MILTON RODRIGUES DE ARAGÃO

O COMEÇO, MEIO E FIM, DO TRATAMENTO DE DADOS PESSOAIS E AS POSSÍVEIS CONSEQUÊNCIAS JURÍDICAS E FINANCEIRAS PARA O ESTADO, SOB A ÉGIDE DA LEI 13.709/2018

Trabalho de Conclusão de Curso Apresentado como requisito para a conclusão da graduação em Direito da EDAP.

Orientador: Prof. Dr. Guilherme Pereira Pinheiro

BRASÍLIA
JULHO, 2020

MILTON RODRIGUES DE ARAGÃO

O COMEÇO, MEIO E FIM, DO TRATAMENTO DE DADOS PESSOAIS E AS POSSÍVEIS CONSEQUÊNCIAS JURÍDICAS E FINANCEIRAS PARA O ESTADO, SOB A ÉGIDE DA LEI 13.709/2018

Trabalho de Conclusão de Curso apresentado à banca examinadora, como requisito para a conclusão do curso de Direito e obtenção do título de bacharel em Direito pela Escola de Direito e Administração Pública – EDAP/IDP.
Orientador: Prof. Dr. Guilherme Pereira Pinheiro.

Brasília, julho de 2020.

Professor Dr. Guilherme Pereira Pinheiro
Membro da Banca Examinadora

Professor Dra. Miriam Wimmer
Membro da Banca Examinadora

Professor Me Alexandre Sankievicz
Membro da Banca Examinadora

O COMEÇO, MEIO E FIM, DO TRATAMENTO DE DADOS PESSOAIS E AS POSSÍVEIS CONSEQUÊNCIAS JURÍDICAS E FINANCEIRAS PARA O ESTADO, SOB A ÉGIDE DA LEI 13.709/2018

THE BEGINNING, MIDDLE AND END, OF THE PROCESSING OF PERSONAL DATA AND THE POSSIBLE LEGAL AND FINANCIAL CONSEQUENCES FOR THE STATE, UNDER LAW 13.709/2018

Milton Rodrigues de Aragão

RESUMO: O presente artigo tem como objetivo avaliar eventuais adequações pelas quais a Lei Geral de Proteção de Dados brasileira passará, pois é evidente a inquietação nos diversos setores da macroeconomia, visto as obscuridades trazidas em seu texto e pelo fato do país não possuir uma base unificada de armazenamento de dados, o que já é cultural e perceptível, principalmente nos órgãos públicos.

PALAVRAS-CHAVE: Formação de Banco de Dados. Vazamentos de Dados. Prejuízo ao Estado. Adequações.

ABSTRACT: The purpose of this article is to evaluate any adjustments that the Brazilian General Data Protection Law will go through, as it is evident the concern in the various sectors of macroeconomics, given the obscurities brought in its text and the fact that the country does not have a unified database of data storage, which is already cultural and noticeable, especially in public agencies.

KEYWORDS: Database Formation. Data Leaks. Loss to the State. Challenge.

INTRODUÇÃO

O desenvolvimento tecnológico rápido, nas décadas de 60 e 70, trouxe as primeiras preocupações sobre o armazenamento e a utilização de dados pessoais, à medida que computadores passariam a ser usados por indivíduos, corporações e governos em todo o mundo, com a capacidade de armazenamento fácil, rápido e amplo de informações, algo nunca testemunhado pela humanidade[1].

A revolução tecnológica advinda do século XX, e a transformação da função do Estado, contribuem para modificar o sentido e o alcance do direito à privacidade. É nesse caminho que o século passado vivenciou o processo de reinvenção da privacidade[2]. Além de adquirir um caráter positivo e de ser reconhecido no âmbito internacional, o direito à privacidade transformou-se para fazer emergir a dimensão de proteção de dados pessoais, à medida que surgiram novos desafios ao ordenamento jurídico a partir do tratamento informatizado dos dados[3]. Essas transformações foram percebidas de forma mais evidente a partir da década de 70, onde chegou-se a um consenso de que os dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto merecem uma tutela jurídica, o que corroborou para a edição de legislações específicas e de decisões judiciais de diversos países, e consequentemente para a aprovação de acordos internacionais em diferentes níveis. O processamento eletrônico de dados nas administrações públicas e nas empresas privadas fez surgir a primeira geração de normas de proteção de dados pessoais, assim como a centralização dos bancos de dados em imensos bancos de dados nacionais.

A proteção de dados pessoais abordada pelas legislações nacionais seguiu o mesmo caminho adotado pela comunidade internacional. Um exemplo disso foi a lei do recenseamento alemã, que visava à coleta de dados dos cidadãos referentes à profissão, moradia e local de trabalho, com a intenção de fornecer à administração

---

[1] SAUAIA, Hugo Moreira Lima. **A proteção dos dados pessoais no Brasil. Rio de Janeiro**: Lumen Juris, 2018. p.93.
[2] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008. p. 15.
[3] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 23.

pública 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 nessa lei, que estabelecia também uma multa para o cidadão que se recusasse a responder. O § 9º desta norma determinava que os dados poderiam ser comparados àqueles presentes em registros públicos, com a finalidade de averiguar a veracidade das informações fornecidas, além de possibilitar a sua transmissão de forma anônima a órgãos federais, gerando assim inúmeras reclamações inconstitucionais contra a lei do recenseamento, ocasionando o julgamento pelo Tribunal Constitucional alemão, em 25 de março de 1982, que considerou a inconstitucionalidade parcial da lei, argumentando a existência de um direito à autodeterminação informativa. Afirmou ainda a Corte que o moderno processamento de dados pessoais configura uma grave ameaça à personalidade do indivíduo, na medida que possibilita o armazenamento ilimitado de dados, bem como permite a sua combinação de modo a formar um retrato complexo da pessoa, sem a sua efetiva participação ou conhecimento[4]. O julgamento foi um marco para a questão da proteção de dados pessoais e consolidou a ideia de que a proteção de dados pessoais baseia-se em um direito subjetivo fundamental, que limitou ao poder legislativo, e passa a estar vinculado à configuração de um direito à autodeterminação da informação.

No Brasil ainda não existia uma lei geral de proteção de dados pessoais, nos moldes europeus, em que a regulação geral do tema se dá por meio de um único instrumento legal, que prevê normas gerais, princípios, direitos e procedimentos, além de estabelecer o controle administrativo, civil e penal. Considerando a ausência dessa lei geral no país, fez-se necessário que a harmonização das mais diversas normas sobre proteção de dados fosse realizada pela doutrina e a jurisprudência, com a finalidade de construir um sistema de proteção de dados que, nos termos da constituição Federal, proteja efetivamente a personalidade do cidadão[5].

A lei n. 13.709/2018, que foi promulgada em agosto de 2018 e foi originária do PLC n. 53/2018, é um novo marco legal brasileiro de grande impacto, tanto para as instituições públicas quanto para as privadas, por tratar da proteção dos dados

[4]MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. p. 29-31.
[5] Ibid., p. 141

pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural ou jurídica. Traz em seu texto a regulamentação de princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionadas às pessoas. Reúne uma série de normas de controle para assegurar o cumprimento das garantias previstas cujo objetivo é a proteção dos direitos humanos[6].

A lei estava prevista para entrar em vigor em agosto de 2020, dando um período de dezoito meses a partir da sua promulgação, assim teriam tempo hábil tanto para a iniciativa pública quanto a privada para a sua adaptação, considerando qualquer porte e segmento de mercado e a necessidade de atender às exigências de forma eficiente e sustentável, atingindo um nível de proteção de dados inclusive em âmbito internacional quanto a tratamento dos dados fora do Brasil. Ao término desse prazo, poderão, então, ser elevadas, seguindo a mesma tendência das demais regulamentações sobre a mesma matéria em outros países, inspirada, especialmente, pelo Regulamento Europeu de Proteção de Dados Pessoais, também conhecido como GDPR. O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter o compromisso de cumprir uma série de princípios, de um lado, e de itens de controles técnicos para o uso de informações que venham a identificar uma pessoa, ou esteja relacionada a ela, incluindo a categoria de dados sensíveis, trazendo a segurança das informações[7].

