INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA
ESCOLA DE DIREITO E ADMINISTRAÇÃO PÚBLICA
MESTRADO ACADÊMICO EM DIREITO CONSTITUCIONAL

CRISTIANE PODGURSKI

O TRATAMENTO DE DADOS PESSOAIS NOS ÂMBITOS GERAL E CRIMINAL: PRINCIPAIS CONVERGÊNCIAS E DIVERGÊNCIAS ENTRE O REGULAMENTO 679 E A DIRETIVA 680 DA UNIÃO EUROPEIA

BRASÍLIA/DF
2021

CRISTIANE PODGURSKI

O TRATAMENTO DE DADOS PESSOAIS NOS ÂMBITOS GERAL E CRIMINAL: PRINCIPAIS CONVERGÊNCIAS E DIVERGÊNCIAS ENTRE O REGULAMENTO 679 E A DIRETIVA 680 DA UNIÃO EUROPEIA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Direito Constitucional do IDP, como requisito para obtenção do título de mestre em Dierito Constitucional

BRASÍLIA/DF

2021

Abreviaturas, siglas e acrônimos

Carta	Carta dos Direitos Fundamentais da União Européia
CDFUE	Carta dos Direitos Fundamentais da União Européia
CIG	Conferência Intergovernamental
JAI	.....
PESC	Política Externa de Segurança Comum
TCE	Tratado que institui a Comunidade Européia
TCEE	Tratado que institui a Comunidade Econômica Européia
TUE	Tratado da União Européia
TFUE	Tratado sobre o Funcionamento da União Européia

SUMÁRIO

RESUMO

A cultura da proteção de dados, já há muito arraigada no âmbito da União Europeia, encontra respaldo em considerável arcabouço normativo para tutelar referido direito fundamental, destacando-se, no atual cenário normativo sobre o tema, o Regulamento 2016/679/UE e a Diretiva 2016/680/UE. A adoção da Diretiva 680, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais realizado pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, bem como à livre circulação de tais dados, deu origem a um quadro normativo peculiar para a proteção e tratamento de dados pessoais no âmbito das investigações e processos criminais, garantindo também um elevado nível de segurança pública e facilitando o intercâmbio de dados pessoais entre autoridades competentes na União. Tanto a Diretiva 680 como o Regulamento 679, principais instrumentos legislativos no domínio da proteção de dados na União Europeia, visam proteger as pessoas singulares no que diz respeito ao tratamento de dados pessoais, divergindo quanto ao âmbito de aplicação e em outros aspectos peculiares às atividades desenvolvidas pelas forças de segurança.

Palavras chave: União Europeia – Proteção de dados – Diretiva 2016/680/UE – âmbito criminal.

INTRODUÇÃO

O século XX testemunhou o uso de dados pessoais por regimes autoritários para espalhar o terror. Aliada ao desenfreado progresso tecnológico em ascensão, além de outros, tal foi a motivação que impulsionou o desenvolvimento do direito à proteção de dados.

O início dos estudos da matéria coincide com o momento em que se inaugura o tratamento de dados pessoais e informações em geral por meios automatizados, o que aumentava, em grande medida, o volume, a possibilidade de tratamento e a complexidade deste tratamento. Paralelamente, aumentava também o poder em potencial que as organizações que tratavam dados pessoais automatizados poderiam ter sobre as pessoas, ou sobre os titulares de dados, como conceituado hoje nas legislações de proteção de dados.

Ante este cenário desenhado nos anos 60, começaram a se estruturar as primeiras respostas normativas. Em 1970, foi aprovada a 1ª lei de que se tem notícias sobre a proteção de dados na Europa e, nos anos que se seguiram, na década de 70, vários países começaram a disciplinar a matéria.

A proteção de dados traz uma nova abordagem de tutela em que se trata a regulamentação de dados pessoais com enfoque diverso daquele em que se considera a privacidade como único bem jurídico tutelado. Não se trata, ainda, o direito a proteção de dados de uma mera repetição do direito a privacidade na era da informática, que histórica e cronologicamente o antecede[1]; ao contrário, ambos coexistem, tendo abordagens diferentes.

As modernas leis de proteção de dados basicamente especificam uma série de critérios com vistas a informar aqueles que tratam dados pessoais, como limites para o tratamento ou direitos dos titulares, versando sobre regras que incidirão não diretamente sobre o indivíduo (como ocorre com relação ao direito à privacidade), mas sobre os seus dados pessoais.

Assim, antes do advento da Lei Geral de Proteção de Dados brasileira – Lei 13.709/18, há muito já figurava no cenário internacional tal matéria em vários países que acabaram, por um motivo ou outro, por introduzir em seus ordenamentos normas de proteção de dados, quando não para fazer frente a demandas externas, para estabelecer padrões de comunicação de dados e interoperabilidade de informações comparáveis e que pudessem, ao menos, interagir com as de outros países.

Pode-se dizer, assim, que a proteção de dados é um assunto que leva a convergência de várias normas internacionais. Eventual incompatibilidade ou mesmo incomunicabilidade das

[1] Os estudos do direito à privacidade remontam ao século XIX, sendo desenvolvidos no século passado e hoje estando razoavelmente consolidados nos diversos ordenamentos, inclusive no pátrio.

normas de proteção de dados entre um Estado e outro ou ainda, a desarmonia, mesmo que formal, entre a legislação de um Estado e outro erige cada vez mais barreiras intransponíveis para que empresas ou mesmo órgãos públicos consigam cooperar com outros congêneres situados em outros países. Cada vez mais se exige, no trânsito internacional de dados, algum tipo de garantia quanto a proteção dos dados que circulam entre um país e outro, visando evitar que sejam tratados de forma abusiva ou descontrolada no país que os recebe, em detrimento à proteção que lhes é conferida no país de origem.

Tal não constitui somente um imperativo comercial, tanto é que, hoje em dia, órgãos que são responsáveis pela investigação criminal, cooperação internacional e vários outros órgãos públicos tem a necessidade cada vez mais óbvia e premente de apresentar, para que possam ter acesso a plataformas de colaboração internacional, garantias de que, internamente, os dados que virão ou aos que terão acesso serão bem tratados[2].

Partindo-se do pressuposto de que nenhum direito é absoluto, em que pese relacionado no catálogo dos direitos fundamentais, também o direito à proteção de dados pessoais é passível de inflexões, especialmente na seara criminal. Em tal universo há que se levar em conta a existência de outro direito fundamental, que é o direito à segurança pública, bem como a natureza das atividades desenvolvidas pelas autoridades das forças de segurança no intuito de manter a ordem e a paz social e preservar o interesse público.

A partir da Convenção Europeia dos Direitos do Homem, uma das primeiras tentativas de positivação do direito à proteção de dados, e seguindo-se com a Convenção 108, a Carta dos Direitos Fundamentais e o Tratado sobre o Funcionamento da União Europeia, o direito fundamental à proteção de dados vem expressamente consagrado na União Europeia.

