, mas não a atualização de uma referência ao nome de uma organização ou outras alterações menores que não incidem no funcionamento do código.

[826] No que respeita aos códigos transnacionais, também é essencial que a autoridade de controle competente assegure que todas as autoridades de controle interessadas tenham conhecimento da aplicação dessa medida. De modo idêntico, no que concerne a esses códigos, a autoridade de controle interessada deve igualmente informar a autoridade de controle competente nos casos em que considere que um responsável pelo tratamento dos dados (que se presume adotar o código) não cumpriu as disposições do código, uma vez que esta constatação pode suscitar dúvidas quanto à eficácia da autoridade de supervisão e do código.

código devido à ausência de supervisão obrigatória do cumprimento das suas disposições. Esse fato pode afetar negativamente a reputação ou os interesses comerciais dos membros do código e implicar uma diminuição da confiança dos respectivos titulares dos dados ou de outras partes interessadas.

Sempre que as circunstâncias o permitam, a revogação só deve ocorrer depois de a Autoridade de Controle competente ter dado ao organismo de supervisão a possibilidade de, com a maior urgência possível, resolver as questões suscitadas ou introduzir melhorias, consoante aplicável, num prazo acordado.

Nos casos que envolvam códigos transnacionais, a Autoridade de Controle competente deve, antes de acordar com o organismo de supervisão a definição de parâmetros com vista a resolver as questões suscitadas, contactar as Autoridades de Controle interessadas sobre o assunto. A decisão de revogar a acreditação de um organismo de supervisão deve também ser comunicada a todas as Autoridades de Controle interessadas e ao Comitê Europeu para a Proteção de Dados (CEPD), para efeitos do artigo 40.º, n.º 11.

o) Códigos do setor público

O artigo 41.º, n.º 6, do RGPD estabelece que a supervisão dos códigos de conduta aprovados não se aplicará ao tratamento realizado por autoridades e organismos públicos. Em suma, esta disposição elimina o requisito de um organismo acreditado para fins de supervisão de um código. Esta isenção em nada reduz a obrigatoriedade da implementação de procedimentos eficazes para fins de supervisão de um código. Para o efeito, é possível adaptar os requisitos existentes em matéria de auditoria de modo a incluir a supervisão do código.

3.1.2. Códigos de Conduta enquanto instrumento para transferências internacionais, nos termos das Diretrizes n.º 4/2021 do Comitê Europeu para a Proteção de Dados[827]

a) Introdução

[827] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 04/2021 relativas aos códigos de conduta enquanto instrumento para as transferências**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de. Acesso em: 15 nov. 2022. A análise apresentada terá por substrato as citadas diretrizes.

A segunda modalidade de códigos de conduta diz respeito à sua utilização para viabilizar transferências internacionais. O RGPD exige, no seu artigo 46.º, que os responsáveis pelo tratamento/subcontratantes estabeleçam garantias adequadas para as transferências de dados pessoais para países terceiros ou organizações internacionais.

Para o efeito, o RGPD diversifica as garantias adequadas que podem ser utilizadas pelas organizações, nos termos do artigo 46.º, para enquadrar as transferências para países terceiros, introduzindo, especialmente, os códigos de conduta enquanto novo mecanismo de transferência [artigo 40.º, n.º 3.º, e artigo 46.º, n.º 2, alínea e)].

A este respeito, tal como previsto no artigo 40.º, n.º 3, uma vez aprovado pela Autoridade de Controle competente e, após lhe ter sido concedida aplicabilidade geral na União Europeia pela Comissão, um código de conduta pode ser adotado e utilizado pelos responsáveis pelo tratamento ou subcontratantes não sujeitos ao Regulamento Geral de Proteção de Dados Pessoais situados em países terceiros (não membros), a fim de fornecer garantias adequadas para os dados transferidos a estes países terceiros.

Os responsáveis pelo tratamento e os subcontratantes são obrigados a assumir compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias adequadas previstas no código, inclusive em relação aos direitos dos titulares dos dados, tal como exigido pelo artigo 40.º, n.º 3. As diretrizes ora em análise fornecem elementos que devem ser abordados nesses compromissos.

Note-se, ademais, que um código destinado às transferências adotado por um importador de dados num país terceiro pode ser utilizado pelos responsáveis pelo tratamento/subcontratantes sujeitos ao RGPD (ou seja, exportadores de dados) para cumprirem as suas obrigações em caso de transferências para países terceiros, em conformidade com o RGPD, sem necessidade de aderirem eles próprios a esse código.

No que diz respeito ao conteúdo de um código destinado às transferências e para fornecer garantias adequadas para viabilizar as transferências de dados internacional na acepção do artigo 46.º, um código de conduta deve incluir os princípios, direitos e obrigações essenciais decorrentes do RGPD para os responsáveis pelo tratamento/subcontratantes, bem como as garantias específicas do contexto das transferências (por exemplo, no que diz respeito à questão das transferências ulteriores, conflitos de leis no país terceiro, etc.). À luz das garantias fornecidas pelos instrumentos de transferência existentes à luz do artigo 46.º do RGPD e para assegurar a coerência do

nível de proteção, bem como tendo em conta o Acórdão Schrems II[828] do TJUE, as diretrizes fornecem uma lista de verificação dos elementos que devem ser abrangido num código de conduta destinado às transferências.

Um código de conduta pode ser originalmente elaborado com o único propósito de especificar a aplicação do RGPD, em conformidade com o artigo 40.º, n.º 2 («código RGPD»), ou também como um código destinado às transferências, em conformidade com o artigo 40.º, n.º 3. Consequentemente, dependendo do âmbito de aplicação e do conteúdo do código originalmente especificados, pode ser necessário alterá-lo, a fim de abranger todos os elementos acima referidos, se for utilizado como instrumento para viabilizar as transferências de dados.

As diretrizes n.º 4/2022, complementam as Diretrizes 1/2019 do CEPD relativas aos Códigos de Conduta e aos Organismos de Supervisão à luz do Regulamento (UE) 2016/679, e clarificam o papel das diferentes entidades envolvidas na criação de um código de conduta instituído com a finalidade de ser utilizado como instrumento para as transferências internacionais, bem como o processo de sua adoção através de fluxogramas.

b) Disclaimer

A presente seção é construída com base nas diretrizes n.º 4/2022[829] do Comitê Europeu para a Proteção de Dados que têm o objetivo de especificar a aplicação do artigo 40.º, n.º 3, do RGPD relativo aos códigos de conduta enquanto garantias adequadas para as transferências de dados pessoais para países terceiros, em conformidade com o artigo 46.º, n.º 2, alínea e), do RGPD. Visa, igualmente, fornecer orientações práticas, especialmente, sobre o conteúdo desses códigos de conduta, o seu processo de adoção e as entidades envolvidas, bem como sobre os requisitos a cumprir e as garantias a incluir num código de conduta para as transferências.

As presentes informações, extraídas das citadas diretrizes devem ainda fornecer uma referência clara sobre os procedimentos envolvidos no processo de apresentação e avaliação desses códigos de conduta. As diretrizes, por sua vez, buscam, entre outros

[828] Acórdão do Tribunal de Justiça (Grande Secção) de 16 de julho de 2020, Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems.
[829] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 04/2021 relativas aos códigos de conduta enquanto instrumento para as transferências**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de. Acesso em: 15 nov. 2022.

propósitos, proporcionar maior transparência, assegurando que os titulares de códigos que pretendam obter aprovação para um código de conduta destinado a ser utilizado como instrumento para as transferências internacionais (a seguir designado por «código(s) destinado(s) às transferências») estão plenamente cientes do processo e compreendem os requisitos formais e os limites adequados necessários para a criação desses códigos de conduta.

As Diretrizes nº 4/2021 complementam as Diretrizes 1/2019 do CEPD relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679, que estabelecem o quadro geral para a adoção de códigos de conduta (a seguir designadas «Diretrizes 1/2019»). As considerações expostas nas Diretrizes 1/2019, especialmente no que se refere à admissibilidade, apresentação e critérios de aprovação, são igualmente válidas no contexto da elaboração de códigos destinados às transferências.

c) O que são os códigos de conduta enquanto instrumento para as transferências?

Como mencionado, o RGPD exige, no seu artigo 46.º, que os responsáveis pelo tratamento/subcontratantes estabeleçam garantias adequadas para as transferências de dados pessoais para países terceiros ou organizações internacionais. Referimos também que, para tanto, o RGPD diversificou as garantias adequadas que poderiam ser utilizadas pelas organizações (com fundamento no artigo 46.º) para enquadrar as transferências para países terceiros, introduzindo, designadamente, os códigos de conduta enquanto novo mecanismo de transferência [artigo 40.º, n.º 3.º, e artigo 46.º, n.º 2, alínea e)].

A esse respeito, tal como previsto no artigo 40.º, n.º 3, uma vez aprovado pela Autoridade de Controle competente (a seguir designada por «AC competente») e após lhe ter sido concedida aplicabilidade geral na União pela Comissão Europeia, um código de conduta pode também ser adotado e utilizado pelos responsáveis pelo tratamento ou subcontratantes não sujeitos ao RGPD situados em países terceiros, a fim de fornecer garantias adequadas para os dados transferidos para países terceiros. Os responsáveis pelo tratamento e os subcontratantes são obrigados a assumir compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias adequadas previstas no código, inclusive em relação aos direitos dos titulares dos dados, tal como exigido pelo artigo 40.º, n.º 3.

Os códigos de conduta podem ser elaborados por associações ou outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes (titulares de códigos), tal como especificado no artigo 40.º, n.º 2.

Ademais, tal como indicado nas Diretrizes 1/2019, uma lista não exaustiva de possíveis titulares de códigos poderia incluir: associações comerciais e representativas, organizações setoriais, instituições universitárias e grupos de interesse. De acordo com as mesmas diretrizes, os códigos destinados às transferências poderiam, por exemplo, ser elaborados por organismos que representam um setor (por exemplo, uma associação/federação do setor bancário e financeiro ou dos seguros), mas também poderiam ser elaborados para setores distintos que partilham uma atividade de tratamento com as mesmas características e necessidades em matéria de tratamento (por exemplo, um código de recursos humanos elaborado por uma associação/federação de profissionais de RH, ou um código sobre dados de crianças).

Esses códigos permitiriam aos responsáveis pelo tratamento e subcontratantes em países terceiros que recebem dados ao abrigo do código, enquadrar essas transferências e responder melhor às necessidades de tratamento específicas do seu setor ou atividades de tratamento comuns. Como tal, poderiam servir como um instrumento mais adaptado do que outros mecanismos de transferência disponíveis nos termos do artigo 46.º. Os códigos de conduta a serem utilizados como instrumento para as transferências permitirão, principalmente, a um determinado responsável pelo tratamento ou subcontratante num país terceiro fornecer garantias adequadas para múltiplas transferências para um país terceiro que sejam específicas de um setor ou de uma atividade de tratamento de dados. Além disso, as entidades que utilizam os códigos de conduta não precisam estar dentro do mesmo grupo para enquadrar as suas transferências (como é o caso das regras vinculativas aplicáveis às empresas).

Note-se, além disso, que um código destinado às transferências adotado por um importador de dados num país terceiro pode ser utilizado pelos responsáveis pelo tratamento/subcontratantes sujeitos ao RGPD (ou seja, exportadores de dados) para cumprirem as suas obrigações em caso de transferências para países terceiros em conformidade com o RGPD, sem necessidade de adotarem eles próprios esse código. Por conseguinte, um código destinado às transferências pode enquadrar as transferências de responsáveis pelo tratamento/subcontratantes que não adotaram esse código de conduta para responsáveis pelo tratamento/subcontratantes num país terceiro que tenham adotado esse código de conduta, desde que seja incluído num instrumento vinculativo o

compromisso de cumprir as obrigações estabelecidas pelo código de conduta aquando do tratamento dos dados transferidos, incluindo, em especial, o que diz respeito aos direitos dos titulares dos dados.

Isso significa que o importador de dados no país terceiro tem de adotar o código destinado às transferências, ao passo que os exportadores de dados sujeitos ao RGPD não têm necessariamente de o fazer. Os grupos de empresas que transferem dados de entidades sujeitas ao RGPD para fora do Espaço Econômico Europeu (EEE) podem também utilizar um código de conduta como instrumento de transferência se as entidades fora do EEE tiverem adotado esse código destinado às transferências e tiverem assumido compromissos vinculativos e com força executiva relacionados com a transferência. [830]

Um código destinado às transferências pode também enquadrar as transferências de responsáveis pelo tratamento/subcontratantes sujeitos ao RGPD para responsáveis pelo tratamento/subcontratantes no país terceiro que tenham aderido ao mesmo código de conduta para as transferências, desde que, em qualquer caso, tal como explicado *supra*, seja incluído num instrumento vinculativo o compromisso de cumprir as obrigações do código de conduta, incluindo o que diz respeito aos direitos dos titulares dos dados, tal como consagrados no RGPD.[831]

---

[830] As Diretrizes n.º 4/2021 exemplificam o assunto do seguinte modo: "Exemplo n.º 1 [Este exemplo não prejudica as Recomendações 01/2020 do CEPD relativas às medidas complementares aos instrumentos de transferência]: A empresa XYZ está sediada na Itália e tem filiais na Alemanha, nos Países Baixos, na Espanha e na Bélgica. Para efeitos de gestão das ferramentas informáticas utilizadas pelo grupo, a empresa XYZ utiliza os serviços de um prestador de serviços de computação em nuvem estabelecido num país terceiro sem presença na UE. Os dados tratados no âmbito da utilização de ferramentas informáticas implicam transferências de dados da empresa XYZ e das suas filiais para o prestador de serviços de computação em nuvem, para efeitos de armazenamento de dados. Uma vez que o prestador de serviços de computação em nuvem no país terceiro adotou um código de conduta a utilizar como instrumento para as transferências relacionadas com serviços de computação em nuvem aprovado nos termos do artigo 40.º, n.º 5, os fluxos de dados da empresa XYZ e das suas filiais para o prestador de serviços de computação em nuvem podem ser enquadrados pelo código de conduta que o prestador de serviços de computação em nuvem adotou. Neste caso, a utilização de um código de conduta pelo prestador de serviços de computação em nuvem, em vez de outros instrumentos de transferência, como as regras vinculativas aplicáveis às empresas, afigura-se mais adequada, uma vez que um código de conduta não exige que o responsável pelo tratamento/subcontratante que atua como importador tenha uma presença no EEE, ao passo que um grupo de empresas tem de ter uma presença no EEE para poder utilizar regras vinculativas aplicáveis às empresas. O código de conduta apresenta igualmente benefícios no tratamento de múltiplas transferências de dados através de um instrumento único, em comparação com soluções (totalmente) contratuais, como as cláusulas contratuais-tipo". UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 04/2021 relativas aos códigos de conduta enquanto instrumento para as transferências**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de. Acesso em: 15 nov. 2022.

[831] As Diretrizes n.º 4/2021 exemplificam o assunto do seguinte modo: "Exemplo n.º 2: Uma associação que representa categorias de responsáveis pelo tratamento/subcontratantes envolvidos no mesmo tipo de atividades de investigação no setor da saúde e que envolvem transferências regulares de dados para responsáveis pelo tratamento/subcontratantes de países terceiros elabora um código de conduta que também se destina a ser utilizado como instrumento para as transferências. Os responsáveis pelo tratamento/subcontratantes relevantes no EEE aderem a este código de conduta, o mesmo acontecendo com

Na medida em que é muito provável que os códigos destinados às transferências sejam utilizados pelas entidades relevantes para enquadrar as transferências a partir de mais do que um Estado-Membro e tendo em conta que esses códigos de conduta devem ser de aplicabilidade geral nos termos do artigo 40.º, n.º 9, do RGPD, eles serão, enquanto tal, considerados «códigos transnacionais», na acepção das Diretrizes 1/2019.[832]

d) Qual deve ser o conteúdo de um código de conduta enquanto instrumento para as transferências?

Tal como acima referido, um código de conduta destinado às transferências é um dos instrumentos que podem ser utilizados pelas organizações que realizam atividades específicas de tratamento de dados – por exemplo, no âmbito de um setor específico ou de uma atividade de tratamento comum que partilham as mesmas características e necessidades em matéria de tratamento – para fornecer garantias adequadas para as transferências de dados pessoais para um país terceiro, em conformidade com o artigo 46.º.

Além disso, as disposições do artigo 40.º, n.º 3, que se referem ao fato de os códigos destinados às transferências poderem ser aplicados por responsáveis pelo tratamento/subcontratantes não sujeitos ao RGPD nos termos do artigo 3.º, sugerem que os códigos destinados a transferências são, no seu todo ou em parte, mais especificamente concebidos para responsáveis pelo tratamento/subcontratantes de países terceiros. Por conseguinte, de acordo com o CEPD, o objetivo de um código destinado às transferências deve ser o de estabelecer as regras que terão de ser cumpridas pelo responsável pelo tratamento/subcontratante do país terceiro (o importador de dados) para assegurar que os dados pessoais são adequadamente protegidos (em conformidade com os requisitos do capítulo V do RGPD) quando são tratados por esse responsável/subcontratante do país terceiro (ou seja, o importador de dados).

Mais especificamente, em termos de conteúdo, a fim de fornecer garantias adequadas na acepção do artigo 46.º, devem ser abordados os seguintes elementos: a)

os responsáveis pelo tratamento/subcontratantes de países terceiros. As transferências de dados para responsáveis pelo tratamento/subcontratantes de países terceiros no âmbito das atividades de investigação podem ser enquadradas por este código de conduta.". UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 04/2021 relativas aos códigos de conduta enquanto instrumento para as transferências**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de. Acesso em: 15 nov. 2022.

[832] Os códigos transnacionais referem-se a um código que abrange as atividades de tratamento realizadas em mais do que um Estado-Membro. Ver: Anexo III — Distinção entre códigos nacionais e transnacionais.

Princípios, direitos e obrigações essenciais decorrentes do RGPD para os responsáveis pelo tratamento/subcontratantes; e b) Garantias específicas do contexto das transferências (por exemplo, no que diz respeito à questão das transferências ulteriores, conflitos de leis no país terceiro, etc.).

A este respeito, importa salientar que um código de conduta pode ser originalmente elaborado com o único propósito de especificar a aplicação do RGPD, em conformidade com o artigo 40.º, n.º 2 («código RGPD»), ou também como um código destinado às transferências, em conformidade com o artigo 40.º, n.º 3. Consequentemente, dependendo do âmbito de aplicação e do conteúdo do código originalmente especificados, pode ser necessário alterá-lo, a fim de abranger todos os elementos acima referidos, se for utilizado como instrumento para as transferências. [833]

Em qualquer caso, em consonância com os esclarecimentos prestados pelo CEPD nas suas Diretrizes 1/2019, todos os elementos que forneçam as garantias adequadas, tal como acima referido, terão de ser estabelecidos no código de modo a facilitar a sua aplicação efetiva e especificar a forma como se aplicam, na prática, à atividade de tratamento ou setor específico.

Mais à frente será fornecida uma lista de verificação dos elementos a incluir num código destinado às transferências para que possa ser considerado como fornecendo as garantias adequadas.

e) Quais são as entidades envolvidas na criação de um código a utilizar como instrumento para as transferências e qual o seu papel?

i. <u>Titular do código</u>

[833] As Diretrizes n.º 4/2021 exemplificam o assunto do seguinte modo: "Exemplo n.º 3: A associação ABC, que reúne organizações que operam no setor do marketing direto a nível da UE, adotou um código de conduta que visa especificar a aplicação do princípio da transparência e dos requisitos associados ao abrigo do RGPD como parte das atividades de tratamento para esse setor. A associação pretende utilizar este código de conduta como instrumento para enquadrar as transferências fora do EEE. Na medida em que o código de conduta se centra no princípio da transparência, ele teria de ser alterado a fim de abranger também as garantias adequadas exigidas para as transferências internacionais de dados pessoais, todos os princípios essenciais e requisitos principais decorrentes do RGPD (que não a transparência), bem como as garantias específicas do contexto das transferências, a fim de obter a aprovação desse código como um código destinado às transferências". UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 04/2021 relativas aos códigos de conduta enquanto instrumento para as transferências**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de. Acesso em: 15 nov. 2022.

O titular do código é a entidade, associação/federação ou outro organismo que irá elaborar um código de conduta destinado às transferências ou alterar um «código RGPD» aprovado para o utilizar como instrumento para as transferências e submetê-lo à aprovação da Autoridade de Controle (AC) competente.[834]

ii. Organismo de supervisão

Tal como em qualquer código de conduta, é necessário que um organismo de supervisão seja identificado no âmbito de um código destinado às transferências e acreditado pela Autoridade de Controle (AC) competente, em conformidade com o artigo 41.º. Mais precisamente, o seu papel consistirá em verificar se os responsáveis pelo tratamento/subcontratantes de países terceiros que aderiram a esse código cumprem as regras nele estabelecidas.[835]

Tendo em conta que os códigos de conduta destinados às transferências visam igualmente ou mais especificamente os responsáveis pelo tratamento/subcontratantes de países terceiros, é necessário garantir que os organismos de supervisão sejam capazes de controlar eficazmente o cumprimento do código, tal como especificado nas Diretrizes 1/2019.

Os organismos de supervisão que atuam no âmbito de códigos para as transferências podem estar localizados apenas dentro ou também fora do Espaço Económico Europeu (EEE), desde que o organismo de supervisão em questão tenha um estabelecimento no Espaço Económico Europeu (EEE). Nesse contexto, o estabelecimento do organismo de supervisão no EEE é o local onde se situa a sua sede ou o local onde são tomadas as decisões finais relativas às atividades de supervisão, exigindo igualmente que uma entidade do EEE seja capaz de controlar as entidades do organismo de supervisão fora do EEE e demonstrar plena responsabilidade por todas as decisões e ações (incluindo a sua responsabilidade por eventuais violações).

Além disso, um organismo de supervisão no EEE pode subcontratar as suas atividades a uma entidade externa fora do EEE, agindo em seu nome, desde que essa entidade mantenha as competências e conhecimentos especializados exigidos pelo código de conduta, bem como dos requisitos de acreditação, e que o organismo de supervisão do

[834] Os requisitos relativos ao titular do código já forram apresentados na discussão das Diretrizes n.º 1/2019.
[835] A necessidade de se criar um organismo de supervisão ao abrigo de um código de conduta também foi discutida na análise das Diretrizes n.º 1/2019.

EEE seja capaz de assegurar um controle efetivo dos serviços prestados pela entidade contratante e mantenha o poder de decisão sobre as atividades de supervisão. A fim de assegurar a conformidade com estes requisitos de acreditação quando o organismo de supervisão subcontrata partes das suas tarefas, deve ser celebrado um contrato ou qualquer outro ato jurídico ao abrigo do direito da União Europeia que vincule o subcontratante perante o organismo de supervisão, de modo a que todas as tarefas subcontratadas cumpram os requisitos do RGPD.

O recurso à subcontratação não resulta na delegação de responsabilidades: em qualquer caso, o organismo de supervisão continua a ser responsável pelo controle do cumprimento do código de conduta perante a Autoridade de Controle competente. O organismo de supervisão assegura que todos os subcontratantes cumprem os requisitos estabelecidos neste documento relativo aos requisitos de acreditação, mormente no que diz respeito à independência, às competências e à ausência de conflitos de interesses. O organismo de supervisão inclui uma cláusula específica no contrato assinado com os subcontratantes, a fim de assegurar a confidencialidade dos dados pessoais que possam, se for caso disso, ser divulgados ao subcontratante durante as tarefas de controle e estabelecerá garantias adequadas em caso de transferência desses dados pessoais para os seus subcontratantes.

iii. Autoridades de Controle

Em conformidade com o artigo 40.º, n.º 5, o papel da Autoridade de Controle competente consistirá em aprovar o projeto de código de conduta destinado às transferências ou as alterações a ele referentes para a sua utilização enquanto instrumento para as transferências, bem como acreditar o organismo de supervisão identificado no âmbito do código no que concerne a requisitos de acreditação adicionais relativos a códigos de conduta para as transferências

iv. Comitê Europeu para a Proteção de Dados (CEDP)

Em conformidade com o artigo 40.º, n.º 7, e o artigo 64.º, n.º 1, alínea b), o CEPD será convidado a emitir um parecer sobre o projeto de decisão de uma AC (Autoridade de Controle) que visa aprovar um código destinado às transferências ou a alteração de um

código de conduta para a sua utilização também como instrumento para as transferências.[836]

v. Comissão Europeia

Tal como previsto no artigo 40.º, n.º 9, a Comissão pode decidir, mediante a adoção de um ato de execução, que um código destinado às transferências e aprovado por uma Autoridade de Controle tem aplicabilidade geral na União. Só os códigos a que tenha sido concedida aplicabilidade geral na União podem ser invocados para enquadrar as transferências, segundo as Diretrizes em comento.

f) Processo de adoção de um código de conduta para as transferências

Resulta do artigo 40.º, n.º 5, e do artigo 40.º, n.º 9, que, para ser adotado, um código destinado às transferências deve primeiro ser aprovado por uma Autoridade de Controle competente no Espaço Econômico Europeu e, em seguida, ser reconhecido pela Comissão Europeia como sendo de aplicabilidade geral na União através de um ato de execução.

Tal como referido supra, na medida em que é muito provável que os códigos destinados às transferências sejam utilizados pelos responsáveis pelo tratamento/subcontratantes para enquadrar as transferências a partir de mais do que um Estado-Membro, os códigos serão considerados «códigos transnacionais» e devem seguir o procedimento de aprovação dos códigos transnacionais, incluindo a necessidade de um parecer do Comitê Europeu para a Proteção de Dados (CEDP), tal como especificado nas Diretrizes n.º 1/2019.

Na prática, podem surgir diferentes cenários quando uma associação/federação ou outro organismo pretende adotar um código de conduta para as transferências, como:

- Um projeto de código é concebido como um «código RGPD» e destina-se a ser utilizado como instrumento de transferência por parte de responsáveis pelo tratamento/subcontratantes de países terceiros. Esse projeto de código terá primeiro de

[836] Ver Documento do CEPD relativo ao procedimento para o desenvolvimento de sessões informais sobre Códigos de Conduta. UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Documento do CEPD relativo ao procedimento para o desenvolvimento de sessões informais sobre Códigos de Conduta**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_documentprocedurecodesconductsessions_pt.pdf. Acesso em: 17 nov. 2022.

ser aprovado pela Autoridade de Controle competente de acordo com o procedimento aplicável aos códigos transnacionais, que prevê a emissão de um parecer do Comitê, e, em seguida, que seja reconhecido pela Comissão como sendo de aplicabilidade geral na União Europeia, em conformidade com o artigo 40.º, n.º 9. Após a conclusão destas etapas, os responsáveis pelo tratamento/subcontratantes em países terceiros podem aderir ao código e este pode ser utilizado para fornecer garantias adequadas para as transferências de dados para países terceiros.

- Um código de conduta é inicialmente concebido e aprovado como «código RGPD». Este código é depois alargado com vista a ser também utilizado como instrumento de transferência por parte de responsáveis pelo tratamento/subcontratantes de países terceiros. A alteração do código relativo às transferências terá de ser submetida à aprovação da Autoridade de Controle competente, que seguirá o procedimento aplicável aos códigos transnacionais que prevê a emissão de um parecer do Comitê. O código alterado terá então de ser reconhecido pela Comissão como sendo de aplicabilidade geral na União, em conformidade com o artigo 40.º, n.º 9, após o que os responsáveis pelo tratamento/subcontratantes num país terceiro podem aderir a esse código e utilizá-lo para fornecer garantias adequadas para as transferências de dados pessoais para países terceiros.

Um fluxograma incluído no Anexo VII especifica as etapas processuais para a adoção de um código de conduta destinado às transferências, tendo em conta os cenários possíveis acima referidos.

g) Quais são as garantias a fornecer ao abrigo do código?

i. <u>Compromissos vinculativos e com força executiva a assumir</u>

O RGPD exige, no seu artigo 40.º, n.º 3, que os responsáveis pelo tratamento e os subcontratantes não sujeitos ao Regime Geral de Proteção de Dados Pessoais que adiram a um código destinado às transferências assumam compromissos vinculativos e com força executiva, através de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias adequadas previstas no código, incluindo, em especial, o que diz respeito aos direitos dos titulares dos dados.

Tal como especificado no RGPD, esses compromissos podem ser assumidos através de um contrato, o que, na visão do Comitê, expresso nas diretrizes n.º 4/2021

parece ser a solução mais simples. Poderão também ser utilizados outros instrumentos, desde que esses responsáveis pelo tratamento/subcontratantes que adiram ao código consigam demonstrar o caráter vinculativo e executório desses outros meios.

Em qualquer caso, o instrumento deve ter uma natureza vinculativa e executória em conformidade com o direito da União Europeia e deve também ser vinculativo e oponível pelos titulares dos dados enquanto terceiros beneficiários.

Um código de conduta utilizado como instrumento de transferência pode ter membros situados no Espaço Econômico Europeu (EEE), bem como membros situados fora do EEE. Uma distinção entre os membros do código situados no EEE e os membros do código situados fora do EEE é a aplicação direta do RGPD aos primeiros, mas não aos segundos (desde que estes últimos não sejam abrangidos pelo artigo 3.º, n.º 2, do RGPD).

No que diz respeito aos membros do código situados fora do Espaço Econômico Europeu, é necessário assegurar que o seu compromisso de observar um «nível específico de proteção de dados» garanta que o nível de proteção de dados previsto no RGPD não seja comprometido. Trata-se de um pré-requisito da sua elegibilidade para participar no código de conduta enquanto instrumento de transferência.

Para o efeito, pode ser assinado um contrato pelo responsável pelo tratamento/subcontratante no país terceiro (ou seja, o importador de dados) com, por exemplo, a entidade que transfere os dados ao abrigo do código (ou seja, o exportador de dados). Na prática, é possível recorrer a um contrato existente (por exemplo, um acordo de serviços entre o exportador e o importador de dados ou o contrato a celebrar em conformidade com o artigo 28.º do RGPD no caso de subcontratantes importadores), no qual poderiam ser incluídos os compromissos vinculativos e com força executiva.

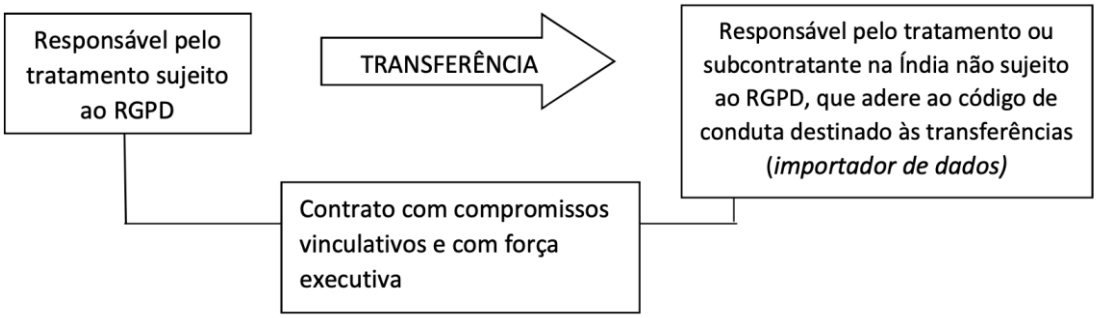
Outra opção seria recorrer a um contrato separado, incluindo no código destinado às transferências um modelo de contrato que teria de ser assinado, por exemplo, pelos responsáveis pelo tratamento/subcontratantes no país terceiro e por todos os seus exportadores de dados.

Deve haver flexibilidade para escolher a opção mais adequada em função da situação específica.

Caso o código de conduta se destine a ser utilizado para transferências e transferências ulteriores de um subcontratante para subcontratantes ulteriores, deve também ser feita referência ao código de conduta e ao instrumento que prevê compromissos vinculativos e com força executiva no acordo de subcontratação assinado

entre o subcontratante e o seu responsável pelo tratamento, sempre que possível. Por exemplo:

Figura 7 - Compromissos vinculativos e com força executiva assumidos pelo importador de dados (exemplo)



Fonte: UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 04/2021 relativas aos códigos de conduta enquanto instrumento para as transferências**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de. Acesso em: 15 nov. 2022.

Em geral, o contrato ou outro instrumento deve estabelecer que o responsável pelo tratamento/subcontratante se compromete a cumprir as regras especificadas no código destinado às transferências aquando do tratamento dos dados recebidos ao abrigo do código.

O contrato ou outro instrumento deve também prever mecanismos que permitam exigir o cumprimento desses compromissos em caso de violação pelo responsável pelo tratamento/subcontratante, em especial no que diz respeito aos direitos dos titulares cujos dados serão transferidos ao abrigo do código.

Mais especificamente, o contrato ou outro instrumento deve abordar:

- A existência dos direitos dos titulares dos dados transferidos ao abrigo do código de exigir o cumprimento das regras estabelecidas no código enquanto terceiros beneficiários;

- A questão da responsabilidade em caso de violação das regras do código por um membro do código fora do Espaço Econômico Europeu. O código deve incluir uma cláusula atributiva de jurisdição que indique que os titulares dos dados têm a possibilidade de, em caso de violação das regras do código por um membro do código fora do EEE, instaurar uma ação, incluindo uma ação de indenização, contra essa entidade junto de uma

Autoridade de Controle do Espaço Econômico Europeu e de um tribunal do Espaço Econômico Europeu da residência habitual do titular dos dados, invocando o seu direito de terceiro beneficiário.

O membro do código fora do EEE deve aceitar a decisão do titular dos dados de assim proceder. Os titulares dos dados têm também a possibilidade de instaurar uma ação, decorrente ou resultante do cumprimento pelo importador do código de conduta, contra o exportador de dados junto da AC (Autoridade de Controle) ou do tribunal competente do local de estabelecimento do exportador de dados ou da residência habitual do titular dos dados. Essa responsabilidade não deve prejudicar os mecanismos de acionamento, com fundamento no código, do organismo de supervisão, que também pode tomar medidas contra os responsáveis pelo tratamento/subcontratantes em conformidade com o código, impondo medidas corretivas.

O importador de dados e o exportador de dados devem, ainda, aceitar que o titular dos dados possa ser representado por um organismo, organização ou associação sem fins lucrativos, nas condições estabelecidas no artigo 80.º, n.º 1, do RGPD.

- A existência de um direito do exportador de exigir o cumprimento, pelo membro do código que atua como importador, das regras estabelecidas no código na qualidade de terceiro beneficiário.