O art. 7º da Lei que trata da questão do consentimento, revela que, ao longo dos anos, a necessidade do assentimento na coleta dos dados, principalmente no ambiente virtual, foi ganhando importância em razão da sensibilidade e da vulnerabilidade que as informações pessoais foram adquirindo com o desenvolvimento da tecnologia. Nesse sentido, garantir que as pessoas/usuários tenham ciência de que devem consentir o uso dos dados, assim como tenham direito

[6] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à Lei n.13.709/2018(LGPD)**. São Paulo: Saraiva, 2018. p.178
[7] Ibid., p. 190-191

de saber a finalidade da coleta e acesso ao seu conteúdo em qualquer momento, é primordial para assegurar a liberdade e a privacidade[8].

Ao mesmo tempo as empresas devem ter a liberdade de utilizar os dados de maneira transparente e ética em troca de um serviço ou acesso, tendo em vista que o desenvolvimento econômico também deve ser garantido a esses sujeitos. Importante destacar que cabe à instituição que realiza o tratamento a demonstração de que estava legítima (detinha o registro do consentimento ou se enquadrava nas hipóteses de exceção). Como já observado, considerando o cenário brasileiro de preocupação com segurança, houve um cuidado com a questão de trazer garantias de exceções de consentimento, por exemplo, na situação da proteção do crédito[9]

Dessa forma, o presente estudo tem como problemática os dados pessoais tratados por empresas públicas e privadas. Procurará demonstrar, principalmente, a fragilidade dos bancos de dados públicos e a dificuldade que as entidades privadas terão na sua coleta, tratamento, eliminação e armazenamento para o adequamento da Lei 13.709/2018. Exporá parte dos resultados da pesquisa desenvolvida na graduação de direito, pela Escola de Direito e Administração Pública – EDAP/IDP.

Na metodologia utilizada no desenvolvimento da pesquisa serão utilizadas leituras bibliográficas, buscando a opinião crítica de seus elaboradores e, leituras de periódicos, sejam revistas, impressas ou digitais. O enfoque no tema é justificado pela percepção da grande necessidade de um marco regulatório mais coeso para a proteção de dados pessoais.

1 BANCO DE DADOS

O Estado tem o seu papel primordial no desenvolvimento da economia da informação, pois tudo começou através da cultura de estatística e de pesquisa de

[8] Ibid., p. 814.
[9] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018(LGPD)**. São Paulo: Saraiva, 2018. p. 833.

informação dos cidadãos, bem como ao transferir para o setor privado essas informações coletadas oficialmente, ainda que de forma anônima.

De posse desses dados empresas do ramo de análise de risco, crédito e marketing direto desenvolveram programas específicos para o mapeamento demográfico das pessoas, uniformizando assim o tratamento para todos os moradores de determinada região[10]. Outra forma da obtenção de dados de pessoas era feito principalmente através de transações comerciais, onde obtinha-se dados cadastrais no momento da compra de algum produto ou realização de serviço. Cadastro esse que era feito na primeira transação comercial, para maior segurança da empresa em caso de pagamento com cheque ou cartão de crédito, ou simplesmente para a obtenção dos dados dos clientes. E era através desses dados obtidos que grandes lojas de departamentos faziam o perfil desse consumidor passando a lhe ofertar produtos específicos, avaliando e classificando o consumidor em relação à sua frequência na loja e ao seu poder aquisitivo.

Hoje, com economia cada vez mais migrando para a internet, onde as empresas não têm a possibilidade de coletar informações de seus clientes de modo pessoal, como ocorria em tempos atrás, onde vendedores conheciam os gostos e hábitos de consumidores por meio do contato pessoal, esses dados são obtidos, muitas vezes sem que o consumidor tenha o conhecimento pleno da coleta.

Ao fazermos uso da tecnologia colocada a nossa disposição, tais como telefone celular, cartões de crédito, as mídias sociais, acabamos por participar ativamente no processo de concessão de suas informações às empresas, eis que muitas das vezes sequer há consciência exata das consequências de sua ação[11]. O fato é que de forma indireta acabamos por participar de uma espécie de tratamento de dados, seja para fins lícitos ou ilícitos, que no mundo empresarial é chamado de persona, que é a representação fictícia do seu cliente, baseando-se em dados reais sobre comportamento e características demográficas dos seu alvos, apresentando suas histórias pessoais, motivações, objetivos, preocupações e desafios. Os dados tratados vão além de uma pesquisa numérica, pois não classifica os dados apenas

[10] MENDES, Laura Schertel**. Privacidade, proteção de dados e defesa do consumidor, linhas gerais de um novo direito fundamental**, São Paulo: Saraiva, 2014. p. 97-98.
[11] Ibid.; p. 95

por sexo, idade ou região, mais sim, pelos hábitos de consumo e preferências pessoais. Veja que nesse contexto a persona anda plenamente em conformidade com a LGPD, no que tange a dados sensíveis (art. 5º, inciso II).

Como demonstrado, a sociedade atual possui variadas fontes de coleta de dados de seus cidadãos, sejam por transações comerciais, os censos e registros realizados por entes públicos, bem como pelas tecnologias disponíveis na internet. No entanto, para que haja o fornecimento, seja de um serviço ou crédito, para a diminuição os riscos iminentes, as empresas precisam lapidar essas informações coletadas, a fim de buscar informações mais completas sobre hábitos e comportamento dos consumidores ou cliente em potencial.

Esta abordagem reflete-se em inúmeros documentos nacionais e internacionais, principalmente na Carta de Direitos Fundamentais da Comunidade Europeia, na qual a proteção de dados é reconhecida como um direito fundamental autônomo. Ainda assim, é cada vez mais difícil respeitar essa presunção geral, uma vez que exigências de segurança interna e internacional, interesses de mercado e a reorganização da administração pública estão levando à diminuição de salvaguardas importantes, ou ao desaparecimento de garantias essenciais.

Cataria Sarmento e Castro refere-se à “criação e manutenção de um conjunto estruturado de dados pessoais como sendo a atividade que implica perigo para os titulares dos dados pessoais e, consequentemente, justifica a sujeição dos responsáveis a certas obrigações[12]

Lembra Rodotà que há alguns anos atrás, Scott MacNally, CEO da Sun Systems, disse com sinceridade: “vocês não têm nenhuma privacidade, e de qualquer modo. Aceitem isso”. Atualmente, podemos sustentar com segurança que a privacidade mental, a mais íntima esfera, está sob ameaça, violando dimensão mais reclusa de uma pessoa. Logo percebe-se que a privacidade, além de não ser mais vista como um direito fundamental, é, de fato, frequentemente considerada um obstáculo à segurança, sendo superada por legislações de emergência. Nesse sentido, alguns dos princípios subjacentes ao sistema de proteção de dados estão

[12] CASTRO, Catarina e Sarmento e. **Direito da Informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005.

sendo ignorados para que certos propósitos possam ser atingidos. E isso tem relação com à separação de dados processados por órgãos públicos e os processados por entidades privadas[13].

Nota-se que a perspectiva levantada por Rodotà adequa-se plenamente à situação atual do Brasil, em relação a sua lei de proteção de dados, que foi aprovada em 14 de agosto de 2018, com previsão da entrada em vigor em 16 de agosto de 2020, e adiada, através da Medida Provisória 959, assinada pelo Presidente Bolsonaro, que prorrogou a vacatio legis da lei para 3 de maio de 2021.

A Lei 13.709, Lei de Proteção de Dados Pessoais, foi sancionada em 14 de agosto de 2018 sem ter uma base sólida, e não demorou para as críticas aparecerem, tanto que nem chegou a vigorar e já houve a sua prorrogação, como dito acima.