Assim sendo, em 5 de maio de 2016, depois de um longo tempo de discussões, o Parlamento da União Europeia exerceu os seus poderes legislativos, nos termos do artigo 16º, nº 2, do Tratado sobre o Funcionamento da União Europeia, promulgando o Regulamento 2016/679/UE a Diretiva 2016/680/UE que revogaram a Diretiva 95/46/CE a Decisão-Quadro 2008/977/JAI, relativas à proteção dos dados pessoais tratados nos âmbitos geral e da cooperação policial e judiciária em matéria penal, respectivamente.

A intenção do parlamento da União Europeia era garantir que a União adotasse uma abordagem abrangente para fins de proteção de dados, levando em consideração os avanços tecnológicos, para a regulamentação de todas as esferas da comunidade da União Europeia, incluindo a aplicação da lei e a prevenção do crime, conforme o Considerando 3 da Diretiva

[2] É o que ocorre, por exemplo, no caso de acesso a sistemas de cooperação como o da Interpol, Europol e Eurojust, e outros.

680. Portanto, a Diretiva 2016/680/UE visa equilibrar o direito à proteção de dados com a prevenção, investigação e/ou repressão de infrações penais na União Europeia.

O presente trabalho destina-se a verificar a existência e identificar e analisar as principais diferenças entre a lei geral de proteção de dados e a lei de proteção de dados em matéria criminal no âmbito da União Europeia, cuja aplicação se iniciou em maio de 2018.

Assim, a partir da experiência havida na União, pretende-se analisar em que medida o Regulamento 2016/679/UE e a Diretiva 2016/680/UE apresentam convergências e divergências em relação aos objetivos, âmbito de aplicação, conceitos gerais, princípios, bases legais e direitos dos titulares.

Tal discussão guarda considerável relevância no campo acadêmico visto que poderá trazer contribuições para o legislador brasileiro, que já se utilizou do modelo europeu para a confecção da Lei Geral de Proteção de Dados pátria. Em que pese tal não seja objeto de análise no presente estudo, há que se considerar que, num futuro próximo, o Brasil será palco de debates neste sentido, ante a existência já, neste momento, de anteprojeto de lei que trata da estruturação da lei de proteção de dados nas áreas criminal e de segurança pública no contexto brasileiro.

A exemplo do que ocorreu na União Europeia (artigo 2º, 2, *d,* do Regulamento 2016/679/UE), também a Lei Geral de Proteção de Dados brasileira relegou a instrumento legal diverso a disciplina sobre o tratamento de dados realizado no âmbito criminal e de segurança pública (artigo 4º, III, *a* a *d*, e parágrafo 1º, da Lei 13.709/18), determinando a edição de lei específica para tanto.

Pretende-se, neste trabalho, identificar a existência de diferenças entre as leis geral de proteção de dados (Regulamento 679) e a que disciplina o tratamento de dados realizado no âmbito criminal (Diretiva 680), considerando-se a experiência da União Europeia havida a partir do ano de 2018, quando passaram a ser aplicadas ambas as leis.

Para tanto, proceder-se-á à comparação entre as duas normas jurídicas citadas mediante a análise dos respectivos textos legais, com amparo em estudos realizados por autores que tratem de referidas leis, com vistas a identificar a existência e a compreender a motivação de tais diferenças, levantamento bibliográfico e documental. Não será objeto de análise a jurisprudências dos Estados-membros e nem tratados internacionais que eventualmente tratem do assunto, mas tão somente os métodos inicialmente indicados.

Havendo um longo, porém atraente e necessário caminho a ser percorrido desde os primeiros traços do que viria a ser o direito à privacidade até a edição das modernas leis de

proteção de dados geral e criminal da União Europeia, pretende-se dar um panorama geral sobre o tema, apresentando ao leitor algumas noções básicas e imprescindíveis para a compreensão do direito à proteção de dados nos moldes atuais e possibilitando, assim, a análise das principais convergências e divergências entre a Regulamento 679 e a Diretiva 680 que eventualmente se venha a detectar.

1. A EVOLUÇÃO NORMATIVA EUROPEIA NA PROTEÇÃO DE DADOS

1.1. BREVES NOÇÕES HISTÓRICAS SOBRE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O direito à privacidade e o direito à proteção de dados pessoais, ainda que intimamente relacionados, são direitos distintos.

As implicações jurídicas do emergente e desenfreado progresso tecnológico fizeram com que os limites do direito à privacidade fossem colocados em debate, vez que a exposição da intimidade e da vida privada do indivíduo, mediante o uso de novas técnicas e instrumentos, passaram a ser atingidas de forma nunca antes imaginada.

Assim, antecedente e prévio a qualquer referência que se venha a fazer quanto à proteção de dados pessoais, é necessário ingressar, ainda que com breves considerações, no campo do direito à privacidade, que teve seu marco histórico nos idos de 1890 com a publicação do artigo intitulado *The Right to Privacy*[3], pelos advogados Samuel Warren e Louis Brandeis[4], na revista Harvard Law Review[5].

Alheia às suas raízes europeias onde, desde século XVI, já despontavam as primeiras noções do que hoje se entende por privacidade, foi nos Estados Unidos que a discussão sobre o tema deixou de estar atrelada ao direito de propriedade, como antes se a tinha. A partir de então, a privacidade passa a ser vista como um direito de proteção à pessoa, de caráter pessoal e individualista, com características de direito negativo (consubstanciado na não intervenção do Estado na esfera privada individual), definida pelos autores no artigo acima referido, em reverência à jurisprudência em ascensão naquele momento, como *the right to be alone* (direito à ser deixado só).

> Um dos tópicos mais importantes e que garantem o interesse até hoje no artigo de Warren e Brandeis de 1890 é a constatação do vínculo da tutela da privacidade ao progresso tecnológico. Esse progresso torna possíveis novas formas de veiculação e obtenção de informações sobre as pessoas, sendo o

[3] Já nessa época em que florescia a imprensa, o mercado aguçava a curiosidade e a bisbilhotice da alta sociedade nas suas colunas sociais. A Sra Warren era tão conhecida pelas suas recepções e festas sociais muito selectivas. Foi a sua revolta pela publicação jornalística das listas dos seus convidados e das iguarias que lhes servia que motivou o artigo jornalístico referido (GOMES *apud* SANTOS, 2017).

[4] Tendo frequentado juntos a Universidade de Harvard no ano de 1877, na época da publicação do artigo eram colegas de escritório de advocacia em Boston. Posteriormente, o primeiro seguiu uma carreira de sucesso na advocacia e o segundo, tornou-se um influente juiz da Suprema Corte Americana.