- A existência de uma obrigação do importador de notificar o exportador de dados e a autoridade de controle do exportador de dados sobre qualquer violação detectada do código pelo mesmo membro do código que atua como importador fora do EEE, bem como sobre quaisquer medidas corretivas tomadas pelo organismo de supervisão em resposta a essa violação.

ii. <u>Lista de verificação dos elementos a incluir num código de conduta destinado às transferências</u>

À luz das garantias fornecidas pelos instrumentos de transferência existentes, com fundamento no artigo 46.º do RGPD (como as regras vinculativas aplicáveis às empresas), e para assegurar a coerência do nível de proteção, bem como em vista do Acórdão Schrems II[837] do TJUE, o Comitê Europeu para a Proteção de Dados (CEDP) considera que, para serem considerados como fornecendo as garantias adequadas, os

[837] Acórdão do Tribunal de Justiça (Grande Secção) de 16 de julho de 2020, Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems.

elementos a abranger num código de conduta destinado às transferências devem incluir o seguinte:

- A descrição das transferências a serem abrangidas pelo código (natureza dos dados transferidos, categorias de titulares dos dados, países etc.);

- A descrição dos princípios de proteção de dados a serem respeitados nos termos do código (transparência, lealdade e licitude, limitação das finalidades, minimização e exatidão dos dados, limitação da conservação dos dados, tratamento de dados sensíveis, segurança, cumprimento pelos subcontratantes das instruções do responsável pelo tratamento etc.), incluindo regras sobre a utilização de subcontratantes ou subcontratantes ulteriores e regras sobre transferências posteriores;

- As medidas de aplicação do princípio da responsabilização a serem adotadas nos termos do código;

- A criação de uma governança adequada através dos encarregados da proteção de dados ou de outro pessoal responsável pelo cumprimento das obrigações de proteção de dados decorrentes do código;

- A existência de um programa de formação adequado sobre as obrigações decorrentes do código;

- A existência de uma auditoria sobre a proteção de dados (realizada por auditores internos ou externos) ou de outro mecanismo interno para controlar o cumprimento do código, independentemente da fiscalização a ser feita pelo organismo de supervisão, tal como em qualquer código de conduta – considerando que o objetivo do programa de auditoria em matéria de proteção de dados é assegurar e demonstrar a conformidade com o código, o objetivo das auditorias realizadas pelo organismo de supervisão é avaliar se o candidato é elegível para participar do código, se continua a ser elegível após se tornar membro e se são necessárias sanções em caso de infração;

- As medidas de transparência, incluindo um acesso fácil, em matéria de utilização do código, em especial no que se refere aos direitos de terceiros beneficiários;

- A atribuição ao titular dos dados dos direitos de acesso, retificação, eliminação, limitação do tratamento, notificação da retificação, apagamento ou limitação do tratamento, oposição ao tratamento, bem como do direito de não ficar sujeito a decisões baseadas exclusivamente no tratamento automatizado, incluindo a definição de perfis, tal como previsto nos artigos 12.º, 13.º, 14.º, 15.º, 16.º, 17.º, 18.º, 19.º, 21.º e 22.º do RGPD;

- A criação de direitos de terceiros beneficiários para que os titulares dos dados possam exigir o cumprimento das regras do código enquanto terceiros beneficiários (bem

como a possibilidade de apresentar uma reclamação junto à Autoridade de Controle competente e aos tribunais do EEE);

- A existência de um processo adequado de tratamento das reclamações relativas a infrações às regras de proteção de dados gerido pelo organismo de supervisão, que, se for considerado adequado, pode ser complementado com um procedimento interno de gestão de reclamações para os membros do código;

- A garantia de que, no momento da adesão ao código, o responsável pelo tratamento/subcontratante do país terceiro não tem motivos para crer que a legislação aplicável ao tratamento de dados pessoais no país terceiro de transferência o impede de cumprir as suas obrigações ao abrigo do código e de aplicar, se necessário, em conjunto com o exportador, medidas complementares[838] para assegurar o nível de proteção exigido ao abrigo do direito do Espaço Econômico Europeu.[839] Além disso, a descrição das medidas a serem adotadas (incluindo a notificação ao exportador no EEE e a aplicação de medidas complementares adequadas) caso, após ter aderido ao código, o responsável pelo tratamento/subcontratante do país terceiro tome conhecimento de qualquer legislação do país terceiro que impeça o cumprimento, por parte do membro do código, dos compromissos assumidos no âmbito do código e das medidas a serem tomadas em caso de pedidos de acesso pelos governos de países terceiros;

- Os mecanismos que tratam das alterações do código;

- As consequências da exclusão de um membro do código;

- O compromisso de que o membro do código e o organismo de supervisão cooperarão com as Autoridades de Controle do Espaço Econômico Europeu;

- O compromisso de que o membro do código aceita estar sujeito à jurisdição das Autoridades de Controle do Espaço Econômico Europeu, em qualquer procedimento destinado a assegurar o cumprimento do código de conduta, e dos tribunais do Espaço Econômico Europeu;

---

[838] O Comitê Europeu para a Proteção de Dados publicou uma recomendação sobre medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE, que podem contribuir para a avaliação do país terceiro e para a identificação de medidas complementares adequadas. UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE**. Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_pt.pdf. Acesso em: 19 nov. 2022.

[839] Isso baseia-se no pressuposto de que as legislações e as práticas que respeitam a essência dos direitos e das liberdades fundamentais e não excedem o necessário e proporcional numa sociedade democrática para salvaguardar um dos objetivos enumerados no artigo 23.º, n.º 1, do Regulamento (UE) 2016/679 e não estão em contradição com as garantias especificadas no código de conduta destinado às transferências.

- Os critérios de seleção do organismo de supervisão para um código destinado às transferências, ou seja, para demonstrar que o organismo de supervisão possui o nível de competências necessário para desempenhar o seu papel de forma eficaz.

De qualquer modo, deve-se notar que estes elementos constituem garantias mínimas que podem ter de ser complementadas por compromissos e medidas adicionais, em função da transferência em causa ao abrigo do código de conduta.

O Comitê Europeu para a Proteção de Dados avaliará o funcionamento das presentes diretrizes à luz da experiência adquirida com a sua aplicação na prática e fornecerá orientações adicionais para clarificar a aplicação dos elementos acima enumerados.

3.1.2. Os Códigos de Conduta na Lei Geral de Proteção de Dados Pessoais

A legislação brasileira relativa aos Códigos de Conduta, diferentemente da europeia, apenas prevê linhas gerais sobre a possibilidade de utilização do instrumento com duas finalidades: a) prestar garantias adequadas para as transferências internacionais de dados (artigo 33, II, "d"); e, b) como forma de demonstrar a efetividade do programa de governança em privacidade formulado por controladores e operadores (artigo 50, §2º, inciso II).

Essas diretrizes, entretanto, são muito genéricas e não permitem identificar com exatidão o procedimento a ser seguido para a formulação, aplicação, aprovação e monitoramento desses instrumentos.

Veja-se o que dispõe a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709, de 14 de agosto de 2018):[840]

> CAPÍTULO V
> DA TRANSFERÊNCIA INTERNACIONAL DE DADOS
> **Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:**
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
> **II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:**
> a) cláusulas contratuais específicas para determinada transferência;

[840] BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 nov. 2022.

b) cláusulas-padrão contratuais;
c) normas corporativas globais;
d) selos, certificados e códigos de conduta regularmente emitidos;
III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
V - quando a autoridade nacional autorizar a transferência;
VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do *caput* do art. 23 desta Lei;
VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.
Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do *caput* do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:
I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
II - a natureza dos dados;
III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
IV - a adoção de medidas de segurança previstas em regulamento;
V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
VI - outras circunstâncias específicas relativas à transferência.

Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do *caput* do art. 33 desta Lei, será realizada pela autoridade nacional.
§ 1º Para a verificação do disposto no *caput* deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.
§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas

diligências de verificação quanto às operações de tratamento, quando necessário.
§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no *caput* deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.
§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.
§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no *caput* deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

Seção II
Das Boas Práticas e da Governança
Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
I - implementar programa de governança em privacidade que, no mínimo:
a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
> **II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.**
> § 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.
>
> Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.
> (Sem grifos no original)

Como se vê, em um primeiro momento, a utilização dos Códigos de Conduta como instrumento de garantia adequado para transferências internacionais, parece se assemelhar ao seu congênere europeu, de modo que, nos termos do artigo 33, II,” d”, ele deverá ser “regularmente aprovado”, a partir de conteúdos mínimos a serem regulamentados pela Autoridade de Controle nacional (artigo 35).

Assim, embora enxuta a disposição, parece que o instituto se assemelha à sua origem europeia. Entretanto, o regulamento a que faz referência ainda não foi aprovado, impossibilitando uma comparação direta sobre o tratamento que lhe será dado pela nossa Autoridade.

Ainda assim, tal qual o modelo europeu, as regras impostas pela legislação nacional deixam clara a existência de uma espécie de corregulação, em que atores públicos e privados dialogarão na construção de uma solução jurídica, técnica e social, além de economicamente adequada, levando em conta diferentes realidades e disponibilidade de informações.

De outro lado, a utilização dos códigos de conduta como instrumento de aplicação da Lei Geral de Proteção de Dados Pessoais, parece ter se distanciado, em muito, de seu correlato europeu.

Isso porque, a legislação brasileira parece ter incluído os Códigos de Conduta relativos à aplicação da própria Lei Geral de Proteção de Dados como instrumento de governança, na categoria de instrumentos de autorregulação, voluntários e sem a participação do Estado, no momento de sua construção. Ao que se extrai da legislação esse instrumento diria respeito unicamente a um modelo de governança empresarial, sem

vinculatividade e descolado de parâmetros de verificação por parte da Autoridade de Controle nacional.

Nesse sentido, cabe uma breve discussão sobre o termo governança, recorrendo-nos às lições de Aranha[841] para aclará-lo:

> Tanto governo (*government*), quanto governança (*governance*) bebem do latim *gubernare*, de dirigir ou pilotar, enquanto regulação (*regulation*) remonta ao latim *regere* ou *regulare*, de guiar ou manter em linha reta.
> Não é incomum o uso do termo governança para se descrever a administração governamental sobre a vida empresarial. A literatura sobre governança, contudo, tem envidado esforços em delimitar a fronteira entre governança empresarial e regulação estatal ao utilizar os termos regulação governamental e governança empresarial como dois polos de um mesmo fenômeno, em que a administração estatal da atividade empresarial – regulação governamental – convive com a operacionalização da atividade empresarial pela própria empresa – governança empresarial.
> De um lado, o Estado administra as leis produzindo normas regulamentares em geral (*government regulations*), opta pelo Estado Regulador, ao privilegiar a administração apoiada em regras (*rule-based governance*), ao invés de se resumir a funções macroeconômicas de tributação ou redistributivas de gastos públicos e, finalmente, implementa modelos de governo regulatório (*regulatory government*), também chamados de regulação no governo (*regulation inside government*), ou, ainda, privilegia modelos de regulação predominantemente descentralizada e apoiada em comunidades normativas presentes no ambiente regulado via governança regulatória (*regulatory governance*).
> De outro lado, tem-se a empresa, seja ela estatal ou não, organizando processos, sistemas e controles segundo orientações de governança empresarial (*corporate governance*), com objetivos diversos, entre eles, o de satisfazer as expectativas de investidores internacionais, o de pura eficiência econômica às expensas de considerações éticas ou o de sistemático diálogo entre ética e objetivos empresariais de mercado. **Ambos os polos de governo e governança participam da vida da empresa sob enfoques distintos: o enfoque governamental de administração extrínseca da vida empresarial, seja por normas gestadas no seio estatal ou garimpadas em normas do modelo de negócios regulados; e o enfoque empresarial de operacionalização intrínseca de sua própria vivência.**
> Governança regulatória e governança empresarial são, portanto, termos que representam momentos distintos de afirmação da governança como método de governo de organizações empresariais mediante técnicas regulatórias apoiadas na participação do regulado para alcance do interesse público – governança regulatória – ou de organização de processos, sistemas e controles movidos pelo interesse empresarial – governança empresarial.

[841] ARANHA, Márcio Iorio. ***Compliance*, governança e regulação**. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 437-452, p. 438-439.

> O significado da governança regulatória é variável, mas sua característica fundamental está na necessidade de que os próprios afetados por um tipo de regulação apoiada em variáveis situadas fora das normas jurídicas (*non-legal variables*), presentes em comunidades normativas para além do Estado, exercitem, em maior grau, habilidades colaborativas e assumam a responsabilidade por seus atos, configurando o modelo de governança regulatória descentralizada (*decentred regulatory governance*).
> Há quem defenda, por exemplo, que a governança regulatória seria uma característica diferencial do Estado Regulador, quando este opta por abordagens regulatórias apoiadas em outros sistemas normativos que não somente o estatal, o que justificaria falar de uma governança regulatória em vários níveis (*multi-level governance*). Como consequência, ao se defender a governança regulatória, estar-se-ia, de pronto, firmando oposição a estilos regulatórios de comando-e-controle.

Nota-se que a atividade regulatória está dentro do espectro da governança, o que não significa que esta última possa ter sua complexidade reduzida à primeira. A atividade de governança costuma ser mais abrangente, envolvendo todo tipo de estrutura de desenvolvimento, coordenação e influência de comportamentos,[842] seja intencional ou não, coordenada ou não.

Zanatta[843] chega a pontar para a necessidade de enxergar a proteção de dados pessoais no Brasil sob uma perspectiva mais ampla, a partir de uma "caixa de ferramentas de governança" que inclui (i) regulação estatal (leis, agências, autoridades administrativas), (ii) instrumentos de autorregulação (códigos técnicos, códigos de conduta, certificação), (iii) normas internacionais (acordos bilaterais e multilaterais), e (iv) tecnologia (criptografia, *privacy by design*, programação).

Assim, percebe-se que o termo governança é muito mais abrangente, abarcando modelos de autorregulação, corregulação, acordos, diretrizes, intenções etc.

No entanto, tanto no primeiro capítulo, como neste expusemos as diversas falhas que envolvem a ausência de participação do Estado em modelos produtivos e de negócios. O recrudescimento da participação dessa espécie de regulação, com frequência, levou a quadros de exploração humana, visto como insumo nos processos produtivos, inclusive o digital.

---

[842] HOFMANN, Jeanette; KATZENBACH, Christian; GOLLATZ, Kirsten. Between Coordination and Regulation: Finding the Governance in Internet Governance. **New Media & Society**. set. 2016. Disponível em: https://ssrn.com/abstract=2836068. Acesso em: 18 nov. 2022.

[843] ZANATTA, Rafael. **A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet**. Disponível em: https://www.researchgate.net/publication/322581135_A_protecao_de_dados_pessoais_entre_leis_codigos_e_programacao_os_limites_do_Marco_Civil_da_Internet. Acesso em: 22 nov. 2022.

Embora o modelo estatal também apresente diversas falhas, expostas na terceira parte do trabalho, não nos parece acertada uma política de proteção de dados pessoais que se mostre mais dura externamente (com a aprovação de seu conteúdo pela Autoridade Nacional), enquanto o mesmo não é exigido quando se trata de operações de tratamento de dados pessoais internas.

Esse tipo de política parece remontar à velha tradição tupiniquim de, num cenário internacional, aparentar conformidade, adotando, todavia, no âmbito doméstico, uma postura muito mais elástica e desprovida de reais garantias de concretização.[844]

Aqui ocorre o mesmo. Enquanto às transferências internacionais os requisitos de conformidade são avaliados pela Autoridade que os aplicará e monitorará, nas tarefas de tratamento internas, bastará um compromisso de intenções, desprovido do *enforcement* necessário para sua aplicação.

Assim, embora não esteja claro pela vagueza legislativa, ao que tudo indica, os códigos de conduta fundados no artigo 50 da LGPD não seriam, de fato, um instrumento híbrido ou dialógico (com participação público-privada), mas um instrumento puramente autorregulatório, ao qual a Autoridade de Controle, apenas dará publicidade, se assim entender pertinente.

Outro critério que também não resta claro diz respeito à diferença entre os códigos de conduta e os códigos de boas práticas (se é que ela existe).

Tanto é assim que o primeiro instrumento nacional desse tipo, utiliza os dois conceitos de forma intercambiável,[845] intitulando o documento produzido de "Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde", para mais à frente afirmar que:

> **Trata-se, portanto**, **de verdadeiro marco de governança e boas práticas, visto que o texto se apresenta como o primeiro Código de Conduta dos Prestadores do Serviço de Saúde para atendimento à LGPD**. A iniciativa, além de orientar quanto às condutas a serem praticadas por hospitais e laboratórios privados, visa incentivar a

[844] Veja-se por exemplo o termo "pra inglês ver". Essa famosa expressão, que tem como significado fingir que fez algo ou fazer malfeito, surgiu na primeira metade do século 19, quando a Inglaterra, por interesses econômicos, tentou abolir a escravidão no mundo, pressionando países, como o Brasil, que tinha nos escravos a base de sua economia, a fazerem o mesmo. No entanto, para ludibriar a potência internacional, o Império brasileiro colocava navios no litoral com a suposta missão de ir atrás das naus negreiras, entretanto, na prática, nada era feito. Tratava-se de mera encenação "para inglês ver".

[845] CNSAÚDE. Confederação Nacional de Saúde. **Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde**. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 10 nov. 2022.

> inovação com responsabilidade e consolidar a confiança dos titulares de dados no setor de saúde. (Sem grifos no original).

A iniciativa, embora extremamente louvável, carecia de um arcabouço normativo nacional que pudesse melhor orientá-la. Em análise sobre a inciativa, Diogo Luís Manganelli de Oliveira aponta que:

> Embora seja extremamente louvável a elaboração do respectivo documento, tendo em vista a insegurança jurídica de determinadas estipulações da LGPD quando da sua aplicação na rotina do setor de saúde de maneira geral no país, é necessário, contudo, que se compreenda de maneira mais adequada e pormenorizada qual a função de códigos de conduta com relação [à] aplicação da legislação. Desta forma, questiona-se qual o seu real papel no tratamento de dados pessoais pelo setor, ou seja, se possuirá caráter vinculativo às entidades de saúde de todo ou país ou se, apenas, deve ser interpretado como "melhores práticas", sem que exista uma imposição taxativa para tanto.
> Código de condutas são documentos que podem ser elaborados por inúmeros setores para regulamentar determinadas práticas tidas como adequadas às intuições que os compõem. Especificamente com relação ao tratamento de dados pessoais, a experiência internacional é salutar neste sentido, encorajando os representantes dos mais diversos ramos da atividade econômico a desenvolvê-los.
> No Reino Unido, a autoridade daquele país ("ICO") destaca a importância [d]e tais documentos para a garantia do cumprimento das normas do Regulamento Geral de Proteção de Dados europeu ("GDPR"), colocando-se à disposição, inclusive, para auxiliar em sua elaboração. Estabelece também que tais construções devem aprovadas pela referida Autoridade no sentido de se garantir que as exigências ali contidas representam, minimamente, o exigido pela legislação. Além disso, enfatiza que tais documentos devem dispor de orientações específicas acerca de como será realizado o monitoramento referente ao seu cumprimento, bem como as medidas aplicáveis em casos de eventuais violações.
> Na mesma linha, seguem também as orientações das autoridades irlandesa e francesa de proteção de dados que, além de ressaltar a importância de tais documentos, pontuam a necessidade de sua aprovação pelo respectivo órgão antes de sua publicização e abertura para assinaturas pelos participantes.
> Diferente do GDPR, que definiu, de maneira expressa em seu artigo 40, 4 e 5, tais obrigações de monitoramento acerca do cumprimento dos códigos por seus integrantes, bem como a necessidade de sua aprovação prévia pela respectiva autoridade nacional, caminhou de maneira distinta o legislador brasileiro. Sem fazer juízo de valor se melhor ou pior que o modelo europeu, a LGPD, ao mencionar a possibilidade de criação de tais códigos no país, não estipulou qualquer exigência [quanto] ao seu conteúdo, [necessidade] de aprovação, monitoramento, taxatividade e penalização pelo seu descumprimento.

Não obstante esse tipo de inciativa deva ser estimulada, é necessário que se estabeleça um procedimento minimamente eficaz, com garantias de que as normas contidas nos códigos de conduta apresentem um conteúdo minimante em conformidade com as orientações da Autoridade Nacional de Proteção de Dados, contando com um sistema de supervisão e monitoramento. Bem assim, que esse sistema seja coerente interna e internacionalmente, evitando que os requisitos de conformidade interna se deem em um nível muito inferior ao externo, como se verificará, caso não sobrevenha um quadro legislativo novo.

Vale ressaltar, em arremate, que os códigos de conduta (como instrumentos de corregulação) são o cerne (o coração) do modelo de regulação que propomos, pois representam um verdadeiro instrumento conciliatório dos interesses empresariais e da proteção dos direitos fundamentais em jogo.

Assim, os instrumentos de governança empresarial, como códigos de boas práticas – os quais defendemos sejam interpretados como instrumentos próprios, apartados dos códigos de conduta, eis que de matiz aurorregulatória – ainda que relevantes, não substituem o modelo de regulação híbrida, porquanto privam o titular de dados de garantias mínimas de sua efetividade.

Por essa razão defendemos um tratamento diverso às duas espécies: os códigos de conduta e os códigos de boas práticas, sob pena de atingirmos um nível de proteção muito menor em nossas operações internas do que aquele supostamente assegurado internacionalmente.

3.2. Mecanismos de certificação, selos e marcas de proteção de dados

O segundo e terceiro mecanismos a serem estudados dizem respeito às certificações e aos selos e marcas de proteção de dados. Embora mecanismos distintivos, serão tratados na mesma seção em razão de sua interdependência. Aliás, como proposto, o modelo regulatório em debate (SDR) necessita de uma análise coerente e integrada entre seus diversos mecanismos.

Assim, abordaremos os dois mecanismos na mesma seção, com uma subdivisão interna que permita se aprofundar em relação a cada um.

3.2.1. Mecanismos de Certificação, selos e marcas de proteção de dados, segundo as Diretrizes n.º 1/2018 do Comitê Europeu para a Proteção de Dados[846]

a) Introdução

O Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679, «o RGPD» ou «o regulamento») previu um quadro modernizado, de responsabilização e de respeito aos direitos fundamentais para a proteção de dados na Europa. Um conjunto de medidas que facilitam o cumprimento das disposições do RGPD são fundamentais para este novo quadro. Entre elas incluem-se requisitos obrigatórios em circunstâncias específicas (incluindo a nomeação de responsáveis pela proteção de dados e a realização de avaliações de impacto sobre a proteção de dados) e medidas voluntárias, como códigos de conduta e procedimentos de certificação.[847]

Antes da adoção do RGPD, o Grupo de Trabalho do artigo 29.º concluiu que a certificação poderia desempenhar um papel importante no quadro de responsabilidade em matéria de proteção de dados.[848] Para que a certificação possa fornecer provas fiáveis da conformidade em matéria de proteção de dados, devem ser estabelecidas regras claras que estabeleçam requisitos para a concessão da certificação.[849] O artigo 42.º do RGPD constitui a base jurídica para a elaboração dessas regras.

O artigo 42.º, n.º 1, do RGPD dispõe que: [850]

> Os Estados-Membros, as autoridades de controle, o Comité e a Comissão promovem, em especial ao nível da União, a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente regulamento. Serão tidas

[846] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022. A análise que se seguirá terá por base as citadas diretrizes.
[847] Tal como as orientações n.º 1/2018, designaremos coletivamente os procedimentos de certificação e os selos e marcas de proteção de dados como «procedimentos de certificação».
[848] Grupo de Trabalho do artigo 29.º, Parecer 3/2010 sobre o princípio da responsabilidade, WP173, 13 de julho de 2010, pontos 69-71.
[849] Parecer do Grupo de Trabalho do artigo 29.º n.º 3/2010 sobre o princípio da responsabilidade (WP173), ponto 69.
[850] UE. União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial** L 119/1, 04 de maio de 2016.

> em conta as necessidades específicas das micro, pequenas e médias empresas.

Os procedimentos de certificação podem melhorar a transparência face aos titulares dos dados, mas também nas relações entre empresas, por exemplo entre responsáveis pelo tratamento e subcontratantes. O considerando 100 do RGPD estabelece que a criação de procedimentos de certificação pode reforçar a transparência e o cumprimento do regulamento e permitir que os titulares dos dados avaliem o nível de proteção de dados proporcionado pelos produtos e serviços em questão.[851]

O RGPD não introduz um direito ou uma obrigação de certificação para os responsáveis pelo tratamento e subcontratantes; nos termos do artigo 42.º, n.º 3, a certificação é um processo voluntário para ajudar a demonstrar a conformidade com o RGPD. Os Estados-Membros e as Autoridades de Controle são convidados a incentivar a criação de procedimentos de certificação e determinarão a participação das partes interessadas no processo de certificação e em seu ciclo de vida.

Além disso, a adesão ou não a procedimentos de certificação aprovados é um fator que as autoridades de supervisão têm de considerar como um fator agravante ou atenuante ao decidir sobre a aplicação de uma multa e ao decidir sobre o montante desta (artigo 83.º, n.º 2, alínea j)).[852]

b) Disclaimer

O principal objetivo destas seções é identificar os requisitos e critérios gerais que possam ser relevantes para todos os tipos de procedimentos de certificação aprovados em conformidade com os artigos 42.º e 43.º do RGPD.

Para o efeito, as informações desta seção, compiladas a partir das Diretrizes n.º 1/2018 do Comitê Europeu para a Proteção de Dados[853] buscam:

---

[851] O considerando 100 estabelece que a criação de procedimentos de certificação deverá ser encorajada a fim de «reforçar a transparência e o cumprimento do [...] regulamento, [para permitir] aos titulares avaliar rapidamente o nível de proteção de dados proporcionado pelos produtos e serviços em causa».

[852] Ver Grupo de Trabalho do artigo 29.º, Diretrizes de aplicação e fixação de multas para efeitos do Regulamento (UE) 2016/679 (WP 253). UE. União Europeia. Comissão Europeia. **Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253/17)**. Disponível em: https://ec.europa.eu/newsroom/article29/items/611237/en. Acesso em: 19 nov. 2022.

[853] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em:

- examinar a fundamentação da certificação como instrumento de responsabilização;

- explicar os conceitos fundamentais das disposições de certificação constantes dos artigos 42.º e 43.º;

- esclarecer o âmbito daquilo que pode ser certificado nos termos dos artigos 42.º e 43.º e o objetivo da certificação;

- contribuir para que o resultado da certificação seja relevante, inequívoco, tão reprodutível quanto possível e comparável, independentemente do certificador (comparabilidade.)

O RGPD prevê várias formas de os Estados-Membros e as Autoridades de Controle aplicarem os artigos 42.º e 43.º. As orientações fornecem conselhos sobre a interpretação e a aplicação das disposições dos artigos 42.º e 43.º e ajudarão os Estados-Membros, as Autoridades de Controle e os organismos nacionais de acreditação a estabelecer uma abordagem mais coerente e harmonizada para a aplicação dos procedimentos de certificação, em conformidade com o RGPD.

As orientações reproduzidos a partir das Diretrizes n.º 1/2018 do Comitê Europeu para a Proteção de Dados[854] serão pertinentes para: a) as Autoridades de Controle competentes e o Comitê Europeu para a Proteção de Dados («o CEPD»), aquando da aprovação dos critérios de certificação nos termos do artigo 42.º, n.º 5, do artigo 58.º, n.º 3, alínea f), e do artigo 70.º, n.º 1, alínea o); b) os organismos de certificação, na elaboração e revisão dos critérios de certificação antes da apresentação à autoridade de controle competente para aprovação, em conformidade com o artigo 42.º, n.º 5; c) o CEPD, ao aprovar um selo europeu de proteção de dados, nos termos do artigo 42.º, n.º 5, e do artigo 70.º, n.º 1, alínea o); d) as Autoridades de Controle, na elaboração dos seus próprios critérios de certificação; e) a Comissão Europeia, que está habilitada a adotar atos delegados a fim de especificar os requisitos a se ter em conta para os procedimentos de certificação nos termos do artigo 43.º, n.º 8; f) o CEPD (Comitê Europeu para a Proteção de Dados), ao dar parecer à Comissão Europeia a respeito dos requisitos de certificação em conformidade com o artigo 70.º, n.º 1, alínea q), e o artigo 43.º, n.º 8; f)

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022.

[854] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022.

os organismos nacionais de acreditação, que terão de ter em conta os critérios de certificação com vista à acreditação dos organismos de certificação, em conformidade com a norma EN-ISO/IEC 17065/2012 e os requisitos adicionais nos termos do artigo 43.º; e g) os responsáveis pelo tratamento e subcontratantes, ao definirem a sua própria estratégia de conformidade com o RGPD e considerarem a certificação como um meio para demonstrá-la.

O Comitê Europeu para a Proteção de Dados publicou orientações separadas para abordar a identificação de critérios para a aprovação de procedimentos de certificação como instrumentos de transferência para países terceiros ou organizações internacionais, em conformidade com o artigo 42.º, n.º 2.[855]

c) Disclaimer

O artigo 42.º, n.º 1, prevê a criação de procedimentos de certificação «para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente regulamento».

O RGPD exemplifica o contexto em que os procedimentos de certificação aprovados podem ser utilizados como um elemento para demonstrar o cumprimento das obrigações dos responsáveis pelo tratamento e dos subcontratantes no que diz respeito, notadamente:

• à aplicação e demonstração de medidas técnicas e organizativas adequadas, tal como referido no artigo 24.º, nºs 1 e 3, no artigo 25.º e no artigo 32.º, nºs 1 e 3;

• à apresentação das garantias suficientes (do subcontratante ao responsável pelo tratamento) a que se refere o artigo 28.º, n.ºs 1 (do subcontratante ulterior ao subcontratante) e 4 (cf. artigo 28.º, n. º 5).

Uma vez que a certificação não prova a conformidade em si e por si só, sendo antes um elemento que pode ser utilizado para demonstrar a conformidade, deve esta ser efetuada de forma transparente. A demonstração da conformidade exige documentação de apoio, nomeadamente relatórios escritos que não só repitam, como descrevam o modo como os critérios são cumpridos e, caso estes não tenham sido inicialmente cumpridos,

[855] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Guidelines 07/2022 on certification as a tool for transfers**. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_pt. Acesso em: 20 nov. 2022. O documento, diferentemente de seu análogo referente aos códigos de conduta não será aqui examinado, eis que ainda não se encontra em versão final, após consulta pública. Isso porque a consulta pública ao documento encerrou-se em 30 de setembro do ano corrente, ainda estando pendente sua consolidação.

detalhem as correções e as medidas corretivas, bem como a sua adequação, fornecendo, assim, as razões para a concessão e manutenção da certificação. Isso inclui as linhas gerais da decisão individual de concessão, renovação ou revogação de um certificado, que deve indicar os motivos, argumentos e provas resultantes da aplicação dos critérios e as conclusões, ilações ou deduções dos fatos ou pressupostos recolhidos durante a certificação.

d) Conceitos fundamentais

A seção seguinte analisa os conceitos fundamentais dos artigos 42.º e 43.º. Esta análise procura contribuir para uma melhor compreensão dos termos básicos e do âmbito da certificação ao abrigo do RGPD.

i. Interpretação do termo «certificação»

Conforme destacam as Diretrizes n.º 1/2018 do Comitê Europeu para a Proteção de Dados:[856]

> O RGPD não define «certificação». A Organização Internacional de Normalização (ISO) estabelece uma definição universal de certificação como «o fornecimento, por um organismo independente, da garantia por escrito (certificado) de que o produto, serviço ou sistema em causa cumpre requisitos específicos.» A certificação é também conhecida por «avaliação da conformidade por terceiros», e os organismos de certificação também podem ser designados como «organismos de avaliação da conformidade (OAC)». Na norma EN-ISO/IEC 17000: 2004 - Avaliação da conformidade - Vocabulário e princípios gerais (a que se refere a norma ISO17065) - a certificação é definida do seguinte modo: «Atestação por terceiros [...] relativa a produtos, processos e serviços».
> Atestação é a «emissão de uma comprovação, com base numa decisão decorrente de uma análise, de que o cumprimento dos requisitos especificados foi demonstrado» (ponto 5.2, ISO 17000: 2004).

[856] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022.

No contexto da certificação, nos termos dos artigos 42.º e 43.º do RGPD, esta se refere a uma atestação por terceiros relativa às operações de tratamento efetuadas por responsáveis pelo tratamento e subcontratantes.

ii. Procedimentos de certificação, selos e marcas

O RGPD também não define «procedimentos de certificação, selos ou marcas», antes utiliza os termos coletivamente. Um certificado é uma declaração de conformidade. O selo ou marca pode ser utilizado para indicar a conclusão com êxito do processo de certificação. Um selo ou uma marca refere-se geralmente a um logotipo ou símbolo cuja presença (para além de um certificado) indica que o objeto da certificação foi avaliado de forma independente num procedimento de certificação e está em conformidade com os requisitos especificados, constantes de documentos normativos, tais como regulamentos, normas ou especificações técnicas.

Estes requisitos no contexto da certificação ao abrigo do RGPD são definidos nos requisitos adicionais que complementam as regras de acreditação dos organismos de certificação na norma EN-ISO/IEC 17065/2012 e nos critérios de certificação aprovados pela Autoridade de Controle competente ou pelo Comitê Europeu para a Proteção de Dados.

Um certificado, selo ou marca nos termos do RGPD só pode ser emitido após a avaliação independente das provas por um organismo de certificação acreditado ou por uma Autoridade de Controle competente, declarando que os critérios de certificação foram cumpridos.[857]

[857] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022.

Figura 8 - Exemplo genérico de um processo de certificação.

Submission of application by controller or processor	Formal Check by CB	Assessment Pre-Evaluation	Assessment Evaluation of ToE	Assessment Validation of results	Information to CSA	Certification	Monitoring	Renewal of certification
Is the description of the target of evaluation (ToE) anambigous and complete including interfaces?	Can the ToE description be accepted?	What are the applicable criteria?	Does the ToE meet the criteria?	Are all relevant criteria specified reflecting the ToE?	Have the reasons for granting or withdrawing certification been provided?	Can the certificate be awarded?	Does the ToE continue to meet the criteria	Does the processing still meet the certification criteria?
Can access to the ToE processing activities be granted?	Are all documents complete and up -to - date?	What are the applicable evaluation methods?	Is the documentation of the ToE correct?	Has the evaluation been sufficiently documented ?		Are the reports ready for publishing?	Is the certificate/seal/trust mark used correctly?	Have areas of development been satisfactorily addressed?
Art. 42(6)	Art. 43(4)	Art. 43(4)	Art. 42(5), Art. 43(4)	Art. 43(4)	Art. 43(1), 43(5)	Art. 43(1); Art. 42 (7)	Art. 42 (7)	Art. 42 (7)

Fonte: UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf. Acesso em: 20 nov. 2022.

e) O papel das Autoridades de Controle

O artigo 42.º, n.º 5, prevê que a certificação seja emitida por um organismo de certificação acreditado ou por uma Autoridade de Controle competente. O RGPD não impõe a emissão de certificações como uma tarefa obrigatória das Autoridades de Controle, permitindo, pelo contrário, que possam adotar vários modelos diferentes. Por exemplo, uma Autoridade de Controle pode decidir por uma ou mais das seguintes opções:

- emitir ela própria a certificação, com respeito ao seu próprio sistema de certificação;

- emitir ela própria a certificação, com respeito ao seu próprio sistema de certificação, mas delegar a terceiros a totalidade ou parte do processo de avaliação;

- criar o seu próprio sistema de certificação e confiar aos organismos de certificação o procedimento da emissão da certificação; e

- incentivar o mercado a desenvolver procedimentos de certificação.