Impossível não notar a contradição. A base de dados de que falamos seria uma base de dados sólido e unificado a nível nacional, com os dados de todos os cidadãos. De tal forma seria como construir uma casa primeiramente pelo telhado, sem uma base que a sustentasse. Desse modo logo percebeu-se que havia fragilidades perceptíveis que tinham que ser sanadas.

Assim, no dia 10 de outubro de 2019 foi assinado pelo presidente Jair Bolsonaro os Decretos nºs 10.046 e 10.047, dando origem respectivamente ao Cadastro Base do Cidadão e o Comitê de Governança de Dados, que será uma base única para a centralização de dados pessoais de todos os brasileiros. A princípio esse cadastro conterá dados contendo nome completo, nome social, filiação, sexo, RG, CPF, naturalidade, nacionalidade, ou de qualquer alteração que possivelmente tenha sofrido, e a indicação de óbito.

Na base de dados estarão contidos tanto dados cadastrais, biográficos, como biométricos, sendo que este último incluí características biológicas e comportamentais mensuráveis da pessoa natural, que poderão ser coletadas, por meios automatizados, tais como a palma da mão, as digitais dos dedos, retina ou íris dos olhos, formato da face, a voz, e a maneira de andar (BRASIL, 2019). De acordo com o decreto, tais

[13] RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008. p. 13-14.

medidas visam o compartilhamento por diferentes órgãos da União, buscando a orientação, otimização, formulação, implementação, avaliação e o monitoramento de políticas públicas. Dispõe ainda o decreto que o compartilhamento desses dados estará disponível em três níveis para as entidades, e que o compartilhamento amplo só será possível quando se tratar de dados públicos que não estejam sujeitos a nenhuma restrição de acesso. Já o segundo nível disporá de dados protegidos por sigilo, como manda a legislação. Todavia essas regras serão simplificadas e estabelecidas pelo Comitê Central de Governança de Dados. O terceiro nível ficará a cargo do gestor de dados, que definirá o compartilhamento específico. De acordo com o decreto 10.046, o cadastro base do cidadão trará informações que unificará os serviços públicos, melhorando a sua gestão e aumentando a confiabilidade nos cadastros existentes (BRASIL, 2019, art. 16).

O Decreto 10.047 expõe quais dados serão disponibilizados no Cadastro Nacional de Informações Sociais (CNIS). O fato é que quando dados forem solicitados para pesquisas não haverá necessidade de contratos ou convênio, ao qual abrirá margem para o compartilhamento de dados com outras entidades privadas.

O Decreto 10.047 trouxe fatos que não passaram despercebidos por especialistas que acompanham há mais de quatro anos o desenrolar da LGPD, pois ao se permitir o acesso a um conjunto de dados tão rico, como demanda o art. 4º ele determina que uma das finalidades é “incentivar o intercâmbio de experiências e de conhecimentos entre órgãos e entidades públicas ou privadas envolvidos na promoção de políticas sociais. “Pode-se gerar uma situação complicada, a pretexto de permitir análise e inovação a um tipo de unificação inédita, como afirma Rafael Zanatta, advogado e pesquisador da Lavits, Rede Latino de Estudos sobre Vigilância, Tecnologia e Sociedade. “Tem informação pessoal que pode escoar para o setor privado com um mero ato normativo”, diz Danilo Doneda, professor de Direito Civil no Instituto de Direito Público, e um dos responsáveis por elaborar o texto da LGPD, ambos, em entrevista concedida ao portal *The Intercept Brasil*[14].

[14] Disponível em: [https://theintercept.com/2019/10/15/governo-ferramenta-vigilancia/?fbclid=IwAR3rCoD-COM1V73pPdq2UeAXTHkNY_F4wuesoT4DESgXuJzRmsEB5qxnoNc]. Acesso em 6 de jan. 2020.

Logo, percebe-se que tais medidas contrariam a Lei Geral de Proteção de Dados, que é a principal regulamentação de privacidade no Brasil. A norma determina que os dados só poderão ser usados para o mesmo fim a que se destina, ou seja para os quais foram permitidos (como por exemplo, o cadastro em um site para a compra de um determinado produto), que após a concretização na operação de compra e venda, o consumidor pode exigir o acesso a seu dados, podendo altera-los ou simplesmente apaga-los (art. 18, VI).

De todo modo percebe-se que as medidas para a contenção da problemática que assola a sociedade estão sendo tomadas, e a percepção de sua eficácia só veremos após a entrada em vigor da lei.

2 O ARMAZENAMENTO DE DADOS

Sabemos que desde o nascimento temos nossos dados armazenados em órgãos governamentais, como cartórios de registros, e que lá ficam. Para se ter qualquer informação a respeito desses dados ali armazenados só o próprio titular ou seu representante, ou por meio de ordem judicial. Com o passar do tempo obteremos novos registros, como o Registro Geral e Cadastro de Pessoa física e esses dados e diversas outras informações serão distribuídos e armazenados entre inúmeras empresas, sejam públicas ou privadas.

Com a chegada a era digital, todas essas informações estão sendo digitalizadas e armazenadas em bancos de dados de empresas públicas ou privadas, trazendo riscos de vazamento, aumento do potencial de desvios de conduta dos funcionários, e ainda ameaças à transparência. Nesse contexto, há o incremento de risco à violação de preceitos básicos da carta magna, especialmente os contidos no art. 5º, X.

Assim ao analisar a problemática dos bancos de dados de proteção ao crédito, no acordão proferido no Resp. 22.337-9/RS, j.13-2-1995, do qual foi relator, o Min. Ruy Rosado de Aguiar, que, ao interpretar o art. 43 do CDC, evidenciou um novo

conceito de privacidade. Como se percebe, ao analisar a problemática dos bancos de dados de proteção ao crédito, o ministro amplia a sua análise para os riscos do processamento de dados pessoais de uma forma geral. Assim, ele inova na jurisprudência brasileira ao chamar a atenção para os riscos advindos da atividade de processamento de dados, tanto pelo setor público quanto pelo privado. Nas suas palavras, o processamento de dados, quando não utilizado para fins lícitos, poderia acarretar “a devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade” ou possibilitar “ao Estado ou ao particular para alcançar fins contrários à moral ou ao direito, como instrumento de perseguição política ou opressão econômica”.

A contribuição que nos traz o acórdão é a percepção da vulnerabilidade do indivíduo em face do processamento de dados pessoais, ao afirmar que “o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo[15]. A necessidade da Proteção de Dados e o Direito à privacidade não abarcam apenas de informações pessoais que podem vir a vazar, ou o risco de ter os dados referentes ao seu trabalho divulgado à concorrência, por uma empresa privada, mas principalmente por existir a má intenção de algumas pessoas; muitas vezes desejando apenas se beneficiar financeiramente com a informação.

Uma das práticas criminosas mais difundidas no ano de 2016, foi o *ransomware*, que visava obtenção de dinheiro fácil e rápido. Tratando-se de um tipo de *malware* que pode ser instalado nos computadores quando o usuário recebe um e-mail e acaba por clicar em links direcionados a sites mal intencionados, anexos infectados ou até mesmo downloads e atualizações de software. Por intermédio de uma criptografia a pessoa que enviou o vírus impede que o usuário acesse seus arquivos, sejam eles armazenados em seu computador ou celular. Assim o fraudador exige pagamento de uma quantia em troca da liberação dos dados capturados. De posse desses dados passa a chantagear o proprietário e somente após o pagamento do exigido, que será efetuado através da moeda *bitcoin*, uma moeda virtual, o

[15]MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. p. 130-132.

desbloqueio dos dados se dará através de uma chave privada que é entregue após efetuação do pagamento. Essa prática delituosa está tipificada no ordenamento jurídico brasileiro no artigo 154-A, § 1º e artigo 158 do Código Penal.

E é exatamente pela possibilidade de não só de perder dinheiro, mas ainda de ter suas informações expostas, que todas as empresas devem se lembrar da importância de proteção de dados que estão sob sua responsabilidade. É obrigação dessas empresas privadas ou da administração pública protegê-los e, mais ainda, manter seguros e íntegros os dados que estão sob sua responsabilidade, pois esses ataques são mais comuns do que se pode imaginar, principalmente para grandes empresas que possuem uma quantidade significativa de dados coletados[16].