[5] O texto foi elaborado em razão da divulgação na imprensa, então em formação, de escritos pessoais e de uma fotografia tirada no casamento da filha de Warren, suntuosa comemoração ocorrida em Boston e que motivou a confecção do artigo (especulou-se na época que a insatisfação de Warren já existia há muito ante a corriqueira presença de sua família nos noticiários cotidianos).

> vetor principal que proporcionou a demanda pela elaboração de um direito à privacidade, que veio a se consolidar em diversos ordenamentos jurídicos desde então. (DONEDA, 2021)

Muito elucidativas são as lições trazidas pela professora Laura Schertel Mendes que, em menção ao artigo em comento, leciona que Warren e Brandeis,

> ao identificarem o direito à privacidade, buscaram igualmente definir os seus limites, nos seguintes termos: (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. (MENDES, 2014)

A publicação de Warren e Brandeis, assim, marca o início do debate moderno sobre a privacidade. Presente na jurisprudência e literatura contemporâneas e reflexo de uma época, tencionava, dentre outros aspectos, as mudanças havidas pela sociedade ante o surgimento das tecnologias de informação (jornais e fotografias) e da comunicação em massa, deixando de lado as estruturas de tutela da propriedade anteriormente adotadas para, então, proteger aspectos da vida privada.[6]

Seguindo em transformação, o conceito de privacidade foi novamente reconstruído no decorrer do século XX. De um direito com conotação negativa, passa, pois, a ser tido como uma garantia de controle do indivíduo sobre suas próprias informações, adquirindo, a partir de então, um caráter positivo. Isto vem em decorrência do tratamento informatizado de dados experimentado na época, bem como das reflexões sobre o quão intrusivo seria o uso intenso de computadores na vida do indivíduo, potencialmente servindo como instrumento de controle da vida privada e dos novos desafios a serem enfrentados pelo direito, dando ensejo, então, a criação de um espaço de proteção de dados pessoais.

Sobre a evolução do conceito de privacidade, memoráveis são as lições do festejado mestre italiano Stefano Rodotà, lecionando que

[6] Sobre a evolução do conceito de privacidade, em riqueza de detalhes, vide item 1.4, intitulado ‘A Caminho da Privacidade’, na obra de Doneda (2019, p. 98-132).

> (....) Depois da definição histórica feita por Warren e Brandeis – "o direito de ser deixado em paz" – outras definições foram desenvolvidas para espelhar diferentes clamores. Num mundo onde nossos dados estão em movimento incessante, "o direito a controlar a maneira na qual os outros utilizam as informações a nosso respeito" (A. Westin) torna-se igualmente importante. (...) As definições mais recentes não superam as anteriores, exatamente porque elas são baseadas em diferentes requisitos e operam em níveis diferentes. Antes mesmo da mencionada aceleração trazida pela evolução tecnológica e científica, a maneira pela qual a definição convencional de privacidade era aplicada já havia evoluído. O direito de ser deixado em paz não foi construído meramente como a expressão da era de ouro da burguesia, que havia protegido sua esfera imaterial por meio da mesma proibição ao esbulho que por muito tempo foi a principal característica da propriedade imobiliária. Sob o impulso dado por Louis Brandeis, emergiu uma visão na qual a privacidade foi vista também como uma ferramenta de proteção a minorias e opiniões dissonantes e, portanto, à livre manifestação e ao direito de livremente desenvolver a personalidade. Aqui surge um aparente paradoxo: a forte proteção da esfera privada em última instância não resguarda a privacidade nem a mantém protegida do olhar indesejável; na verdade, permite que crenças e opiniões individuais sejam tornadas públicas livremente. Isto abriu o caminho para aproximar ainda mais a associação entre privacidade e liberdade. (RODOTÀ, 2008, p. 15-16).

A partir da década de 70, ante a edição da primeira lei americana que tratava da privacidade de forma ampla[7], o direito associou cada vez mais a privacidade com casos de informações armazenadas em banco de dados, em especial os que contém informações sobre consumidores.

> Hoje, quando se fala sobre privacidade, geralmente refere-se não apenas ao direito de manter o caráter confidencial de fatos pessoais, porém ao direito de saber quais informações sobre si próprio são armazenadas e utilizadas por outros, e também o direito de manter essas informações atualizadas e verdadeiras. (SMITH *apud* DONEDA, 2019, p. 128)

Foi neste mesmo viés e também na década de 70 que se deu a evolução do conceito de privacidade na Europa, amparado nos debates travados em outros países sobre a expansão dos computadores e processadores de dados, situação captada à perfeição pelo já citado mestre Stefano Rodotà[8] que, anos mais tarde, diria que a privacidade é "o direito de manter o controle

[7] Trata-se do *Fair Credit Reporting Act,* de 1970.

[8] Em 1971, após períodos de magistério e pesquisa em Oxford e Stanford, Rodotà publicou o artigo *Elaboratori elettronici, strutture amministrative e garanzia della collettività,* embrião do livro que publicaria em 1973, *Elaboratori elettronici e controllo sociale,* obra visionária ao estabelecer os parâmetros para que o conceito de privacidade passasse a ser visto na integralidade de seu impacto para a pessoa e não meramente em seu aspecto individualístico – ou, nos termos do próprio Rodotà, evitando que a privacidade seja tratada meramente como um "direito dos egoísmos privados". Ao mapear o debate inaugurado por Alan Westin (1929-2013) e outros estudiosos, Rodotà percebeu que a discussão sobre privacidade estava profundamente conectada com princípios

sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada" (RODOTÀ *apud* DONEDA, 2019, p. 132).

Ainda naquela época surgiram casos emblemáticos como forma de reação da sociedade aos novos efeitos do uso da informática para a operação de informações pessoais. Tais casos consistiram nos primeiros desafios experimentados pelo direito frente às tecnologias que emergiam na época e que geravam grande fluxo informacional, a partir da informatização do tratamento de dados.[9]

Assim, impulsionado pelo surgimento de projetos como o do *National Data Center* e do SAFARI, e outros que se verificaram em diversos países neste mesmo viés, começaram a tomar forma as leis de vanguarda sobre a proteção de dados. Essas leis – doutrinariamente chamadas leis de 1ª geração[10] – pretendiam controlar a coleta e manutenção de informações em grandes centros de processamento de dados existentes nos órgãos públicos, bem como sua posterior utilização pelo Estado. A legislação que então surgia tencionava preservar os direitos e liberdades fundamentais de eventuais violações decorrentes da coleta ilimitada de dados pessoais pelo Estado, destinatário inicial de tais normas protetivas.