Uma Autoridade de Controle terá também de considerar o seu papel à luz das decisões tomadas a nível nacional sobre os procedimentos de acreditação – em especial se a própria Autoridade de Controle estiver habilitada a acreditar organismos de

certificação nos termos do artigo 43.º, n.º 1, do RGPD. Assim, cada Autoridade de Controle determinará qual a abordagem a adotar para prosseguir o objetivo geral da certificação ao abrigo do RGPD.

Isso será determinado no contexto não só das atribuições e dos poderes previstos nos artigos 57.º e 58.º, mas também na contabilização da certificação como fator a ter em conta na fixação das multas e, de um modo mais geral, como meio de demonstrar a conformidade.

i. A Autoridade de Controle como organismo de certificação

Se uma Autoridade de Controle decidir realizar a certificação, terá de avaliar cuidadosamente o seu papel no que diz respeito às atribuições que lhe incumbem ao abrigo do RGPD. O seu papel deve ser transparente no exercício das suas funções. Terá de ter em conta, especificamente, a separação de poderes em matéria de investigação e de execução, a fim de evitar potenciais conflitos de interesses.

Ao atuar na qualidade de organismo de certificação, uma Autoridade de Controle terá de garantir a criação adequada de um procedimento de certificação e desenvolver os seus próprios critérios de certificação ou adotar tais critérios. Além disso, cada Autoridade de Controle que emita certificações tem a atribuição de proceder à sua revisão periódica (artigo 57.º, n.º 1, alínea o) e o poder de as revogar se os requisitos de certificação não estiverem ou deixarem de estar cumpridos (artigo 58.º, n.º 2, alínea h).

Para cumprir estes requisitos, é útil prever um procedimento de certificação e requisitos processuais e, salvo disposto em contrário pela legislação nacional, estabelecer um acordo juridicamente vinculativo para a prestação de atividades de certificação com a organização candidata individual.

Deve garantir-se que este acordo em matéria de certificação exija que o requerente cumpra, pelo menos, os critérios de certificação, incluindo os procedimentos necessários para realizar a avaliação, o controle do cumprimento dos critérios e a revisão periódica, incluindo o acesso a informações e/ou instalações, a documentação e a publicação de relatórios e resultados, bem como a investigação de reclamações. Espera-se também que uma Autoridade de Controle siga os requisitos estabelecidos nas orientações para a acreditação de organismos de certificação, para além dos requisitos previstos no artigo 43.º, n.º 2.

ii. Outras atribuições da Autoridade de Controle em matéria de certificação

Nos Estados-Membros em que comecem a operar organismos de certificação, a Autoridade de Controle, independentemente das suas próprias atividades, tem as seguintes atribuições e poderes:

- avaliar os critérios de um sistema de certificação e elaborar um projeto de decisão (artigo 42.º, n.º 5);

- comunicar ao Comitê Europeu para a Proteção de Dados o projeto de decisão quando pretenda aprovar os critérios de certificação (artigo 64.º, n.º 1, alínea c), e artigo 64.º, n.º 7)) e ter em conta o parecer do Comitê (artigo 64.º, n.º 1, alínea c), e artigo 70.º, n.º 1, alínea t));

- aprovar os critérios de certificação (artigo 58.º, n.º 3, alínea f)) antes de a acreditação e a certificação poderem ter lugar (artigo 42.º, n.º 5, e artigo 43.º, n.º 2, alínea b));

- publicar os critérios de certificação (artigo 43.º, n.º 6);

- atuar como Autoridade competente para os sistemas de certificação à escala (nível) da UE, o que pode dar lugar a um selo europeu de proteção de dados aprovado pelo Comitê Europeu para a Proteção de Dados (artigo 42.º, n.º 5, e artigo 70.º, n.º 1, alínea o)); e

- ordenar a um organismo de certificação: a) que não emita uma certificação ou b) que retire a certificação se os requisitos de certificação (procedimentos ou critérios de certificação) não estiverem ou deixarem de ser cumpridos (artigo 58.º, n.º 2, alínea h).

O RGPD encarrega a Autoridade de Controle da aprovação dos critérios de certificação, mas não do desenvolvimento de critérios. A fim de aprovar os critérios de certificação nos termos do artigo 42.º, n.º 5, a Autoridade de Controle deve ter um conhecimento claro do que esperar, especificamente em termos de âmbito e conteúdo, para demonstrar a conformidade com o RGPD e no que se refere à sua atribuição de controlar e fazer cumprir o regulamento. O Anexo VIII fornece orientações para garantir uma abordagem harmonizada por ocasião da avaliação dos critérios para efeitos de aprovação.

O artigo 43.º, n.º 1, exige que, antes de emitirem ou renovarem as certificações, os organismos de certificação informem a Autoridade de Controle competente para que esta possa exercer os seus poderes de correção nos termos do artigo 58.º, n.º 2, alínea h). Além disso, o artigo 43.º, n.º 5, exige também que os organismos de certificação forneçam

à Autoridade de Controle competente os motivos para a concessão ou revogação da certificação solicitada. Embora o RGPD permita que as Autoridades de Controle determinem o modo como receber, reconhecer, analisar e tratar estas informações do ponto de vista operacional (o que pode incluir, por exemplo, soluções tecnológicas que permitam a elaboração de relatórios pelos organismos de certificação), poderão adotar-se processos e critérios para tratar as informações e os relatórios apresentados pelo organismo de certificação sobre cada projeto de certificação bem sucedido, em conformidade com o artigo 43.º, n.º 1.

Com base nestas informações, a Autoridade de Controle pode exercer o seu poder de ordenar ao organismo de certificação que retire ou não emita uma certificação (artigo 58.º, n.º 2, alínea h), bem como de controlar e fazer cumprir os requisitos e critérios de certificação ao abrigo do RGPD (artigo 57.º, n.º 1, alínea a), e artigo 58.º, n.º 2, alínea h)). Isso permitirá uma abordagem harmonizada e a comparabilidade da certificação por diferentes organismos de certificação, além de garantir que as Autoridades de Controle conheçam as informações sobre o estatuto de certificação de uma organização.

f) O papel do organismo de certificação

O papel do organismo de certificação consiste em emitir, rever, renovar e retirar certificações (artigo 42.º, n.ºs 5 e 7)) com base num procedimento de certificação e em critérios aprovados (artigo 43.º, n.º 1). Isso exige que o organismo de certificação ou o proprietário do sistema de certificação determine e estabeleça critérios e procedimentos de certificação, incluindo mecanismos de controle do cumprimento, revisão, tratamento de reclamações e revogação. Os critérios de certificação são examinados no âmbito do processo de acreditação, que analisa as regras e os procedimentos à luz dos quais são emitidas as certificações, os selos ou as marcas (artigo 43.º, n.º 2, alínea c).

A existência de um procedimento e de critérios de certificação é necessária para que o organismo de certificação possa obter a acreditação nos termos do artigo 43.º. O âmbito e o tipo de critérios de certificação que influem nos procedimentos de certificação têm um impacto importante sobre o que faz um organismo de certificação e vice-versa. Critérios específicos podem, por exemplo, exigir métodos de avaliação específicos, como inspeções no local e a análise de códigos. Estes procedimentos são obrigatórios para efeitos de acreditação e são explicados de forma mais pormenorizada nas orientações relativas à acreditação.

O RGPD exige que o organismo de certificação forneça informações às Autoridades de Controle, principalmente sobre as certificações individuais, o que é necessário para controlar a aplicação do procedimento de certificação (artigo 42.º, n.º 7, artigo 43.º, n.º 5, e artigo 58, n.º 2, alínea h).

g) Aprovação dos critérios de certificação

Os critérios de certificação fazem parte integrante de qualquer procedimento de certificação. Por conseguinte, o RGPD exige que os critérios de certificação de um procedimento de certificação sejam aprovados pela Autoridade de Controle competente (artigos 42.º, n.º 5, e artigo 43.º, n.º 2, alínea b)). No caso de um selo europeu de proteção de dados, os critérios de certificação são aprovados pelo Comitê Europeu para a Proteção de Dados – CEPD (artigo 42.º, n.º 5, e artigo 70.º, n.º 1, alínea o)). Ambas as vias de aprovação dos critérios de certificação são explicadas a seguir.

O CEPD reconhece os seguintes objetivos para a aprovação dos critérios de certificação: a) refletir adequadamente os requisitos e princípios relativos à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, tal como estabelecidos no Regulamento (UE) 2016/679; e b) contribuir para a aplicação coerente do RGPD.

A aprovação é concedida com base no requisito do RGPD segundo o qual o procedimento de certificação deve permitir aos responsáveis pelo tratamento e aos subcontratantes demonstrar que a conformidade com o RGPD está plenamente refletida nos critérios de certificação.

i. <u>Aprovação dos critérios pela Autoridade de Controle competente</u>

Os critérios de certificação devem ser aprovados pela Autoridade de Controle competente antes ou durante o processo de acreditação de um organismo de certificação. É igualmente necessária a aprovação de regimes ou conjuntos de critérios atualizados ou adicionais, ao abrigo da norma ISO 17065, pelo mesmo organismo de certificação, antes de serem utilizados os procedimentos de certificação alterados (artigo 42.º, n.º 5, e artigo 43.º, n.º 2, alínea b). As Autoridades de Controle devem tratar todos os pedidos de aprovação de critérios de certificação de forma equitativa e não discriminatória, de acordo

com um procedimento publicamente disponível que especifique as condições gerais a preencher e a descrição do processo de aprovação.

Um organismo de certificação só pode emitir uma certificação num determinado Estado-Membro de acordo com os critérios aprovados pela Autoridade de Controle desse Estado-Membro. Por outras palavras, os critérios de certificação têm de ser aprovados pela Autoridade de Controle competente do país onde o organismo de certificação pretenda realizar a certificação e obter acreditação.

ii. Aprovação de critérios pelo Comitê (CEPD) para o Selo Europeu de Proteção de Dados

Um organismo de certificação também pode emitir uma certificação de acordo com os critérios aprovados pelo CEPD para um selo europeu de proteção de dados. Os critérios de certificação aprovados pelo CEPD nos termos do artigo 63.º podem dar lugar ao Selo Europeu de Proteção de Dados (artigo 42.º, n.º 5). À luz das atuais convenções em matéria de certificação e acreditação, o Comitê Europeu para Proteção de Dados (CEPD) reconhece que é desejável evitar a fragmentação do mercado da certificação em matéria de proteção de dados. Observa que o artigo 42.º, n.º 1, prevê que os Estados-Membros, as Autoridades de Controle, o Comitê e a Comissão promovam, em especial ao nível da União, a criação de procedimentos de certificação.

ii.i Pedido de aprovação

O pedido de aprovação de critérios, nos termos do artigo 42.º, n.º 5, e do artigo 70.º, n.º 1, alínea o), pelo Comitê Europeu para Proteção de Dados deve ser apresentado através de uma Autoridade de Controle competente e indicar a intenção do proprietário do sistema e do organismo de certificação candidato ou acreditado de cumprir os critérios, em um procedimento de certificação aplicável aos responsáveis pelo tratamento e aos subcontratantes em todos os Estados-Membros. A Autoridade de Controle competente apresentará um projeto ao CEPD quando considerar que os critérios podem ser por estes aprovados.

A escolha do local onde apresentar um pedido de aprovação dos critérios dependerá do local da sede dos proprietários dos sistemas de certificação ou dos organismos de certificação.

Se um organismo de certificação apresentar um pedido, encontrar-se-á normalmente em processo de requisição da acreditação, ou estará já acreditado pela Autoridade de Controle competente ou pelo organismo nacional de acreditação do respectivo Estado-Membro. Se o organismo de certificação já estiver acreditado para um procedimento de certificação nos termos do RGPD, isso poderá ajudar a agilizar o processo de aprovação.

ii.ii Critérios do Selo Europeu de Proteção de Dados

O Comitê Europeu para Proteção de Dados coordenará o processo de avaliação e aprovará os critérios relativos ao Selo Europeu de Proteção de Dados, conforme exigido.

A avaliação incidirá em domínios como o âmbito dos critérios e a capacidade de ser utilizada como uma certificação comum (no âmbito europeu). Caso os critérios sejam aprovados pelo CEPD, a Autoridade de Controle competente para a sede da União Europeia (UE) do organismo de certificação deverá tratar as reclamações relativas ao próprio procedimento e informar as restantes Autoridades de Controle. Essa Autoridade de Controle será igualmente competente para tomar medidas contra o organismo de certificação. Se for caso disso, a Autoridade de Controle competente notificará as restantes Autoridades de Controle e o CEPD.

Os critérios de certificação aplicáveis a uma certificação comum estão sujeitos a exigências a nível da União Europeia e deverão fornecer um procedimento específico para fazer face a estas exigências. Os procedimentos de certificação europeus devem destinar-se a ser utilizados em todos os Estados-Membros. Com base no artigo 42.º, n.º 5, o procedimento relativo ao Selo Europeu de Proteção de Dados, bem como os seus critérios, deve poder ser adaptado de modo a ter em conta a regulamentação setorial nacional, quando aplicável, por exemplo para o tratamento de dados nas escolas, e prever uma aplicação à escala europeia. [858]

[858] As Diretrizes n.º 1/2018 exemplificam o assunto do seguinte modo: "Exemplo: Uma escola internacional que oferece educação escolar a titulares de dados na União tem a sua sede no Estado-Membro «A». A escola deseja certificar o seu processo de candidatura em linha com um sistema de certificação a nível da UE para obter um selo europeu de proteção de dados e pretende solicitar a certificação das operações de tratamento oferecidas por um organismo de certificação estabelecido no Estado-Membro «B» com base num selo europeu de proteção de dados. Os critérios do selo, concebidos e documentados no procedimento apropriado, devem poder ter em conta a regulamentação aplicável às escolas do Estado-Membro «A». Os critérios devem também exigir que o processo de candidatura em linha da escola forneça informações e tenha em conta os requisitos aplicáveis do Estado-Membro em matéria de proteção de dados, que podem diferir entre Estados-Membros. É o caso, por exemplo, dos conjuntos de dados pessoais que devem ser apresentados para efeitos de candidatura, tais como notas ou resultados de exames de jardins de infância,

Nos critérios de nível elevado para a aprovação de um procedimento relativo ao Selo Europeu de Proteção de Dados incluem-se: a) critérios aprovados pelo Comitê; b) aplicação em todos os países, refletindo, se for caso disso, os requisitos legais nacionais e os regulamentos setoriais específicos; c) critérios harmonizados que possam ser adaptados de modo a refletir os requisitos nacionais; d) descrição do procedimento de certificação, especificando: os acordos de certificação que cumpram os requisitos pan-europeus; e) procedimentos para garantir e fornecer soluções para as variações nacionais e garantir que o selo contribui para demonstrar a conformidade com o RGPD; e f) a língua dos relatórios dirigidos a todas as Autoridades de Controle em causa.

O anexo IX contém igualmente recomendações sobre os critérios relativos ao Selo Europeu de Proteção de Dados, fornecidos pelo Comitê Europeu para a Proteção de Dados.

ii.iii Papel da acreditação

Tal como indicado acima, quando os critérios são identificados como adequados para a certificação comum e forem aprovados como tal pelo Comitê, nos termos do artigo 42.º, n.º 5, os organismos de certificação podem ser acreditados para realizar a certificação à luz desses critérios no nível da União.

Os sistemas que se destinem a ser oferecidos apenas em determinados Estados-Membros não serão candidatos aos selos da UE. A acreditação para o âmbito de aplicação de um selo europeu de proteção de dados necessitará de uma acreditação no Estado-Membro da sede do organismo de certificação que pretende gerir o sistema, ou seja, que é responsável pela emissão de certificações e pela gestão das atividades de certificação das suas entidades e filiais noutros Estados-Membros. Nos casos em que outros estabelecimentos ou serviços gerem e realizam a certificação de forma autônoma, cada um desses estabelecimentos ou serviços deverá ser objeto de uma acreditação separada no Estado-Membro em que se encontram estabelecidos. Por outras palavras, a acreditação só é necessária no Estado-Membro da sede do organismo de certificação nos casos em que apenas esta entidade emite os certificados.

diferentes períodos de conservação, recolha ou tratamento de dados financeiros ou biométricos, outras limitações de tratamento adicionais". UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022.

Em contrapartida, quando outros estabelecimentos do organismo de certificação também emitem certificados, esses estabelecimentos devem igualmente ser acreditados.

Por conseguinte, se um organismo de certificação não estiver acreditado para certificar ao abrigo do Selo Europeu de Proteção de Dados, os critérios aprovados pelo CEPD não podem ser utilizados e o selo não pode ser concedido.

h) Elaboração dos critérios de certificação

O RGPD estabeleceu o quadro para a elaboração de critérios de certificação. Embora os artigos 42.º e 43.º abordem os requisitos fundamentais relativos ao processo de certificação, prevendo ao mesmo tempo critérios essenciais para os procedimentos de certificação, a base dos critérios de certificação deve decorrer dos princípios e regras do RGPD e ajudar a garantir que estes são cumpridos.

A elaboração dos critérios de certificação deve se centrar na verificabilidade, relevância e adequação destes últimos para demonstrar a conformidade com o regulamento. Os critérios de certificação devem ser formulados de forma a serem claros e compreensíveis e a permitirem uma aplicação prática.

Se for caso disso, na elaboração dos critérios de certificação devem ser tidos em conta, entre outros, os seguintes aspectos de conformidade em apoio à avaliação das operações de tratamento:

- a licitude do tratamento, nos termos do artigo 6.º;
- os princípios relativos ao tratamento de dados pessoais, nos termos do artigo 5.º;
- os direitos dos titulares dos dados, nos termos dos artigos 12.º a 23.º;
- a obrigação de notificar as violações de dados, nos termos do artigo 33.º;
- a obrigação de proteção de dados desde a concepção (*privacy by design*) e por padrão (*privacy by default*), nos termos do artigo 25.º;
- se foi realizada uma avaliação de impacto sobre a proteção de dados, nos termos do artigo 35.º, n.º 7, alínea d), se aplicável; e
- as medidas técnicas e organizativas adotadas, nos termos do artigo 32.º.

O impacto destas considerações nos critérios pode variar em função do âmbito da certificação, que pode incluir o tipo de operação(ões) de tratamento e o domínio da certificação (por exemplo, o setor da saúde).

i. O que pode ser certificado ao abrigo do RGPD?

O Comitê Europeu para Proteção de Dados considera que o RGPD prevê um âmbito alargado para o que pode ser certificado ao seu abrigo, desde que a tônica seja colocada na comprovação de conformidade das operações de tratamento dos responsáveis pelo tratamento e dos subcontratantes com o regulamento (artigo 42.º, n.º 1).

Na avaliação de uma operação de tratamento, devem ser tidos em conta, quando aplicável, os três componentes principais seguintes: (1) dados pessoais (âmbito material do RGPD); (2) sistemas técnicos - as infraestruturas, como o *hardware* e o *software*, utilizadas para tratar os dados pessoais; e (3) processos e procedimentos relacionados com a(s) operação(ões) de tratamento.

Cada componente utilizada nas operações de tratamento deve ser sujeita a uma avaliação em função dos critérios definidos. Pelo menos quatro fatores relevantes diferentes podem ter influência: 1) a organização e a estrutura jurídica do responsável pelo tratamento ou do subcontratante; 2) o departamento, o ambiente e as pessoas envolvidas na(s) operação(ões) de tratamento; 3) a descrição técnica dos elementos a avaliar; e, por último, 4) a infraestrutura informática de apoio à operação de tratamento, incluindo sistemas operativos, sistemas virtuais, bases de dados, sistemas de autenticação e autorização, encaminhadores (*routers*) e barreiras de segurança (*firewalls*), sistemas de armazenamento, infraestruturas de comunicação ou acesso à Internet e medidas técnicas associadas.

Os três componentes principais são relevantes para a concepção dos procedimentos e critérios de certificação. A sua tomada em consideração pode variar consoante o objeto da certificação. Por exemplo, em alguns casos, algumas componentes podem ser ignoradas se forem consideradas não pertinentes para o objeto da certificação.

Para especificar mais pormenorizadamente o que pode ser certificado nos termos do RGPD, este contém orientações adicionais. Decorre do artigo 42.º, n.º 7, que as certificações ao abrigo do RGPD são emitidas apenas aos responsáveis pelo tratamento de dados e aos subcontratantes, o que exclui, por exemplo, a certificação de responsáveis pela proteção de dados. O artigo 43.º, n.º 1, alínea b), faz referência à norma ISO 17065, que prevê a acreditação dos organismos de certificação que avaliam a conformidade de produtos, serviços e processos. Uma operação ou um conjunto de operações de tratamento pode dar lugar a um produto ou serviço na terminologia da norma ISO 17065, que, como tal, pode ser objeto de certificação. Por exemplo, o tratamento de dados dos trabalhadores

para efeitos de pagamento de salários ou de gestão de licenças constitui um conjunto de operações na acepção do RGPD e pode dar lugar a um produto, um processo ou um serviço na terminologia da ISO.

Com base nestas considerações, o CEPD (Comitê Europeu para Proteção de Dados) considera que o âmbito da certificação ao abrigo do RGPD diz respeito a operações ou conjuntos de operações de tratamento. Estas podem incluir processos de governança no sentido de medidas organizativas, ou seja, como parte integrante de uma operação de tratamento (por exemplo, o processo de governança estabelecido para o tratamento de reclamações no âmbito do tratamento de dados dos trabalhadores para efeitos de pagamento de salários).

A fim de avaliar a conformidade da operação de tratamento com os critérios de certificação, deve ser apresentado um caso de utilização. Por exemplo, a conformidade da utilização de uma infraestrutura técnica implantada numa operação de tratamento depende das categorias de dados que visa tratar. As medidas organizativas dependem das categorias e do volume de dados e da infraestrutura técnica utilizada para o tratamento, tendo em conta a natureza, o âmbito, o conteúdo e as finalidades do tratamento, bem como os riscos para os direitos e liberdades dos titulares de dados.

Além disso, há que ter em mente que as aplicações informáticas podem ser muito diferentes, ainda que sirvam aos mesmos fins de tratamento. Por conseguinte, este aspecto deve ser tido em conta na definição do âmbito dos procedimentos de certificação e na elaboração dos critérios de certificação, ou seja, o âmbito da certificação e os critérios não devem ser tão restritos que excluam as aplicações informáticas concebidas de forma diferente.

ii. <u>Determinação do objeto da certificação</u>

O âmbito de um procedimento de certificação deve ser distinguido do objeto – também denominado «alvo de avaliação» (do inglês «*target of evaluation*», TOE) – em projetos de certificação individuais sob a alçada de um procedimento de certificação.

Um procedimento de certificação pode definir o seu âmbito, quer de um modo geral quer em relação a um tipo ou domínio específico de operações de tratamento, podendo, assim, já identificar os objetos da certificação que se inserem no seu âmbito (por exemplo, armazenamento seguro e proteção de dados pessoais contidos num cofre digital).

Em qualquer caso, uma avaliação fiável e significativa da conformidade só pode ocorrer se o objeto individual de um projeto de certificação for descrito com precisão. Essa avaliação deve descrever claramente quais as operações de tratamento que são incluídas no objeto da certificação e, em seguida, as componentes essenciais, ou seja, os dados, processos e infraestruturas técnicas que serão avaliados e os que não o serão. Para tal, as interfaces com outros processos devem ser sempre consideradas e descritas. Evidentemente, o que não é conhecido não pode fazer parte da avaliação e, por conseguinte, não pode ser certificado. Em todo o caso, o objeto individual da certificação deve ser relevante no que respeita à mensagem ou alegação formulada na/pela certificação e não deve induzir a erro o utilizador, o cliente ou o consumidor.

O Comitê Europeu para Proteção de Dados por meio das Diretrizes n.º 1/2018 do Comitê Europeu para a Proteção de Dados fornece os seguintes exemplos:[859]

> [Exemplo 1]
> Um banco oferece aos seus clientes um sítio Web para a prestação de serviços bancários em linha. No âmbito deste serviço, existe a possibilidade de efetuar transferências, comprar ações, criar ordens permanentes e gerir a conta. O banco pretende certificar os seguintes elementos no âmbito de um procedimento de certificação em matéria de proteção de dados de alcance geral, com base em critérios genéricos:
> a) Início de sessão («*log-in*») seguro
> O início de sessão seguro é uma operação de tratamento que é compreensível para o utilizador final e é relevante do ponto de vista da proteção de dados, uma vez que desempenha um papel importante para garantir a segurança dos dados pessoais em causa. Por conseguinte, esta operação de tratamento é necessária para iniciar uma sessão segura, podendo, portanto, constituir um alvo de avaliação relevante se o certificado indicar claramente que só a operação de início de sessão é certificada.
> b) «*Web front-end*» (interface frontal da Web)
> Embora possa ser pertinente do ponto de vista da proteção de dados, o «*Web front-end*» não é compreensível para o utilizador final e, portanto, não pode constituir um alvo de avaliação relevante. Além disso, o utilizador não sabe de forma clara que serviços no sítio Web e, logo, que operações de tratamento são abrangidas pela certificação.
> c) Operações bancárias em linha
> As operações a nível da interface frontal, ou seja do lado do utilizador, («*front-end web*») e da interface a nível do servidor («*back-end web*) são operações de tratamento prestadas no âmbito do serviço bancário em linha, que podem ser significativas para o utilizador. Neste contexto, ambas devem ser incluídas nos alvos de avaliação, ao passo que as

[859] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022.

operações de tratamento que não estejam diretamente relacionadas com a prestação do serviço bancário em linha, tais como as operações de tratamento para efeitos de prevenção do branqueamento de capitais, podem ser excluídas dos alvos de avaliação.
No entanto, os serviços bancários em linha oferecidos pelo banco através do seu sítio Web podem também incluir outros serviços que, por sua vez, necessitam das suas próprias operações de tratamento. Neste contexto, outros serviços podem incluir, por exemplo, a oferta de um produto de seguros. Uma vez que este serviço adicional não está diretamente relacionado com a finalidade de prestar serviços bancários em linha, pode ser excluído dos alvos de avaliação. Se este serviço adicional (seguros) for excluído dos alvos de avaliação, as interfaces para este serviço integrado no sítio Web fazem parte dos alvos de avaliação, devendo, por conseguinte, ser descritas de modo a estabelecer uma distinção clara entre os serviços. Essa descrição é necessária para identificar e avaliar possíveis fluxos de dados entre os dois serviços.

[Exemplo 2]
Um banco oferece aos seus clientes um serviço que lhes permite agregar as informações relativas a diferentes contas e cartões de crédito de vários bancos (agregação de contas) e pretende ter o seu serviço certificado ao abrigo do RGPD. A autoridade de controle competente aprovou um conjunto específico de critérios de certificação centrados neste tipo de atividade. O âmbito do procedimento de certificação incide apenas nos seguintes aspetos de conformidade:

- autenticação do utilizador; e
- formas aceitáveis de obter de outros bancos/serviços os dados a serem agregados.

Uma vez que o âmbito deste procedimento de certificação define o alvo de avaliação por si só, não é possível restringir este último de forma relevante sob o âmbito proposto e certificar apenas as características específicas ou uma única atividade de tratamento. Neste cenário, um alvo de avaliação deve corresponder a um âmbito específico.

iii. Métodos de avaliação e metodologia de avaliação

Uma avaliação da conformidade que ajude a demonstrar a conformidade das operações de tratamento de dados exige a identificação e determinação dos métodos de avaliação e da metodologia de avaliação. É importante saber se a informação para a avaliação é recolhida apenas com base na documentação (que, por si só, não seria suficiente) ou se é recolhida de forma ativa no local e mediante acesso direto ou indireto. A forma como a informação é recolhida tem impacto na relevância da certificação, pelo que deve ser definida e descrita.

Os procedimentos para a emissão e a revisão periódica das certificações devem incluir especificações para identificar o nível adequado de avaliação (profundidade e granularidade) para cumprir os critérios de certificação e incluir, designadamente:

- o fornecimento de informações e especificações sobre os métodos de avaliação aplicados e os resultados obtidos, por exemplo, durante auditorias no local ou a partir de documentação;
- métodos de avaliação centrados nas operações de tratamento (dados, sistemas, processos) e na finalidade do tratamento;
- a identificação das categorias de dados e das necessidades de proteção e a determinação da participação ou não de subcontratantes ou de terceiros;
- a identificação das funções e existência de um mecanismo de controle de acesso definido em função dos papéis e das responsabilidades.

A profundidade da avaliação terá impacto na relevância e valor da certificação. Ao reduzir a profundidade da avaliação para fins pragmáticos ou redução dos custos, a relevância de uma certificação em matéria de proteção de dados será diminuída. As decisões sobre a granularidade da avaliação, por outro lado, podem exceder as capacidades financeiras do candidato e, muitas vezes, a capacidade dos avaliadores e auditores. Para fins de demonstração da conformidade, pode nem sempre ser crucial obter uma análise muito pormenorizada dos sistemas informáticos utilizados para continuar a ser relevante.

iv. Documentação da avaliação

A documentação de certificação deve ser exaustiva e completa. A falta de documentação significa que não é possível realizar uma avaliação adequada. A função essencial da documentação de certificação é garantir a transparência do processo de avaliação nos termos do procedimento de certificação. A documentação dá resposta às perguntas sobre os requisitos estabelecidos por lei. Os procedimentos de certificação devem prever uma metodologia normalizada de documentação. A avaliação posterior permitirá a comparação da documentação de certificação com o estado real no local e com os critérios de certificação.

Uma documentação completa do que foi certificado e da metodologia adotada favorece a transparência. Nos termos do artigo 43.º, n.º 2, alínea c), os procedimentos de certificação devem estabelecer procedimentos que permitam a revisão das certificações. A fim de permitir à Autoridade de Controle avaliar se, e em que medida, a certificação pode ser reconhecida em investigações formais; uma documentação pormenorizada pode

ser o meio mais adequado de comunicação. A documentação apresentada durante a avaliação deve, por conseguinte, incidir em três aspetos principais:

- consistência e coerência dos métodos de avaliação executados;
- métodos de avaliação destinados a demonstrar a conformidade do objeto de certificação com os critérios de certificação e, consequentemente, com o regulamento; e
- demonstração de que os resultados da avaliação foram validados por um organismo de certificação independente e imparcial.

v. Documentação dos resultados

O considerando 100 do RGPD contém informação sobre os objetivos perseguidos com a introdução da certificação: [860]

> A fim de reforçar a transparência e o cumprimento do presente regulamento, deverá ser encorajada a criação de procedimentos de certificação e selos e marcas de proteção de dados, que permitam aos titulares avaliar rapidamente o nível de proteção de dados proporcionado pelos produtos e serviços em causa.

Para reforçar a transparência, a documentação e a comunicação dos resultados desempenham um papel importante. Os organismos de certificação que utilizam procedimentos de certificação, selos ou marcas direcionados para os titulares de dados (na sua qualidade de consumidores ou de clientes) devem fornecer informações facilmente acessíveis, inteligíveis e pertinentes sobre a(s) operação(ões) de tratamento certificada(s). Esta informação ao público deve incluir, pelo menos, (1) a descrição do alvo de avaliação; (2) a referência aos critérios aprovados aplicados ao alvo de avaliação específico; (3) a metodologia para a avaliação dos critérios (avaliação no local, documentação, etc.); (4) o período de validade do certificado; e (5) deve permitir às Autoridades de Controle e ao público comparar os resultados.

i) Orientações para a definição dos critérios de certificação

[860] UE. União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial** L 119/1, 04 de maio de 2016.

Os critérios de certificação são parte integrante de um procedimento de certificação. O procedimento de certificação inclui os requisitos que dizem respeito à indicação de «como, por quem e em que medida», bem como a granularidade da avaliação a se realizar em projetos de certificação individuais relativos a um objeto específico ou ao alvo de avaliação. Os critérios de certificação estabelecem os requisitos nominais em relação aos quais é avaliada a operação de tratamento definida no alvo de avaliação.

Nesse sentido, as diretrizes n.º 1/2018 fornecem conselhos genéricos que facilitarão a avaliação dos critérios de certificação para efeitos de aprovação, nos seguintes termos:[861]

> As considerações gerais que se seguem devem ser tidas em conta aquando da aprovação ou definição dos critérios de certificação. Os critérios de certificação devem:
> - ser uniformes e verificáveis,
> - ser passíveis de auditoria, a fim de facilitar a avaliação das operações de tratamento efetuadas ao abrigo do RGPD, especificando, em especial, os objetivos e as orientações de execução para a realização desses objetivos;
> - ser pertinentes em relação ao público visado (por exemplo, entre empresas, B2B [business to business], e entre empresas e consumidores, B2C [business to consumers]);
> - ter em conta e, se for caso disso, ser interoperáveis com outras normas (como as normas ISO e as normas a nível nacional); e
> - ser flexíveis e redimensionáveis para a aplicação a diferentes tipos e dimensões de organizações, incluindo micro, pequenas e médias empresas, em conformidade com o artigo 42.º, n.º 1, e a abordagem baseada no risco, em conformidade com o considerando 77.

Uma pequena empresa local, como um retalhista, realizará, normalmente, operações de tratamento menos complexas do que um grande retalhista multinacional. Embora os requisitos de licitude das operações de tratamento sejam os mesmos, o âmbito do tratamento dos dados e a sua complexidade devem ser tidos em conta, sendo necessário, por conseguinte, que os procedimentos de certificação e os seus critérios sejam redimensionáveis de acordo com a atividade de tratamento em causa.

i. <u>Normas existentes</u>

[861] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022.

Os organismos de certificação terão de analisar a forma como critérios específicos tomam em consideração os instrumentos pertinentes existentes, como os códigos de conduta, as normas técnicas ou as iniciativas regulamentares e jurídicas nacionais. Idealmente, os critérios serão interoperáveis com as normas existentes, que podem ajudar um responsável pelo tratamento ou um subcontratante a cumprir as obrigações que lhe incumbem o RGPD. No entanto, embora as normas da indústria se centrem frequentemente na proteção e segurança da organização contra ameaças, o RGPD visa a proteção dos direitos fundamentais das pessoas singulares. Esta diferente perspectiva deve ser tida em conta quando da conceção dos critérios ou da aprovação de critérios ou procedimentos de certificação com base nas normas do setor.

ii. Definição de critérios

Os critérios de certificação devem corresponder à declaração de certificação (mensagem ou alegação) de um procedimento ou sistema de certificação e ir ao encontro das expectativas que este suscita. A designação de um procedimento de certificação poderá já identificar o âmbito de aplicação e terá impacto na determinação dos critérios.

O Comitê Europeu para Proteção de Dados, por meio das Diretrizes n.º 1/2018, fornece os seguintes exemplos:[862]

> [Exemplo 3]
> Um procedimento denominado «*Health Privacy Mark*» deve limitar o seu âmbito ao setor da saúde. O nome do selo gera a expectativa de que os requisitos em matéria de proteção de dados relacionados com os dados relativos à saúde foram examinados. Por conseguinte, os critérios deste procedimento devem ser adequados para avaliar os requisitos em matéria de proteção de dados neste setor.
> [Exemplo 4]
> Um procedimento relacionado com a certificação das operações de tratamento que incluem sistemas de governação no tratamento de dados deve identificar critérios que permitam o reconhecimento e a avaliação dos processos de governação e das respetivas medidas técnicas e organizativas de apoio.
> [Exemplo 5]
> Os critérios aplicáveis a um procedimento relacionado com a computação em nuvem devem ter em conta os requisitos técnicos especiais necessários para a utilização de serviços baseados na

[862] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022.