Assim, percebe-se o qual da responsabilidade das organizações na salvaguarda dos dados que irá coletar e armazenar em seu banco de dados, pois a LGPD irá lhe impor não só a medida financeira, como também a moral.

2.1 Score de Crédito

As empresas da iniciativa privada correm atrás de informações precisas para a formação e armazenamento de seus bancos de dados, sejam estas informações positivas ou negativas, já que são na sua grande maioria, fornecedoras de crédito.

Por isso, a partir do ano de 2013 passaram a elaborar, bancos de dados secretos, que receberam diversas denominações, como: Credscore, Score, Score de Crédito, Rating, dentre outros. Esses bancos de dados armazenados serviram como um escudo contra maus pagadores.

Todavia esse procedimento não passou despercebidos e gerou inúmeras ações na justiça por parte de consumidores, sentindo-se prejudicados. As teses contra o cadastro negativo ou o positivo alegavam a sua ilegalidade, pois o consumidor deveria ser previamente comunicado da inclusão de seu nome nesses cadastros o qual deveria conter sua autorização prévia, para a coleta dessas informações; vale

[16] ALCANTARA, Larissa Kakizaki. **Big Data e Internet das Coisas: Desafios da Privacidade e da Proteção de Dados no Direito Digita**l. São Paulo: LKA, 2017. p. 798

ressaltar que esses cadastros, positivos e negativos não tem nada a ver com o Sistema de Proteção ao Crédito (SPC) e o Serasa, pois nestes o indivíduo tem o nome incluso caso não honre um compromisso e deverá ser retirado ao cumpri-lo, ou após 5 (cinco) anos, caso não honre o referido compromisso, independentemente de prescrição[17].

É claro que o pedido final veio acompanhado da tese, de que, as informações deveriam ser canceladas e os danos causados pelo cadastro irregular indenizados. E foi assim com cerca de 100 mil ações judiciais sobre o tema, onde boa parte de seu autores sequer havia sido consultada ou teve o créditos negado[18]. O poder judiciário, ao perceber as inúmeras ações em face do Score, julgou o Resp. nº 1.419.697/RS, tendo como relator o Ministro Paulo de Tarso Sanseverino, do Superior Tribunal de Justiça, recomendando a suspensão de todos os processos sobre o tema, até o julgamento final, nos termos do art. 543-C do CPC[19].

Em seu voto o Ministro de Tarso Sanserino disse:" Eminentes colegas. Consigo, inicialmente, que este é um daqueles processos em cujo julgamento parte-se praticamente do "zero", pois não tinha uma noção clara acerca do que seria o chamado "credit scoring", ou simplesmente "credscore"[20].

O fato é que o Score, no julgamento do Recurso Repetitivo, que originou a Súmula 550 do STJ considerou esse método de avaliação de crédito, não um banco de dados e sim um método estatístico de avaliação de risco, dispensando assim o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações valoradas e as fontes consideradas no respectivo cálculo. (BRASIL, 2015)[21]

---

[17] BRASIL. Supremo Tribunal de Justiça. **Súmula 323**. DJe, Brasília 16 dez. 2009.
[18] MIRANDA, Leandro Alvarenga. **A proteção de dados pessoais e o paradigma da privacidade.** São Paulo. All Print, 2018. p. 240-241.
[19] "Art. 543-C. Quando houver multiplicidade de recursos com fundamento em idêntica questão de direito, o recurso especial será processado nos termos deste artigo".
§ 1º Caberá ao presidente do tribunal de origem admitir um ou mais recursos representativos da controvérsia, os quais serão encaminhados ao Superior Tribunal de Justiça, ficando suspensos os demais recursos especiais até o pronunciamento definitivo do Superior Tribunal de Justiça.

[20] Disponível em: [https://stj.jusbrasil.com.br/jurisprudencia/152068666/recurso-especial-resp-1419697-rs-2013-0386285-0/relatorio-e-voto-152068681]. Acesso em: 16 de dez. 2019.
[21] BRASIL. Supremo Tribunal de Justiça. **Súmula 550**. DJe, Brasília, 19 out. 2015.

Vale relembrar que os debates acerca da Lei de Proteção de Dados (LGPD) começaram no ano 2000 e culminaram com a sua promulgação em 14 de agosto de 2018, com a precisão da sua entrada em vigor para agosto de 2020, o que não ocorrerá, sendo prorrogado, pelo Congresso Nacional, devido a pandemia do Covid-19, onde tramitam diversos projetos de lei, sendo um deles, o PL 1.179, que foi aprovado pelo Senado Federal, e prevê a vigência da lei a partir do dia 1º de janeiro de 2021. Pelo texto, as multas e sanções para as empresas que não conseguirem se adequar à lei passariam a valer somente em 15 de agosto de 2021.

Em seu art. 7º, I, da LGPD, a Lei diz que para realizar tal cadastro o operador precisará do consentimento, e que esse procedimento deverá ser por escrito (Inciso I), e que caberá ao controlador provar que este foi obtido em conformidade com a lei (Inciso II), ambos disposto no art. 8º.

Resta saber de que forma o titular fará isso, por exemplo em um cadastro feito pela internet, onde lhe apresentado um formulário imenso, com as cláusulas do contrato, que ninguém lê, e com um quadradinho concordando com os termos e posteriormente nos debruçaremos naquela questão previsto nas normas do direito brasileiro, em seu artigo 3º, onde se diz: “Ninguém se escusa a cumprir a lei, alegando que não a conhece”[22]. E então o controlador desses dados apresentará este contrato, com a concordância do titular, que com certeza alegará que foi enganado.

É bem certo afirmar que as empresas busquem os seu meios de defesa contra a inadimplência. Só nos resta saber como ficará a questão do cadastro negativo (score de crédito) ante ao artigo 7º, I, da LGPD, ou se diante da incerteza da sua entrada em vigor mudanças nos esperam.

2.2 Da boa-fé

Assim como em diversas legislações, e não foi diferente na brasileira, a boa-fé passou a ser positivada nos contratos, quando se criou um aspecto de tensão sobre

[22] Decreto-Lei nº 4.657, de 4 de setembro de 1942. Disposto em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm>. Acesso em: 2 abr. 2020.

o princípio, que era até então pouco questionado nas cláusulas contatuais, o da *pacta sunt servanda.*

Ante a observância da *pacta sunt servanda*, não demorou para que houvesse uma revisão doutrinária, do Código Civil Brasileiro, como nos seguintes artigos:

> Art. 113. Os negócios jurídicos devem ser interpretados conforme a boa-fé e os usos do lugar de sua celebração.
>
> Art. 422. Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé.

A boa-fé é vista com tamanha relevância nas relações jurídicas, que o violador desse princípio arcará com as consequências jurídicas previstas, inclusive com indenização ao prejudicado. Veja o que diz o artigo 187 da Lei consumerista.