Assim, a primeira lei que tratava da proteção de dados foi a do *Land* alemão de Hesse (*Hessisches Datenschutzgesetz*)[11], em 1970.[12] Composta por 17 artigos e com os objetivos acima indicados, trouxe como inovação não só a figura de uma autoridade de proteção de dados (responsável pelo controle do confronto entre os dados pessoais e os mantidos pela administração pública), mas também a própria expressão "proteção de dados", bem como uma

---

democráticos e liberdades civis, e que o tradicional conceito de Warren e Brandeis de *privacy* como "direito a ser deixado só", do final do século XIX, precisava ser atualizado. Rodotà lançava as bases, em uma sociedade na qual o tratamento de dados pessoais dava seus primeiros passos para ser ubíquo, para que a privacidade passasse a ser considerada como o direito de "controlar como outros utilizam informações sobre você". (...) Posteriormente, Rodotà deu continuidade à sua análise sobre privacidade e proteção de dados pessoais, qualificando o direito de privacidade como o direito de reter controle sobre informações relacionadas a si próprio e determinar a maneira como "sua esfera privada é construída", em particular no livro *Tecnologie e diritti* (1995) – no qual, inclusive, trata igualmente de outra área de fronteira com a qual passaria a trabalhar, que é a bioética e direito. Rodotà e equilíbrio entre direito, tecnologia e política. DONEDA D. ZANATTA R. A. F. Rodotà e equilíbrio entre direito, tecnologia e política. site Jota.info, em 28/06/2017, por. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/rodota-e-equilibrio-entre-direito-tecnologia-e-politica-28062017. Acesso em 27/03/2021.

[9] Trata-se dos casos do *National Data Center*, SAFARI e da decisão no caso do censo alemão, proferida pelo Tribunal Constitucional Alemão, a serem melhor estudados adiante.

[10] Essa categorização das gerações de leis de proteção de dados, proposta por Viktor Mayer-Schonberger (*General development of data protection in Europe*), é largamente utilizada pela doutrina e também dela se lançará mão no presente estudo, para fins didáticos.

[11] A Lei de Proteção de Dados Pessoais do *Land* de Hesse, pertencente à extinta Alemanha Ocidental, é o marco inicial na estruturação de uma lei europeia sobre a matéria. Esta foi seguida pela Bavária, no mesmo ano e, posteriormente, por outros *Lander* alemães, até a edição de uma Lei Federal Alemã sobre a Proteção de Dados (1977).

[12] Nos Estados Unidos, a primeira lei que tratou sobre a proteção de dados foi o *Privacy Act,* em 1974; anterior à ele e tratando exclusivamente de dados referentes a crédito de consumo, o *Fair Credit Reporting Act,* de 1971.

nova visão nesta matéria que ia além da segurança da informação, da privacidade ou do sigilo, lançando as bases de um modelo normativo autônomo – o da proteção de dados pessoais.

Já a primeira lei nacional que tratava da proteção de dados[13] surgiu na Suécia[14], em 1973, e se referia ao controle de informações contidas em bancos de dados[15], seguida por outros países europeus até a edição da Lei Federal sobre a Proteção de Dados da República Federativa da Alemanha (*Bundesdatenschutzgesetz*), em 1977.

Estas legislações se concentravam em regular a atividade do processamento dos dados previamente, mediante a exigência de registro nos órgãos competentes e/ou a expedição de licença prévia para funcionamento, com acompanhamento detalhado de cada caso. Tal prática, todavia, restou inviabilizada ante o aumento exacerbado dos centros de processamento de dados, razão pela qual as leis de 1ª geração logo foram superadas.

Assim, com a pulverização dos centros de tratamentos de dados, cujo monopólio já não mais pertencia ao Estado, mas passando também a entes privados, aliado ao crescente descontentamento da população com uso indiscriminado de seus dados pessoais por terceiros, o foco da legislação passa a ser a ser este, bem como o desenvolvimento de instrumentos para sua tutela. Começa, então, a se delinear uma nova linhagem de leis de proteção de dados – as leis de 2ª geração.

As leis sobre a matéria, então, concentram-se na privacidade e na proteção de dados pessoais como uma liberdade negativa a ser exercida pelo próprio cidadão, como ocorreu na França[16] , em 1978, na Lei Austríaca e nas Constituições Portuguesa e Espanhola.

Dentre as perturbações surgidas com o advento destas legislações, uma das principais se refere ao fato de que a entrega de dados pessoais pelo cidadão ao Estado ou a um ente privado tinha se tornado, em algum momento, imprescindível para sua presença no contexto social. A interrupção de tal fluxo de informações consistia, assim, em verdadeira exclusão do indivíduo

[13] Denominada 'Estatuto para Banco de Dados' (*Data Legen 289* ou *Datalag*).
[14] País com tradição em questões referentes à informação, a Suécia desde 1776 já havia legislado sobre a matéria e adotado o princípio da publicidade, ante a promulgação de uma lei que dava acesso a registros públicos e atos do governo e que influenciaria na posterior edição da lei de liberdade de imprensa, de 1810.
[15] Nesta época, na Suécia, os dados (inclusive pessoais) eram largamente utilizados pelo Estado para fins de planejamento social e se pretendia, desde 1963, paulatinamente, o cruzamento destes dados com dados do registro imobiliário, policiais, registro civil e de veículos, dentre outros. Na realidade, mediante a utilização do número de identificação único dos cidadãos existente no país desde 1947, o objetivo do governo, com o cruzamento dos dados em seu Escritório Central de Estatística, era a formação de um Registro Central de Contribuintes. Tal situação gerou uma série de questionamentos por parte da sociedade que acabaram redundando, como consequência, na interrupção de alguns programas existentes neste sentido e na edição de uma lei nacional de proteção de dados pessoais.
[16] Chamada *Informatique et Libertés,* dentre outros, continha dispositivos que instituíram um órgão para garantir sua observância, a *Commission Nationale de l'Informatique et des Libertés.*

de algum aspecto da cena social, tornando inviável para o cidadão comum a vida em sociedade.

Essa abundância de iniciativas legislativas ecoou, também, no âmbito internacional, onde começou a despontar a idéia de que a questão não seria solucionável tão somente pelo direito interno dos Estados. Tendo em conta que dados pessoais não respeitam fronteiras e facilmente seriam coletados e utilizados fora dos limites dos Estados, organizações internacionais como a OCDE – Organização para a Cooperação e Desenvolvimento Econômico – trabalharam no sentido de estabelecer diretrizes para regular o regular o tráfego transfronteiriço de dados. Dos estudos realizados pela OCCD resultaram as chamadas *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[17], em 1980.

Posteriormente, no decorrer da década de 80, surgem as chamadas leis de proteção de dados de 3ª geração[18]. Considerando o cidadão como um ser inserido em um contexto social e sua participação neste, e sob a influência da decisão proferida pelo Tribunal Constitucional Alemão, as leis que versam sobre a proteção de dados passaram a proteger, também, a concretização da liberdade do cidadão em fornecer ou não seus dados pessoais. Ou seja, buscavam preservar a autodeterminação informativa.