> computação em nuvem. Por exemplo, se os servidores forem utilizados fora da UE, os critérios devem ter em conta as condições estabelecidas no capítulo V do RGPD no que diz respeito às transferências de dados para países terceiros.

Os critérios concebidos para se adequarem a diferentes alvos de avaliação em diferentes setores e/ou Estados-Membros devem permitir a aplicação a diferentes cenários e a identificação das medidas adequadas para se adequarem a pequenas, médias ou grandes operações de tratamento e refletirem os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, em conformidade com o RGPD.

Por conseguinte, os procedimentos de certificação (por exemplo, para a documentação, os testes, ou o método e a profundidade da avaliação), que complementam os critérios, devem responder a essas necessidades, além de permitir e estabelecer regras, por exemplo, para aplicar os critérios pertinentes em projetos de certificação individuais. Os critérios devem facilitar a avaliação da existência, ou não, de garantias suficientes para a aplicação de medidas técnicas e organizativas adequadas.

iii. Vigência dos critérios de certificação

Os critérios de certificação, embora devam ser fiáveis ao longo do tempo, não devem ser imutáveis. Serão sujeitos a revisão, por exemplo, sempre que:

- o quadro jurídico seja alterado;
- os termos e disposições sejam interpretados por acórdãos do Tribunal de Justiça das Comunidades Europeias; ou
- o estado da técnica tenha evoluído.

3.2.2. Mecanismos de Certificação, selos e marcas de proteção de dados na Lei Geral de Proteção de Dados Pessoais

Novamente, a legislação brasileira apenas prevê linhas gerais sobre a possibilidade de utilização de mecanismos de certificação, selos e marcas de proteção de dados.

Aqui, de fato, tais instrumentos somente são aplicados como instrumento de comprovação de garantias adequadas para as transferências internacionais de dados (artigo 33, II, "d"), conforme se observa:[863]

> CAPÍTULO V
> DA TRANSFERÊNCIA INTERNACIONAL DE DADOS
> **Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:**
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
> **II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:**
> a) cláusulas contratuais específicas para determinada transferência;
> b) cláusulas-padrão contratuais;
> c) normas corporativas globais;
> **d) selos, certificados e códigos de conduta regularmente emitidos;**
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
> IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> V - quando a autoridade nacional autorizar a transferência;
> VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
> VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do *caput* do art. 23 desta Lei;
> VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
> IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.
> Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.
>
> Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do *caput* do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:
> I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
> II - a natureza dos dados;

[863] BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 nov. 2022.

> III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
> IV - a adoção de medidas de segurança previstas em regulamento;
> V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
> VI - outras circunstâncias específicas relativas à transferência.
>
> **Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do *caput* do art. 33 desta Lei, será realizada pela autoridade nacional.**
> § 1º Para a verificação do disposto no *caput* deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.
> § 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.
> **§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no *caput* deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.**
> **§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.**
> § 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no *caput* deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.
>
> Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.
> (Sem grifos no original)

A opção do legislador foi deixar de fora a utilização de processos de certificação, selos e marcas do âmbito interno, o que, possivelmente, comprometerá, em muito, a capacidade da Autoridade Nacional de adotar medidas adequadas para o real cumprimento dos requisitos de adequação.

Nesse sentido, cabe notar as dificuldades que a autoridade nacional teve para ser efetivamente implementada, com um patamar de garantias mínimas (como sua autonomia) para desempenhar suas atividades com independência.

Parte desses argumentos se vincularam aos gastos que a implantação de tal Autoridade geraria, de modo que, num primeiro momento, ela foi criada de forma vinculada à Presidência da República.

Esse cenário subjacente à criação da Autoridade de Controle exaspera uma de nossas preocupações centrais, expressas no início desta seção, que se refere à escassez de recursos, de diversas ordens: financeiros, materiais, humanos, naturais, etc.

Especificamente no caso de nossa Autoridade de Controle, estaremos diante de um alargado campo regulatório, envolvendo a peculiar construção de nosso modelo federativo, que confere autonomia aos municípios. Assim, enfrentaremos, somente no que se refere à aplicação da Lei Geral de Proteção de Dados no setor público, à necessidade de fiscalização quanto à União (e suas entidades autônomas), aos 26 estados federados (e suas entidades autônomas), ao Distrito Federal (e entidades autônomas), além dos 5.568 municípios (e suas entidades autônomas).

As alargadas dimensões político-territoriais brasileiras imporão um cenário de restrição muito mais elevada que em outros países. Mais alargado, talvez, que o cenário europeu, que diversificou (mais que nós) seus mecanismos de fiscalização e controle no Espaço Econômico Europeu.

Para se ter uma dimensão da questão, pontuamos os dados trazidos pela Conselheira Titular no Conselho Nacional de Proteção de Dados – CNPD, Patricia Peck, em recente palestra sobre a Lei Geral de Proteção de Dados Pessoais no Tribunal de Contas do Estado de Mato Grosso[864] apontando a existência de 6.141 demandas recebidas pela Autoridade Nacional de Proteção de Dados (ANPD) até 31/07/2022 – Anexo X.

Esse número, no entanto, já teria chegado a 6.664, em 31/10/2022, conforme dados da Autoridade Nacional de Proteção de Dados.[865] Isso revela o cenário dilatado de trabalho à cargo da recém-criada autoridade.

Nesse sentido, um modelo de fiscalização que contasse com a possibilidade de certificação de operações internas, como o europeu, poderia contribuir sobremaneira com as atividades desempenhadas pelas Autoridade Nacional de Proteção de Dados.

---

[864] PECK, Patricia. Palestra proferida por Patricia Peck na Escola Superior do Tribunal de Contas do Estado de Mato Grosso, sobre o tema "**Impactos da LGPD para órgãos de controle**", em 23 de agosto de 2022.
[865] BRASIL. Autoridade Nacional de Proteção de Dados. **Ouvidoria em números**. Disponível em: https://app.powerbi.com/view?r=eyJrIjoiMjJmZTFiYjQtZjVmYy00MjRkLWJlNzYtN2JhY2E1MjUxZDAwIiwidCI6IjFjYzNjNTA4LTAxYzctNDQ2MC1iZDJiLWFmZTk1ZTgwYjhhZiJ9&pageName=ReportSectionf292577b6e0ea006d936. Acesso em: 23 nov. 2022.

Aliás, especificamente no setor público, o Conselho Nacional de Justiça (CNJ) tem boas-práticas relacionadas à conferência de selos de produtividade, contribuindo para o melhor desempenho do Poder Judiciário nacional, conhecidamente abarrotado.

Assim, os órgãos do Poder Judiciário são inspecionados e classificados segundo diversos critérios de qualidade que representam seu desempenho em diversos fatores previamente estabelecido pelo Conselho, que, mais tarde, os fiscaliza, atribuindo um selo de identidade visual que qualifica o respectivo Tribunal frente à qualidade de sua prestação jurisdicional.[866]

Igualmente, os selos são amplamente utilizados em relação à certificação de produtos ambiental e socialmente sustentáveis, como dá conta a dissertação de Fernanda Brandão Cançado,[867] e como bem apontado pelas Diretrizes n.º 1/2018 do Comitê Europeu para a Proteção de Dados[868] e pelo trabalho de Felipe Melazzo do Nascimento Santos,[869] tem o potencial de serem aplicados à proteção de dados pessoais.

Ademais a ideia de utilização dos processos de certificação, selos e marcas é estimular o *compliance* ativo (e não apenas o passivo, por meio de denúncias) propiciando uma forma de identificação de fácil acesso ao titular de dados de que determinado processo, produto ou atividade têm garantias de adotar as melhores práticas em matéria de proteção de dados pessoais.

Outra vantagem dos selos, marcas e processos de certificação é vista por Acquisti e Grossklags[870] que, em 2005, aplicaram uma pesquisa sobre atitudes e comportamentos de privacidade individual. Na ocasião eles descobriram que vários dos participantes da pesquisa combinaram questões de segurança e privacidade quando relataram a sensação de que sua privacidade estava protegida por comerciantes que ofereciam conexões SLL

---

866 BRASIL. Conselho Nacional de Justiça. **Selo Justiça em Números**. Disponível em: https://www.cnj.jus.br/pesquisas-judiciarias/selo-justica-em-numeros/. Acesso em: 15 set. 2022.

867 CANÇADO, Fernanda Brandão. **A criação de selos sociais como um mecanismo alternativo para o combate do trabalho escravo contemporâneo na cadeia produtiva da carne bovina mato-grossense**. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal de Mato Grosso, p. 161. 2020.

868 UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022. A análise que se seguirá terá por base as citadas diretrizes.

869 SANTOS. Felipe Melazzo do Nascimento**. Nudges e os tratamentos de dados pessoais autorizados pelo consentimento: proposta de matriz de análise a partir da investigação empírica em startups da Região dos Inconfidentes**. Dissertação (Mestrado em Direito) – Escola de Direito, Turismo e Museologia, da Universidade Federal de Ouro Preto, p. 176, 2022.

870 ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and Rationality in Individual Decision Making. **IEEE Security & Privacy**. 2005, v. 2., n. 1, p. 26-33. Disponível em: http://doi.org/10.1109/MSP.2005.22. Acesso em: 15 set. 2022.

para concluir pagamentos online. Da mesma forma, quando havia uma política de privacidade (códigos de condutas), os usuários se sentiam mais seguros, independentemente de seu conteúdo. Além disso, se um site possuía um selo de segurança, as pessoas tendiam a interpretá-lo como confiável.

Um exemplo bastante interessante sobre a utilização de sinais visuais para a modificação de comportamentos e o estabelecimento de certos padrões comportamentais é fornecido por Thaler e Sunstein.[871] Os autores analisam um exemplo americano sobre a redução no consumo de energia, que, em nossa perspectiva teria um efeito semelhante na seara da privacidade e proteção de dados pessoais.

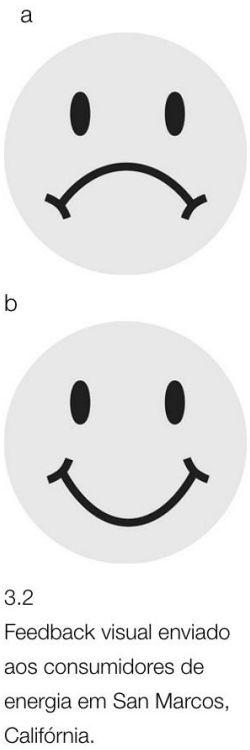
Os autores narram que 300 casas em San Marcos, Califórnia receberam a informação de quanta energia tinham gastado nas semanas anteriores. Receberam, ainda, a informação precisa do consumo médio de energia nas demais casas de seu bairro. O resultado foi que, nas semanas seguintes, os moradores que consumiam acima da média reduziram bastante seu consumo, em decorrência de um *nudge* social – as pessoas tendem a se comportar como o grupo (os autores avaliam decisões colegiadas para ilustrar isso); enquanto os que estavam abaixo da média passaram a consumir mais ("efeito bumerangue" – "se você deseja orientar as pessoas a apresentar comportamentos socialmente desejáveis, nunca deixe que elas saibam que já estão se comportando melhor do que a norma social").[872]

No entanto, quando a informação precisa foi substituída um sinal visual, o resultado mudou.

Conforme descrevem os autos, uma parte dos lares recebeu na conta de luz não só informações descritivas, **como também um sinal não verbal aprovando ou desaprovando seu consumo**. Para ser mais específico, a conta de luz das casas que consumiam mais do que a média chegava com um emoticon triste (figura 9a), enquanto a das que consumiam menos que a média chegava com um emoticon feliz (figura 9b), conforme figuras abaixo.

[871] THALER, Richard H.; SUNSTEIN, Cass R. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Rio de Janeiro: Objetiva, 2019. Edição do Kindle. p. 103.
[872] THALER, Richard H.; SUNSTEIN, Cass R.. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Rio de Janeiro: Objetiva, 2019. Edição do Kindle. p. 104.

Figura 9 - Nudge visual



3.2
Feedback visual enviado aos consumidores de energia em San Marcos, Califórnia.

Fonte: THALER, Richard H.; SUNSTEIN, Cass R. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Rio de Janeiro: Objetiva, 2019. Edição do Kindle. p. 105.

O resultado foi significativo, mas não surpreendente. Os grandes consumidores de energia mostraram uma redução ainda maior quando recebiam o emoticon descontente na conta, porém a maior descoberta foi que os moradores que estavam abaixo da média de consumo não passaram a consumir mais ao receber a conta com o emoticon sorridente: ou seja, o efeito bumerangue desapareceu por completo.

Quando meramente informados de que consumiam menos que a média, os consumidores achavam que tinham margem para aumentar, mas quando a informação foi combinada com um *nudge* emocional, eles não sentiram necessidade de mudar seus hábitos.

Esse experimento demonstra a usabilidade de sinais visuais representados pelos selos e marcas, que poderiam ser inseridos tanto em sítios eletrônicos quanto em lojas de apps, e facilmente verificáveis por QR codes. Esses selos e marcas seriam capazes de informar aos titulares de dados onde encontrariam ambientes de navegação e negócios mais seguros, estimulando uma cultura de proteção de dados, bem como uma adequação dos atores privados à LGPD.

A utilização de *nudges* para essa tarefa parece a forma de intervenção menos radical. Isso porque, por sua natureza, os *nudges* são pequenos incentivos capazes de influir em uma arquitetura de decisão, promovendo um efeito desejado.[873] Nesse sentido, Thaler e Sunstein demonstram que por mais que as teorias econômicas apregoem um mercado inteligente que se autorregule e pessoas que consegue lidar com essas informações para se comportar de maneira eficiente; em verdade, muitos de nós não agimos de maneira otimizada, o tempo todo, em nossa vida, ao contrário, somos emotivos, nos deixamos influenciar perceptível ou imperceptivelmente por outras pessoas, dados e informações; agimos por impulso; enfim, somos pessoas reais.[874]

Muito disso ocorre porque, em diversas decisões que tomamos, agimos utilizando um sistema automático de respostas, que apesar de muito rápido e eficiente energeticamente, não é capaz de grandes esforços racionais.

Esse sistema, desenvolvido como um mecanismo de resposta rápida, permitiu que pudéssemos sobreviver em ambientes hostis. Baer[875] explica que nossos cérebros, apesar de constituírem apenas 2% de nossos pesos corporais, representam cerca de 20% de nosso gasto energético. Ele explica, assim como Thaler e Sunstein,[876] que possuímos dois sistemas básicos de respostas: um sistema automático e outro racional. O primeiro apesar de rápido e eficiente energicamente, não é capaz de processar grandes informações. O segundo, ao contrário, é muito mais demorado e energeticamente ineficiente, mas é onde conseguimos realizar nossas maiores capacidades.

Baer[877] aponta que se utilizássemos o segundo sistema o tempo todo, para evitar toda espécie de erro ou engano (vieses heurísticos), necessitaríamos viver nos alimentando para suprir o gasto enérgico que o sistema racional demandaria.

Além disso, não seriamos capazes de fazer simplificações e agir com velocidade, em situações que assim exigissem. É considerando a existência desses dois sistemas que

---

[873] THALER, Richard H.; SUNSTEIN, Cass R. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Rio de Janeiro: Objetiva, 2019. Edição do Kindle. p. 11-12.

[874] Os autores chegam a fazer uma distinção entre o *homo economicus* (o ser racional e capaz de grandes cálculos e considerações em todos os aspectos da vida, descrito por economistas) e o *homo sapiens* (o ser humano real e que se deixa levar por emoções, vontades, desejos e outras variáveis que dissipam sua objetividade e racionalidade em certas ocasiões).

[875] BAER, Tobias. **Understand, Manage, and Prevent Algorithmic Bias**. Kaufbeuren: Apress, 2019, p. 10.

[876] THALER, Richard H.; SUNSTEIN, Cass R.. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Rio de Janeiro: Objetiva, 2019. Edição do Kindle. p. 103.

[877] BAER, Tobias. **Understand, Manage, and Prevent Algorithmic Bias**. Kaufbeuren: Apress, 2019, p. 10.

Thaler e Sunstein,[878] procuram analisar seus os efeitos em nossas decisões, descobrindo que somos influenciados por diversos vieses cognitivos e, até mesmo, por uma arquitetura de escolhas (pelo *design* que nos é apresentado, diante de uma decisão – como a disposição de frutas em uma vitrine – na qual as peças dispostas mais à frente têm uma tendência maior de serem escolhidas – ou no desincentivo que é o preenchimento de formulários ao invés de se estabelecer uma escolha por padrão).

São essas vaiáveis decisórias que os mecanismos regulatórios propostos procuram abordar. Isso porque, até mesmo os códigos de conduta, passam uma mensagem de maior segurança aos usuários, independentemente de seu conteúdo.

As experiências de Thaler e Sunstein,[879] têm sito vistas com seriedade pelos governos, tendo levado o Reino Unido à instalação do "*The Behavioural Insights Team*", conhecido popularmente como a "*Nudge Unit*" do governo britânico, que, estabelecida em 2010, pelo governo de David Cameron, busca aplicar a ciência comportamental à condução das políticas públicas do país.

Fruto de seu trabalho a *Nudge Unit* já apresentou dois relatórios práticos: o "*MINDSPACE: Influencing behaviour through public policy, that explores how behaviour change theory can help meet current policy challenges, such as how to: reduce crime; tackle obesity; ensure environmental sustainability*"; e o "Behavioural *Government: Using behavioural science to improve how governments make decisions. The report elected point how elected and unelected government officials are themselves influenced by the same heuristics and biases that they try to address in others. This report explores how this happens – and how these biases can be addressed or mitigated. To do this, it focuses on three core activities of policymaking: noticing, deliberating and executing*".[880]

Em resumo, o primeiro relatório trata da teoria do comportamento e como os governos podem explorá-la em políticas estratégicas, como redução da criminalidade, luta contra a obesidade e na busca da sustentabilidade ambiental. O segundo analisa os vieses heurísticos e cognitivos a estamos sujeitos (inclusive formuladores de políticas públicas),

---

[878] THALER, Richard H.; SUNSTEIN, Cass R.. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Rio de Janeiro: Objetiva, 2019. Edição do Kindle. p. 103.

[879] THALER, Richard H.; SUNSTEIN, Cass R.. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Rio de Janeiro: Objetiva, 2019. Edição do Kindle. p. 103.

[880] UK. United Kingdom. **Relatório Mindspace**. Disponível em: https://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf. Acesso em: 10 set. 2022. UK. United Kingdom. **Relatório Behavioural Government**. Disponível em: https://www.bi.team/wp-content/uploads/2018/08/BIT-Behavioural-Government-Report-2018.pdf. Acesso em: 10 set. 2022.

bem como formas de mitigá-los. Para isso, o trabalho foca em três atividades básicas dos processos de formulação de políticas públicas: perceber, deliberar e executar.

Essas experiência, aliadas aos ensinamentos de Thaler e Sunstein,[881] nos levam a crer que a adoção desses mecanismos teria aptidão de estimular o *compliance* com a legislação nacional em matéria de privacidade e proteção de dados, a criação de um ambiente fomentador da cultura de proteção de dados, ainda em desenvolvimento aqui.

3.3. Listas sujas

As listas sujas por sua vez, são instrumentos destinados à divulgação de incidentes de vazamento de dados, resultados de autuações, perda de certificações, selos e marcas, aplicação de multas e outras sanções envolvendo a atuação da Autoridade Nacional de Proteção de Dados.

As listas-sujas são comuns em áreas como o direito tributário,[882] no combate ao trabalho escravo[883] e na proteção contra a discriminação,[884] por exemplo, demonstrando certa semelhança, até mesmo quanto a seus efeitos, com os cadastros negativos de crédito.

Esses mecanismos, no entanto, são subutilizados na área da proteção de dados, não obstante alguns artigos científicos comecem a catalogar os incidentes de vazamento de dados ao redor do globo, provendo uma fonte de informação confiável sobre a periodicidade, quantidade, responsabilidades e desdobramentos desses incidentes.[885]

---

[881] THALER, Richard H.; SUNSTEIN, Cass R.. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Rio de Janeiro: Objetiva, 2019. Edição do Kindle. p. 103.

[882] Veja, por exemplo a lista de devedores ao fisco e à segurança social em Portugal, disponível em: https://www.portaldasfinancas.gov.pt/pt/menu.action?pai=100.

[883] A lista de empregadores que submeteram trabalhadores a condições análogas à de escravo, disponível em: https://www.gov.br/mdh/pt-br/navegue-por-temas/combate-ao-trabalho-escravo/cadastro-de-empregadores-201clista-suja201d e https://www.gov.br/trabalho-e-previdencia/pt-br/composicao/orgaos-especificos/secretaria-de-trabalho/inspecao/areas-de-atuacao/combate-ao-trabalho-escravo-e-analogo-ao-de-escravo.

[884] Visível tanto no direito europeu, quanto de seus estados-membros. Sendo exemplo a publicidade das sentenças condenatórias em matéria de discriminação contra a pessoa com deficiência, após o trânsito em julgado, às expensas dos responsáveis, em uma das publicações periódicas diárias de maior circulação do país (art. 7º, no 3), previsto da Lei nº 46/2006, de 28 de agosto, que proíbe e pune a discriminação em razão da deficiência e da existência de risco agravado de saúde. Ou, ainda, a disposição do Código do Trabalho Português de 12 de fevereiro de 2009, que prevê a publicidade da decisão condenatória (em matéria contra-ordenacional) consiste na inclusão em registo público, disponibilizado na página electrónica do serviço com competência inspetiva do ministério responsável pela área laboral, de um extrato com a caracterização da contra-ordenação, a norma violada, a identificação do infrator, o sector de atividade, o lugar da prática da infracção e a sanção aplicada (art. 562.º, n.º 3). A autoridade de controle portuguesa (Comissão Nacional de Proteção de Dados) já chegou a se manifestar sobre a possibilidade de aplicação desse tipo de punição, desde que o banco de dados criado não seja indexado a mecanismos gerais de buscas.

[885] Ver: NOVAES NETO, Nelson; et. al. Developing a Global Data Breach Database and the Challenges Encountered. **Journal of Data and Information** Quality, New York, v. 13, n. 1, 2021. ISSN: 19361963.

Não obstante, ainda que não se tenha notícia de um catálogo específico envolvendo um cadastro negativo (lista-suja) em matéria de privacidade e proteção de dados pessoais,[886] a LGPD (Lei Geral de Proteção de Dados), em seu artigo 48, lança as bases para que isso seja viável no futuro:

> **Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.**
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - os riscos relacionados ao incidente;
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
> **§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:**
> **I - ampla divulgação do fato em meios de comunicação; e**
> II - medidas para reverter ou mitigar os efeitos do incidente.
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

A possibilidade de divulgação dos incidentes de vazamento e das infrações aplicadas pela Autoridade Nacional de Proteção de Dados cumpre duas finalidades: a) alertar aos titulares sobre possíveis desdobramentos desses casos, nomeadamente, fraudes e roubo de identidade associados; e, b) permitir que o titular dos dados exerça ativamente sua autodeterminação informativa, avaliando a possibilidade de voltar ou não a utilizar de produtos ou serviços associados a tais casos de vazamentos.

A necessidade desse tipo de ferramenta decorre do imperativo de se pensar outras formas de promover a adesão dos responsáveis pelo tratamento de dados às diretrizes da LGPD, que não envolvam, sempre, a aplicação de multas.

DOI: 10.1145/3439873. Disponível em: https://dl.acm.org/doi/abs/10.1145/3439873. Acesso em: 7 maio. 2021.

[886] Diante das recente atualizações normativas e atitudinais adotadas pela Autoridade Nacional de Proteção de Dados Pessoais, em março de 2023, conferir o ANEXO XI, contendo as razões que nos levam a crer que ainda inexiste um cadastro negativo nos moldes que propomos.

Embora a sanção pecuniária seja relevante instrumento de sanção, tanto para agentes públicos quanto privados, ela deve ser muito bem ponderada, sob pena de trazer efeitos colaterais mais gravosos que os benefícios que visava prosseguir.

No caso de entidades públicas, por exemplo, se aplicada uma multa ao próprio ente federativo, ao fim e ao cabo, essa multa será paga por toda a coletividade. Já sob a perspectiva do agente privado uma multa desarrazoada pode trazer desequilíbrio financeiro à entidade.

Assim, no sistema dialógico que propomos os mecanismos de listagem cumpriria um papel importante de garantir adesão dos responsáveis por meio de uma política de *blaming and shaming*[887]. Enquanto os selos, marcas e processos de certificação representariam uma espécie de bônus aos atores que seguissem a LGPD, os mecanismos de listagem teria um efeito dissuasório em uma política de *sticks and carrots*[888].

A listas também serviriam de *input* na tomada de decisões pelos titulares de dados. Isso porque, como diagnosticam Thaler e Sunstein as pessoas "avaliam o risco de algo acontecer de acordo com a facilidade com que conseguem pensar na questão".[889] Assim, uma boa forma de aumentar o nível de preocupação é relembrar aos usuários os incidentes que tiveram consequências negativas, a partir de sua catalogação em listas sujas, alimentadas pela Autoridade Controladora, em decorrência de seus processos fiscalizatórios. Tendo em conta o viés da disponibilidade, essas pessoas serão capazes de melhor refletir sobre os riscos associados às operações de tratamento de dados, tomando atitudes mais responsáveis.

Vale ressaltar que as listas utilizam a mesma lógica das ferramentas de e-commerce, em que a reputação dos usuários e empresas exerce um forte papel regulatório. As listas permitiriam, assim, aumentar a probabilidade de que as pessoas tenham uma real percepção da importância de seus dados e os riscos em concretos associados a determinada empresa, sítio ou plataforma, contribuindo para uma cultura de proteção de dados pessoais.

---

[887] SKEEL, David A. Jr. Shaming in Corporate Law. **University of Pennsylvania Law Review**, vol. 149, n. 6, jun. 2001, p. 1811-1868. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/pnlr149&i=1823. Acesso em:12 nov. 2021.

[888] UNDERHILL, Kristen. When Extrinsic Incentives Displace Intrinsic Motivation: Designing Legal Carrots and Sticks to Confront the Challenge of Motivational Crowding-Out. **Yale Journal on Regulation**, vol. 33, n. 1, 2016, p. 213-280. HeinOnline. Disponivel em: https://heinonline.org/HOL/P?h=hein.journals/yjor33&i=215. Acesso em: 13 nov. 2021.

[889] THALER, Richard H.; SUNSTEIN, Cass R. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Rio de Janeiro: Objetiva, 2019. Edição do Kindle. p. 125. É por isso que a ocorrência de desastres naturais impulsiona a aquisição de apólices de seguros, por exemplo

No caminho oposto, a adequação dos listados a eventuais medidas mitigatórias impostas pela Autoridade Nacional de Proteção de Dados, possíveis de serem incluídas no sistema, incentivaria seu cumprimento, para que deixassem de ali constar.

Constituindo sanção, no entanto, o mecanismo dependeria de regulamentação pela Autoridade Nacional de Proteção de Dados (ANPD).

Desta forma, a lista suja fecharia o conjunto de mecanismos de incentivos (selos, marcas e processos de certificação) e desincentivos (listas sujas), para o cumprimento das regras estabelecidas dialogicamente, por meio dos códigos de condutas.

4. Vantagem competitiva e necessidade de pesquisas empíricas

Desde o princípio, buscamos discutir um modelo regulatório responsável, transparente e aberto à participação dos interessados, especialmente dos criadores de tecnologia, contemplando a inovação com responsabilidade, naquilo que o Professor Emérito de Direito Público da Universidade de Hamburgo, Wolfgang Hoffmann-Riem, defende como a "responsabilidade pela criação", explorando o papel não só do Estado, mas do mercado e dos desenvolvedores na busca de uma regulação mais aderente à realidade dos novos tempos.

Essa busca culminou em uma estratégia regulatória construída por meio do diálogo (o modelo sistemático-dialógico de regulação edificado a partir da utilização de códigos de condutas), complementada por mecanismos que incentivassem e desincentivassem comportamentos no ambiente virtual. Essa preocupação tem lugar, porque em se tratando da proteção de dados, muitas vezes, o dano, após surgido, é irreparável ou de difícil reparação, como nos ilustram os grandes vazamento de dados pessoais. Não há outras atitudes a serem tomadas pelos agentes reguladores ou atores privados capazes de retornar ao *status quo ante*. A partir da ocorrência do evento, somente medidas mitigadoras para o futuro podem ser adotadas.

É por isso que se faz tão necessário o incentivo a mecanismos que previnam o surgimento dos riscos associados à exploração dos dados pessoais por todos os atores (*stakeholders*) envolvidos na criação e utilização das novas tecnologias. Uma vez ocorrida a devassa de dados pessoais, é difícil expectar suas consequências e apresentar remédios à situação.

Nosso foco, desde o início, em trazer para perto o agente privado (que desenvolve suas atividades no mercado) tem a ver com o referencial teórico de Lawrence

Lessig de que a arquitetura do cyberespaço está ligada, em grande medida, à regulação através do código. Essa assertiva deixa antever que uma parte da regulação é feita pelos próprios particulares (empresas, plataformas, fabricantes etc.), ao embutirem regras e limitações no próprio código de seus produtos, serviços e plataformas.

É exemplo disso os mecanismos de "não me rastreie" para evitar a coleta informações destinadas a uma publicidade direcionada, os novos mecanismos de "retransmissão de IP" ou de "ocultar e-mail", implementados pela Apple. Mecanismos recentes que levam em conta uma tendência de mercado que começa a ser explorada: a busca por tecnologias que aumentem nossa privacidade e nos protejam da maior quantidade de riscos virtuais possíveis.

Essa tendência é vista como uma busca por uma vantagem competitiva e foi muito bem explorada por Maximilian von Grafenstein, no ensaio "*Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design*".[890]

O autor em seu brilhante ensaio analisa o estado da arte no que se refere à utilização dos códigos de conduta e mecanismos de certificação como formas de promover uma vantagem competitiva aos atores que aderirem à sua utilização.

Fundado em extensa literatura, o autor identifica que os códigos de conduta podem servir como um mecanismo eficaz para a promoção da segurança jurídica, na medida em que permitem delimitar as regras elásticas (de natureza principiológica) existentes na legislação de proteção de dados europeia.

Esse modelo de abordagem europeu (também reproduzido no Brasil), visa adaptar a legislação a diferentes situações e cenários decorrente da diversidade, multiplicidade e perene evolução tecnológica, que não permitiram modelos fechados de regulação, sob pena de se tornarem obsoletas ou irrelevantes com o tempo.

O autor também identifica que os processos de certificação, nos quais se incluem selos e marcas, também seriam aptos a promover uma vantagem competitiva, desde que a partir de sua construção se pudesse estabelecer níveis diferentes de conformidade (para ao que propõe a possibilidade de certificação por módulos), não sendo assim, os selos seriam capazes apenas de indicar a conformidade, sem efeitos competitivos. Ele aponta,

---

[890] GRAFENSTEIN, Maximilian von. **Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design**. Forthcoming in González-Fuster, G., van Brakel, R. and P. De Hert Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing. Disponível em: https://ssrn.com/abstract=3336990. Acesso em: 30 set. 2022.

ainda que os mecanismos de certificação, considerando a busca pelo "estado da arte" prevista no regulamento europeu, poderiam promover uma busca pela adequação às normas de proteção de dados, estimulando, na área dos desenvolvedores de soluções tecnológicas, que estes produzam novas ferramentas capazes de aumentar os níveis de segurança e privacidade ofertados.

O trabalho buscou analisar se a promessa de que o RGPD seria capaz de promover uma vantagem competitiva àqueles que se adequarem a ele seria real ou não, chegando às seguintes conclusões:[891]

> As considerações anteriores abordaram em que condições a promessa política que o GDPR dá aos seus regulados de uma possível vantagem competitiva seria possível de ser aplicada na prática comercial. Integrando à equação conceitos de teorias evolutivas de mercado e pesquisas de empreendedorismo, o regulador é, pelo menos em princípio, capaz de fortalecer a concorrência no(s) mercado(s) de proteção de dados. A este respeito, os princípios jurídicos e os termos jurídicos gerais, como os requisitos de proteção de dados e *security-by-design*, combinados com instrumentos de corregulação, em particular, os mecanismos de certificação de proteção de dados e códigos de conduta, podem desempenhar um papel importante. A razão para isso é que em ambientes inovadores e dinâmicos, o regulador dificilmente consegue centralizar o conhecimento sobre os riscos específicos do contexto e, portanto, os instrumentos de proteção necessários. Princípios jurídicos e termos jurídicos amplos podem, portanto, ser instrumentos regulatórios apropriados, pois deixam aos destinatários da regulamentação espaço suficiente para explorar, de acordo com seu contexto específico, os riscos e, assim, a melhor solução para mitigá-los. Ao usar códigos de conduta e, mais ainda, mecanismos de certificação de proteção de dados, os controladores e processadores de dados podem transformar a imprecisão da lei em uma vantagem competitiva. Esses efeitos podem ser demonstrados em três níveis diferentes:
> No nível microeconômico, os controladores de dados e subcontratantes são capazes de aumentar a segurança jurídica especificando e padronizando princípios jurídicos e termos jurídicos amplos por meio desses instrumentos de corregulação. O aumento da segurança jurídica lhes oferece uma vantagem competitiva porque reduz a complexidade de seu processo empresarial. Esta função é inerente a ambos os instrumentos, ou seja, códigos de conduta e mecanismos de certificação de proteção de dados (e BCR [*Binding Corporate Rules*, ou regras corporativas vinculadas], de forma muito limitada). No entanto, a análise (...) mostrou que ambos os instrumentos aumentam a segurança jurídica, quanto mais detalhados eles especificam a lei; se apenas repetem o texto da lei, sua função de aumentar a segurança jurídica é

[891] GRAFENSTEIN, Maximilian von. **Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design**. Forthcoming in González-Fuster, G., van Brakel, R. and P. De Hert Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing. Disponível em: https://ssrn.com/abstract=3336990. Acesso em: 30 set. 2022.

nula. O incentivo dos controladores e processadores de dados para usar esses instrumentos legais varia de acordo com o que eles perdem ou ganham quando podem demonstrar o cumprimento da lei ou, vice-versa, quando se verifica que eles violam a lei. Quanto maiores forem os investimentos ou os lucros esperados, mais provável é que eles queiram garantir que estão em conformidade legal. A questão de como esses incentivos positivos e negativos (ganhar a confiança dos consumidores ou clientes comerciais versus receber uma multa) devem ser projetados para garantir que o potencial da função de aumento da segurança jurídica seja totalmente explorado também deve ser pesquisado empiricamente.