> Art. 187. Também comete ato ilícito o titular de um direito que ao, exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

Como visto, embora a LGPD não traga em seu bojo o rol de princípios que norteia a boa-fé, isso em nada diminui a sua importância isso porque possui bases legais para o tratamento de dados pessoais[23], com fundo contratual, com destaque para o consentimento[24], nesse caso poderá incidir os efeitos do princípio da boa-fé contratual, ora previstos no Código Civil, incidindo os seu efeitos nas relações jurídicas que nos trazem sobre o tema, como explanou Cots e Oliveira.[25]

2.3 Proteção do Crédito

Em seu artigo 43, O Código de Defesa do Consumidor (CDC) previu a criação de bancos de dados por parte das entidades de proteção ao crédito. Valendo-se dessa premissa entidades como: Serasa Experian e o Serviço de Proteção ao Crédito (SPC),

---

[23] Verificar o art. 7°.
[24] Verificar o art.8°.
[25] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. São Paulo: Thomson Reuters Brasil, 2018. p. 99.

criaram mecanismos, dos quais tentam mapear e precaver e os riscos de mercado, que envolve determinadas atividades. Vale ressaltar que o oferecimento de crédito é uma atividade de risco e quanto maior esse ele for, maior será o custo do crédito. Em linhas gerais, se uma determinado entidade financeira oferece um crédito a juros X, dependendo do nível de inadimplemento sobre esse crédito, a linha de crédito Y terá uma taxa de juros que poderá variar pra mais ou pra menos. A pretensão, lógico, é eliminar, ou diminuir ao máximo o inadimplemento. Todavia essa lógica acaba por causar distorções, pois um consumidor que sempre honrou seus compromissos, às vezes, por motivo de força maior, como o desemprego, acaba por ser enquadrado no mesmo nível de um consumidor com um elevado padrão de vida, mais que não honra os devidos compromissos, apenas por um desvio de caráter. Para evitar tais disparates foi criado o cadastro positivo, pela Lei 14.414/2011, que teve como escorpo a criação de um banco de dados de bons pagadores (adimplentes), ou seja, quanto mais pontual em suas obrigações assumidas, melhor será classificado, fazendo com que o crédito oferecido fique maior do que para pessoas que não constam nesse cadastro.

Vale ressalvar o quanto o crédito financeiro é importante para a economia, pois é através dessa importante ferramenta que se promove o desenvolvimento dos agentes macroeconômicos, injetando recursos beneficiando os seu personagens como um todo. Mas se por um lado existem aqueles que se sentem discriminados pelo não oferecimento de crédito por parte dos agentes financeiros, de outro lado estes tem que proteger o seu patrimônio, buscando mecanismos ao seu alcance, pois é de interesse do próprio Estado fomentar esse mecanismo. Diante desse impasse entre as partes a LGPD estabeleceu em seu art. 8º a base legal sobre o tratamento de dados e a proteção do crédito.

3 ELIMINAÇÃO DE DADOS

Em seu artigo 7º, incisos II e V, da LGPD, estabelece que o tratamento desses dados terá fim para o cumprimento da obrigação firmada entre as partes e consequentemente e execução do contrato.

A eliminação dos dados pelo controlador se dará após cumprimento da obrigação para o qual foi destinado, e sua conservação só é autorizada para o cumprimento legal ou regulatórios pelo controlador (art. 16, I). Nesse contexto a LGPD garantirá que as empresas não serão prejudicadas em processos em que comprometem-se a cumprir as regras (compliance), por exemplo em casos em que precisem manter registros completos dos dados de seus clientes.

Já previsto no Marco Civil da Internet, o direito à eliminação de dados foi regulamentado pela Lei Geral de Proteção de Dados (LGPD). Prevê que o titular pode a qualquer momento solicitar que a empresa controladora de seus dados elimine essas informações de seu sistemas (art. 18). No entanto desde que o controlador comprove que não irá compartilhar os dados utilizados com quaisquer outras organizações, poderá haver um acordo quanto a exclusão desses dados. A fiscalização ficará a cargo da Autoridade Nacional de Proteção de Dados (ANPD), que já era prevista na LGPD e constituída pela Medida Provisória nº 869, em dezembro de 2018.

Como concatenou o professor Danilo Doneda “na legislação dos Estados modernos é necessário hoje um *Habeas Data,* um reconhecimento do direito do cidadão de dispor dos próprios dados pessoais, assim como ele tem o direito de dispor livremente do próprio corpo”[26]

A grosso modo a Lei diz que se um consumidor fizer um cadastro em uma empresa para adquirir um determinado produto ou serviço, e desde que a obrigação esteja cumprida e que não haja pendencias contratuais, por parte do titular dos dados, este poderá exigir a eliminação de seus dados do sistema desta organização.

Vale lembrar que as discussões a respeito da Lei Geral de Proteção de Dados brasileira se arrastou por 10 (dez) anos, desde o começo do ano de 2000. Na União Europeia, a General Data Protection Regulation (GDPR) foi anunciada em abril de 2016 e entrou em vigor em maio de 2018. Por lá as empresas também tiveram um período de dois anos para se adequar à Lei. No entanto muitas chegaram ao fim do prazo sem terem estabelecidos processos bem definidos para o cumprimento da norma. Em uma pesquisa realizada pelo instituto de pesquisa *Talend*, constatou que cerca de 70% das empresas não estavam em acordo com a Lei (compliance). Entre

[26] DONEDA, Danilo. **Iguais mas separados: Habeas Data no ordenamento jurídico brasileiro e a proteção de dados pessoais.** Caderno da Escola de Direito e Relações Internacionais, Curitiba, p.20, 2008.

elas, há as que preferiram não cumprir determinados preceitos da GDPR, como a eliminação de dados, pois consideram estes um dos seus maiores ativos, valendo mais a pena arcar com multas, do que apagá-los[27].

Talvez, no Brasil com a entrada em vigor de sua LGPD as organizações privadas resolvam seguir pelo mesmo caminho de suas coirmãs europeias, pois é sabido que por aqui empresas tomam multas por diversos motivos, em decorrência do descumprimento de leis vigentes no pais. Esses processos se arrastam por anos a fio e muitas delas não pagam esses débitos, que na grande maioria das vezes caducam. No entanto a multa cobrada, seja pela LGPD, no Brasil, ou pela GDPR, não será a única perda de uma organização que escolher não seguir com a norma da exigência do direito à eliminação de dados.

Casos, como o ocorrido com o Facebook, que lida com imensas quantidades de dados pessoais, ocorrido na Europa, e o caso Google, considerado o primeiro caso de descumprimento da GDPR, identificado em janeiro de 2019 e multado em 57 milhões de dólares, pela comissão Nacional de Informática e Liberdade (CNIL), órgão independente da França que regulamenta questões de privacidade. A CNIL argumentou que o Google não esclareceu de que forma a informações pessoais de seus usuários é coletada e o que a empresa faz com elas. Ressaltou ainda que também não foi solicitado desses usuários o consentimento para a exibição de anúncios personalizados; o que fez com que as pessoas se preocupem cada vez mais com esse tema[28].

No artigo 3º(2) (a) do GDPR há a indicação de que haverá incidência a companhias que ofereçam bens ou serviços aos titulares que se encontrem fisicamente no território da União, mesmo que não haja a cobrança de valores para tanto. Existindo ainda a possibilidade de aplicação do GDPR, mesmo a empresas que não se encontrem no território da União[29]

Aqui percebe-se o quão será o alcance da LGPD, que seguirá os mesmos preceitos da GDPR, diante do risco de vazamento de seus dados e seguindo uma tendência mundial de valorização da privacidade, onde o consumidor é colocado no

---

[27] **Direito à eliminação de dados e o controle de informações pessoais**. **Disponível em: <**https://blog.idwall.co/direito-a-eliminacao-de-dados-controle-informacoes-pessoais/**>.** Acesso em: 14 de mar de 2020.

[28] Ibid.;

[29] MALDONADO, Viviane Nobrega; BLUM, Renato Opice. **Comentários ao GDPR, Regulamento Geral de Proteção de dados da União Europeia.** 4º ed. São Paulo: Thomson Reuters Brasil, 2018.

comando de seu dados pessoais, há um risco não só de prejuízo em decorrência de uma possível multa aplicada pela Autoridade nacional, mas principalmente um prejuízo imensurável à imagem e à reputação desta empresa diante da sociedade e do mercado.