Leciona a professora Laura Schertel Mendes (2014), que

> A principal diferença em relação à segunda geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como a opção entre "tudo ou nada" (MENDES, 2014, p. 42)

Esta nova safra de leis foi impulsionada, também, pela dificuldade em se localizar os dados pessoais após a coleta (armazenamento e transmissão), ante o advento da interligação dos bancos de dados em rede. Consideravam a participação do titular dos dados, foco principal de sua estrutura, no processo de tratamento pelo responsável pela recolha e por terceiros, bem como já alinhavavam algumas garantias ao titular, como o dever de informação. Todavia, há que se considerar que o cidadão era levado a concordar com determinadas situações, nem sempre perfeitas, para que pudesse exercitar o direito à autodeterminação informativa, suportando, por vezes, prejuízos sociais ou econômicos.

[17] As principais diretrizes internacionais sobre a proteção de dados serão objeto de estudo em tópico específico deste trabalho.

[18] São exemplos da 3ª geração de leis, dentre outras, a previsão constitucional da proteção de dados pessoais da Holanda, as alterações ocorridas nas leis de proteção de dados da Alemanha, Áustria, Noruega e Finlândia e, ainda, as leis dos Estados alemães editadas após a decisão proferida pelo Tribunal Constitucional Alemão.

Por fim, segundo Doneda (2019), a evolução geracional da normativa sobre a proteção de dados culminou, no momento atual, em leis que buscam

> fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo o desequilíbrio nesta relação, que não era resolvido com medidas que simplesmente reconheciam o direito à autodeterminação informativa; outra, paradoxalmente, é a própria redução do papel da decisão individual de autodeterminação informativa. Isso ocorre porque se parte do pressuposto de que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, à qual não pode ser conferida exclusivamente a uma decisão individual (DONEDA, 2019, p. 179)

A moderna normativa sobre a proteção de dados – leis de 4ª geração – avançou considerando a necessidade de proteção do direito de forma coletiva, com instrumentos adequados para tanto e buscando alcançar resultados concretos. Tal direcionamento inclui a atuação de autoridades independentes para a aplicação da lei, com a diminuição da autonomia do indivíduo em conceder autorização para tratamento dos seus dados (algumas legislações vedam, inclusive, o tratamento de dados sensíveis de tal forma que nem a autorização do próprio titular pode legitimar tal prática) e, também a edição de normas específicas (normas setoriais) para alguns setores que tratam dados pessoais e que apresentam peculiaridades, como o setor de crédito ao consumidor e da saúde, em complementação às normas gerais de proteção de dados já existente no respectivo país.

Sobre o caminho trilhado pela normativa da proteção de dados e brevemente esboçado nessa seção, com maestria a professora Laura Schertel Mendes conclui que

> (...) tal disciplina passou por uma transformação dinâmica e significativa no período das últimas quatro décadas, especialmente em razão das modificações tecnológicas. Ademais, percebe-se que a evolução das gerações de normas de proteção de dados pessoais reflete a tentativa de se buscar, cada vez mais, um modelo que garanta efetivamente a autodeterminação do indivíduo, não obstante as diversas dificuldades encontradas para tanto. Por fim, é notável como, ao longo do desenvolvimento do regime de proteção de dados pessoais, fortaleceu-se o conceito da tutela da personalidade do cidadão, tanto na sua vertente da proteção da autodeterminação como na vertente de proteção de dados sensíveis (MENDES, 2014, p. 44)

Na medida em que evoluíram as normas de proteção de dados, mais se firmava a diferenciação entre os direitos à privacidade e a proteção de dados pessoais.

1.1.1 Casos emblemáticos que influenciaram na evolução do conceito de privacidade e formação da atual legislação de Proteção de Dados

A preocupação com o avanço incessante do processamento automatizado de dados pessoais e o receio do sacrifício do direito à privacidade ante o controle da vida privada dos indivíduos pelos computadores tomou ainda mais importância com a divulgação de casos emblemáticos que acabaram por contribuir com a formação do atual modelo de proteção de dados.

Nesta linha, o primeiro caso que se tem como referência é o do *National Data Center*, ocorrido nos Estados Unidos, em 1965, envolvendo o Escritório do Orçamento Nacional (*Bureau of Budget*). O projeto, capitaneado por dito órgão governamental, agregando dados dos cidadãos norte-americanos disponíveis em diversos setores da administração federal (tais como dados fiscais, trabalhistas, previdenciários e, ainda, os obtidos através do censo) e utilizando-se da tecnologia então recém surgida, todavia sem levar em conta a privacidade do cidadão, pretendia constituir uma central única de armazenamento de informações pessoais – o *National Data Center*, visando a eficiência da atividade administrativa. Assim, "Ainda que a proposta pudesse incrementar a eficiência da burocracia estatal, ela também representava uma série de ameaças a privacidade" (KRAUS *apud* DONEDA, 2021, p. 07).

Referido projeto foi objeto de ampla discussão no Congresso norte-americano na época. O debate se deu em torno da problemática observada pela concentração de dados em um único órgão, em especial sendo este a Administração Pública, resultando num grande incremento no poder estatal, contrário, inclusive, à tradição liberal democrata reinante nos Estados Unidos.

> Um outro ponto relevante no debate de então foi a menção difusa à dignidade e à proteção da personalidade como fundamento das medidas propostas (contrárias à instituição do NDC). Outro, ainda, foi a conclusão, relacionada à diversidade de estatutos da informação pessoal, de que nem todas as informações sobre uma pessoa possuem idêntica importância e, sendo assim, não devem ser protegidas da curiosidade alheia da mesma forma. Também restou clara a menção a alguns dos primeiros princípios orientadores da proteção das informações pessoais. (DONEDA, 2019, p. 163)

Ao final dos trabalhos, concluiu-se pela impossibilidade de se implantar um banco nacional de dados sem que houvesse regras suficientes que conferissem garantias adequadas à

privacidade dos cidadãos que dele fizessem parte; para tanto, a disposição de informações pessoais de forma descentralizada era uma garantia possível.

Embora tenha-se-lhe negado seguimento pelo Congresso Nacional americano, fato é que o debate do *National Data Center* ecoou na sociedade norte-americana e foi o incentivo a partir do qual iniciativas tomaram forma, como a formulação do *Fair Credit Reporting Act* (FCRA), a legislação sobre informes de crédito e dados pessoais, em 1970, e também o *Privacy Act,* de 1974.