Ao contrário dos códigos de conduta, os mecanismos de certificação de proteção de dados também podem oferecer, pelo menos em princípio, uma vantagem competitiva em nível mesoeconômico. A razão para isso é que os controladores e processadores podem: primeiro, usar a imprecisão dos requisitos legais como uma oportunidade de negócios para oferecer a seus consumidores ou clientes comerciais um nível mais alto de proteção do que seus concorrentes (para que seus clientes e/ou consumidores paguem um preço mais alto ou comprem mais produtos desta qualidade superior). Se o GDPR permite tal função competitiva ou visa apenas a função de conformidade (ou seja, reduzir a segurança jurídica) é debatido na literatura jurídica. Independentemente do resultado desse debate, a análise anterior mostrou que são poucos os casos em que tal função competitiva pode se tornar relevante. Em primeiro lugar, a questão só se torna relevante se existir (1) uma operação de tratamento específica com (2) um risco especificamente definido e (3) diferentes salvaguardas conduzindo, de fato, a um nível de proteção superior ou inferior. Dada a multiplicidade de operações de processamento e riscos diferentes (se os riscos são realmente diferentes ou apenas maiores ou menores), a maioria dos mecanismos de certificação de proteção de dados não sinaliza um nível de proteção maior ou menor, mas simplesmente se refere a um outro caso (incomparável). Em segundo lugar, mesmo que duas (ou mais) operações de processamento específicas criem o mesmo risco e assim, as salvaguardas possam fornecer um nível de proteção maior ou menor (o que pode ser sinalizado por um mecanismo de certificação de proteção de dados), há outro mecanismo legal que limita a vantagem competitiva potencial dessa situação. Esse mecanismo legal é o "estado da arte" – requisito do art. 25 e 32 GDPR, que obriga os controladores de dados e, em alguns casos, os processadores, a estar constantemente na mesma página que o novo nível de proteção mais alto oferecido no mercado (ou pelo menos "levá-lo em consideração"). Portanto, há apenas uma pequena margem de manobra em que diferentes níveis de proteção se tornam relevantes. Tal limitação à variedade de mecanismos de certificação de proteção de dados no mercado pode não ser o pior resultado, pois já é bastante difícil sinalizar um nível específico de proteção de uma operação de tratamento específica para o titular dos dados, para que ele entenda corretamente. Como isso, no final das contas, o que deve ser feito não pode ser respondido apenas por especialistas jurídicos e técnicos, mas, também, por meio do design da experiência do usuário.

O requisito de "estado da arte" previsto no art. 25 e 32 GDPR é outro fator que pode impulsionar a inovação mesmo no nível macroeconômico. Essa exigência pode potencializar a inovação se as empresas especializadas focarem no desenvolvimento do "estado da

arte" e o colocarem como sua proposta de valor central para os demais destinatários "normais" da regulamentação. Estas entidades especializadas podem utilizar a exigência como uma oportunidade de negócio que se renova constantemente, pressionando outros destinatários da regulação a implementar (e comprar) o "estado da arte", que eles mesmos estão desenvolvendo e aprimorando repetidamente. Se este mecanismo criar um mercado dinâmico para soluções de proteção de dados por design, pode ser bastante difícil para controladores de dados e processadores verem qual é atualmente o "estado da arte" de uma solução contra um risco específico causado por uma determinada operação de processamento de dados. A este respeito, os organismos de certificação (e DPA) podem desempenhar um papel importante. Se um mecanismo de certificação oferecido por esses órgãos tiver que provar, de acordo com seus critérios, atendimento ao requisito "estado da arte", e possivelmente não apenas no momento em que o certificado, selo ou marca é emitido, mas também durante todo o período em que está em uso, o organismo de certificação pode monitorar constantemente o mercado do "estado da arte" e reavaliar frequentemente se o responsável pelo tratamento de dados ainda o cumpre ou não. Tal função dos mecanismos de certificação de proteção de dados pode ser um benefício importante e, portanto, um incentivo para os controladores de dados usarem esses mecanismos de certificação porque reduzem a complexidade para cumprir a norma.

No entanto, isso não significa que o processo pelo qual os controladores de dados e processadores devem passar para certificar uma ou mais de suas operações de processamento não são complexos. O legislador viu claramente que a complexidade dos mecanismos de certificação pode conflitar com as necessidades das micro, pequenas e médias empresas devido aos seus recursos limitados [e estabeleceu a necessidade de se considerar essas necessidades]. Uma maneira de reduzir essa complexidade é limitar o escopo de um mecanismo de certificação de proteção, promover ajudas financeiras ou reduzir a profundidade de como o cumprimento dos critérios de tal mecanismo são controlados. Por exemplo, se um controlador de dados pode escolher um mecanismo de certificação que aborda apenas um risco específico para uma determinada operação de processamento dos quais o controlador pensa que seu nível de proteção é mais relevante para ser sinalizado no mercado, a complexidade processual limita-se a este caso particular. Ao contrário, o procedimento e a complexidade aumentam quanto mais operações de processamento de dados e mais riscos o mecanismo de certificação visa cobrir. Para encontrar um equilíbrio entre dimensionar os mecanismos e reduzir sua complexidade, estes podem ser modularizados para que os controladores e processadores de dados possam começar com um módulo que cobre um risco específico de uma determinada operação, adicionando mais módulos passo a passo, expandindo para novos riscos e outras operações. Como tal mecanismo modularizado deve ser projetado para que os titulares de dados possam realmente entender qual risco, de qual operação de processamento, o módulo especificado na certificação de proteção de dados cobre, depende não apenas de conhecimento jurídico e técnico, mas também de pesquisa no campo do design de experiência do usuário.

Finalmente, do ponto de vista dos titulares dos dados, o grau de complexidade dos dados mecanismos de certificação de proteção também é relevante. As considerações anteriores mostraram que o sucesso de mercado de tais mecanismos depende de os titulares dos

> dados poderem realmente entender qual mecanismo sinaliza qual nível de proteção para qual operação de processamento. Para os titulares de dados, esta é uma questão já muito complexa, e tanto mais válida quanto mais mecanismos de certificação são oferecidos no mercado mais complexo se torna. Uma solução para reduzir essa complexidade é reduzir o número de mecanismos de certificação. A este respeito, o Selo Europeu de Proteção de Dados pode ser crucial, uma vez que este mecanismo harmoniza os critérios segundo os quais os mecanismos nacionais de certificação são emitidos para responsáveis pelo tratamento e subcontratantes. No entanto, esse mecanismo não deve levar à situação em que a criatividade do mercado perca sua capacidade de reagir rápida e eficazmente a riscos recém-descobertos ou mesmo a operações desconhecidas. Esta situação pode ser evitada se os Selos Europeus de Proteção de Dados forem suficientemente específicos, ou seja, não se basearem em critérios abstratos-gerais, mas se referirem a riscos específicos de determinadas operações de tratamento. Isso, de fato, coloca as mesmas questões de antes.
> Afinal, essas são apenas algumas das questões que restam; e mesmo essas poucas perguntas mostram que a pesquisa sobre o impacto dos instrumentos regulatórios na inovação baseada em dados e na vantagem competitiva é uma questão bastante complexa. A complexidade requer a capacidade de um regulador aprender e, assim, frequentemente (re)avaliar e (re)adaptar seus instrumentos regulatórios de acordo com seus objetivos. Se bem-feito, essa abordagem pelo menos aumentará a racionalidade da lei, independentemente de a promessa política que o GDPR fornece para a vantagem competitiva se tornar verdadeira ou não.[892]

De nossa parte, consideramos salutar a tentativa da União Europeia de utilizar mecanismos de mercado para incentivar a adesão a padrões de tutela e salvaguarda definidos em suas normas sobre proteção de dados pessoais. Tais mecanismos geralmente funcionam em uma base de troca, sendo que os agentes que optarem por aderir a tais regras poderiam receber benefícios competitivos por isso.

O exemplo mais óbvio dessa política é justamente o sistema de certificação analisado, que permitiria às empresas utilizar certos certificados e selos de qualidade quando seja constatado o cumprimento substancial das normas em vigor. No contexto atual, em que a privacidade ganha importância para o cidadão comum, a possibilidade de uma vantagem competitiva oferecida acabaria por criar interesses convergentes nas duas pontas da transação. Isso porque, proteger a privacidade do usuário acabaria por deixar de ser visto apenas como um custo para se tornar um diferencial competitivo e uma fonte

[892] Tradução do autor. Ver original em: GRAFENSTEIN, Maximilian von. **Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design**. Forthcoming in González-Fuster, G., van Brakel, R. and P. De Hert Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing. Disponível em: https://ssrn.com/abstract=3336990. Acesso em: 30 set. 2022.

de receitas diante de um possível incremento da procura por solução que propiciem aos usuários mais segurança e privacidade.[893]

Embora a análise mercadológica e os efeitos que esses mecanismos possam produzir em concreto seja um cenário complexo de se considerar em sua inteireza, demandando pesquisas empíricas quando estiverem em funcionamento, estamos certos de que uma abordagem regulatória híbrida e dialógica é a única capaz de lidar com a fragmentação da informação (e do poder), permitindo arranjos regulatórios que possam mitigar a complexidade e interdependência dos diversos fatores em considerações, na tentativa de evitar as exploradas falhas regulatórias do Estado e do mercado.

O modelo de regulação SDR que se propõe a ser sistemático (integrado e coeso) e dialógico (aberto à participação plural e democrática), com soluções bem engendradas na construção do diálogo coletivo (por meio dos códigos de conduta), de mecanismos de incentivo à conformação (selos, marcas, mecanismos de certificação) e desincentivo à infração (e listas sujas) nos parece cobrir um campo mais alargado de capacidades. Esse modelo, embora não esteja livre de erros e críticas, no entanto, parece explorar um potencial maior de mecanismos que, entre si, possam suprir necessidades, explorar aptidões e mitigar imperfeições.

Conquanto tenhamos nos debruçado à fundo sobre o cenário regulatório, reconhecemos que somente uma pesquisa empírica, caso essa espécie regulatória seja implementada, é que seria capaz de avaliar a utilidade prática do modelo.

Não obstante, parte do sistema (no que concerne aos códigos de conduta, mecanismos de certificação, selos e marcas) já estão se desenvolvendo, restando a integração ao sistemas de mecanismos de desincentivo como as listas sujas, cuja aplicabilidade na seara de proteção de dados ainda não é feita.

Assim, esperamos que a pesquisa possa contribuir com iniciativas executivas e regulamentares que possam incentivar a adoção do modelo proposto, que, desde sua concepção, teve em conta a abordagem de necessidades bastante práticas, apesar das limitações impostas, por se tratar de uma nova abordagem a conhecidos mecanismos regulatórios.

Em que pese o modelo teórico ser novo e faltar dados empíricos capazes de confirmar, na prática, sua efetividade, as soluções engendradas se desenvolvem a partir

[893] GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018, p. 85-109.

da experiência positiva de sua aplicação em outras áreas do conhecimento. A busca da pesquisa foi reinventar e reinterpretar instituto jurídicos-regulatórios já em uso, conferindo-lhes nova roupagens e capacidades (aptidões).

A inovação da pesquisa é justamente buscar a efetividades da regulação em matéria de privacidade e proteção de dados a partir de elementos já propostos, mas reinterpretados e aplicados em outros contextos, de forma sistêmica e coesa, ao invés de simplesmente propor um novo quadro legislativo, em um arcabouço jurídico tão dilatado quanto o nosso.

Espera-se que esse objetivo tenha sido cumprido, não obstante a necessidade de mais dados empíricos que possam comprovar a efetividade do modelo, caso posto em prática. Todavia, do ponto de vista teórico, o sistema de regulação apresenta aptidão de aplicação, já sendo estimulada a sua utilização, ainda que em parte, no contexto europeu.

Essa reconfiguração dos modelos em uso, para um novo modelo proposto, tem um ar de esperança em busca de um sistema plural, coeso e democrático de proteção da privacidade e dos dados pessoais de milhões de cidadãos. O objetivo de toda essa incursão foi oferecer novos horizontes à proteção de dados pessoais no Brasil de forma a se salvaguardar os direitos dos titulares de dados pessoais, sem que representem um obstáculo ao desenvolvimento tecnológico, na busca de uma sociedade digital livre, próspera e segura.

CONCLUSÃO

1. O objeto da tese circunscreve-se à utilização de mecanismos regulatórios de natureza híbrida na seara da privacidade e proteção de dados pessoais.

2. O problema por ela abordado é representado pela pergunta: “como se garantir um adequado grau de intervenção regulatória de modo a se conciliar a proteção de direitos fundamentais dos cidadãos, sem sufocar a capacidade atuação dos agentes privados, responsáveis, em grande medida pela inovação e pelo desenvolvimento em nossas sociedades?”.

3. Para investigar o tema analisou-se diferentes graus de intervenção do Estado na regulação da privacidade e da proteção de dados pessoais.

4. Em um primeiro momento abordou-se como os modelos produtivos se desenvolveram, desde a primeira revolução industrial até a indústria 4.0. Percebeu-se aí

os problemas gerados por formas de produzir que fogem ao controle estatal, por meio da inovação, acarretando, frequentemente, cenários de exploração de grupo mais vulneráveis, como os trabalhadores.

5. Na sequência, analisamos como o modelo produtivo se especializou na coleta e utilização de dados, especialmente de caráter pessoal, para: a) promover vantagens competitivas por meio da redução dos custos de produção (utilizando-se de um modelo de produção flexível e integrada globalmente); e b) para criar tendências e induzir comportamentos sobre os consumidores, a partir de modelos preditivos e da publicidade em massa ou direcionada.

6. Essas características da economia de dados introduziram o leitor às novas possibilidade de aplicação da tecnologia.

7. A partir disso, apontamos alguns conceitos e noções sobre o funcionamento dessas tecnologias, para ao final, abordarmos a miríade de riscos (e, também, alguns benefícios) criados por esse novo cenário tecnológico.

8. A primeira seção expôs a base factual da pesquisa, fornecendo elementos que permitissem compreender a gramática das novas tecnologias e demonstrasse os efeitos colaterais da ausência da regulação estatal.

9. A segunda parte teve o propósito de entender como a regulação do ciberespaço e, mais tarde, da proteção da privacidade e dos dados pessoais se consolidou.

10. Se a primeira parte demonstrou a necessidade da regulação, a segunda cumpriu a finalidade de desenvolver a história e teoria por trás dos modelos que se consolidaram na contemporaneidade. Buscou-se entender o estado da arte em matéria de privacidade e proteção de dados pessoais.

11. Assim, percebemos que apesar ter sido concebido como um espaço de liberdade, os desafios nascentes no ciberespaço logo demandaram que este fosse regulado. Abordamos, desse modo, as teorias de regulação do ciberespaço, que evoluíram (não sob concesso) de uma postura que refutavam qualquer espécie de regulação, para outras que percebiam que a própria internet (e seus serviços) embutiam no próprio código uma espécie de controle, de regulação – na medida em que só era possível se fazer aquilo que era permitido pelo código.

12. Chegou-se à percepção de que múltiplos fatores influenciam na regulação do ciberespaço. *Lessig* observou quatro desses fatores de constrangimento: a lei, as normas sociais, o mercado e a arquitetura do código. Isso rompeu com a ideia de absoluta

impossibilidade de regulação do meio virtual, para se começar a cogitar de modelos que, a partir desses quatro fatores, poderiam influenciar os comportamentos adotados na rede.

13. Além disso, diversas medidas de ordem técnica adotadas por países de viés mais autoritários vieram a desmontar a real possibilidade de se controlar a internet.

14. A percepção de que era possível regular o ciberespaço levou ao surgirem de diversos modelos que aplicavam em concreto um sistema normativo de regulação, por meio do direito.

15. Esses modelos que tutelavam a privacidade e a proteção e dados pessoais se organizaram de diferentes modos ao redor do globo, sendo expoentes desses arquétipos regulatórios os modelos europeu e o estadunidense.

16. Assim, a segunda parte do trabalho dedicou-se a estudar esses modelos e compará-los, abordando, ainda, o modelo uruguaio (com uma abordagem mais fechada) e o brasileiro, objeto de nossas proposições.

17. Da análise dos modelos notou-se que o sistema americano (ex-colônia inglesa), possui um cariz mais liberal, percebendo os dados como um insumo produtivo (uma espécie de mercadoria), deixando às expensas do usuário decidir sobre o fornecimento ou não de seus dados a empresas e ao poder público. É dada uma tônica especial à capacidade do indivíduo de decidir sobre seus dados, conferindo-lhe ampla liberdade de negociá-los.

18. Eventuais abusos e desvios por parte dos utilizadores deveriam ser corrigidos pelo Poder Judiciário e, em alguns setores específicos, por agências reguladoras.

19. O modelo americano não apresenta uma lei geral de proteção de dados pessoais, tratando, tão somente, de forma setorial de algumas atividades que envolvem mais risco, como os dados relativos à saúde e o tratamento de dados relativos a crianças e adolescentes, por exemplo.

20. Esse modelo prestigia sobremaneira o vetor da liberdade, como é característico do Estado americano, muito provavelmente por seu histórico de ex-colônia.

21. O maior problema desse modelo é que o cidadão, as empresas e o poder público não se encontram em relações de igualdade, de modo que o consentimento no tratamento de dados pessoais do titular nem sempre é verdadeiramente livre e informado.

22. Além disso, a correção de desvios por meio do sistema judicial nem sempre oferece respostas rápidas e eficientes, relegando o titular de dados a um papel de submissão e vulnerabilidade.

23. O sistema europeu, por sua vez, apresenta um apanhado de estratégias regulatórias. Ele é encabeçado por uma lei geral, que busca, por meio de um viés mais principiológico, estabelecer diretrizes gerais aos agentes públicos e privados no momento de realizarem qualquer atividade de tratamento de dados pessoais.

24. O modelo, de matriz corregulatória, e intervenção *a posteriori*, baseia-se na ideia de mitigação de riscos, prevendo análises de impacto para atividade potencialmente perigosas e conferindo ao controlador ou encarregado de dados a adoção das salvaguardas previstas no regime jurídico-regulatório.

25. Esse agente controlador ou encarregado de dados deve, desse modo, promover a adequação da organização à disciplina do Regulamento Geral de Proteção de Dados Pessoais e, ainda, ser capaz de comprovar tal adequação à Autoridade de Controle.

26. A principal dificuldade do modelo europeu decorre de sua própria estrutura concentrada, que busca em uma Lei Geral a base para a resolução dos diferentes desafios tecnológicos que emergem, circunstância que já tem levado à necessidade de diversos outros regulamentos em matérias específicas (como a inteligência artificial, o *algorithmic trading*, as plataformas de intermediação de trabalho, e muitos outros casos) para abordar questões especificas e mais sensíveis.

27. De outra banda, a exposição do modelo uruguaio teve a finalidade de apresenta uma solução bastante centrada na autoridade pública pelo governo local. Como forma de tutelar os direitos dos usuários e procurar mitigar os riscos, o modelo uruguaio impôs o registro prévio de bancos de dados de maior conjuntura.

28. O modelo é o mais intervencionista e limitador da liberdade dos agentes regulados entre aqueles analisados. No entanto, os riscos emergentes na sociedade da informação obstam que o prévio registro tenham efeitos mais concretos, para além da mera especulação em relação aos riscos imediatamente considerados.

29. O modelo, ainda, relega ao judiciário grande parte do papel de tutelar os interesses dos usuários, por meio da figura do *habeas data*.

30. Por fim, o modelo brasileiro foi apresentado, de forma sucinta, haja visa sua inspiração no sistema europeu.

31. Nosso modelo, assim como o europeu, funda-se em uma Lei Geral de Proteção de Dados Pessoais (de matriz principiológica), assegurada por uma Autoridade de Controle com diversas prerrogativas.

32. No entanto, o modelo brasileiro se distanciou do europeu ao mitigar a independência da Autoridade de Controle (somente recentemente recobrando a

autonomia devida), e diminuindo a garantia do pedido de revisão, por um humano, das decisões tomadas por meios automatizados.

33. Ademais, em virtude de nossa forte cultura litigiosa, é expectável um forte papel do judiciário na concretização das salvaguardas disciplinadas pela Lei, não obstante a atuação da Autoridade Reguladora esteja em expansão.[894]

34. Alfim, a terceira parte incumbiu-se fazer o contraponto à primeira seção da pesquisa, apresentando as diversas dificuldade de uma regulação centralizadora na figura do Estado.

35. Entre essas dificuldades destacou-se a ideia de que, em se tratando do ciberespaço, as relações entre os atores são complexas e fragmentadas, de modo que nenhum ator social, seja o Estado ou os agentes privados seria capaz de deter todo o conhecimento e capacidades necessárias para regular esse ambiente.

36. Além disso, o Estado lida, inevitavelmente, com recursos escassos, o que, frente às diversas atividades que lhe cabe regular (e diante da própria complexidade do ato regulatório), tende a tornar-se ineficiente e custoso.

37. A partir disso, destacamos o surgimento de novas teorias, como o *Estado Pós-Regulatório,* a *Descentralização Administrativa,* o *Direito Administrativo Global*, o *Constitucionalismo Global,* e o *Renew Deal*, que propagam a conciliação de teorias contrárias, em um processo de hibridização da marcha regulatória, por meio da partição do Estado e de representes do mercado (agentes privados).

38. Essas teorias serviram de substrato para a proposição do nosso modelo regulatório, intitulado de modelo de "regulação sistemático-dialógico" (*systematic-dialogical regulation - SDR*).

39. O modelo proposto baseia-se na ideia de formação de um sistema aberto de interação entre atores estatais e não estatais, possível por meio da produção de códigos de conduta (setoriais ou não), integrados por mecanismos de estímulo à *compliance* (*e.g.* por meio de selos, marcas e processos de certificações – *seals, stamps and certification processes*) e de desestímulo a condutas incompatíveis com o sistema regulatório (*e.g.* listas-sujas – *black lists*).

40. Embora todos esses instrumentos sejam previstos de algum modo no modelo regulatório brasileiro, não são visto de modo integrado, possuindo uma restrita aplicação aos casos de transferências internacionais de dados, não obstante seu potencial

[894] 29. Uma avaliação mais profunda dos instrumentos de proteção de dados apresentados pela legislação brasileira foi postergada para a última parte

de aplicação também nas relações internas, como reconhece a União Europeia em suas Diretrizes nº 1/2019 relativas aos Códigos de Conduta e Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679.

41. O modelo é pensado justamente com a ideia de se conceber um regime conciliatório, capaz de promover as adaptações necessárias para amalgamar diferentes potencialidades contra um amplo conjunto de riscos regulatórios, na busca de uma integração hábil a estimular o aprendizado, a adaptação e a melhoria entre os diversos mecanismos de intervenção e arenas de debate.

42. Esse sistema funcionaria a partir de um *core* (núcleo) representado pelos códigos de conduta, capaz de promover o diálogo democrático entre os atores envolvidos em todo o processo de regulação, especialmente os desenvolvedores de tecnologia, empresas e o próprio Estado.

43. Esse modelo permitiria um fórum de debate hábil à participação dos diversos *stakeholders* na formulação de um política de privacidade e proteção de dados pessoais mais justa e democrática.

44. Com isso em mente, o trabalho apresenta o funcionamento dos três mecanismos de tutela, tendo por base a experiência europeia, que se encontram em fase mais avançada de desenvolvimento. O terceiro capítulo da parte final do trabalho, portanto, analisa o funcionamento pormenorizado dos mecanismos, na Europa e sua possibilidade de aplicação no Brasil.

45. Tal análise demonstra que tanto os códigos de conduta, quanto os mecanismos de certificação, selos e marcas de proteção de dados, são abordados de forma muito restrita na legislação nacional.

46. É curioso notar que, embora os códigos de conduta e mecanismos de certificação (incluindo selos e marcas) sejam adotados para as transferências internacionais (isto é às vistas da comunidade internacional), são ignorados ou restringidos pela legislação nacional quando se trata de sua utilização internamente, não obstante, o Brasil represente um mercado de considerável proporções.

47. Como exemplo disso, destacamos a extensão da arena regulatória brasileira no que se refere ao Poder Público, perfazendo bem mais de cinco mil entidades a serem fiscalizadas pela Autoridade Nacional de Proteção de Dados.

48. Em relação às listas sujas pontuamos que a legislação brasileira dá indícios da possibilidade de sua adoção, por meio do artigo 48, §2º, inciso I, que permite a

divulgação de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares.

49. Tal iniciativa cumpriria a função de: a) alertar aos titulares sobre possíveis desdobramentos desses casos, nomeadamente, fraudes e roubo de identidade associados; e, b) permitir que estes exerçam ativamente sua autodeterminação informativa, avaliando a possibilidade de voltar ou não a utilizar os produtos ou serviços associados a tais casos de vazamentos.

50. Essa possibilidade de divulgação de incidentes de proteção de dados pessoais pode ser vista como um embrião para a futura criação de um cadastro ou lista destinado à divulgação de incidentes de vazamento de dados, resultados de autuações, procedimentos de perda de certificação, autos de infração e aplicação de multas, entre outras sanções envolvendo a atuação da Autoridade Nacional de Proteção de Dados.

51. Tal mecanismo baseado em uma política de *blaming and shaming* serviriam de *input* na tomada de decisões pelos titulares de dados. Isso porque, como diagnosticam Thaler e Sunstein as pessoas "avaliam o risco de algo acontecer de acordo com a facilidade com que conseguem pensar na questão". [895] Logo, uma boa forma de aumentar o nível de preocupação é lembrar aos usuários os incidentes que tiveram consequências negativas, a partir de sua catalogação em listas-sujas, alimentadas pela Autoridade de Controle, em decorrência de seus processos fiscalizatórios. Tendo em vista o viés da disponibilidade, esses indivíduos seriam capazes de melhor refletir sobre os riscos associados às operações de tratamento de dados, tomando atitudes mais responsáveis.

52. De outro lado, os processos de certificação já foram objeto de avaliação do grupo de trabalho do artigo 29, da União Europeia que concluiu por sua importância no quadro de responsabilização da União (Grupo de Trabalho do artigo 29.º, Parecer 3/2010 sobre o princípio da responsabilidade, WP173, 13 de julho de 2010, pontos 69-71).

53. Esses mecanismos possibilitam, sobretudo, a descentralização de parte da atividade fiscalizatória, além de fornecer um sinal claro ao titular de dados a respeito do nível de proteção de determinado produto ou serviço.

---

[895] THALER, Richard H.; SUNSTEIN, Cass R. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Rio de Janeiro: Objetiva, 2019. Edição do Kindle. p. 125. É por isso que a ocorrência de desastres naturais impulsiona a aquisição de apólices de seguros, por exemplo

54. Outra vantagem dos selos, marcas e processos de certificação foi notada por Acquisti e Grossklags[896] que, em 2005, aplicaram uma pesquisa sobre atitudes e comportamentos de privacidade individual. Eles descobriram que vários participantes combinaram questões de segurança e privacidade quando relataram a sensação de que sua privacidade estava protegida por comerciantes que ofereciam conexões SLL para concluir pagamentos on-line. Da mesma forma, quando havia uma política de privacidade (como podem ser interpretados os códigos de condutas), os usuários se sentiam mais seguros, independentemente de seu conteúdo. Além disso, se um site possuía um selo de segurança, as pessoas tendiam a interpretá-lo como confiável.

55. Novamente recorrendo a Thaler e Sunstein apontamos o impacto dos signos visuais na tomada de decisões individuais, ressaltando que tais signos funcionam como *nudges* que nos estimulam à tomadas de certas decisões, dentro de uma arquitetura de escolhas.

56. Apontamos, desse modo, como os selos e marcas seriam capazes de informar aos titulares de dados sobre onde encontrariam ambientes de navegação e negócios mais seguros, estimulando uma cultura de proteção de dados, bem como uma adequação dos atores privados à LGPD.

57. Ressaltamos que efeitos semelhantes ocorreriam com as listagens, que utilizam a mesma lógica das ferramentas de e-commerce, nas quais a reputação dos usuários e empresas exerce um forte papel regulatório. As listas ou cadastros permitiriam, assim, aumentar a probabilidade de que as pessoas tenham uma real percepção da importância de seus dados e os riscos em concretos associados a determinada empresa, sítio ou plataforma, contribuindo, também, para uma cultura de proteção de dados pessoais.

58. De tal modo, enquanto os selos, marcas e processos de certificação representariam uma espécie de bônus aos atores que seguissem a LGPD, os mecanismos de listagem teria um efeito dissuasório, em uma espécie de política de *sticks and carrots*.

59. Isso tudo permitiria um sistema integrado de controle, o modelo de regulação *SDR* que se propõe ser sistemático (por ser integrado e coeso) e dialógico (aberto à participação plural), com soluções bem engendradas na construção do diálogo coletivo (por meio dos códigos de conduta), na presença de mecanismos de incentivo à

[896] ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and Rationality in Individual Decision Making. **IEEE Security & Privacy**. 2005, v. 2., n. 1, p. 26-33. Disponível em: http://doi.org/10.1109/MSP.2005.22. Acesso em: 15 set. 2022.

conformação (selos, marcas, mecanismos de certificação) e de desincentivo à infração (e listas sujas) que nos parece cobrir um campo mais alargado de capacidades e potencialidades do que uma solução individual, centrada no mercado ou no Estado.

60. Analisamos, na sequência, o potencial efeito dos códigos de conduta e mecanismos de certificação (incluindo selos e marcas de proteção de dados pessoais), como vantagem competitiva.

61. Nessa seção apontamos o trabalho de Maximilian von Grafenstein que encontra nos códigos de conduta e mecanismos de certificação a possibilidade de se diminuir incertezas e inseguranças na aplicação da Lei. O trabalho sugere, ainda, a aptidão desses elementos de promover um incremento na competição e na busca de soluções tecnológicas inovadoras.

62. Não obstante, também são relatadas algumas dificuldades relativas à criação de selos e mecanismos de certificação, sobretudo na hipótese de não se conseguir demonstrar níveis diferentes de certificação (fator que representa uma vantagem competitiva) e a possibilidade de que o mercado de organismos certificadores se expanda de tal modo a dificultar a tarefa do titular de dados de perceber o que exatamente um selo certifica, por sua pluralidade e extensão.

63. Não obstante, concluímos que enquanto um sistema integrado o modelo dialógico tem a aptidão de fomentar uma cultura de proteção de dados pessoais em diferentes níveis; de repartir responsabilidade entre atores públicos e privados (gerando, inclusive, diminuição de custos, em alguns cenários); e de promover um modelo de diálogo mais abrange e menos propenso a cair em erros comuns de cenários regulatórios exclusivamente estatais ou, tão somente, autorregulatórios.

64. Não obstante, como modelo a ser (não implementado), entendemos a limitação da pesquisa, que carece de novas investigações empíricas capazes de abordar os efeitos práticos do sistema no mercado e na atitude dos titulares de dados.

65. Contudo, do ponto de vista teórico, as muitas ideias que sustentam o modelo proposto parecem de todo coesas, de forma que esperamos poder contribuir para o oferecimento de novos horizontes à proteção de dados pessoais no Brasil na salvaguarda dos direitos fundamentais dos titulares de dados pessoais à privacidade e proteção de dados pessoais, sem que a regulação represente um obstáculo ao desenvolvimento tecnológico, na busca de uma sociedade digital livre, próspera e segura.

REFERÊNCIAS

ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and Rationality in Individual Decision Making. **IEEE Security & Privacy**. 2005, v. 2., n. 1, p. 26-33. Disponível em: http://doi.org/10.1109/MSP.2005.22. Acesso em: 15 set. 2022.

AFFELT, Amy. Big Data, Big Opportunity. **Australian Law Librarian**, vol. 21, n. 2, 2013, p. 78-89. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/auslwlib21&i=86. Acesso em: 21 nov. 2021.

AGREL, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge, **Harvard Journal of Law & Technology**, v. 11, n. 3, Summer 1998, p. 871-880.

ALBRECHT, Jan Philipp. **Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung**. Überblich und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog. CR, 2016.

ALCALÁ, Humberto Nogueira. Autodeterminación informativa y hábeas data en Chile e información comparative. **Anuário de Derecho Constitucional Latinoamericano** 2005, t. II, Konrad Adenauer Stiftung.

ALENCAR, A. R. V.; LEAL, C. R. F.; RODRIGUES, D. R. N.; GURGEL, I. A. P. **Novas configurações do trabalho no século XXI: como o ser humano se tornou um serviço na era da economia digital**. In: LEAL, Carla Reita Faria; MARANHÃO, Ney; PADILHA, Norma Sueli. (Org.). Sociedade, tecnologia e meio ambiente do trabalho: discussões contemporâneas. 1. ed. Cuiabá: EdUFMT, 2021.

ALENCAR, Antônio Raul Veloso de; LEAL, Carla Reita Faria. "Jobfishing": a expansão dos riscos aos candidatos a empregos na sociedade da informação. O livre. Disponível em: https://olivre.com.br/jobfishing-a-expansao-dos-riscos-aos-candidatos-a-empregos-na-sociedade-da-informacao. Acesso em: 12 maio 2022.

ALVES, Paula Ribeiro. Os desafios digitais no mercado segurador. In **Fintech: Desafios da Tecnologia Financeira**. 2ª ed. Coimbra: Almedina, 2019, p. 28-62.

ALVES, Paulo. Facebook e Cambridge Analytica: sete fatos que você precisa saber. **TechTudo**. São Paulo, 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/03/facebook-e-cambridge-analytica-sete-fatos-que-voce-precisa-saber.ghtml. Acesso em: 05 maio 2021.

ANTUNES, Luís Filipe Colaço. **O direito administrativo sem estado: crise ou fim de um paradigma?** Coimbra: Coimbra Editora, 2008; Administração Estado, ver: OTERO, Paulo. **Manual de Direito Administrativo** - vol. 1. Coimbra: Almedina, 2013.

ANTUNES, Luís. **Pôr em Prática o RGPD: o que muda para nós? E para as organizações?**. Lisboa: FCA, 2018.

ANTUNES, Ricardo. **Adeus ao trabalho?**: ensaio sobre as metamorfoses e a centralidade do mundo do trabalho. 15. ed. São Paulo: Cortez, 2011.

ARANHA, Márcio Iorio. ***Compliance*, governança e regulação**. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 437-452.

ARANHA, Márcio Iorio. ***Compliance*, governança e regulação**. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 437-452.

ASHTON, Kevin. That 'Internet of Things' Thing. **RFID Journal**, 2009. Disponível em: http://www.rfidjournal.com/articles/view?4986. Acesso em: 10 jun. 2021.

AUSTRÁLIA. Office of Regulation Review. **A Guide to Regulation**. 2. ed. Australia, 1998, p. B2. Disponível em: https://www.pc.gov.au/research/supporting/regulation-guide/reguide2.pdf. Acesso em: 23 set. 2022.

BALDWIN, Robert, CAVE, Martin e LODGE, Martin. **Understanding Regulation**, 2. ed. Oxford: Oxford University Press, 2012.

BAPTISTA, Patrícia Ferreira; RIBEIRO, Leonardo Coelho. **Direito administrativo global: uma nova ótica para a regulação financeira de investimentos**. *In:* RIBEIRO, Marilda Rosado Sá. Direito internacional dos investimentos. Rio de Janeiro: Renovar, 2014.

BARLOW, John Perry. **A Declaration of the Independence of Cyberspace**. Disponível em: https://www.eff.org/cyberspace-independence. Acesso em: 21 set. 2022.

BARLOW, John. Selling Wine Without Bottles: The Economy of Mind on the Global Net. **Duke Law & Technology Review**, Durham, v. 18, n. 1, 2019. ISSN: 2328-9600. Disponível em: https://scholarship.law.duke.edu/dltr/vol18/iss1/3. Acesso em: 3 maio. 2021.