4 ARQUIVAMENTO DE DADOS

Como dito anteriormente, ao nascermos obtemos o nosso primeiro registro, que é a certidão de nascimento, e ao logo de nossas vidas obteremos outros, como o Registro Geral (RG) E o Cadastro de Pessoa Física (CPF). Ao passarmos por esta vida, a pergunta que fica é o que é feito com esses dados. O Sistema de Controle de Óbitos (SISOBI) foi criado em 28 de julho de 2017 e é o responsável por colher informações de óbitos dos cartórios de registro civil de pessoas naturais do Brasil[30]. No entanto o INSS criou desde 19 de março de 2001, através da portaria nº. 847, o SISOBINET, onde foi criado um banco de dados de óbitos de todo o pais, que será abastecido por informações de todos os cartórios de Registro Civil, que terão como responsável o titular do referido cartório. Informa ainda a página que o cadastro de todos os usuários de cartórios que farão uso SEO-cartório deverão solicitar o cadastramento às agências executivas do INSS e adverte ainda que a falta de comunicação na época própria, bem como o envio de informação inexatas sujeitará o titular à multa, com base nos artigos 68 e 92 da Lei nº 8.212/91. Responsabilizará também de forma administrativa, civil e penal o acesso não autorizado, ou disponibilização voluntária ou acidental de senhas ou quebra de sigilo[31]. Veja por exemplo a tentativa de um usuário de consultar o referido banco de dados do SISOBE:

> “Prezado, boa tarde! Gostaria de saber se é possível ter acesso à base SISOBI, a fim de verificar eventual óbito de clientes. Tentei contato pelo e-mail sisobi.arquivo@previdenci.gov.br, mas parece não estar ativo. Muito obrigado.
>
> - Prezado Senhor, informamos que não é possível “consultar óbitos de clientes” pelo Sistema de Óbitos – SISOBI. Os registros constantes

[30] **Sistema de Controle de Óbitos**. Disponível em: https://ck.govdata.gov.br/dataset/sisobi. Acesso em: 9 jun. 2020.

[31] Disponível em: <http://www.dataprev.gov.br/sisobi/>. Acesso em: 12 mai. 2020.

> do SISOBI são considerados dados de caráter pessoal, não sendo possível seu fornecimento por meio eletrônico (e-SIC) uma vez que, conforme o art. 55 a 60 do Decreto 7.724/2012, faz-se necessária a identificação pessoal do titular das informações ou de seu representante legal (curador, tutor, procurador). Atenciosamente, Serviço de Informações ao Cidadão – INSS".[32]

A tentativa de consulta foi feita em 27 de outubro de 2016 e a resposta foi dada no mesmo dia, e até a data dessa consulta ainda encontra-se na página. Veja que se fosse talvez uma empresa tentando a consulta para se precaver de um possível golpe não conseguiria obter as informações.

Em setembro de 2019 a Polícia Federal desbaratou uma quadrilha que falsificava documentos de pessoas já mortas para aplicar golpes causando um prejuízo de cerca de 60 bilhões de reais ao INSS. Muitas das vezes a quadrilha chegava a oferecer dinheiro para os familiares da pessoa morta para ficar com os seus documentos. De posse desses documentos, trocavam as suas fotos, colocando no lugar fotos de um idosos laranjas, que eram levados até lotéricas, acompanhados de membros da quadrilha para fazer prova de vida.

A quadrilha foi presa com mais de 1382 Registros Gerais falsificados dos quais em sua grande maioria espelhos das secretarias de segurança dos Estados do Maranhão e Piauí. Dentre os documentos falsificados foi encontrado também documentos originais de pessoas já falecidas, dentre elas o RG de uma pessoa, que falecera em 2009 e só teve o benefício cancelado em maio de 2019. Foi constatado, que embora a pessoa esteja morta há mais de dez anos, sequer foi emitido uma certidão de óbito, para que seus dados fossem retirados de um possível cadastro de pessoas vivas e colocadas em um de pessoas mortas. O pior disso é que parentes diante do túmulo do falecido, portando apenas a informação dia do falecimento do parente, declara que o cemitério não exigia a certidão de óbito para o sepultamento do corpo.

Mas as organizações criminosas não se valem apenas do cadastro de pessoas mortas. Uma dessas quadrilhas conseguiu também se valer de identidades criadas por eles mesmos os quais eram registradas no instituto de identificação "João

---

[32] Acesso à base do SISOBE. Disponível em: <http://www.consultaesic.cgu.gov.br/busca/dados/Lists/Pedido/Item/displayifs.aspx?List=0c839f31%2D47d7%2D4485%2Dab65%2Dab0cee9cf8fe&ID=514805&Web=88cc5f44%2D8cfe%2D4964%2D8ff4%2D376b5ebb3bef>. Acesso em: 11 mai. 2020.

de Deus Martins", da Secretaria de Segurança Pública, em Teresina, no Piauí. Esses registros eram usados por laranjas para sacar o Benefício de Prestação Continuada, pagos a pessoas idosas com deficiência de baixa renda.

A Polícia Federal descobriu também que um dos principais integrantes da dessa quadrilha era um vereador da localidade, da cidade de Piripiri, que chegou a ser preso e em seu poder estava diversos cartões de benefícios assistenciais fraudulentos, mais solto continua dando expediente na câmara de vereadores daquela cidade e de acordo com o delegado encarregado do caso chegou a dar um prejuízo de mais de R$ 100 (cem) milhões de reais aos cofres públicos, ficou constatado também que apenas uma única pessoa chegou a assumir a identidade de mais de trezentos e vinte e duas pessoas e que toda a operação contava com a participação de funcionários do INSS.[33]

Vale muito bem ressalvar, que desde o começo do ano de 2019 o país vem passando por uma reforma da Previdência Social, que enfrenta críticas por diversos setores da sociedade. Especialistas afirmam que se fosse feito uma melhor gestão desta não haveria necessidade de tal reforma.

O Cadastro Base do Cidadão, instituído pelo Decreto 10.046 de 2019 traz em seu art. 16, VI, que será realizado o cruzamento de informações das bases de dados cadastrais oficiais a partir do número de inscrição do CPF do cidadão. No entanto isso já poderia ter sido feito, como mostra o caso acima, da fraude contra o INSS, pois já existia um banco de dados desde o ano de 2001. Já para o Decreto 10.047, chamamos a atenção e concordamos com Rafael Zanatta "É um conjunto de dados muito rico armazenado em um só lugar, e como melhor expressou o Professor Doneda "Tais informações podem escoar para o setor privado com um mero ato normativo"[34].

Fica evidente o quando o próprio Estado terá que se adequar as suas próprias normatizações, pois é perceptível a falta de entrosamento entre os seus entes, ante aos fatos narrados.

---

[33] **Golpe de quadrilha no INSS gera prejuízo de milhões de reais aos cofres públicos**. Disponível em: https://globoplay.globo.com/v/7888984/. Acesso em 01 set. 2019.

[34] **Aqui estão todas as suas informações que o governo vai reunir numa megabase de vigilância.** Disponível em: <https://theintercept.com/2019/10/15/governo-ferramenta-vigilancia/>. Acesso em 6 jan. 2020.

5 CONSEQUÊNCIAS JURÍDICAS E FINANCEIRAS PARA O ESTADO

É de vital importância a obrigação de proteger os dados pessoais que estarão sob a responsabilidade das organizações, seja de caráter privado ou público. Os ataques a essas entidades são mais comuns do que se imagina, principalmente para grandes empresas, que possuem quantidades significativas de dados coletados. Já dispõe a Lei 12.527/2011 em seu artigo 6º, inciso III:

> Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:
>
> III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Já a Lei 13.709/2018 em seu artigo 52 prevê sanções administrativas e financeiras que serão aplicadas pela autoridade nacional em razão das infrações cometidas ao infringir as normas previstas na Lei. Dentre elas está previsto no inciso II, que irá deste uma multa simples e 2% (dois por cento), podendo chegar a R$ 50.000.000,00 (cinquenta milhões) de reais do faturamento da pessoa jurídica de direito privado, do grupo ou conglomerado no país no seu último exercício.