Doutrinariamente, todavia, a herança mais sistemática do período é um relatório elaborado pelo Departamento de Saúde, Educação e Bem-Estar, denominado *Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automaated Personal Data Systems*[19]*,* que influenciou na formação de uma legislação federal sobre a proteção de dados nos Estados Unidos – nele se propôs a observância dos *Fair Information Practice Principles,* algo como "princípios para o tratamento leal da informação". Referido documento trouxe os delineamentos iniciais de alguns princípios que hoje norteiam a disciplina da proteção de dados pessoais, tais como o da finalidade, livre acesso, transparência, segurança e qualidade/correção dos dados, influenciando, inclusive, a discussão sobre o tema em outros países e o início da formação das bases do direito à proteção de dados pessoais em território europeu (DONEDA, 2021).

Tal relatório propunha, ainda, a redefinição de um conceito de privacidade[20], bem como "uma base para o estabelecimento de procedimentos que asseguram ao indivíduo o direito de

[19] Registros, computadores e Direitos do Cidadão. Relatório do Comitê Consultivo do Secretário sobre Sistemas Automatizados de Dados Pessoais. Julho/1973. Disponível em: https://epic.org/privacy/hew1973report/. Acesso em 27/03/2021.

[20] "Da mesma forma, é igualmente incompatível com a mutualidade das relações geradoras de registros atribuir à instituição um papel unilateral na tomada de decisões sobre o conteúdo e o uso de seus registros sobre indivíduos. No entanto, é nossa observação que as organizações que mantêm registros sobre as pessoas comumente se comportam como se tivessem recebido um papel unilateral. Isso não significa que as decisões sempre são feitas em prejuízo do sujeito do registro; o contrário é freqüentemente o caso. O fato, entretanto, é que o sujeito do registro geralmente não tem direito a um papel nas decisões que as organizações tomam sobre os registros que lhe pertencem. Sua oportunidade de participar dessas decisões depende da disposição da organização de manutenção de registros em deixá-lo participar e, em alguns casos. Aqui está o cerne da questão. A privacidade pessoal, no que se refere à manutenção de registros de dados pessoais, deve ser entendida em termos de um conceito de mutualidade. Assim, oferecemos a seguinte formulação: 'A privacidade pessoal de um indivíduo é diretamente afetada pelo tipo de divulgação e uso feito de informações identificáveis sobre ele em um registro. Um registro contendo informações sobre um indivíduo em forma identificável deve, portanto, ser regido por procedimentos que concedem ao indivíduo o direito de participar na decisão de qual será o conteúdo do registro, e qual divulgação e uso serão feitos das informações identificáveis em isto. Qualquer registro, divulgação e uso de informações pessoais identificáveis não regidas por tais procedimentos deve ser considerado uma prática injusta de informação, a menos que tal registro, divulgação ou uso seja especificamente autorizado por lei'. Esta formulação não fornece a base para determinar 'a priori' quais dados devem ou podem ser registrados e usados, ou por que e quando. No entanto, fornece uma base para o estabelecimento de procedimentos que asseguram ao indivíduo o direito de participar de uma forma significativa nas decisões sobre o que entra nos registros sobre ele e como essa informação deve ser usada". (Registros, computadores e Direitos

participar de uma forma significativa nas decisões sobre o que entra nos registros sobre ele e como essa informação deve ser usada"[21].

Outros países iniciaram, nesta mesma época, projetos semelhantes ao *NDC*. Digno de nota e que ocorreu na França, também na década de 70, foi o caso SAFARI – *Système Automatisé pour les Fichiers Administratifs et le Repertoire des Individus*, projeto do *Instituit National de la Statistique.* Igualmente sob a justificativa de melhores resultados na gestão administrativa, o SAFARI também pretendia concentrar as informações existentes em poder do governo em uma só central de dados, a conexão dos dados em poder do governo com dados estatísticos e, ainda, atribuir um número identificador a cada cidadão, com o qual o indivíduo permaneceria por toda a vida, com pretensões nitidamente discriminatórias.

Apelidado pela imprensa local de "caça aos franceses", o projeto SAFARI foi vetado em 1974 por um ato do governo francês, que proibiu a troca de dados entre os órgãos do governo. Logo em seguida, foi elaborada a lei francesa proteção de dados, em 1978 – *Loi Informatique, Fichiers et Libertés.*

No mesmo viés dos casos antes narrados, porém com solução jurídica, e não política, foi o julgamento realizado pelo Tribunal Constitucional Alemão, que envolvia a própria lei que instituiu o Censo Alemão de 1982, mais precisamente no tocante ao método de coleta de informações e ao destino destas[22].

---

do Cidadão. Relatório do Comitê Consultivo do Secretário sobre Sistemas Automatizados de Dados Pessoais. Salvaguardas de Privacidade. Julho/1973 Disponível em: https://epic.org/privacy/hew1973report/c3.htm. Acesso em 07/04/2021).

[21] "As salvaguardas da privacidade pessoal baseadas em nosso conceito de mutualidade na manutenção de registros exigiram a adesão das organizações de manutenção de registros a certos princípios fundamentais de práticas justas de informação. 1. Não deve haver sistemas de manutenção de registros de dados pessoais cuja existência seja secreta. 2. Deve haver uma maneira de um indivíduo descobrir quais informações sobre ele estão em um registro e como elas são usadas. 3. Deve haver uma maneira de um indivíduo impedir que as informações sobre ele obtidas para um propósito sejam usadas ou disponibilizadas para outros propósitos sem o seu consentimento. 4. Deve haver uma maneira de um indivíduo corrigir ou alterar um registro de informações identificáveis sobre ele. 5. Qualquer organização que crie, mantenha, use ou divulgue registros de dados pessoais identificáveis deve garantir a confiabilidade dos dados para o uso pretendido e deve tomar precauções razoáveis para evitar o uso indevido dos dados. Esses princípios devem reger a conduta de todos os sistemas de manutenção de registros de dados pessoais. Desvios em relação a eles devem ser permitidos apenas se for claro que algum interesse significativo da pessoa em questão será atendido ou se algum interesse social primordial puder ser claramente demonstrado; nenhum desvio deve ser permitido, exceto conforme especificamente previsto por lei". (Registros, computadores e Direitos do Cidadão. Relatório do Comitê Consultivo do Secretário sobre Sistemas Automatizados de Dados Pessoais. Salvaguardas de Privacidade. Julho/1973 Disponível em: https://epic.org/privacy/hew1973report/c3.htm Acesso em 06/04/2021)

[22] As respostas dadas pelos cidadãos às 160 perguntas contidas no formulário do censo seriam, posteriormente, submetidas a tratamento informatizado disponível na época. Os dados coletados poderiam ser compartilhados com as autoridades federais e com os Länder (cada um dos 16 estados federados da Alemanha), ou confrontados com os dados do registro civil com possiblidade de retificação do próprio registro. Havia previsão, ainda, de aplicação de multa para quem não respondesse ao censo e de benefício aos delatores destes. Tais circunstâncias geraram um sentimento de insegurança na sociedade ante a possibilidade de controle pelo governo dos cidadãos

Há muito a Alemanha já mantinha uma cultura de proteção de dados e, desde 1977, havia uma lei federal dispondo sobre a matéria; todavia, tal se mostrou insuficiente para proteger o cidadão de possíveis violações a direitos, naquele contexto histórico.