BARRETT, Brian. Spotify clears up its controversial Privacy Policy. **Wired Online**. 2015. Disponível em: https://www.wired.com/2015/08/spotify-clears-up-its-privacy-policy/. Acesso em: 25 out. 2022.

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. São Paulo: Zahar, 2013.

BBB. Better Business Bureau. BBB **Study: Looking for a job? Be careful! Job scams increased during pandemic**. Disponível em: https://www.bbb.org/article/investigations/24596-bbb-investigation-job-scams. Acesso em: 12 maio 2022.

BBC. **Como 52 pessoas foram enganadas para trabalhar em agência falsa de design**. Disponível em: https://www.bbc.com/portuguese/internacional-60477755. Acesso em: 12 maio 2022.

BECK, Ulrich. **Sociedade de Risco**. NASCIMENTO, Sebastião (trad.). São Paulo: Editora 34, 2010.

BENKLER, Yochai. Freedom in the commons: Towards a political economy of information. **Duke Law Journal**. v. 52, p. 1245-1276, 2002.
BENKLER, Yochai. **The Penguin and the Leviathan: How Cooperation Triumphs over Self-Interest**. New York: Crown Business, 2011.

BENKLER, Yochai. **The Wealth of Networks: How Social Production Transforms Markets and Freedom**. New Haven: Yale University Press, 2006. Disponível em: http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf. Acesso em: 25 set. 2022.

BERTRAND, Marianne; MULLAINATHAN, Sendhil. **Are Emily and Greg More Employable than Lakisha and Jamal?**: A Field Experiment on Labor Market Discrimination. 2003. Disponível em: URL: https://doi.org/10.4324/9780429499821-53. Acesso em: 15 jun. 2022.

BIANCHI, José Flavio. **A ICANN entre governança e Regulação: análise da atuação regulatória da ICANN nos programas de expansão dos gTLDs no Sistema de Nomes de Domínio (DNS) da Internet**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade Nacional de Brasília, p. 300. 2018.

BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: Transformações Político-Jurídicas, Econômicas e Institucionais do Direito Administrativo Ordenador**. Belo Horizonte: Fórum, 2016.

BLACK, Julia. Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. **Current Legal Problems**, v. 54, n. 1. Oxford: Oxford University Press, p. 103-146, 2001.

BOBBIO, Norberto. **Teoria do ordenamento jurídico**. São Paulo: Polis, 1989.

BOTTA, Marco; VIOLA, Mario. La protezione dei dati personali nelle relazioni tra UE e USA: le negoziazioni sui trasferimento dei PNR' (2010), **Diritto dell'informazione e dell'informatica**, v. 26, n. 2, 2010.

BOWER, Joseph L; CHRISTENSEN, Clayton M. Disruptive Technologies: Catching the Wave. **Harvard Business Review (HBR)**, 1995. Disponível em: https://hbr.org/1995/01/disruptive-technologies-catching-the-wave. Acesso em: 25 out. 2022.

BRAITHWAITE, J. **Regulatory Capitalism: How it Works, Ideas for Making it Work Better**. Cheltenham: Edward Elgar, 2008.

BRASIL. Autoridade Nacional de Proteção de Dados. **ANPD divulga lista de processos sancionatórios**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-sancionatorios. Acesso em: 23 mar. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Ouvidoria em números**. Disponível em: https://app.powerbi.com/view?r=eyJrIjoiMjJmZTFiYjQtZjVmYy00MjRkLWJlNzYtN2JhY2E1MjUxZDAwIiwidCI6IjFjYzNjNTA4LTAxYzctNDQ2MC1iZDJiLWFmZTk1Z

TgwYjhhZiJ9&pageName=ReportSectionf292577b6e0ea006d936. Acesso em: 23 nov. 2022.

BRASIL. Comitê Gestor da Internet no Brasil – CGI.br. **Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC Kids online Brasil 2015**. Núcleo de Informação e Coordenação do Ponto BR [editor]. São Paulo: Comitê Gestor da Internet no Brasil, 2016, p. 170. Disponível em: https://cetic.br/media/docs/publicacoes/2/TIC_Kids_2015_LIVRO_ELETRONICO.pdf. Acesso em: 10 out. 2021.

BRASIL. Conselho Nacional de Justiça. **Selo Justiça em Números**. Disponível em: https://www.cnj.jus.br/pesquisas-judiciarias/selo-justica-em-numeros/. Acesso em: 15 set. 2022.

BRASIL. Instituto Brasileiro de Geografia e Estatística – IBGE. **PNAD Contínua TIC 2019: internet chega a 82,7% dos domicílios do país**. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/30521-pnad-continua-tic-2019-internet-chega-a-82-7-dos-domicilios-do-pais. Acesso em: 5 out. 2021.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). **Lei 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 nov. 2022.

BUDD, J., MILLER, B.S., MANNING, E.M. et al. Digital technologies in the public-health response to COVID-19. **Nature Medicine**, n. 26, ago. p. 1183–1192, 2020. Disponível em: https://doi.org/10.1038/s41591-020-1011-4. Acesso em: 25 fev. 2022.

BUELENS, Jan; RIGAUX, Marc. (eds.). **From Social Competition to Social Dumping**. Antwerp and Portland: Intersentia (Cambridge Core), 2016.

CADWALLADR, Carole. The great British Brexit robbery: how our democracy was hijacked. **The Guardian**, 7 mai. 2017. Disponível em: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy. Acesso em: 14 set. 2022.

CALVÃO, Filipa Calvão. **O modelo de supervisão de tratamentos de dados pessoais na União Europeia: da atual diretiva ao futuro regulamento**, 2015. In: Revista Fórum de Proteção de Dados. n.1, p. 36-48, p. 42. Disponível em: https://www.cnpd.pt/media/owgnsrp2/forum_1_af_web_low.pdf. Acesso em: 15 nov. 2022.

CAMBRIDGE DICTIONARY. *Catfish*. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/catfish. Acesso em: 12 maio 2022

CANÇADO, Fernanda Brandão. **A criação de selos sociais como um mecanismo alternativo para o combate do trabalho escravo contemporâneo na cadeia produtiva da carne bovina mato-grossense**. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Federal de Mato Grosso, p. 161. 2020.

CARVALHO, Maria João; LOPES, Paulo Simões. **Da Privacidade à Proteção de Dados**, 2019. Disponível em: URL: https://www.uc.pt/protecao-de-dados/protecao-de-dados-pessoais/privacidade-e-protecao-dados/. Acesso em: 17 set. 2022.

CASE, Tony. WTF is jobfishing (and how to avoid it). **Worklife**. [s.l.], 2022. Disponível em: https://www.worklife.news/talent/wtf-is-jobfishing-and-how-to-avoid-it/. Acesso em: 25 jun. 2022.

CASEMINE. **Prince Albert v. Stange 64 ER 293 (1848)**. Disponível em: https://www.casemine.com/judgement/uk/5a8ff8d260d03e7f57ecdced#. Acesso em: 10 jul. 2022

CASTETS-RENARD, Céline. **Droit de l'internet: droit français et européen**. 2. ed. Paris: Montchrestien, 2012. p. 26.

CATOZZZO, Franceslly. **Estudo da OCDE sugere políticas públicas para compras voltadas ao desenvolvimento de uma Conduta Empresarial Responsável**, 2022. Disponível em: https://sollicita.com.br/Noticia/?p_idNoticia=18969&n=estudo-da-ocde-sugere-pol%C3%ADticas-p%C3%BAblicas-para-compras. Acesso em: 15 nov. 2022.

CDPC. **Convenção sobre os Direitos das Pessoas com Deficiência e seu Protocolo Facultativo**. Nova York, 2006. Disponível em: http://www.pcdlegal.com.br/convencaoonu/wp-content/themes/convencaoonu/downloads/ONU_Cartilha.pdf. Acesso em: 29 jun. 2022.

CFA. Conselho Federal de Administração. **Conheça as quatro Revoluções Industriais que moldaram a trajetória do mundo**. Disponível em: https://cfa.org.br/as-outras-revolucoes-industriais/. Acesso em: 19 outubro 2022.

CLARKE, Roger. Profiling: A Hidden Challenge to the Regulation of Data Surveillance. **Journal of Law and Information Science**, vol. 4, no. 2, 1993, p. 403-419. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/jlinfos4&i=405. Acesso em: 19 fev. 2022.

CNSAÚDE. Confederação Nacional de Saúde. **Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde**. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 10 nov. 2022.

COGLIANESE, Carry, MENDELSON, Evan. **Meta-Regulation and Self-Regulation**. In: BALDWIN, Robert, CAVE, Martin, LODGE, Martin. The Oxford Handbook of Regulation. Oxford: Oxford University Press, 2010, pp. 146-168, p. 147).

COHN, Cindy. **John Perry Barlow, Internet Pioneer, 1947-2018**. Disponível em: https://www.eff.org/deeplinks/2018/02/john-perry-barlow-internet-pioneer-1947-2018. acesso em: 21 set. 2022.

CONDORCET, Jean-Antoine-Nicolas de Caritat. **Esquisse d'un tableau historique des progrès de l'esprit humain**. Bibliothèque nationale de France. Disponível em: https://gallica.bnf.fr/ark:/12148/bpt6k281802. Acesso em: 22 ago. 2022.

CONESA, F. **Derecho a la intimidad, informática y Estado de Derecho**. Valencia: Universidad, 1984.

CONFESSORE, Nicholas. Cambridge Analytica and Facebook: the scandal and the fallout so far. **The New York Times**. New York, 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 05 maio 2021.

CORACCINI, Raphael. Fotos e até salários estão entre os dados vazados de 223 milhões de brasileiros. **CNN Brasil**. São Paulo, 2021. Disponível em: https://www.cnnbrasil.com.br/business/2021/01/27/fotos-e-ate-salarios-estao-entre-os-dados-vazados-de-223-milhoes-de-brasileiros. Acesso em: 05 maio 2021.

COSTA, Aline Moreira da; ALMEIDA, Victor Hugo de. Meio ambiente do trabalho: uma abordagem propedêutica. In: FELICIANO, Guilherme Guimarães et al. (Coord.). **Direito ambiental do trabalho**: apontamentos para uma teoria geral. São Paulo: LTr, v. 3, 2017.

COUTINHO, Juliana Ferraz. **O público e o privado na organização administrativa: da relevância do sujeito à especialidade da função**. Coimbra: Almedina, 2017, p. 669.

CRAWFORD, Susan P. The Internet and the Project of Communications Law, **UCLA Law Review**, n. 55, pp. 360-393, 2007.

CUNHA, Mario Viola de Azevedo. Privacy, Security and the Council Framework Decision 2008/977/JHA. **World Jurist Association Law and Technology Journal**, v. 43, p. 1-18, 2010. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1666140. Acesso em: 14 mar. 2021. de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade

DE LA CUEVA, Pablo Lucas Murillo. La construcción del derecho a la autodeterminación informative. **Revista de Estudios Políticos**, Madrid, 104, (Nueva Época), Abril/Junio 1999.

DE STEFANO, Valerio. The rise of the "just-in-time workforce": on-demand work, crowdwork and labour protection in the "gig-economy". Geneva: ILO, 2016. **Conditions of work and employment series**. n. 71. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_443267.pdf. Acesso em: 10 set. 2022.

DENARDIS, Laura. **The Global War for Internet Governance**. New Haven: Yale University Press. 2014.

DI FELLICE, Massimo; LEMOS, Ronaldo. **A Vida em Rede**. São Paulo: Paprius, 2014.

DIMITROPOULOS, Georgios. Global Administrative Law as 'Enabling Law': How to Monitor and Evaluate Indicator-Based Performance of Global Actors, 2012. **IRPA**. SSRN. Disponível em: http://dx.doi.org/10.2139/ssrn.2167405. Acesso em: 26 out.

DOMINGOS, Pedro. **The master algorithm:** how the quest for the ultimate learning machine will remake our world. New York: Basic Books, 2015.

DONEDA, Danilo. **A proteção da privacidade e de dados pessoais no Brasil**. Observatório Itaú Cultural: Direito, Tecnologia e Sociedade, Rio de Janeiro, ed. 16, p. 136-149, jan/jun 2014.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019.

DUARTE, Tatiana. Artigo 9.º. *In:* PINHEIRO, Alexandre Sousa. **Comentários ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018, p. 234-334.

DUNBAR, Robin. **Grooming, Gossip, and the Evolution of Language**. Cambridge: Harvard University Press, 1998.

ESTADOS UNIDOS DA AMÉRICA. Children's Online Privacy Protection Act, **Public Law**, Washinton D.C., 21 out. 1998.

ESTADOS UNIDOS DA AMÉRICA. Children's Online Privacy Protection Act, 15 U.S.C. §6501-6506., **Public Law**, Washinton D.C., 21 out. 1998.

ESTADOS UNIDOS DA AMÉRICA. Electronic Communications Privacy Act, 18 U.S.C. §2510 e ss., **Public Law**, Washinton D.C., 21 out. 1986.

ESTADOS UNIDOS DA AMÉRICA. Federal Trade Comission Act, 15 U.S.C. §41-58., **Public Law**, Washinton D.C., 1914.

ESTADOS UNIDOS DA AMÉRICA. Privacy Act, 88 Stat. 1896, **Public Law**, Washinton D.C., 31 dez. 1974.

EUBANKS, Virginia. **Automating inequality**: how high-tech tools profile, police, and punish the poor. New York: St. Martin's Press, 201.

FELICIANO, Guilherme Guimarães et al. (Coord.). **Direito ambiental do trabalho**: apontamentos para uma teoria geral. São Paulo: LTr, v. 3, 2017.

FELICIANO, Guilherme Guimarães; PASQUALETO, Olívia de Quintana Figueiredo. (Re)descobrindo o direito do trabalho: gig economy, uberização do trabalho e outras reflexões. In: FELICIANO, Guilherme Guimarães; MISKULIN, Ana Paula Silva Campos (Org.) **Infoproletários e a uberização do trabalho**: direito e justiça em um novo horizonte de possibilidades. São Paulo: LTr Editora, 13-20, 2019.

FLORIDI, Luciano. *The 4th revolution.* How the infosphere is reshaping human reality. Oxford: Oxford University Press, 2014.

KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018.

FUX, Luiz. Apresentação, *In*: LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. São Paulo: Juspodivm, 2022.

GARFINKEL, Simson. **Database National: the death of privacy in the 21th century**. California: O'Reilly Media, 2000.

GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha:** a tensão entre a demanda estatal por informações e os limites jurídicos impostos. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 13 nov. 2021.

GINSBERG, J., MOHEBBI, M., PATEL, R. et al. Detecting influenza epidemics using search engine query data. **Nature** n. 457, p. 1012–1014, 2009. Disponível em: https://doi.org/10.1038/nature07634. Acesso em: 10 jan. 2021.

GOLDMAN, Eric. **The Third Wave of Internet Exceptionalism**. In: SZOKA, Berin; MARCUS, Adam (ed.). The Next Digital Decade: Essays on the Future of the Internet. Washington, D.C: TechFreedom, 2010.

GOLDSMITH, Jack L; WU, Tim. **Who controls the internet?: illusions of a borderless world**. New York: Oxford University Press, 2006.

GRAFENSTEIN, Maximilian von. **Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design**. Forthcoming in González-Fuster, G., van Brakel, R. and P. De Hert Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing. Disponível em: https://ssrn.com/abstract=3336990. Acesso em: 30 set. 2022.

GRAFENSTEIN, Maximilian von. **The Principle of Purpose Limitation in Data Protection Laws**. The Risk- Based Approach, Principles, and Private Standards as Elements for Regulating Innovation. Baden-Baden: Nomos, 2018.

GREENWALD, Glenn; MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian Online**, June 7, 2013. Disponível em: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em: 30.11.16.

GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios para Proteção de Dados Pessoais**. *In:* BRANCO, Sérgio; TEFFÉ, Chiara de (org.). Privacidade em Perspectivas. 1. ed. Rio de Janeiro: Lumen Juris, 2018.

GUIMARÃES, Pollyanna Silva. **A tecnologia aliada à Construção do Direito do Trabalho**. São Paulo: LTr, 2016.

HAN, Byung-Chul. Byung-Chul Han: "Hoje o indivíduo se explora e acredita que isso é realização". GELI, Carles. **El país**, Barcelona, 2018. Disponível em: https://brasil.elpais.com/brasil/2018/02/07/cultura/1517989873_086219.html. Acesso em: 27 out. 2022.

HAN, Byung-Chul. O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han. **El País**. Disponível em: https://brasil.elpais.com/ideas/2020-03-22/o-

coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html. Acesso em: 15 nov. 2021.

HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Paulo Giachini. Petrópolis: Vozes, 2019.

HARARI, Yuval Noah. **Sapiens**: uma breve história da humanidade. Tradução de Janaína Marcoantonio. 1. ed. Porto Alegre: L&PM, 2015.

HARVEY, David. **Condição pós-moderna**: uma pesquisa sobre as origens da mudança cultural. Tradução de Adail Ubirajara Sobral e Maria Stela Gonçalves. 17. ed. São Paulo: Edições Loyola, 2008.

HEGEL. Georg F. *Apud* DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019, p. 58.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Rio de Janeiro: Forense, 2021.

HOLMES, Stephen; SUNSTEIN, Cass. **The cost of rights: why liberty depends on taxes**. New York: W.W. Norton & Company, 1999.

HUNTER, Dan. **Cyberspace as Place, and the Tragedy of the Digital Anticommons**. SSRN. Disponível em: https://dx.doi.org/10.2139/ssrn.306662. Acesso em: 15 jul. 2022.

JOHNSON, David. R, POST, David. Law & Borders: The Rise of Law in Cyberspace, **Stanford Law Review**, n. 48, p. 1.367-1.403, 1996.

JURVETSON, Steve. Transcending Moore's Law with Molecular Electronics and Nanotechnology. **Nanotechnology Law & Business**, vol. 1, n. 1, 2004, p. 70-90. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/nantechlb1&i=72. Acesso em: 24 nov. 2021.

KELLER, Clara Iglesias. **Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado**. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, p. 300. 2018.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. **Proceedings of the National Academy of Sciences of the United States of America**, Washington, v. 110, n. 15, p. 5802–5805, 2013. Disponível em: www.pnas.org/cgi/doi/10.1073/pnas.1218772110. Acesso em: 13 mar. 2021.

LANE, Randall. Covid-19 provoca a maior aceleração da riqueza em toda a história da humanidade. **Forbes Brasil**. São Paulo, 2021. Disponível: https://forbes.com.br/forbes-money/2021/04/covid-19-provoca-a-maior-aceleracao-da-riqueza-em-toda-a-historia-da-humanidade/. Acesso em: 29 abr. 2021.

LATOUR, Bruno**. Reagregando o Social: uma introdução à Teoria do Ator-Rede**. SOUSA, Gilson César Cardoso de (trad.). Salvador/Bauru: Edufba/Edusc, 2012.

LEAL, Ana Alves. Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação. In Fintech: Desafios da Tecnologia Financeira. 2ª ed. Coimbra: Almedina, 2019, p. 79-218.

LEE, Jongho; LEE, Keun. Is the fourth industrial revolution a continuation of the third industrial revolution or something new under the sun? Analyzing technological regimes using US patent data. **Industrial and Corporate Change**, vol. 30, n. 1, 2021, p. 157

LEITE, Harisson. **Manual de direito financeiro**. 5. ed. Salvador: JusPODIVM, 2016, p. 49-52.

LEME, Ana Carolina Reis Paes. **Da máquina à nuvem**: caminhos para o acesso à justiça pela via de direitos dos motoristas da Uber. São Paulo: LTr, 2019, p. 67-69.

LEMLEY, Mark A. **Place and Cyberspace**. Disponível em: http://dx.doi.org/10.2139/ssrn.349760. Acesso em 20 jul. 2022.

LESSIG, Lawrence. **Code: And Other Laws of Cyberspace, Version 2.0**. New York: Basic Books, 2006.

LEVI-FAUR, David. Regulation & Regulatory Governance. **Jerusalem Papers in Regulation & Governance**. Working Paper n. 1, 2010.

LIMBERGER, Têmis. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí, v. 14. n. 2, p. 27–53, 2009. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/1767. Acesso em: 7 mar. 2021.

LOBEL, O. The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought. **Minnesota Law Review**, v. 89, p. 342-370, 2004.

LOEFFLER, John. No More Transistors: The End of Moore's Law. **Interesting Engineering**. Delaware, 2018. Disponível em: https://interestingengineering.com/no-more-transistors-the-end-of-moores-law. Acesso em: 12 nov. 2021.

LORDELO, João Paulo. **Constitucionalismo digital e devido processo legal**. São Paulo: Juspodivm, 2022.

LUHMANN, Niklas. **Introduction to systems theory**. BAECKER, Dirk (ed.). GILGEN, Peter (trad.). Cambridge: Polity Press, 2013.

MACHLUP, Fritz. **The production and distribution of knowledge in the United States**. Princeton, Princeton University Press, 1962.

MARS, Amanda. Como a desinformação influenciou nas eleições presidenciais? **El País**. Nova York, 2018. Disponível em: https://brasil.elpais.com/brasil/2018/02/24/internacional/1519484655_450950.html. Acesso em: 25 jun. 2022.

MARSDEN, Christopher T. **Internet Co-regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace**. Cambridge: Cambridge University Press, 2011.

MARTINEZ, Luciano; MALTEZ, Mariana. O direito fundamental à proteção em face da automação. **Revista de direito do trabalho**, São Paulo, SP, v. 43, n. 182, p. 21-59, out. 2017.

MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005.

MARVIT, Moshe Z. **How crowdworkers became the ghosts in the digital machine**. The Nation, 2014. Disponível em: https://www.thenation.com/article/archive/how-crowdworkers-became-ghosts-digital-machine/. Acesso em: 23 out. 2022.

MAYER-SCHÖNBERGER, Viktor. Demystifying Lessig. **Wisconsin Law Review**. v. 4., p. 713-746, 2008.

MAYER-SCHÖNBERGER, Viktor. **Generational development of data protection in Europe**. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: The MIT Press, 2001.

MAYER-SCHÖNBERGER; Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work, and think. New York: Mariner Book, 2014.

MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **Revista Direito Público**, Brasília, v. 16, n. 90, p. 39–64, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em: 2 maio 2021.

MICHAEL, David. "What and Where Is My Data." MICHAEL, David. What and Where Is My Data. **GP Solo**, vol. 34, n. 2, mar./abr. 2017, p. 46-49, p. 47. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/gpsolo34&i=132. Acesso em: 5 out. 2021.

MIRANDOLA, Pico Della. **Discurso sobre a dignidade do homem**. Belo Horizonte: Editora Âyiné, 2021, [p. 323] Edição do Kindle.

MOOR, James. The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years. **AI Magazine**. Palo Alto: Association for the Advancement of Artificial Intelligence, v. 27, n. 4, p. 87–91, 2006.

MOORE, Gordon M. Cramming more components onto integrated circuits. **Electronics**, [S. l.], v. 38, n. 8, p. 114, 1965. Disponível em: https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/moores-law-electronics.pdf. Acesso em: 12 nov. 2021.

MORAIS, Carlos Blanco de. As Autoridades Independentes na ordem jurídica portuguesa. In: **Revista da Ordem dos Advogados**. n. 61. p. 101-154, 2001, p. 114-ss. Juliana Ferraz Coutinho, igualmente, menciona a presumida ideia de ineficiência da Administração como uma das razões para se terem criado tais entidades.

MOREIRA, Vital. As Entidades Administrativas Independentes e o Provedor de Justiça. In: **O Cidadão, o Provedor de Justiça e as Entidades Administrativas Independentes**. Lisboa: Provedoria de Justiça – Divisão de Documentação, 2012.

MOSES, Lyria Bennett. How to think about law, regulation and technology: problems with technology as a regulatory target. **Law, Innovation and Technology**, n. 5, v. 1, 2013.

MURRAY, Andrew D. Nodes and Gravity in Virtual Space. **Legisprudence**. v. 5. n. 2, oct., 2011, pp. 195-222. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/legisp5&i=195. Acesso em: 29 de set. 2022.

MURRAY, Andrew D.; SCOTT, Colin. Controlling the New Media: Hybrid Responses to New Forms of Power. **The Modern Law Review**. v. 65. n. 4, 2002, pp. 491–516.JSTOR. Disponível em: http://www.jstor.org/stable/1097592. Acesso em: 29 set. 2022.

MURRAY, Andrew. Symbiotic Regulation. **John Marshall Journal of Computer and Information Law**, vol. 26, no. 2, Winter 2008, pp. 207-228. HeinOnline, Disponível em: https://heinonline.org/HOL/P?h=hein.journals/jmjcila26&i=211. Acesso em: 15 out. 2022.

MURRAY, Andrew D..**The Regulation of Cyberspace: Control in the Online Environment**. New York: Taylor e Francisco, 2007.

NADER, Ralph *apud* ZANATTA, Rafael. A. F. **Perfilização, Discriminação e Direitos**: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais/download. Acesso em: 21 jun. 2021.

NAPOL, Igor. Dados de 57 milhões de usuários da Uber foram acessados por hackers. **Tecmundo**, São Paulo, 2017. Disponível em: https://www.tecmundo.com.br/seguranca/124408-uber-omitiu-ciberataque-expos-dados-57-milhoes-pessoas.htm. Acesso em: 14 nov. 2018.

NEWMAN, Abraham. L. Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive. **International Organization**. Cambridge: Cambridge University Press, n. 62, ed. 1, pp. 103–130

NOVAES NETO, Nelson; et. al. Developing a Global Data Breach Database and the Challenges Encountered. **Journal of Data and Information** Quality, New York, v. 13,

n. 1, 2021. ISSN: 19361963. DOI: 10.1145/3439873. Disponível em: https://dl.acm.org/doi/abs/10.1145/3439873. Acesso em: 7 maio. 2021.

O'NEILL, Patrick Howell; RYAN-MOSLEY, Tate; JOHNSON, Bobbie. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. MIT Technology Review. (maio), 2020. Disponível em: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. Acesso em: 05 mar. 2022.

O'NEIL, Cathy. **Weapons of math destructio**n: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016.

OFFE, Claus. **Contradictions of the Welfare State**. London: Hutchinson & Co. (Publishers) Ltd, 1984.

OIT. Organização Internacional do Trabalho. **Constituição da Organização Internacional Do Trabalho.** Declaração de Filadélfia. Filadélfia, 1944. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/---ilo-brasilia/documents/genericdocument/wcms_336957.pdf. Acesso em: 23 out. 2022.

OLIVEIRA, Madalena Perestrelo de. As recentes tendências da FinTech: disruptivas e colaborativas. CORDEIRO, António Menezes, OLIVEIRA, Ana Perestrelo, DUARTE, Diogo Pereira (coord.). **Fintech: Desafios da Tecnologia Financeira.** 2. ed. Coimbra: Almedina.

OLIVEIRA, Simone. A qualidade da qualidade: uma perspectiva em saúde do trabalhador. **Cad. Saúde Públ.**, Rio de Janeiro, 13 (4), pp. 625-634, out-dez, 1997. p. 632. Disponível em: https://www.scielosp.org/pdf/csp/1997.v13n4/625-634/pt. Acesso em: 21 meio 2020.

ONI. Open Net Initiative. Country Profiles: China, 2012. Disponível em: https://opennet.net/research/profiles/china-including-hong-kong. Acesso em: 25 out. 2022. 05/01/2018.

OTERO, Paulo. **Manual de Direito Administrativo**. vol. 1. Coimbra: Almedina, 2013.

PAGALLO, Ugo. **Il diritto nell'età dell'informazione**: Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti. Torino: G. Giappichelli Editore, 2014.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2016.

PAUL, Ian. Instagram updates Privacy Policy, inspiring backlash. **PC World**. 2012. Disponível em: https://www.pcworld.com/article/456103/instagram-updates-privacy-policy-inspiring-backlash.html. Acesso em: 26 set. 2022.

PECK, Patricia. Palestra proferida por Patricia Peck na Escola Superior do Tribunal de Contas do Estado de Mato Grosso, sobre o tema "**Impactos da LGPD para órgãos de controle**", em 23 de agosto de 2022.

PEREIRA, André Gonçalo Dias. Inteligência Artificial, Saúde e Direito: Considerações jurídicas em torno medicina de conforto e da medicina transparente. In: Julgar: Lisboa, n. 45, p. 235-262, 2021.

Pietro Perlingieri. **Normativa comunitaria e ordinamento interno**. In: I giuristi e l'Europa. Luigi Moccia (org.). Laterza: Bari, 1997.

POST, David G. What Larry doesn't get: code, law, and liberty in cyberspace. **Stanford Law Review**. v. 52. n. 5, p. 1439–1459, 2000.

PRASSL, Jeremias. **Human as a service**: The promisse and perils of work in the gig economy. Oxford: Oxford University Press, 2018.

REDINHA, Maria Regina Gomes. **Da protecção da personalidade no Código do Trabalho**. In: Fernandes, F., & Redinha, M., Para Jorge Leite: escritos jurídico-laborais. p. 819-853. Coimbra: Coimbra Editora, 2014.

REICHMAN, Nancy. Computer Matching: Toward Computerized Systems of Regulation. **Law & Policy**. vol. 9, n. 4, October 1987, p. 387-416. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/lawpol9&i=397. Acesso em: 19 fev. 2022.

EINDENBERG, Joel R. Lex Informatica: The Formulation of Information Policy Rules Through Technology. **Texas Law Review**, v. 76, n. 3, 1998, p. 553-584. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/tlr76&i=571. Acesso em: 24 out. 2021.

REINSEL, David; GANTZ, John; RYDNING, John. International Data Corporation. **The Digitization of the World:** from Edge to Core. Framingham, 2018. Disponível em: https://www.seagate.com/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. Acesso em: 9 mar. 2021.

RENARD, Céline. **Droit de l'internet: droit français et européen**. 2. ed. Paris: Montchrestien, 2012.

RICHARDSON, Rashida; SCHULTZ, Jason M.; CRAWFORD, Kate. **Dirty data, bad predictions: how civil rights violations impact police data, predictive policing systems, and justice**. New York: New York University Law Review, 2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Trad. Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROHR, Altieres. Vazamento de dados do Yahoo: Veja o que você precisa saber. **G1**, São Paulo, 2016. Disponível em: https://g1.globo.com/tecnologia/blog/seguranca-digital/post/vazamento-de-dados-do-yahoo-veja-o-que-voce-precisa-saber.html. Acesso em: 14 nov. 2022.

RULE, James B. **Private Lives and Public** Surveillance: Social Control in the Computer Age. New York: Schocken Books, 1974.

SALTZER, Jerome H.; REED, David Patrick; CLARK, David D. End-To-End Arguments in System Design. M.I.T. Laboratory for Computer Science. **ACM Transactions on Computer Systems**, v. 2, n. 4, nov. 1984, p. 277-288. Disponível em: https://groups.csail.mit.edu/ana/Publications/PubPDFs/End-to-End%20Arguments%20in%20System%20Design.pdf. Acesso em: 12 ago. 2022.

SAMBRANA, Carlos. Exclusivo: Novo vazamento expõe mais de 100 milhões de contas de celular. **NEOFeed**. São Paulo, 2021. Disponível em: https://neofeed.com.br/blog/home/exclusivo-novo-vazamento-expoe-mais-de-100-milhoes-de-contas-de-celular/. Acesso em: 5 maio 2021.

SAMUEL, A. L. Some studies in machine learning using the game of checkers. **IBM Journal of Research and Development**. New York, v. 3, n. 3, p. 210–229, 1959.

SANTOS. Felipe Melazzo do Nascimento**. Nudges e os tratamentos de dados pessoais autorizados pelo consentimento: proposta de matriz de análise a partir da investigação empírica em startups da Região dos Inconfidentes**. Dissertação (Mestrado em Direito) – Escola de Direito, Turismo e Museologia, da Universidade Federal de Ouro Preto, p. 176, 2022.

SCHOOTEN, Hanneke van e VERSCHUUREN, Jonathan (Orgs.). **International Governance and Law: State Regulation and Non-State Law**. Cheltenham: Edward Elgar Publishing, 2008. SSRN. Disponível em: https://ssrn.com/abstract=1291162. Acesso em 12 set. 2022.

SCHUCK, Peter Apud LOBEL, Orly. The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought. **Minnesota Law Review**, v. 89, p. 342-370, 2004.

SCHULZ, Wolfgang, HELD, Thorsten. **Regulated Self-regulation as a modern form of government**. Indiana: John Libbey, 2004.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. Tradução de Daniel Moreira Miranda. 1. ed., São Paulo: Edipro, 2016.

SCOTT, Colin. Accountability in the Regulatory State. **Journal of Law and Society**. v. 27. n. 1. mar. 2000, p. 38-60. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/jlsocty27&i=46. Acesso em: 27 set. 2022.

SCOTT, Colin. Analyzing Regulatory Space: Fragmented Resouces and Instituional Design. **Public Law** (Summer), p. 283-305, 2001.

SCOTT, Colin. Regulation in the Age of Governance: the rise of the post-regulatory state In: JORDANA, Jacin; LEVI-FAUR, David. **The Politics of Regulation** – Institutions and Regulatory Reform for the Age of Governance. Cheltenham: Edward Elgar, pp. 145-176, p. 146, 2004.

SELZNICK, Phillip. Focusing Organizational Research on Regulation. In: NOLL, Richard. **Regulatory Policy and Social Sciences**. Bereley; Los Angeels: University of California, 1985.

SILVA, João Nuno Galvão da. **Mercados e Estados: serviços de interesse económico geral**. Coimbra: Almedina, 2008.

SILVA, Renata Valério; MOREIRA, Jani Alves da Silva. A educação, reformas curriculares e as propostas do banco mundial no contexto pós-golpe (2016-2018). **Colloquium Humanarum**, [S. l.], v. 16, n. 1, p. 145–162, 2019. Disponível em: https://journal.unoeste.br/index.php/ch/article/view/2975. Acesso em: 12 nov. 2022.

SKEEL, David A. Jr. Shaming in Corporate Law. **University of Pennsylvania Law Review**, vol. 149, n. 6, jun. 2001, p. 1811-1868. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/pnlr149&i=1823. Acesso em:12 nov. 2021.

SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019,.

SOTTO, L.J.; SIMPSON, A.P. United States In: **Data Protection & Privacy 2015**, Londres: Law Business Research, p. 208-209, 2015.

STANDAGE, Tom. **The Victorian Internet**: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers. New York: Berkley Books, 1999.

STOBBE, Antje; JUST, Tobias. The dawn of technological convergence. Economics 56. **Deutsche Bank Research**. Frankfurt a.M., may 3, 2006.

SUNSTEIN, Cass. **Republic.com**. Princeton: Princeton University Press, 2002.

SUPIOT, Alain. Por uma reforma digna do nome. E se refundarmos a legislação trabalhista?. **Le Mond Diplomatique**, França, Ed. 123, 4 out. 2017. Disponível em: https://diplomatique.org.br/reforma-trabalhista-na-franca-e-se-refundarmos-a-legislacao/. Acesso em: 15 set. 2022.