Veja que a Lei faz menção apenas às empresas privadas. Todavia os casos que vêm a público sobre vazamento de dados geralmente são advindos da pessoa jurídica pública, como no caso mencionado acima envolvendo golpes contra o INSS. E diante deste se assemelham tantos outros, como o ocorrido no Instituto de Previdência do Distrito Federal, que teve que suspender 1846 benefícios, pois seus beneficiários não apareceram para se recadastrar e fazer a chamada prova de vida. O recadastramento dos beneficiários começou em março de 2019 e eles tem que comparecer a uma agência do Banco de Brasília e atestar que estão vivos por meio de sua impressão digital. De janeiro a junho do presente ano o Governo do Distrito Federal já suspendeu 1846 aposentadorias, pois os seus beneficiários não apareceram o que ocasionou uma economia de R$ 250 (duzentos e cinquenta) milhões de reais aos cofres do Governo do Distrito Federal. O próximo passo será

investigar se alguém estava sacando esses benefícios, e o primeiro passo adotado para essa investigação será solicitar imagens das agências onde as aposentadorias foram sacadas e identificar os sacadores. Alerta ainda o presidente do Iprev, Ney Ferraz Júnior, se caso o beneficiário esteja vivo e teve a sua aposentadoria suspensa e só procurar a agencia para regularizar a sua situação e terá o seu benefício integralmente pago e desbloqueado para os saques futuros.

Se prevalecer esse quadro informa o presidente do Iprev que o Governo do Distrito Federal terá uma economia de R$ 500 (quinhentos) milhões de reais até o final do ano, quantia essa que é bem-vinda, pois o instituto já possui um rombo de R$ 1,2 bilhões de reais. O presidente ressalta ainda que a situação do Estado não é tão preocupante, pois ainda possui mais ativos, 85 (oitenta e cinco) mil, do que inativos, 63 (sessenta e três) mil[35].

Já em outubro de 2019 dados sigilosos da Secretaria de Segurança Pública do Rio Grande do Sul foram parar nas mãos de criminosos no estado e passaram a ser usados para o planejamento de crimes. De dentro de uma penitenciária de alta segurança, em Charqueadas, na região de Porto Alegre, o preso fala com um comparsa, de como consultar um sistema para acessar uma foto de um homem e seu endereço para posteriormente executa-lo. Segundo a polícia o criminoso se referia ao banco de dados sigilosos da Secretaria de Segurança do Rio Grande do Sul, onde estão cadastradas todas as ocorrências policiais e ordens de prisão, além de dados pessoais de todos os cidadãos do Estado e também registros de veículos do Detran. A polícia levantou que a quadrilha usava senhas de um policial militar e um policial civil para acessar o sistema, e investiga se essas senhas foram roubadas ou vendidas. Os dados conseguidos pela quadrilha foram usados para a prática de diversos delitos, tais como: a clonagem de veículos roubados.

Diante da descoberta o governo gaúcho restringiu o acesso aos dados de diversas autoridades e a associação dos magistrados daquela localidade pediu ao Tribunal de Justiça do RS, que as informações inerentes a todos os juízes fiquem ocultas nesse sistema.

---

[35] **Iprev corta 1,8 mil benefícios "fantasmas"**. Disponível em: <https://globoplay.globo.com/v/7931482/>. Acesso em 18 set. 2019.

Já no Rio Grande do Norte cerca de 70 (setenta) milhões de dados de brasileiros ficaram expostos na internet por causa de uma falha de um aplicativo do Detran daquele estado, que está interligado ao banco de dados nacional. Pra se ter uma ideia com o número do Cadastro de Pessoa Física (CPF) de uma pessoa, que possua habilitação ou veículo seria possível levantar diversos dados dela, tais como: endereço, foto, RG, telefone e causar um verdadeiro estrago em sua vida[36].

E não para por aí. Veja o acontecimento em plena pandemia do Covid-19, onde pessoas estão precisando de auxílio do governo e muita das vezes não conseguem ter o benefício aprovado em um levantamento da CGU (Controladoria-Geral da União) obtido pelo "Fantástico", da TV Globo, aponta que mais de 27 mil foragidos da Justiça tiveram o auxílio emergencial de R$ 600 aprovado pelo governo federal. O pagamento do benefício aos criminosos custou mais de R$ 16 milhões aos cofres públicos. Só no estado de São Paulo, segundo a reportagem do "Fantástico", 6.879 foragidos tiveram o auxílio aprovado em seu nome. No Rio de Janeiro, foram mais 825. Não se sabe, porém, se os criminosos ficaram com o dinheiro que receberam de forma indevida ou se seus dados estão sendo usados por terceiros.

A fraude não é a única verificada pela CGU: o órgão também identificou golpistas que conseguiram a aprovação para receber os R$ 600 usando informações de pessoas que já morreram. Os cadastros, ainda de acordo com o "Fantástico", podem ter sido feitos por presos a partir de celulares que circulam clandestinamente nas cadeias. A CGU também apontou que quase 23 mil de brasileiros que moram no exterior também estão tendo seus nomes aprovados de forma irregular. Uma brasileira que mora em Portugal relatou à reportagem que ela mesma fez o teste e conseguiu a aprovação do Ministério da Cidadania para receber o auxílio. Ela já entrou com um pedido para devolver o dinheiro. O órgão estima que 233 mil brasileiros podem ter recebido o auxílio emergencial indevidamente. Se todos os pagamentos forem confirmados, isso representaria um custo de quase R$ 140 milhões à União[37].

---

[36] **Criminosos roubam dados sigilosos da secretaria de segurança pública do RS**. Disponível em: [https://globoplay.globo.com/v/7990092/]. Acesso em 9 de out. de 2019.

[37] **11 dos 22 criminosos mais procurados do Brasil têm auxilio emergencial liberado**. Disponível em: <https://globoplay.globo.com/v/8593068/programa/>. Acesso em: 1 de jun. 2020

Com a internet se tornando cada vez mais um campo vasto de dados pessoais, as entidades públicas parecem não conseguir manter o passo do nível de segurança da informação das empresas privadas. E por mais medidas de precauções sejam adotadas os piratas da internet acabam por criar mecanismos de fraudes causando inúmeros prejuízos a pessoas, onde gerarão processos que se arrastarão por anos a fio sem uma conclusão.

Nesses moldes estão por exemplo casos de leilões virtuais com páginas falsas, em que suas vítimas diante de tanta perfeição e atraídos por valores bem abaixo do mercado acabam por cair em golpes. E só é preciso colocar uma busca por algum veículo por exemplo, para que apareça alguma página de algum leilão falso, bem atrativo, com preço em até 40% (quarenta por cento) abaixo de preço de mercado. De acordo com a associação da Leiloaria Oficial do Brasil (Aleibras) foi preciso criar uma lista de leilões falsos, que são denunciados e detectados por essa entidade.

Esclarece o especialista em leilões, Antônio Sato, da Sato Leilões, que para enganar a vítima chegam a replicar a identidade visual de algum site de boa reputação para se apossar de dados de usuários e posteriormente usa-los para aplicar outros golpes. É preciso verificar muito bem antes de se cadastrar e fornecer seus dados na internet, revela, e ao efetuar o pagamento verificar se o leiloeiro é pessoa física, confirmando na Junta Comercial (do Estado em que o leiloeiro se encontra), se o profissional está realmente credenciado para exercer a atividade. Também não faça o pagamento para qualquer pessoa, exceto o próprio profissional cadastrado pela junta comercial como leiloeiro oficial. Logo, a conta bancária para o depósito ou transferência sempre tem que estar no nome do leiloeiro.

Uma das vítimas, que pagou cerca de R$ 15 (quinze) mil reais, ao tentar comprar um veículo, ao entrar em um destes sites falsos e dar um lance no veículo, mas após fazer a transferência bancária e marcar a entrega do produto, os supostos organizadores do leilão explicaram que ela tinha caído em um golpe, e ainda

desdenharam “Nem venha atrás do carro, que a senhora caiu em um golpe”, disseram a ela por telefone[38].

O site leilãoseguro.org.br já conta com 820 (oitocentos e vinte) registros de sites falsos, e de acordo com informações pra cada site que é retirado do ar surgem mais 8 (oito) no lugar e se você resolver pesquisar um veículo na internet com certeza algum tempo depois lá estará um *cookie* de algum desses sites falsos lhe perseguindo, veiculados pelo Google[39].