> Alguns comissários de proteção de dados pessoais[23] e entidades da sociedade civil organizada chamaram a atenção para os problemas que o censo, na forma que foi planejado, poderia acarretar aos alemães. Este protesto deu origem a um processo que provocou uma sentença constitucional, suspendendo provisoriamente o censo e declarando que a lei que o instituíra era inconstitucional em relação aos artigos 1.1 e 2.1 da Lei Fundamental[24], exatamente a base sobre a qual se estruturava o direito geral da personalidade – *allgemeines Persönlichkeitsrecht.* (DONEDA, 2019, p. 166-167)

Na célebre sentença, a Corte Constitucional Alemã reconheceu princípios que hoje estruturam a proteção de dados. Um deles foi o da finalidade, quando considerou incompatível a coleta de dados para fins estatísticos, com a posterior utilização de tais dados para guarnecer órgãos administrativos onde seria necessário identificar os cidadãos – utilização para finalidade diversa da declarada no momento da coleta. Outro, o da autodeterminação informativa, um dos fundamentos da proteção de dados e já presente na doutrina americana – o direito do indivíduo de controlar as informações que lhe digam respeito, inclusive decidindo, por si só, quando e dentro de quais limites seus dados podem ser utilizados.

Referido julgado joga luz, ainda, na questão sobre os dados considerados sem importância. Em que pese inicialmente pareça que um dado não tem importância, considerando o avanço da informática e dos métodos de processamento de informações, com a manipulação de grande volume de dados de forma automática e a capacidade de armazenamento destes praticamente ilimitada, aliado, ainda, ao cruzamento com outros dados para a formação de perfis pessoais, sobre os quais os indivíduos titulares dos dados não tem qualquer controle – tanto em relação à composição quanto à correção e veracidade dos mesmos – a verdade é que, hoje, não há mais nenhum dado sem importância.

---

[23] No sistema federal alemão, os Estados (*Länder*) tem competência para legislar sobre a proteção de dados pessoais e também para instituir suas próprias autoridades para a atuação destas leis. (DONEDA, 2019, p. 166)

[24] Que assim dispõe, em tradução livre: "A dignidade humana é inviolável. É dever de todo poder estatal respeitá-la e defendê-la", e ao artigo 2, inciso 1: "Todos tem direito ao livre desenvolvimento da própria personalidade, desde que não viole os direitos alheios e não transgrida o ordenamento constitucional e a lei moral" (DONEDA, 2019, p. 166)

> Ao reconhecer a centralidade do controle sobre as próprias informações para a proteção da personalidade no contexto do tratamento automatizado de dados, o Tribunal realizou notável trabalho de atualização das garantias fundamentais em vista das circunstâncias tecnológicas da época. Esse trabalho de atualização por conta da mudança de um contexto tecnológico pode ser observado em outras situações, com certas similaridades. (DONEDA, 2021, p. 03-20)

Por fim, digno de nota é que, dentre os muitos avanços, a sentença proferida pela Corte também vem consolidar o entendimento sobre a necessidade de se atribuir contornos constitucionais ao direito à proteção de dados pessoais, nivelando-o como direito fundamental e tornando possível, assim, a tutela da personalidade, mesmo numa área específica como a de proteção de dados.

1.2 PRINCÍPIOS PARA A PROTEÇÃO DE DADOS PESSOAIS

A evolução geracional que sofreram as normativas sobre a proteção de dados em busca de modelos mais completos guardou simetria nos diversos países cujos ordenamentos jurídicos tratavam da matéria. Tal desenvolvimento deu-se de forma simultânea nos Estados Unidos e na Europa, com objetivos semelhantes e a preservação de determinados princípios comuns, resultando na edição de leis semelhantes sobre a matéria em tais países, bem como no fortalecimento de alguns princípios básicos vinculados à proteção a pessoa e aos direitos fundamentais.

Alguns destes princípios já se encontravam delineados nas leis de 1ª e 2ª geração; outros, sua origem remonta a segunda metade da década de 60, época em que o caso do *National Data Center*, rechaçado pelo Congresso americano, fomentou uma série de iniciativas semelhantes (bancos de dados menores continuaram a ser instalados, por exemplo). Vários dos temas surgidos durante a discussão sobre a viabilidade do NDC permaneceram em voga, em especial na área da saúde, ante a inquietação com o tratamento de dados médicos em sistemas informatizados e que ensejou a realização de um estudo pelo Departamento de Saúde, Educação e Bem-Estar americano. Tal estudo culminou com a emissão do relatório *Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automaated Personal Data Systems*[25], no ano de 1973, que concluía pela relação direta entre a privacidade e o tratamento de dados pessoais e pela necessidade de estabelecer regras

[25] Sobre o tema, vide item 1.1.1, e notas de rodapé 15 a 17.

para o controle das próprias informações, formulando o que chamaram de 'princípios fundamentais de práticas justas de informação' – *Fair Information Practice Principles*[26].

O que se percebe é que, "Ao longo do desenvolvimento do conceito de privacidade como proteção de dados pessoais estabeleceu-se, por meio de instrumentos internacionais e transnacionais, um consenso em torno de um quadro básico de princípios que devem nortear a atividade de tratamento de dados". (BENNETT *apud* MENDES, 2014, p. 68)

Assim, estes princípios passaram a constituir uma espécie de 'núcleo duro' em matéria de proteção de dados, presentes nas várias legislações que se seguiram, com pouquíssimas diferenças. A aptidão como um conjunto de princípios a direcionar a disciplina da proteção de dados pessoais se evidenciou ainda mais com a edição da Convenção 108 e das *Guidelines* da OCDE, no início da década de 80, passando a integrar diversos tratados, convenções e legislações nacionais.

Conforme bem observa a professora Laura Schertel Mendes, "Esses princípios têm como finalidade impor limitações ao tratamento de dados, bem como atribuir poder ao indivíduo para que esse possa controlar o fluxo de dados". (MENDES, 2014, p. 68).