SWEENEY, Latanya. Discrimination in Online Ad Delivery. **SSRN Electronic Journal**. 2013. Disponível em: https://doi.org/10.2139/ssrn.2208240. Acesso em: 17 jun. 2022.

TAYLOR, Frederick Winslow. **The Principles of Scientific Management**. 1911. Disponível em: https://www.gutenberg.org/ebooks/6435. Acesso em: 05 nov. 2022.

TEUBNER, Gunther. After Legal Instrumentalism: Strategic Models of Post-Regulatory Law In: TEUBNER, Gunter (org). **Dilemmas of Law in the Welfare State**. Berlin: De Gruyter, 1986.

TEUBNER, Gunther. **Constitutional Fragments: Societal Constitutionalism and Globalization**. Oxford: Oxford University Press, 2012.

TEUBNER, Gunther. **Global Bukowina: Legal Pluralism in the World-Society**. Global Law Without A State. Gunther Teubner (ed.). Dartmouth: Brookfield, 1997, pp. 3-28. SRRN. Disponível em: https://ssrn.com/abstract=896478. Acesso em: 10 set. 2021.

TEUBNER, Gunther. **Self-Constitutionalizing TNCs? On the Linkage of "Private" and "Public" Corporate Codes of Conduct**, Indiana Journal of Global Legal Studies, Vol. 18, pp. 617-638, 2011. Disponível em: https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1457&context=ijgls Acesso em: 12 nov. 2022.

THALER, Richard H.; SUNSTEIN, Cass R.. **Nudge: como tomar melhores decisões sobre saúde, dinheiro e felicidade**. Rio de Janeiro: Objetiva, 2019.

TIMMONS, Kelly Cahill. Pre-Employment Personality Tests, Algorithmic Bias, and the Americans with Disabilities Act. **Penn State Law Review**, v. 125, n. 2, winter 2021, p. 389-452. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/dlr125&i=405. Acesso em: 28 jan. 2022.

TRUBEK, David M.; TRUBEK, Louise G. Hard and Soft Law in the Construction of Social Europe: The Role of the Open Method Co-Ordination. **European Law Journal**, v. 11, n. 3, p. 343- 64, 2005.

TURCO, Ronald N. Psychological Profiling. **International Journal of Offender Therapy and Comparative Criminology**, vol. 34, n. 2, September 1990, p. 147-154. HeinOnline, Disponível em: https://heinonline.org/HOL/P?h=hein.journals/ijotcc34&i=152. Acesso em: 10 fev. 2022.

TURGOT, Anne-Robert-Jacques. **Oeuvres de Turgot**. 1975. Disponível em: https://www.institutcoppet.org/turgot-discours-sur-les-progres-successifs-de-lesprit-humain-1750/. Acesso em: 22 ago. 2022.

UE. União Europeia. **Proposta de Regulamento do Parlamento Europeu e do Conselho harmonizadas em matéria de inteligência artificial (regulamento inteligência artificial)**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN. Acesso em: 22 nov. 2021.

UE. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0679. Acesso em: 3 set. 2021.

UE. União Europeia. Comissão Europeia. Decisão 2000/520/CE. Decisão da Comissão de 26 de julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípio de “porto seguro” e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América. **Jornal Oficial** L 215, 25 de agosto de 2000.

UE. União Europeia. Comissão Europeia. **Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253/17)**. Disponível em: https://ec.europa.eu/newsroom/article29/items/611237/en. Acesso em: 19 nov. 2022

UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 04/2021 relativas aos códigos de conduta enquanto instrumento para as transferências**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de. Acesso em: 15 nov. 2022.

UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022.

UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 04/2021 relativas aos códigos de conduta enquanto instrumento para as transferências**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de. Acesso em: 15 nov. 2022.

UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Documento do CEPD relativo ao procedimento para o desenvolvimento de sessões informais sobre Códigos de Conduta**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_documentprocedurecodesconductsessions_pt.pdf. Acesso em: 17 nov. 2022.

UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Guidelines 07/2022 on certification as a tool for transfers**. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_pt. Acesso em: 20 nov. 2022.

UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE**. Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_pt.pdf. Acesso em: 19 nov. 2022.

UE. União Europeia. Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. **Jornal Oficial** L. 207/1, 01 de agosto de 2016.

UE. União Europeia. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas. **Jornal Oficial** L. 201, 31 de julho de 2002.

UE. União Europeia. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao

tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial** L. 119/89, 4 de maio de 2016.

UE. União Europeia. **Mercado Único Digital**. Disponível em: https://www.consilium.europa.eu/pt/policies/digital-single-market/. Acesso em: 30 jun. 2021.

UE. União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial** L 119/1, 04 de maio de 2016.

UE. União Europeia. Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE. **Jornal Oficial** L. 295/39, 21 de novembro de 2018.

UE. União Europeia. **Tipos de legislação**. Disponível em: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt. Acesso em: 25 jun. 2021.

UK. United Kingdom. Office of Comunnications. **Online protection: A survey of consumer, industry and regulatory mechanisms and systems**, [s.l], 2006. Disponível em: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/27586/report.pdf. Acesso em: 20 set. 2022.

UK. United Kingdom. **Relatório Mindspace**. Disponível em: https://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf. Acesso em: 10 set. 2022.

UK. United Kingdom. **Relatório Behavioural Government**. Disponível em: https://www.bi.team/wp-content/uploads/2018/08/BIT-Behavioural-Government-Report-2018.pdf. Acesso em: 10 set. 2022.

UNDERHILL, Kristen. When Extrinsic Incentives Displace Intrinsic Motivation: Designing Legal Carrots and Sticks to Confront the Challenge of Motivational Crowding-Out. **Yale Journal on Regulation**, vol. 33, n. 1, 2016, p. 213-280. HeinOnline. Disponivel em: https://heinonline.org/HOL/P?h=hein.journals/yjor33&i=215. Acesso em: 13 nov. 2021.

URUGUAI. Decreto nº 414 de 2009. **Diario Oficial**, Montevideo, 31 ago. 2009.

URUGUAI. Lei nº 18.331 de 2008 sobre a Proteção de dados pessoais e a ação de ‘Habeas Data’. **Diario Oficial**, Montevideo, 18 ago. 2008.

URUGUAI. Lei nº 18.331 de 2008 sobre a Proteção de dados pessoais e a ação de 'Habeas Data'. **Diario Oficial**, Montevideo, 18 ago. 2008.

VENKATASUBRAMANIAN, Akarsh. The Human Rights Challenges to Digital COVID-19 Surveillance. **Health and Human Rights Journal**, vol. 22, n. 2, December 2020, p. 79-84. HeinOnline. Disponível em: https://heinonline.org/HOL/P?h=hein.journals/harhrj22&i=505. Acesso em: 20 fev. 2022.

VERMEULE, Adrian. Local and Global Knowledge in the Administrative State, 2012. Public Law & Legal Theory Working Paper Series Paper No. 13-01. **Harvard Law School**. Disponível em: http://dx.doi.org/10.2139/ssrn.2169939. Acesso em: 14 out. 2022.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, 1890.

WESTIN, Alan. Privacy and Freedom, New York: Atheneum, 1970 *apud* PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. 1. ed. 6. imp, Curitiba: Juruá, 2011.

WU, Tim. **Is Internet Exceptionalism Dead?**. In: SZOKA, Berin; MARCUS, Adam (ed.). The Next Digital Decade: Essays on the Future of the Internet. Washington, D.C: TechFreedom, 201.

ZANATTA, Rafael. **A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet**. Disponível em: https://www.researchgate.net/publication/322581135_A_protecao_de_dados_pessoais_entre_leis_codigos_e_programacao_os_limites_do_Marco_Civil_da_Internet. Acesso em: 22 nov. 2022.

ZANATTA, Rafael. A. F. **Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais**. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais/download. Acesso em: 21 jun. 2021.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução George Schlesinger. Rio de Janeiro: Intrínseca, 2021.

ANEXO I

Tabela 3 - MIT revisão de rastreadores de contato COVID-19.[897]

Local	Nome	Notas	Voluntariedade	Limitação	Destruição dos dados	Minimização	Transparência	Tecnologia
Argélia	Algeria's App	A aplicação da Argélia foi investigada pela Anistia Internacional.	☆	☆	☆	☆	☆	☆
Austrália	COVIDSafe	Especialistas australianos criticaram o governo por falta de transparência e não resposta às questões de privacidade.	★	★	★	★	★	Bluetooth
Áustria	Stopp Corona	A Áustria foi uma das primeiras grandes nações europeias a se alinhar com a API do Google/Apple.	★	★	★	★	★	Bluetooth, Google/Apple
Bahrein	BeAware	Embora 25% do país tenha baixado o BeAware, há poucas informações públicas sobre o aplicativo. A partir de janeiro de 2021, os usuários também podem agendar consultas de vacinas através do aplicativo.	★	★	☆	☆	☆	Bluetooth, Localização
Bangladesh	Corona TracerBD	O aplicativo foi construído por Shohoz, uma "plataforma online de compartilhamento de caronas e bilheterias." Meses após seu	★	★	☆	☆	☆	Bluetooth, GPS

[897] Tradução do autor. Adaptado de: O'NEILL, Patrick Howell; RYAN-MOSLEY, Tate; JOHNSON, Bobbie. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. MIT Technology Review. (maio), 2020. Disponível em: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. Acesso em: 05 mar. 2022.

		lançamento em junho, o aplicativo não tinha se mostrado muito eficaz.						
Bélgica	Coronalert	O código da Bélgica é baseado em Aplicativo Corona-Warn da Alemanha. É de código aberto e bem documentado.	★	★	★	★	★	Bluetooth, Google/Apple, DP3T
Bulgária	ViruSafe	A Bulgária lançou seu aplicativo no início de abril e começou a levantar restrições de movimentação no início de maio.	★	★	★	☆	★	Localização
Canadá	COVID Alert	O aplicativo do Canadá foi lançado para 8 províncias e territórios. Seu site contém números de uso e explicações claras de como funciona.	★	★	★	★	★	Bluetooth, Google/Apple
China	Chinese health code system	Há muito pouca informação disponível ao público sobre como a tecnologia da China funciona.	☆	☆	☆	☆	☆	Localização, Mineração de dados
Chipre	CovTracer	O aplicativo Cypriot foi um dos primeiros esforços de lançamento em fevereiro.	★	☆	★	★	★	Localização
República Checa	eRouska	eRouska é uma parte do maior plano de "quarentena inteligente" do governo tcheco. O aplicativo foi relançado em setembro para resolver problemas com a primeira versão.	★	★	★	★	★	Bluetooth
Dinamarca	Smittestop	Em setembro, este aplicativo notificou as pessoas que haviam sido expostas quando, na verdade, não tinham, devido a um erro técnico.	★	★	★	★	★	Bluetooth, Google/Apple

Estônia	HOIA	Lançado em 19/08/20.	★	☆	☆	★	☆	Bluetooth, DP-3T, Google/Apple
Fiji	CareFiji	CareFiji foi lançado no final de junho e foi modelado após o Aplicativo de Cingapura TraceTogethe.	★	☆	☆	★	★	Bluetooth
Finlândia	Koronavilkku	O aplicativo piloto da Finlândia não está mais em uso. A política de privacidade do aplicativo atual está bem documentada.	★	★	★	★	★	Bluetooth, Google/Apple
França	TousAntiCovid	A França, assim como o Reino Unido e a Noruega, França negociou com a Apple e o Google, mas decidiu não usar seus padrões.	★	★	★	★	★	Bluetooth
Alemanha	Corona-WarnApp	A Alemanha optou pelo API Google/Apple depois de inicialmente ter como objetivo construir um sistema centralizado.	★	★	★	★	★	Bluetooth, Google/Apple
Gana	GH COVID-19 Tracker	O aplicativo de Gana está focado na coleta de dados de localização dos usuários.	★	☆	☆	☆	☆	Localização
Gibraltar	Beat Covid Gibraltar	O aplicativo do Gibralter foi lançado em 18 de junho e mais de 25% da população o baixou. Trabalha em conjunto com aplicativos da Irlanda do Norte, Jersey, República da Irlanda, Escócia, Inglaterra e País de Gales.	★	★	★	★	★	Bluetooth
Hungria	VirusRadar	O aplicativo voluntário alerta as pessoas que chegaram a 2m de uma pessoa infectada por pelo menos 20min.	★	☆	★	★	★	Bluetooth

Islândia	Raknin[g C-19]	A Islândia decidiu não usar Bluetooth porque não era confiável e, em vez disso, usou dados de localização	★	★	★	★	★	Localização
Índia	Aarogya Setu	O judiciário indiano determinou o não compartilhamento dos dados da aplicação com outros departamentos e agências do governohttps://www.livelaw.in/top-stories/karnataka-high-court-restrains-centre-nic-from-sharing-response-data-of-persons-collected-through-aarogya-setu-168886https://www.livelaw.in/top-stories/karnataka-high-court-restrains-centre-nic-from-sharing-response-data-of-persons-collected-through-aarogya-setu-168886.	☆	★	★	☆	☆	Bluetooth, Localização
Indonésia	PeduliLindungi	O aplicativo da indonésia usa dados de localização de indivíduos para cruzar referências com dados do provedor de telecomunicações.	★	☆	☆	☆	☆	Bluetooth, Localização
Irã	AC-19	Este aplicativo parece não estar mais em uso.	☆	☆	☆	☆	☆	NA
Irlanda	Covid Tracker	Ao contrário de seu vizinho, Reino Unido, a Irlanda optou por usar a API do Google/Apple desde o início. O aplicativo da Irlanda do Norte funciona com aplicativos da Inglaterra, Jersey, República da Irlanda, Escócia e País de Gales.	★	★	★	★	★	Bluetooth, Google/Apple

Israel	HaMagen	Funcionários disseram que o aplicativo não é suficientemente preciso porque é baseado apenas em GPS e informações voluntárias.	☆	★	★	★	★	Localização
Itália	Immuni	Depois da China, a Itália foi a primeira nação ocidental devastada pelo covid-19. Eles lançaram seu aplicativo no início de junho.	★	★	★	★	★	Bluetooth, Google/Apple
Japão	COCOA	O aplicativo do Japão tem sido repleto de problemas desde que foi lançado, e foi suspenso pelo menos duas vezes.	★	★	★	★	★	Bluetooth, Google/Apple
Kuaite	Shlonik	Um relatório recente da Anistia Internacional destacou o aplicativo do Kuwait como um dos mais invasivos do mundo.	★	☆	☆	☆	☆	Localização
Malásia	MyTrace	As permissões permitidas para o uso de dados são excessivamente amplas. Originalmente disponível apenas para Android, agora também disponível para iPhone.	★	☆	★	☆	☆	Bluetooth
México	CovidRadar	As políticas específicas de privacidade e dados para o aplicativo mexicano são atualmente bastante finas e vagas.	★	☆	☆	☆	☆	Bluetooth
Nova Zalândia	NZ COVID Tracer	O aplicativo da Nova Zelândia é baseado em um sistema de check-in usando códigos QR em áreas públicas. O aplicativo foi renovado no início de dezembro de 2020 para incluir Bluetooth e tecnologia Apple/Google.	★	★	★	☆	★	Bluetooth, QR codes

Macedônia do Norte	StopKorona	Aplicativos para Android e iOS foram lançados em meados de abril.	★	★	★	★	★	Bluetooth
Irlanda do Norte	StopCOVID NI	O aplicativo da Irlanda do Norte funciona com aplicativos da Inglaterra, Jersey, República da Irlanda, Escócia e País de Gales.	★	☆	☆	☆	☆	Bluetooth, Google/Apple
Noruega	Smittestopp	Este é o segundo aplicativo implantado na Noruega. O primeiro foi descontinuado após preocupações com privacidade.	★	★	★	★	★	Bluetooth, Google/Apple
Filipinas	StaySafe	O aplicativo foi lançado em abril e tem sérias preocupações de privacidade que desencadearam uma carta exigindo melhores proteções das principais organizações.	★	☆	☆	☆	☆	Bluetooth
Polônia	ProteGO Safe	A versão inicial deste aplicativo foi criticada por questões de privacidade. A versão mais recente foi adaptada para ser mais segura.	★	★	★	★	★	Bluetooth
Catar	Ehteraz	O aplicativo é obrigatório para todos os cidadãos e requer acesso a fotos. Também teve uma grande falha de segurança no lançamento.	☆	☆	☆	☆	☆	Bluetooth, Localização
Arábia Saudita	Tawakkalna	O aplicativo Tawakkalna combina dados com o Tabaud, o aplicativo de rastreamento de contatos, e permite que os cidadãos solicitem "licenças de movimento" para mobilidade ao redor da cidade. A partir de meados de junho, Tawakkalna e Tabaud toranram-se obrigatórios para se entrar em prédios dos Ministérios.	★	☆	★	☆	☆	Localização

Arábia Saudita	Tabaud	Enquanto o Tabaud usa o sistema GoogleApple, sua política de privacidade observa "links externos" nos aplicativos, pelos quais o aplicativo não tem responsabilidade de privacidade. Não está claro quais são os "links externos". Tabaud também não é de código aberto.	★	★	★	★	☆	Bluetooth, Google/Apple
Cingapura	TraceTogether	TraceTogether foi o primeiro grande aplicativo de rastreamento de contato Bluetooth.	☆	☆	★	★	★	Bluetooth, BlueTrace
África do Sul	COVID Alert SA	A África do Sul tentou várias outras estratégias de rastreamento de contato antes de passar para essa opção de proteção à privacidade.	★	★	★	★	☆	Bluetooth, Google/Apple
Suíça	SwissCovid	Inicialmente, os suíços optaram por usar DP-3T em vez do API do Google/Apple. Agora parece que eles usarão ambos.	★	★	★	★	★	Bluetooth, DP-3T, Google/Apple
Tailândia	MorChana	Tailândia emparelhou o aplicativo de rastreamento de contato de proximidade com um sistema de check-in de código QR, chamado Thai Chana	☆	☆	☆	☆	☆	Bluetooth, Localização
Tunísia	E7mi	O governo da Tunísia diz que o aplicativo permanecerá voluntário enquanto as taxas de download forem altas.	★	★	★	☆	☆	Bluetooth

Turquia	Hayat Eve Sığar	Turquia obriga as pessoas que testam positivo a fazerem download do aplicativo, que pode compartilhar dados com a polícia.	☆	☆	☆	★	☆	Bluetooth, Localização
EAU	TraceCovid	O aplicativo é em sua maioria descentralizado, mas os cidadãos podem ser multados por recusar a instalação ou o cadastro para o aplicativo.	☆	☆	☆	★	☆	Bluetooth
UK	NHS COVID19 App	O aplicativo foi lançado em 24 de setembro, mas continua enfrentando críticas por ser confuso e ineficaz. Trabalha com aplicativos da Irlanda do Norte, Jersey, República da Irlanda, Escócia, Gibraltar e País de Gales	★	★	★	★	★	Bluetooth, Google/Apple
Vietnã	BlueZone	O Vietnã está usando um sistema descentralizado, mas requer acesso a contatos e outras mídias em dispositivos móveis como fotos.	★	★	☆	☆	★	Bluetooth

Fonte: MIT Technology Review's Covid Tracing Tracker DB . *Ainda não implantado; Última atualização: 16/03/21 às 12:25pm. Tradução do autor.

ANEXO II

Tabela 4 - Regulatory strategies: posited strengths and weaknesses

Strategy	Example	Strengths	Weaknesses
1. Command & Control	Health and Safety at Work	Force of law.	Intervenes in management.
		Fixed standards set minimum acceptable levels of behaviour.	Prone to capture.
		Screens entry.	Complex rules tend to multiply.
		Prohibits unacceptable behaviour immediately.	Inflexible.
		Seen as highly protective of public.	Informational requirements severe.
		Use of penalties indicates forceful stance by authorities.	Expensive to administer.
			Setting standards is difficult and costly.
			Anti-competitive effects.

			Incentive is to meet the standard, not go better.
			Enforcement costly.
			Compliance costs high.
			Inhibits desirable behaviour.
2. Incentives	Differential tax on leaded and unleaded petrol	Low regulator discretion.	Rules are required.
		Low-cost application.	Poor response to problems arising from irrational or careless behaviour.
		Low intervention in management.	
		Incentive to reduce harm to zero, not just to standard.	Predicting outcome from given incentive difficult.
		Economic pressure to behave acceptably.	Mechanical, so inflexible.
			Regulatory lag.

			Politically contentious as rewards wrongdoer and fails to prohibit offence.
3. Market-harnessing controls		Responses to market driven by firms, not bureaucrats.	No expert agency to solve technical or commercial problems in the industry.
(a) Competition laws	Airline industry	Can be applied across industries.	
		Economies of scale in use of general rules.	Uncertainties and transaction costs.
		Low level of intervention.	Courts slow to generate guidance.
		Flexibility for firms.	Principles develop sporadically.
(b) Franchising	Rail, television, radio	Enforcement is low cost to public.	Evidential difficulties.
		Low level of restriction.	Need to specify service.
		Respects managerial freedoms.	Tension of specification and responsiveness/innovation.
		Allows competition for market as substitute for competition in the market.	Uncertainties impose costs on consumers.

		Managers rather than bureaucrats respond to market preferences.	Requires competition for franchise but may be few bidders.
			Need to enforce terms of franchise.
(c) Contracting	Local authority refuse services	Combines control with service provision.	Potential confusion of regulatory and service roles.
		Sanctioning by economic incentive or non-renewal.	Poor transparency and accountability.
		Easier to operate than licensing system.	Judicial control weak.
(d) Tradable permits	Sulphur dioxide emissions (USA)	Pollution by greatest wealth producer.	Enforcement may require inspectorate.
		Incentive to reduce harm to zero.	Regulatory lag, lack of rapid response in crisis.
		Managerial freedom considerable.	No compensation for victims.
		Regulatory discretion low.	Requires healthy market for permits.

		Regulatory costs low.	Barriers to entry may be created.
			Some harms need to be prohibited absolutely.
4. Disclosure	Mandatory disclosure in food/drink sector	Low intervention.	Information users may make mistakes.
		Allows consumer to decide issues.	
		Lower danger of capture.	Economic incentives (e.g. price) may prevail over information (on, e.g., risk).
		Useful in low-risk sectors.	
			Cost of producing information may be high.
			Risks may be so severe as to call for prohibition.
			Policing of information quality and fraud may be required.
			Information may be in form undermining its utility.

5. Direct action and design solutions			
(a) Direct interventions	State-supplied work premises	Can separate infrastructure provision from operation.	Fairness of subsidies may be contentious.
			Funding costly.
		Assures acceptable level of provision.	Public sector involvement contentious.
		Useful where small firms in poor position to behave responsibly.	Innovations may not be market driven.
		Allows state to plan long-term investments.	
(b) 'Nudge' strategies	Consent to organ donation is assumed unless positive opt-out is exercised	Low cost, combines influence with residual freedom of choice.	Freedoms may be undermined if opt-out is less than easy.
			Transparency and accountability of nudging may be low.
			May not work well where decision processes are complex.

			May impact poorly on regulated parties who are committed to errant conduct.
6. Rights and liabilities laws	Rules of tort law; right to, e.g., light or clean water	Self-help.	May not prevent undesired events that result from accidents and irrational behaviour.
		Low intervention.	
		Low cost to state.	
			Individuals may not enforce due to costs.
			Evidential difficulties and legal uncertainties reduce enforcement.
			Victims may lack resolve and information to proceed, so deterrence sub-optimal.
			Difficult for courts to deter efficiently.
			Insurance may temper deterrent effects.
7. Public compensation / social insurance	Workplace safety schemes (USA, Canada, Japan, New Zealand)	Insurers provide economic incentives.	Incidence levels may be too low to allow risk discrimination.

	Low intervention in management.	Tension of loss-spreading and incentive to behave responsibly.
	Low danger of capture.	
	Encourages accurate reporting of incidents.	
	Makes employers aware of costs of activities.	Inspection and scrutiny of performance expensive.
	Good coverage, applied to all employers.	May operate in very similar manner to command and control mechanism.
	No need to legislate for each individual harm.	

Fonte: BALDWIN, Robert, CAVE, Martin e LODGE, Martin. **Understanding Regulation**, 2. ed. Oxford: Oxford University Press, 2012, p. 134.

ANEXO III

Distinção entre códigos nacionais e transnacionais, segundo as Diretrizes n.º 1/2019 do Comitê Europeu para a Proteção de Dados[898]

Um código transnacional refere-se a um código relacionado com as atividades de tratamento realizadas em mais do que um Estado-Membro. Nesse sentido, pode estar relacionado com atividades de tratamento realizadas por vários responsáveis pelo tratamento ou por vários subcontratantes em vários Estados-Membros, sem que essas atividades constituam necessariamente um «tratamento transfronteiriço» na acepção do artigo 4.º, n.º 23, do RGPD.

Por conseguinte, sempre que um código de conduta adotado por uma associação nacional num Estado-Membro abranja as atividades de tratamento dos seus membros em vários Estados-Membros, será considerado um código transnacional.

No entanto, se uma associação com um código aprovado a nível nacional tiver um membro internacional que realize tratamento transfronteiriço, esse membro só pode usufruir do direito a beneficiar das disposições do código aprovado para as atividades de tratamento no Estado-Membro em que o código foi aprovado.[899] Devem existir procedimentos que assegurem a transparência adequada, no que respeita ao âmbito de aplicação territorial efetivo do código.

[898] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

[899] No entanto, utilizando o mesmo exemplo, os titulares de códigos também poderiam considerar a possibilidade de ampliar o âmbito de aplicação do código e obter aprovação para um código transnacional.

ANEXO IV

Escolha de uma autoridade de controle competente, segundo as Diretrizes n.º 1/2019 do Comitê Europeu para a Proteção de Dados[900]

Os titulares de códigos podem ter uma possibilidade de escolha no que respeita à identificação de uma autoridade de controle competente para efeitos de aprovação do seu projeto de código transnacional.[901] O RGPD não estabelece regras específicas para a identificação da autoridade de controle competente mais adequada para realizar a avaliação de um projeto de código. No entanto, para auxiliar os titulares de códigos na identificação da autoridade de controle competente mais adequada para avaliar o seu código, alguns dos fatores a ter em conta podem incluir o seguinte:[902]

(i) A localização da maior densidade da atividade ou do setor de tratamento; (ii) A localização da maior densidade de titulares de dados afetados pela atividade ou pelo setor de tratamento; (iii) A localização da sede do titular do código; (iv) A localização da sede do organismo de supervisão proposto; ou (v) As iniciativas desenvolvidas por uma autoridade de controle num domínio específico[903].

Embora estes fatores não constituam critérios imperativos, a decisão de escolha de uma autoridade de controle competente é importante e deve ser ponderada cuidadosamente.[904] A função de autoridade de controle competente inclui, nomeadamente, agir como ponto de contato único para os titulares de códigos durante o processo de aprovação, gerir o processo de candidatura na sua fase de cooperação, proceder à acreditação do organismo de supervisão (se for caso disso) e agir como a principal autoridade de controle com vista a assegurar a supervisão eficaz de um código aprovado.

---

[900] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

[901] Ver artigo 55.º em conjugação com o considerando 122 do RGPD.

[902] Esta lista é não exaustiva e não é hierárquica.

[903] Por exemplo, uma autoridade de controle pode ter publicado um documento de orientação circunstanciado e importante relacionado diretamente com a atividade de tratamento que é objeto do código.

[904] A apresentação de um projeto de código para aprovação não pode ser recusada por uma autoridade de controle competente com o fundamento de que não é cumprido nenhum (ou são cumpridos apenas alguns) dos critérios da lista não exaustiva indicada no Anexo IV. Apenas pode ser recusada com base no não cumprimento dos critérios indicados na seção intitulada «Admissibilidade de um projeto de código».

ANEXO V

Lista de verificação para apresentação, segundo as Diretrizes n.º 1/2019 do Comitê Europeu para a Proteção de Dados[905]

Antes de enviar um projeto de código à autoridade de controle competente, é importante certificar-se de que as seguintes informações (se for o caso) foram apresentadas/indicadas e estão corretamente sinalizadas na documentação:

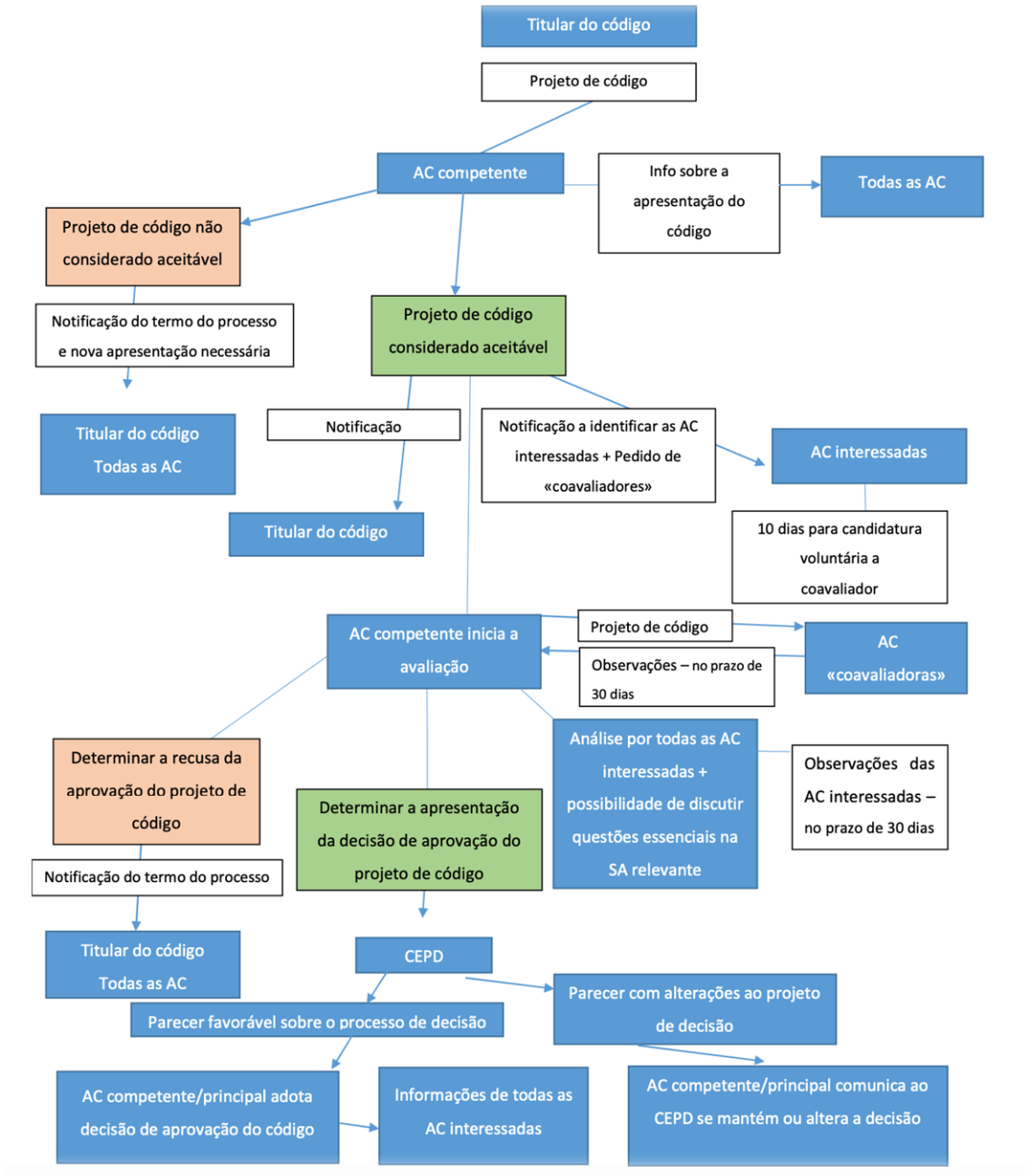
1. Apresentou uma exposição de motivos e toda a documentação de apoio relevante? (n.º 20)
2. É uma associação ou outro organismo representante de categorias de responsáveis pelo tratamento ou de subcontratantes? (n.º 21)
3. Na sua apresentação, forneceu informações para comprovar que é um organismo representante efetivo capaz de compreender as necessidades dos seus membros? (n.º 22)
4. Definiu claramente a atividade ou o setor de tratamento e os problemas de tratamento que o código se destina a resolver? (n.º 23)
5. Identificou o âmbito de aplicação territorial do código e incluiu uma lista de todas as autoridades de controle interessadas (se for caso disso)? (n.º 24)
6. Forneceu informações para justificar a identificação da autoridade de controle competente? (n.º 25)
7. Incluiu procedimentos que permitam a supervisão eficaz do cumprimento das disposições do código? (n.º 26)
8. Identificou um organismo de supervisão e explicou a forma como este observará os requisitos de supervisão do código? (n.º 27)
9. Incluiu informações sobre o alcance da consulta realizada na elaboração do código? (n.º 28)
10. Forneceu uma confirmação de que o projeto do código cumpre a legislação do(s) Estado(s)Membro(s) (se for caso disso)? (n.º 29)
11. Cumpriu os requisitos linguísticos? (n.º 30)

A apresentação inclui informações suficientes para demonstrar a correta aplicação do RGPD? (N.ºs 32 a 41)

[905] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

ANEXO VI

Figura 10 - Fluxograma de código transnacional, segundo as Diretrizes n.º 1/2019 do Comitê Europeu para a Proteção de Dados

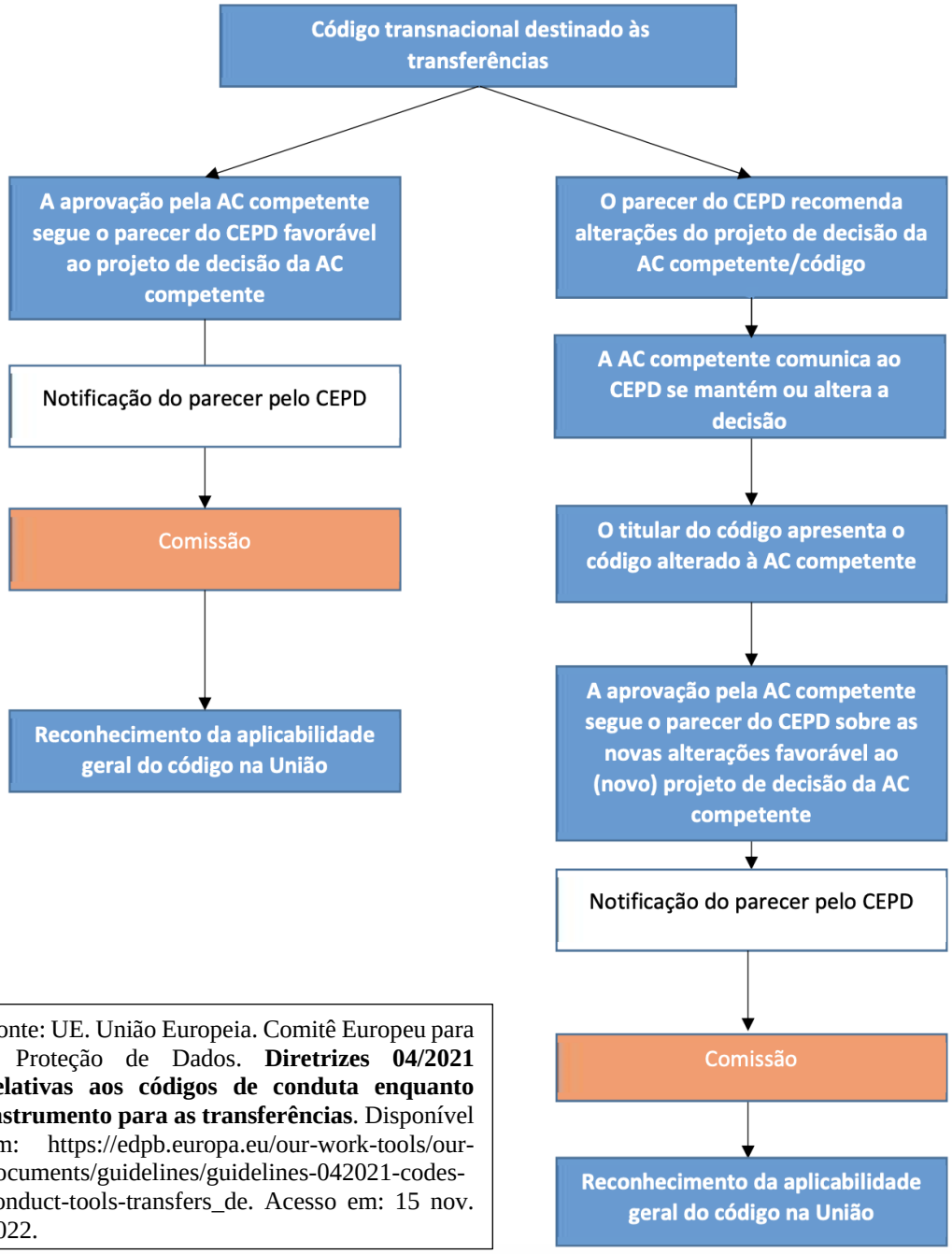


Fonte: UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2019 relativas aos Códigos de Conduta e aos Organismos de Supervisão ao abrigo do Regulamento (UE) 2016/679**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidemonitoring-bodies-0_pt. Acesso em: 15 nov. 2022.