Algumas vítimas dos golpes, através de suas representações afirmam que entraram com o ajuizamento de ações contra o Google e os bancos. E é claro essas ações judiciais desembocarão em grande demanda no poder judiciário e sabemos que a sua grande maioria não dará em nada, pois 100% (cem por cento) desses sites falsos são hospedados fora do país e é muito difícil o seu rastreamento.

Todavia, o que foi mostrado representa uma pequena parcela de dados circulando pela internet, contudo, se por um lado temos a questão da boa-fé de pessoas que querem apenas adquirir um produto e são vítimas de malfeitores, por outro lado veremos o próprio Estado sendo vítima, o que, é causado, na maioria das vezes, por atos de corrupção de seus próprios agentes públicos, responsáveis por salvaguardar informações de cidadãos armazenados em seus bancos de dados.

Novamente relembramos que o texto da LGPD brasileira prevê punição de forma severa apenas às empresas privadas. Porém o que é constatado é que dados vazados e utilizados em fraudes na sua maioria das vezes são vazados dos bancos de dados públicos. Resta-nos saber se diante dessas informações as pessoas as quais tiverem os seus dados utilizados em fraudes, seja contra as entidades públicas ou privadas serão indenizadas por danos morais, e as empresas privadas também vítimas de falsários ao invés de serem punidas, serão compensados pelos próprios erros advindos do Estado.

---

[38] **Golpe de sites de leilão falsos: veja como se defender.** Disponível em: [https://economia.ig.com.br/2020-01-20/golpe-de-sites-de-leilao-falsos-veja-como-se-defender.html]. Acesso em 10 de Abr. de 2020.

[39] Sites falsos. Disponível em: [https://www.leilaoseguro.org.br/falsos/]. Acessado em 10 de abr. de 2020.

As sanções previstas no artigo 52, X, XI, XII seriam no entanto inviáveis a essas entidades, pois como seria o Detran por exemplo com seu banco de dados suspenso por 6 (seis) meses, ou mesmo ter a proibição parcial ou total de suas atividades? No entanto, vale ressaltar que, se esses dados forem usados em fraudes contra qualquer entidade privada, o artigo 42 da LGPD, prevê a responsabilização civil, pelo Poder Judiciário, nos termos do artigo 927, parágrafo único, do Código Civil Brasileiro, podendo a entidade pública responsável pelo vazamento desses dados ser condenada a pagamento pecuniário, a quem sofreu o dano. Havendo, assim a responsabilização administrativa e civil combinadas, em decorrência da lesão sofrida.

CONCLUSÃO

O tratamento de dados cria a discussão sobre os desafios e problemas que o Estado tem de enfrentar diante da quantidade de dados que possui agora e o quão rápido tem sido o seu crescimento diante de tudo o que é armazenado na internet. Mostra também o quanto a tendência é apenas aumentar os riscos da situação atual. Analisamos nesse artigo o que o Brasil vem fazendo para tratar deste assunto, quais são as Leis existentes para proteger os dados de seu cidadão e os desafios que a nossa jurisprudência irá enfrentar.

Hoje, a maior parte desse controle está limitado às relações consumeristas por meio do cadastro positivo, mas que significa uma pequena parcela dos dados que hoje estão em circulação. A boa-fé e a confiabilidade nas instituições, na maneira como tratarão os dados pessoais coletados, serão o diferencial nesse período em que a autodeterminação informativa passa a ter um relevante papel na sociedade, com o empoderamento do indivíduo no controle da utilização de seus dados pessoais, criando novos deveres às empresas que pretendem trabalhar com esses dados, devendo mostrar efetivo benefício com a máxima segurança, para lhe seja permitido acesso aos dados.

A LGPD deverá garantir a efetividade da proteção desses dados, por meio da garantia da aplicação dos princípios como os da finalidade, necessidade e adequação. Assim deve-se permitir um amplo acesso e efetivo poder de controle ao titular, para

que disponha dos direitos e poderes que a lei lhe confere conforme seu livre-arbítrio, inclusive opinando sobre a comercialização ou não destes dados.

Entretanto, o adequado funcionamento dos bancos de dados será legitimado pela atuação dentro dos limites jurídicos constitucionais, estabelecidos na Carta Magno, leis infraconstitucionais, tratados internacionais e na própria imagem e confiabilidade que transmitirão à sociedade, que devem ter o poder efetivo de controle sobre os dados, principalmente no que tange ao poder público diante da abrangência de dados de seus cidadãos que lhe serão expostos.

REFERÊNCIAS BIBLIOGRÁFICAS

ALCANTARA, Larissa Kakizaki. **Big Data e Internet das coisas: Desafios da Privacidade e da Proteção de Dados no Direito Digital**.1ª ed., São Paulo: LKA, 2017.

Aqui estão todas as suas informações que o governo vai reunir numa megabase de vigilância. Disponível em: <https://theintercept.com/2019/10/15/governo-ferramenta-vigilancia/>. Acesso: 6 jan. 2020.

BRASIL. Presidência da República. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Dispõe sobre a proteção de dados pessoais. **Diário Oficial da União**, Brasília, DF, 2018. Disponível em: [http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm]. Acesso em: 15 set. 2019

BRASIL. Secretaria-Geral. Decreto nº 9.920, de 22 de julho de 2019. Dispõe sobre o Sistema Nacional de Informações de Registro Civil – Sirc e sobre o seu comitê gestor, e dá outras providências. **Diário Oficial da República Federativa do Brasil.** Brasília, DF, 22, jun. 2019. Disponível em: [http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9929.htm#art12]. Acesso em 07 jan. 2020.

BRASIL. Secretaria-Geral. Decreto nº 10.046, de 9 de outubro de 2019. Institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados – Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal. **Diário Oficial da República Federativa do Brasil.** Brasília, DF, 9, out. 2019. Disponível em: [http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm] Acesso em 07 jan. 2020.

BRASIL. Supremo Tribunal de Justiça. **Súmula 323**. DJe, Brasília, 12 dez. 2009.

_____. Supremo Tribunal de Justiça. **Súmula 550**. DJe, Brasília, 19 out. 2015.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**.1ª ed.; São Paulo: Thomson Reuters Brasil. 2018.

CASTRO, Catarina e Sarmento e. **Direito da Informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1ª ed., Rio de Janeiro: Renovar, 2006.

_____. **Iguais mas separados: Habeas Data no ordenamento jurídico brasileiro e a proteção de dados pessoais.** Caderno da Escola de Direito e Relações Internacionais, Curitiba, p.20, 2008.

Golpe de quadrilha no INSS gera prejuízo de milhões de reais aos cofres públicos. Disponível em: [https://globoplay.globo.com/v/7888984/]. Acesso em 01 set. 2019.

Iprev corta 1,8 mil benefícios "fantasmas". Disponível em: [https://globoplay.globo.com/v/7931482/]. Acesso em 18 set. 2019.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. 1ª ed., São Paulo: Saraiva, 2014.

MIRANDA, Leandro Alvarenga. **A Proteção de Dados Pessoais e o Paradigma da Privacidade**. 1ª ed.; São Paulo: All Print, 2018.

MALDONADO, Viviane Nobrega; BLUM, Renato Opice. **Comentários ao GDPR Regulamento Geral de Proteção de Dados da União Europeia.** 4º ed. São Paulo: Thomson Reuters Brasil, 2018.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018**. 1ª ed., São Paulo: Saraiva, 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**.1ª ed., Rio de Janeiro: Renovar, 2008.

SAUAIA, Hugo Moreira Lima. **A Proteção dos dados pessoais no Brasil.** Rio de Janeiro: Lumen Juris, 2008.

Sites falsos. Disponível em: https://www.leilaoseguro.org.br/falsos/. Acesso em: 10 abr. 2020.

11 dos 22 criminosos mais procurados do Brasil têm auxilio emergencial liberado. Disponível em: [https://globoplay.globo.com/v/8593068/programa/]. Acesso em: 01 jun. 2020.