ANEXO VII

Adoção do código de conduta para as transferências internacionais – Fluxograma, nos termos das Diretrizes n.º 4/202**1** do Comitê Europeu para a Proteção de Dados[906]

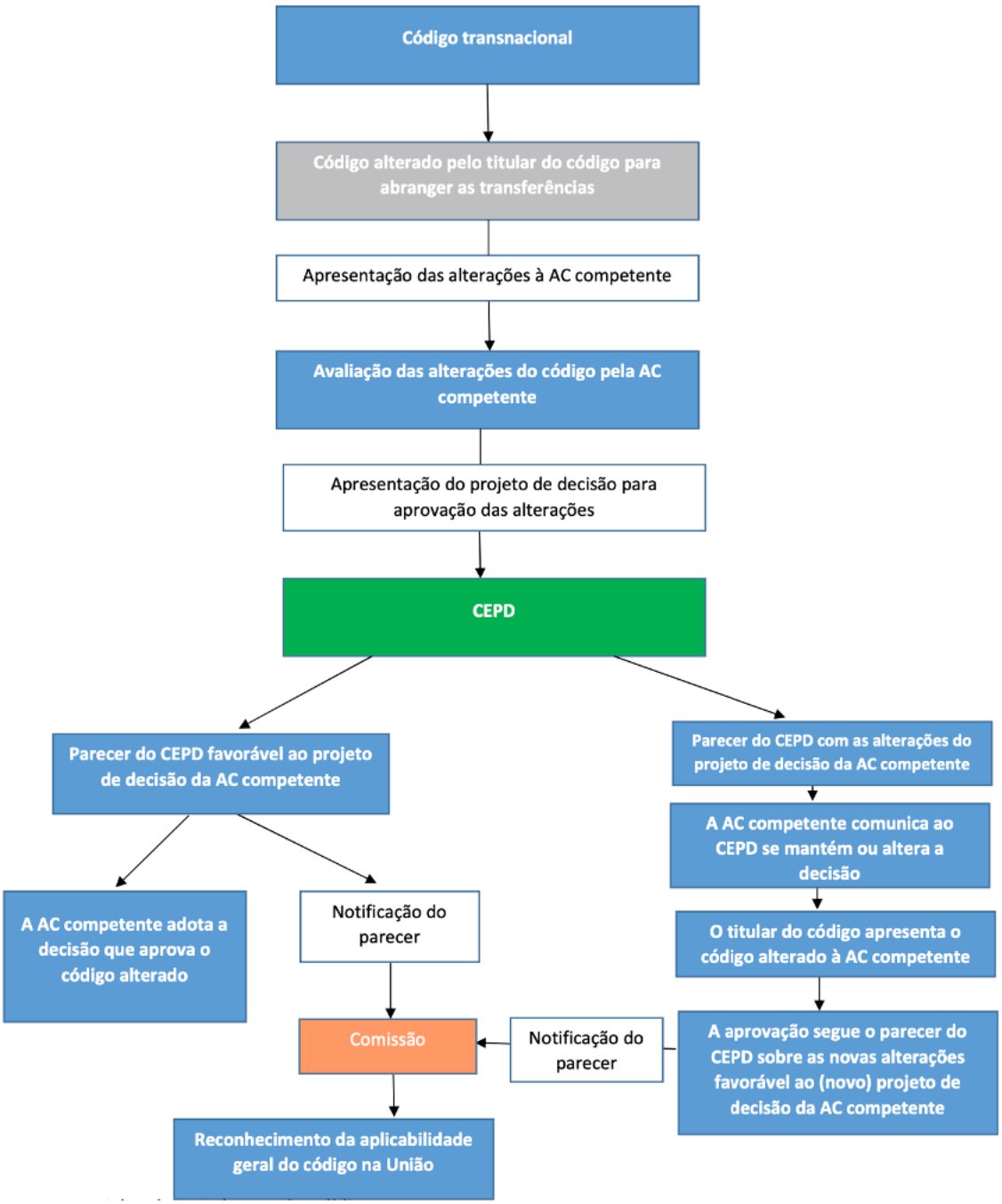
Figura 11 - Fluxograma (a) - Adoção de um código transnacional destinado às transferências



Fonte: UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 04/2021 relativas aos códigos de conduta enquanto instrumento para as transferências**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de. Acesso em: 15 nov. 2022.

[906] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 04/2021 relativas aos códigos de conduta enquanto instrumento para as transferências**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de. Acesso em: 15 nov. 2022.

Figura 12 - Fluxograma (b) - Alterações de um código transnacional a utilizar como código destinado às transferências



Fonte: UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 04/2021 relativas aos códigos de conduta enquanto instrumento para as transferências**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de. Acesso em: 15 nov. 2022.

ANEXO VIII

Tabela 5 - Atribuições e poderes das autoridades de controle em matéria de certificação em conformidade

	Disposições	Requisitos
Atribuições	Artigo 43.º, n.º 6	Estabelece que as autoridades de controle publiquem os critérios referidos no artigo 42.º, n.º 5, sob uma forma facilmente acessível e que os comuniquem ao Comitê.
	Artigo 57.º, n.º 1, alínea n)	Exige que a autoridade de controle aprove os critérios de certificação nos termos do artigo 42.º, n.º 5.
	Artigo 57.º, n.º 1, alínea o)	Estabelece que, se necessário (ou seja, quando emite uma certificação), a autoridade de controle proceda a uma revisão periódica das certificações emitidas, nos termos do artigo 42.º, n.º 7.
	Artigo 64.º, n.º 1, alínea c)	Exige que a autoridade de controle envie o projeto de decisão ao Comitê, quando vise aprovar os critérios de certificação a que se refere o artigo 42.º, n.º 5.
Poderes	Artigo 58.º, n.º 1, alínea c)	Estabelece que a autoridade de controle dispõe do poder de rever as certificações emitidas nos termos do artigo 42.º, n.º 7.
	Artigo 58.º, n.º 2, alínea h)	Estabelece que a autoridade de controle dispõe do poder de retirar ou ordenar ao organismo de certificação que retire uma certificação, ou de ordenar ao organismo de certificação que não emita uma certificação.
	Artigo 58.º, n.º 3, alínea e)	Estabelece que a autoridade de controle dispõe do poder de acreditar organismos de certificação.
	Artigo 58.º, n.º 3, alínea f)	Estabelece que a autoridade de controle dispõe do poder de emitir certificações e aprovar os critérios de certificação.
	Artigo 58.º, n.º 3, alínea e)	Estabelece que a autoridade de controle dispõe do poder de acreditar organismos de certificação.
	Artigo 58.º, n.º 3, alínea f)	Estabelece que a autoridade de controle dispõe do poder de emitir certificações e aprovar os critérios de certificação.

Fonte: UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022. (Com adaptações).

ANEXO IX

Orientações para garantir uma abordagem harmonizada aquando da avaliação dos critérios para efeitos de aprovação (Selo Europeu), segundo as Diretrizes n.º 1/2018 do Comitê Europeu para a Proteção de Dados[907]

1 Introdução

O anexo 2 fornece diretrizes para a análise e avaliação dos critérios de certificação nos termos do artigo 42.º, n.º 5. Identifica os tópicos que a autoridade responsável pela proteção de dados e o CEPD irão analisar e aplicar para a aprovação de critérios de certificação de um mecanismo de certificação. As perguntas que devem ser tidas em conta pelos organismos de certificação e pelos proprietários de sistemas de certificação que pretendem definir e apresentar critérios para aprovação. A lista não é exaustiva, mas apresenta os tópicos mínimos a considerar. Nem todas as perguntas serão aplicáveis; no entanto, devem ser tidas em conta no momento da elaboração dos critérios e, se for caso disso, será necessário explicar por que razão os critérios não abrangem determinados aspectos em específico. Algumas questões são repetidas, embora sob uma perspectiva diferente. Estas diretrizes devem ser consideradas em conformidade com os requisitos legais previstos pelo RGPD e, se for caso disso, pela legislação nacional.

2 Âmbito do mecanismo de certificação e alvo da avaliação («*Target of Evaluation*» - *ToE*)

a. O âmbito do mecanismo de certificação (para o qual devem ser aplicados os critérios de proteção de dados) é claramente descrito?

b. O âmbito do mecanismo de certificação é relevante para o público destinatário e não é suscetível de induzir a erro?

- *Exemplo: Um «selo de empresa de confiança» sugere que o conjunto das atividades de tratamento de uma empresa foram controladas, embora apenas certas*

[907] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf. Acesso em: 20 nov. 2022. A análise apresentada terá por substrato as citadas diretrizes. A análise que se seguirá terá por base as citadas diretrizes.

operações de tratamento específicas, como, por exemplo, o tratamento dos pagamentos em linha, são de fato sujeitas a certificação. O âmbito de aplicação induz, por conseguinte, a erro de percepção.

c. O âmbito do mecanismo de certificação reflete todos os aspectos relevantes das operações de tratamento?

- *Exemplo: Uma «marca de privacidade no domínio da saúde» deve incluir todos os dados de avaliação relativos à saúde, a fim de satisfazer os requisitos estabelecidos no artigo 9.º.*

d. O âmbito do mecanismo de certificação permite uma certificação de proteção de dados relevante, tendo em conta a natureza, o conteúdo e o risco das operações de tratamento conexas?

- *Exemplo: Se o âmbito do mecanismo de certificação se centrar apenas em aspectos específicos das operações de tratamento, como a recolha de dados, mas não sobre as operações de tratamento adicionais, como o tratamento para efeitos de criação de perfis para publicidade ou da gestão dos direitos dos titulares de dados, não seria relevante para os titulares dos dados.*

e. O âmbito do mecanismo de certificação abrange o tratamento de dados pessoais no país de aplicação pertinente ou compreende o tratamento transfronteiriço e/ou as transferências?

f. Os critérios de certificação descrevem suficientemente a forma como os ToE devem ser definidos?

- *Exemplo: Um «selo de privacidade» que ofereça um âmbito geral que exija «uma especificação do tratamento que é objeto da certificação» não fornece orientações claras e suficientes sobre a forma de estabelecer e descrever os ToE.*
- *Exemplo: Um âmbito (específico) de um «selo de privacidade para os cofres digitais», relativo à conservação segura dos dados pessoais, deveriam descrever pormenorizadamente os requisitos a preencher, como a definição de cofre, os requisitos do sistema, as medidas técnicas e organizativas obrigatórias. Deste modo, o âmbito pode definir claramente o ToE.*

(1) Os critérios exigem que o ToE inclua uma identificação de todas as operações de tratamento relevantes, uma ilustração dos fluxos de dados e a determinação do âmbito do TOE?

- *Exemplo: Um mecanismo de certificação oferece a certificação de operações de tratamento de responsáveis pelo*

tratamento de dados ao abrigo do RGPD sem especificar em pormenor o âmbito de aplicação (âmbito geral). Os critérios utilizados pelo mecanismo exigem que o responsável pelo tratamento de dados determine a operação de tratamento visada (ToE) em termos de tipos de dados, de sistemas e de processos utilizados.

(2) Os critérios exigem que o requerente indique claramente onde tem início e onde termina o tratamento sujeito a avaliação? Os critérios exigem que o ToE inclua interfaces sempre que as operações de tratamento interdependentes não estejam incluídas no ToE? E tal justifica-se de forma satisfatória?

- *Exemplo: Um ToE que descreve suficientemente em pormenor as operações de tratamento de um serviço em linha, como, por exemplo, o registo dos utilizadores, a prestação de serviços, a faturação, o registo dos endereços IP, as interfaces com os utilizadores e com terceiros, mas não o alojamento em servidor (incluindo todavia os contratos de tratamento e os contratos relativos às medidas técnicas e organizativas).*

g. Os critérios garantem que cada um dos ToE pode ser compreendido pelo público visado, incluindo, se for caso disso, os titulares dos dados?

3 Requisitos gerais

a. O conjunto dos termos pertinentes utilizados no catálogo de critérios (ou seja, no conjunto completo de critérios de certificação) são identificados, explicados e descritos?

b. Todas as referências normativas são identificadas?

c. Os critérios incluem a definição das responsabilidades em matéria de proteção de dados, dos procedimentos e do tratamento abrangidos pelo âmbito do mecanismo de certificação?

4 Operação de tratamento, artigo 42.º, n.º 1

No que diz respeito ao âmbito do mecanismo de certificação (geral ou específico), todos os componentes relevantes das operações de tratamento (dados, sistemas e processos) são abrangidos pelos critérios?

a. Os critérios exigem a identificação das bases jurídicas válidas do tratamento no que diz respeito ao ToE?

b. No que diz respeito ao ToE, os critérios reconhecem as fases relevantes do tratamento e todo o ciclo de vida completo dos dados, incluindo o apagamento e/ou anonimização?

c. No que diz respeito ao ToE, os critérios exigem a portabilidade dos dados?

d. No que diz respeito ao ToE, os critérios permitem identificar e refletir tipos especiais de operações de tratamento, como, por exemplo, a tomada de decisões automatizadas, a definição de perfis etc.?

e. No que diz respeito ao ToE, os critérios permitem identificar categorias especiais de dados?

f. Os critérios permitem e exigem a avaliação do risco das operações individuais de tratamento e das necessidades de proteção dos direitos e liberdades dos titulares dos dados?

g. Os critérios permitem e exigem uma contabilização adequada dos riscos para os direitos e liberdades das pessoas singulares?

...

5 Licitude do tratamento

a. Os critérios exigem a verificação da licitude do tratamento para as operações individuais de tratamento no que diz respeito à finalidade e à necessidade do tratamento?

b. Os critérios exigem o controle de todos os requisitos de uma base jurídica para operações individuais de tratamento?

6 Princípios, artigo 5.º

a. Os critérios integram de forma adequada todos os princípios de proteção de dados, em conformidade com o artigo 5.º?

b. Os critérios exigem a demonstração da minimização de dados para cada ToE?

...

7 Obrigações gerais dos responsáveis pelo tratamento e dos subcontratantes

a. Os critérios exigem prova de acordos contratuais entre subcontratantes e responsáveis pelo tratamento?

b. Os contratos entre responsáveis pelo tratamento e subcontratantes são sujeitos a avaliação?

c. Os critérios refletem as obrigações do responsável pelo tratamento nos termos do capítulo IV?

d. Os critérios exigem prova de revisão e atualização das medidas técnicas e organizativas implementadas pelo responsável pelo tratamento nos termos do artigo 24.º, n.º 1?

e. Os critérios verificam se a organização avaliou se um encarregado da proteção de dados (EPD) deve ser nomeado em conformidade com o artigo 37.º? Se for caso disso, o EPD preenche os requisitos previstos nos artigos 37.º a 39.º?

f. Os critérios verificam que os registos relativos às atividades de tratamento são exigidos em conformidade com o artigo 30.º, n.º 5, e respondem de forma adequada aos requisitos previstos no artigo 30.º?

8 Direitos dos titulares dos dados

a. Os critérios têm em conta de forma adequada o direito do titular dos dados à informação e exigem a adoção de medidas nesse sentido?

b. Os critérios exigem que aos titulares dos dados seja garantido um acesso e um controle adequados, ou mesmo maiores, dos seus dados, incluindo a portabilidade dos dados?

c. Os critérios exigem a adoção de medidas que prevejam a possibilidade de intervir na operação de tratamento de dados, a fim de garantir os direitos dos titulares dos dados e permitir as retificações, o apagamento ou a limitação do tratamento?

...

9 Riscos para os direitos e liberdades das pessoas singulares

a. Os critérios permitem e exigem uma avaliação dos riscos para os direitos e liberdades das pessoas singulares?

b. Os critérios preveem ou exigem uma metodologia de avaliação do risco reconhecida? Se for caso disso, é esta proporcional?

c. Os critérios permitem e exigem uma avaliação do impacto previsto do tratamento de dados nos direitos e liberdades das pessoas singulares?

d. Os critérios exigem uma consulta prévia sobre os riscos remanescentes que não possam ser atenuados, com base nos resultados da avaliação de impacto sobre a proteção de dados (AIPD)?

10 Medidas técnicas e organizativas que garantam a proteção

a. Os critérios exigem a aplicação de medidas técnicas e organizativas que prevejam a confidencialidade das operações de tratamento?

b. Os critérios exigem a aplicação de medidas técnicas e organizativas que prevejam a integridade das operações de tratamento?

c. Os critérios exigem a aplicação de medidas técnicas e organizativas que prevejam a disponibilidade das operações de tratamento?

d. Os critérios exigem a aplicação de medidas que garantam a transparência das operações de tratamento de dados no que respeita a:

e. Responsabilidade?

f. Direitos dos titulares de dados?

g. Avaliação de operações individuais de tratamento, por exemplo, em matéria de transparência algorítmica?

h. Os critérios exigem a aplicação de medidas técnicas e organizativas que garantam os direitos dos titulares dos dados, por exemplo, a capacidade de prestar informações ou a portabilidade dos dados?

i. Os critérios exigem a aplicação de medidas técnicas e organizativas que prevejam a possibilidade de intervir na operação de tratamento de dados, a fim de garantir o direito dos titulares dos dados e permitir as retificações, o apagamento ou a limitação do tratamento?

j. Os critérios exigem a aplicação de medidas que prevejam a possibilidade de intervir na operação de tratamento de dados, a fim de reparar ou verificar o sistema ou o processo?

k. Os critérios exigem a aplicação de medidas técnicas e organizativas para garantir a minimização dos dados, por exemplo, dissociando ou separando os dados do titular dos dados, mediante processos de anonimização ou de pseudonimização ou ainda de isolamento dos sistemas de dados?

l. Os critérios exigem medidas técnicas para implementar a proteção de dados por padrão?

m. Os critérios exigem medidas técnicas e organizativas para implementar a proteção de dados desde a concepção, por exemplo, um sistema de gestão da proteção de dados para demonstrar, informar, controlar e fazer cumprir os requisitos em matéria de proteção de dados?

n. Os critérios exigem a adoção de medidas técnicas e organizativas para assegurar a formação e educação periódicas adequadas para o pessoal que tem acesso permanente ou regular aos dados pessoais?

o. Os critérios exigem medidas de revisão?

p. Os critérios exigem uma autoavaliação/auditoria interna?

q. Os critérios exigem a adoção de uma medida que garanta que os deveres relativos à notificação de uma violação de dados pessoais são efetuados em tempo útil e com o alcance adequado?

r. Os critérios exigem o estabelecimento e a verificação de procedimentos de gestão de incidentes?

s. Os critérios exigem o acompanhamento da evolução das questões relacionadas com a privacidade e a tecnologia, bem como a atualização do sistema em função das necessidades?

...

11 Outras características especiais que respeitam a proteção dos dados

a. Os critérios exigem a aplicação de técnicas de reforço da proteção de dados? Tal poderia incluir critérios que exijam uma maior proteção dos dados, através da eliminação ou redução dos dados pessoais e/ou do risco para a proteção de dados.

Exemplo: Os critérios que exigem uma indissociação reforçada utilizando uma tecnologia de gestão da identidade centrada no utilizador, como a tecnologia «attribute-based credentials» (ABC), em vez de um método de gestão da identidade centrada na organização, iriam no sentido de uma técnica de reforço da proteção de dados.

b. Os critérios exigem a realização de controles reforçados dos titulares dos dados para facilitar a autodeterminação e a liberdade de escolha?

...

12 Critérios para demonstrar a existência de garantias adequadas para a transferência de dados pessoais

Estes critérios são tratados nas diretrizes n.º 07/2022, que ainda não se encontram em versão final, tendo em vista as contribuições recebidas pelo Comitê Europeu para a Proteção de Dados em consulta pública.[908]

13 Critérios adicionais para um selo europeu de proteção de dados

a. Os critérios preveem a cobertura de todos os Estados-Membros?

b. Os critérios podem ter em conta a legislação ou os cenários em matéria de proteção de dados dos Estados-Membros?

c. Os critérios exigem uma avaliação de cada ToE no que diz respeito às disposições setoriais da legislação dos Estados-Membros em matéria de proteção de dados?

d. Os critérios exigem que o responsável pelo tratamento ou o subcontratante forneçam informações aos titulares dos dados e às partes interessadas nas línguas dos Estados-Membros:

e. sobre o tratamento/ToE?

f. sobre a documentação do tratamento/ToE?

g. sobre os resultados da avaliação?

[908] UE. União Europeia. Comitê Europeu para a Proteção de Dados. **Guidelines 07/2022 on certification as a tool for transfers**. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-072022-certification-tool-transfers_pt. Acesso em: 20 nov. 2022. O documento, diferentemente de seu análogo referente aos códigos de conduta não será aqui examinado, eis que ainda não se encontra em versão final, após consulta pública. Isso porque a consulta pública ao documento encerrou-se em 30 de setembro do ano corrente, ainda estando pendente sua consolidação.

...

14 Avaliação global dos critérios

a. Os critérios abrangem integralmente o âmbito do mecanismo de certificação (ou seja, são critérios abrangentes) para oferecer garantias suficientes de que a certificação é de confiança?

Exemplo: Se o âmbito do mecanismo de certificação se centrar nas operações de tratamento de dados de saúde, deve ser garantido um nível elevado de proteção de dados mediante a definição de critérios que garantam, por exemplo, uma avaliação aprofundada e a aplicação de princípios de privacidade desde a conceção e de privacidade por defeito.

b. Os critérios são consentâneos com a dimensão da operação de tratamento abrangida pelo âmbito do mecanismo de certificação, com a sensibilidade das informações e com o risco de tratamento?

c. São os critérios suscetíveis de melhorar a proteção dos dados dos responsáveis pelo tratamento e dos subcontratantes?

d. Os titulares dos dados irão beneficiar no que diz respeito aos seus direitos de ser informados, incluindo a explicação dos resultados pretendidos?

ANEXO X

Figura 13 - Demandas recebidas até 31/07/2022

Fonte: PECK, Patricia. Palestra proferida por Patricia Peck na Escola Superior do Tribunal de Contas do Estado de Mato Grosso, sobre o tema "**Impactos da LGPD para órgãos de controle**", em 23 de agosto de 2022.

Figura 14 - Demandas recebidas até 31/10/2022.

Fonte: BRASIL. Autoridade Nacional de Proteção de Dados. **Ouvidoria em números**. Disponível em: https://app.powerbi.com/view?r=eyJrIjoiMjJmZTFiYjQtZjVmYy00MjRkLWJlNzYtN2JhY2E1MjUxZDAwIiwidCI6IjFjYzNjNTA4LTAxYzctNDQ2MC1iZDJiLWFmZTk1ZTgwYjhhZiJ9&pageName=ReportSectionf292577b6e0ea006d936. Acesso em: 23 nov. 2022.

ANEXO XI

Em nosso sentir, embora não tenhamos notícias de um cadastro negativo específico (lista-suja) que envolva os incidentes e infrações em matéria de privacidade e proteção de dados pessoais, existem duas previsões normativas na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) que, ainda que não se confundam com a listagem, representariam um estímulo a essa prática.

Referimo-nos à previsão do artigo 48, §2º, inciso I, disciplinando a possibilidade de divulgação de incidentes de vazamento de dados pessoais (tratado no corpo da tese – parte III, capítulo 3.3. Listas sujas); e a do artigo 52, inciso IV, tratando da possibilidade de aplicação da sanção de publicização da infração, após devidamente apurada e confirmada a sua ocorrência pela Autoridade de Nacional de Proteção de Dados Pessoais, veja-se:

> **Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.**
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - os riscos relacionados ao incidente;
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
> **§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:**
> **I - ampla divulgação do fato em meios de comunicação; e**
> II - medidas para reverter ou mitigar os efeitos do incidente.
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.
>
> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III - multa diária, observado o limite total a que se refere o inciso II;
IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI - eliminação dos dados pessoais a que se refere a infração;
VII - (VETADO);
VIII - (VETADO);
IX - (VETADO).
X - (VETADO);
XI - (VETADO);
XII - (VETADO).
X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)
§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
II - a boa-fé do infrator;
III - a vantagem auferida ou pretendida pelo infrator;
IV - a condição econômica do infrator;
V - a reincidência;
VI - o grau do dano;
VII - a cooperação do infrator;
VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
IX - a adoção de política de boas práticas e governança;
X - a pronta adoção de medidas corretivas; e
XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.
§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica.
§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal) , na Lei nº 8.429, de 2 de junho

de 1992 (Lei de Improbidade Administrativa) , e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.
§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.
§ 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995.
§ 6º (VETADO).
§ 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas:
I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e
II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos.
§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (Sem grifos no original).

A previsão, no que diz respeito à aplicação da sanção de publicização da infração, no entanto, dependia de regulamentação o que veio a ser feito recentemente pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD), por meio da edição da Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, que aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas pela Autoridade Nacional de Proteção de Dados Pessoais.

O regulamento disciplina a forma de aplicação da sanção de publicização das infrações cometidas por pessoas jurídica de direito público ou privado, nos seguintes termos:

CAPÍTULO II
DA APLICAÇÃO DAS SANÇÕES
Seção I
Das Sanções Administrativas
Art. 3º As infrações sujeitarão o infrator às seguintes sanções administrativas:

I - advertência, nos termos do art. 9º deste Regulamento;
II - multa simples, nos termos dos arts. 10 a 15 deste Regulamento;
III - multa diária, nos termos do art. 16 deste Regulamento;
IV - publicização da infração, após devidamente apurada e confirmada a sua ocorrência, nos termos dos arts. 20 e 21 deste Regulamento;
V - bloqueio dos dados pessoais a que se refere a infração, até a sua regularização, nos termos do art. 22 deste Regulamento;
VI - eliminação dos dados pessoais a que se refere a infração, nos termos do art. 23 deste Regulamento;
VII - suspensão parcial do funcionamento do banco de dados a que se refere a infração, nos termos do art. 24 deste Regulamento;
VIII - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração, nos termos do art. 25 deste Regulamento; e
IX - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados, nos termos do art. 26 deste Regulamento.
§ 1º As sanções previstas nos incisos VII, VIII e IX do caput deste artigo somente serão aplicadas após já ter sido imposta ao menos uma das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto.
§ 2º Na hipótese do § 1º deste artigo, a ANPD dará ciência ao principal órgão ou entidade reguladora setorial, com competências sancionatórias, a que se submete o controlador, durante a fase de instrução, para que se manifeste sobre eventuais consequências da imposição das sanções para o exercício de atividades econômicas reguladas desenvolvidas pelo controlador, especialmente na prestação de serviços públicos, assim como forneça outras informações que entender pertinentes.
§ 3º O órgão ou entidade reguladora setorial terá prazo de até 20 (vinte) dias úteis, prorrogável uma única vez por igual período, após o qual o processo poderá ter prosseguimento e ser decidido mesmo sem a manifestação.
§ 4º O infrator poderá se manifestar sobre as informações apresentadas pelo órgão ou entidade reguladora setorial em suas alegações finais.
§ 5º O disposto nos incisos I e IV a IX, do caput deste artigo, poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.

Seção VII
Da Publicização da Infração
Art. 20. A ANPD poderá aplicar ao infrator a sanção de publicização, considerando a relevância e o interesse público da matéria.
§ 1º A sanção de publicização consiste na divulgação da infração pelo próprio infrator, após devidamente apurada e confirmada a sua ocorrência.
§ 2º A sanção de publicização deverá indicar o teor, o meio, a duração e o prazo para o seu cumprimento.
§ 3º Os ônus relacionados à publicização da infração serão suportados exclusivamente pelo infrator.

Art. 21. A sanção de publicização da infração não se confunde com a publicação de decisão de aplicação de sanção administrativa no Diário

> Oficial da União ou com os demais atos realizados pela ANPD, para fins de atendimento ao princípio da publicidade administrativa. (Sem grifos no original).

A sanção de publicização da infração, embora possa inspirar o desenvolvimento de um cadastro de infratores (uma listagem ou lista suja), com ela não se confunde. Enquanto a elaboração de um cadastro negativo centraliza a informação sobre incidentes, infrações e outras formas de atuação da Autoridade Nacional de Proteção de Dados Pessoais; a sanção de publicização, consistente na divulgação da infração pelo próprio infrator, tem seu alcance reduzido, ficando restrita, portanto, aos usuários do serviço ou produto ofertado pela pessoa jurídica sancionada.

A sanção, ali, teria um escopo específico de alertar os usuários do serviço ou produto afetado, oferecendo-lhes informações sobre o ocorrido. O papel desse tipo de atuação continuaria circunscrito a pequenos nichos de mercado e disperso na rede, tal como ocorre atualmente com as sistemáticas notícias veiculadas a respeito de incidentes de segurança envolvendo os dados pessoais de centenas de milhões de indivíduos.

Assim, a sanção de publicização teria um escopo restrito frente à listagem.

Hodiernamente, no entanto, a medida que mais se assemelha à listagem foi adotada de forma recentíssima (em 23/03/2023) pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e consiste na divulgação, com fundamento no princípio da publicidade[909] e na ideia de transparência ativa, de uma lista de processos sancionatórios de empresas e órgãos públicos que aguardam conclusão pela Autoridade Nacional de Proteção de Dados Pessoais.[910]

A lista dos processos administrativos sancionatórios instaurados (e ainda ainda não concluídos) pela Coordenação-Geral de Fiscalização (CGF) contém o nome do órgão público ou empresa privada fiscalizada, a conduta, em tese, realizada, o setor de atuação do ente fiscalizado, a fase em que se encontra o processo e o número do processo aberto na ANPD.

---

[909] Estampado no artigo 48, da Portaria nº 1, de 8 de março de 2021, que Estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados - ANPD., veja-se:
"CAPÍTULO II
DOS PROCEDIMENTOS ADMINISTRATIVOS
Art. 48. As atividades da ANPD obedecerão, além dos princípios estabelecidos na Lei n° 13.709, de 2018, aos princípios da legalidade, motivação, moralidade, eficiência, celeridade, interesse público, impessoalidade, igualdade, devido processo legal, ampla defesa, contraditório, razoabilidade, proporcionalidade, imparcialidade, **publicidade**, economicidade, segurança jurídica, entre outros."

[910] BRASIL. Autoridade Nacional de Proteção de Dados. **ANPD divulga lista de processos sancionatórios**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-sancionatorios. Acesso em: 23 mar. 2023.

A notícia veiculada pela Autoridade[911] informa que os dados sobre quais sanções serão aplicadas para cada caso, somente se tornarão públicas após a conclusão da investigação que confirme que a conduta do agente resulta ou não em uma punição de fato, respeitados os direitos de ampla defesa e do contraditório.

A nota divulgada ainda aponta que, conforme, "orientação da procuradoria da ANPD, a sanção de publicização, prevista na Lei Geral de Proteção de Dados Pessoais, não impede e não se confunde com a divulgação dos dados e informações referentes ao processo administrativo sancionador em curso" e que "a Coordenação-Geral de Fiscalização e a Assessoria de Comunicação criarão uma página no sítio eletrônico da ANPD em que essas informações ficarão disponíveis para livre conhecimento de qualquer cidadão". [912]

A criação da lista pela ANPD, como mecanismos de publicidade e transparência ativa, se assemelha com os mecanismos de listagem (lista suja) aqui tratado, mas com ela não confunde. Isso porque, embora a nota divulgada traga a ideia de que após concluídos os processos fiscalizatórios, o resultado da atuação da Autoridade de Controle será publicizado, dando amplo conhecimento à sociedade sobre o resultado da fiscalização, esse resultado pode se referir à constatação ou não de uma infração, caso em que será aplicada ou não uma sanção.

A listagem elaborada pela ANDP, relativa aos processos em curso, por se tratar de um instrumento de transparência e publicidade, não possui os mesmos efeitos de um cadastro negativo, na medida em que reúne todos os processos em curso, ainda que, ao final, não se constate a ocorrência de uma infração a ser punida pela Autoridade de Nacional de Proteção de Dados Pessoais.

O cadastro negativo, ao contrário, reuniria apenas os processos finalizados, que resultassem em alguma forma de infração comprovada, de forma que o simples fato da pessoa jurídica de direito público ou privado figurar nesse cadastro fosse desabonador o suficiente para evitar condutas desconformes.

Assim, a nosso ver, a previsão do artigo 48, §2º, inciso I, da Lei Geral de Proteção de Dados Pessoais, disciplinando a possibilidade de divulgação de incidentes de

[911] BRASIL. Autoridade Nacional de Proteção de Dados. **ANPD divulga lista de processos sancionatórios**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-sancionatorios. Acesso em: 23 mar. 2023.
[912] BRASIL. Autoridade Nacional de Proteção de Dados. **ANPD divulga lista de processos sancionatórios**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-sancionatorios. Acesso em: 23 mar. 2023.

vazamento de dados pessoais, é aquela que mais se adequa à ideia que defendemos, como estímulo a que a regulamentação de um cadastro ou listagem negativa (lista suja) seja regulamentada no futuro.[913]

Por essa razão, apenas a disciplina do artigo 48, §2º, inciso I, da Lei Geral de Proteção de Dados Pessoais foi tratada no corpo do texto, apresentando-se este esclarecimento (*disclaimer*) ao final.

[913] Regulamentação esta que poderia prever, inclusive, forma de reabilitação da pessoa jurídica infratora, nas situação em que esteja em causa uma irregularidade sanável.