Assim, pode-se elencar os princípios básicos da proteção de dados pessoais da seguinte forma:

1) **Princípio da Finalidade:** a utilização dos dados pessoais deve corresponder à finalidade declarada ao titular dos dados por ocasião da coleta destes, podendo-se também, a partir deste princípio, "estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade)" (DONEDA, 2019, p. 182). Com base neste princípio fundamenta-se, também, a restrição de transferência de dados à terceiros. "Por fim, esse princípio exige que o responsável pelo tratamento de dados estabeleça de forma expressa e limitada, a finalidade do tratamento de dados, sob pena de se considerar ilegítimo o tratamento realizado com base em finalidades amplas ou genéricas." (ROSSNAGEL *apud* MENDES, 2014, p. 71)

2) **Princípio da Publicidade** (ou da Transparência): a existência de um banco de dados pessoais deve ser de conhecimento público. Cabe ao banco o dever de publicar seu nome, sede e conteúdo, podendo também a publicidade ser dada mediante o envio de relatórios periódicos. Este princípio "reafirma o preceito democrático, segundo o qual não podem existir bancos de dados sigilosos, e baseia-se na ideia de que a transparência é uma das principais

[26] Na mesma época, o Comitê de Privacidade da Grã-Bretanha, liderado por Kenneth Younger, também desenvolvia um estudo, mas no tocante aos riscos do tratamento automatizado de dados pessoais realizado por organizações privadas, que resultou na posterior emissão de um relatório com 10 princípios para a proteção da privacidade, nos mesmos moldes daqueles contidos no relatório americano.

formas de se combaterem os abusos" (BENNETT *apud* MENDES, 2014, p. 71). "Em alguns países, exige-se autorização estatal prévia ou notificação ao órgão supervisor como pressuposto para o funcionamento dos bancos de dados. Percebe-se, assim, que princípio da transparência é condição essencial da *accountability* dos bancos de dados." (MENDES, 2014, p. 71)

3) **Princípio da Qualidade dos Dados** (ou da Exatidão): os dados armazenados devem retratar a realidade e ser objetivos, exatos e atualizados, o que exige que sua coleta tenha sido feita com cuidado e correção. "Tal princípio enseja cautela na formação do banco de dados, assim como demanda a sua constante atualização, de forma a impedir que os dados restem ultrapassados com o passar do tempo. Para a efetividade do princípio da qualidade dos dados, é fundamental a garantia dos direitos de acesso, retificação e cancelamento dos dados." (MENDES, 2014, p. 71) Há que se considerar, também, que dados inexatos, imprecisos ou incompletos podem revelar um perfil equivocado da pessoa natural com resultados que lhe sejam danosos, como ocorre em casos de *profiling, scoring* ou histórico de saúde.

4) **Princípio do Livre Acesso:** aos titulares deve ser franqueado o acesso ao banco onde seus dados estão guardados fornecendo-se-lhes, inclusive, para fins de controle, cópias de tais registros. "Depois deste acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo poder-se-á proceder à eventuais acréscimos". (DONEDA, 2019, p. 182)

5) **Princípio da segurança física e lógica:** os dados devem ser protegidos contra os riscos de violações, sejam elas acidentais ou intencionais, envolvendo a destruição, extravio, alteração, divulgação ou o acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Os princípios aqui elencados, mesmo que com algumas variações, constituem a estrutura de diversas leis, tratados, convenções ou acordos na área da proteção de dados pessoais, aos quais os ordenamentos devem buscar para solucionar as questões surgidas nesta matéria.

A observância destes princípios, em diversos ordenamentos jurídicos, revelava uma propensão à confirmação da autonomia da proteção de dados pessoais e à sua elevação ao patamar de direito fundamental, adotada, primeiramente por países que inauguravam novas ordens constitucionais e que, a vista disso, introduziram, desde logo, as questões relacionadas à informática e à proteção de dados pessoais em nível constitucional. É o caso das

constituições de Espanha (1978) e Portugal (1976)[27], desta última constando, inclusive, menção expressa à proteção de dados pessoais.[28]

[27] A Constituição de Portugal de 1976, em seu artigo 35º, foi a primeira constituição do mundo a proteger expressamente os dados pessoais.

[28] Artigo 35.º Utilização da informática 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei. Disponível em: https://www.uc.pt/protecao-de-dados/legislacao_complementar Acesso em 08/04/2021.

2. A LEGISLAÇÃO EUROPEIA SOBRE A PROTEÇÃO DE DADOS

A história da Europa vem escrita através de uma sucessão de conflitos, inclusive internos; todavia, a união do continente europeu operou-se através do Direito, e não da força, que implicou uma integração do direito no continente europeu iniciada a cerca de 70 anos.

Conforme leciona o professor Danilo Doneda,

> A União Europeia consiste basicamente na formação de um bloco de países com um equilíbrio de poderes entre os estados e as instituições comunitárias. Seu processo de formação remonta à reconstrução europeia após a Segunda Guerra Mundial quando, sob a inspiração de Jean Monet, Robert Schuman e Altiero Spinelli, foram criados organismos com a finalidade de derrubar barreiras comerciais e econômicas entre países europeus, como a Comunidade Europeia do Carvão e do Aço. Em 1957, com o Tratado de Roma, surge a Comunidade Econômica Europeia, continuando o estreitamento econômico entre os países europeus. Esse estreitamento tendia a se tornar também político, o que foi consolidado pelo Tratado de Maastrich, firmado em 1992, que criou a União Europeia. A União Europeia é tida como uma "organização internacional *sui generis*", a qual os países membros transferiram parte da sua soberania e que, assim, tem a possibilidade de construir e criar seu próprio direito comunitário, aplicável no espaço europeu. (DONEDA, 2019, p. 190)

Este contexto de grandes transformações e incertezas trouxe consigo inúmeras inquietações, nas quais tinha lugar de destaque a proteção contra a ingerência de terceiros, incluindo o próprio Estado, na vida privada do indivíduo. Tal preocupação foi reverenciada pela primeira vez na legislação internacional sobre direitos humanos na Declaração Universal dos Direitos do Homem das Nações Unidas (1948)[29]. Este foi o primeiro instrumento jurídico internacional a tratar sobre o respeito pela vida privada e familiar, influenciando no surgimento de outras ferramentas de proteção aos direitos humanos na Europa. Inaugurou-se, a partir dela, uma estrutura legislativa com concepções que, posteriormente, tornariam possível a elaboração de uma legislação de proteção de dados, como a existente nos dias atuais.

No período pós Segunda Guerra Mundial, o objetivo no continente europeu era promover o Estado de Direito, a democracia, os direitos humanos e o desenvolvimento social. É nesse período que surge o Conselho da Europa, composto por todos os estados europeus e

[29] Art. 12. Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. (Declaração Universal dos Direitos Humanos. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em 14/03/2021).

que editou, para a concretização dos objetivos então perseguidos, a Convenção Europeia dos Direitos do Homem (1950)[30], onde o direito à proteção de dados, ainda que não diretamente, encontra espaço de tutela no artigo 8º, inserido no Título I, que trata dos Direitos e Liberdades[31]. Veja-se que, muito antes de se pensar em computadores e *internet,* tais diplomas legais já tutelavam estes direitos.

Posteriormente, emergiu a necessidade da criação de um órgão capaz de assegurar o efetivo cumprimento das obrigações assumidas quando da adesão à Convenção Europeia Dos Direitos do Homem pelos Estados Membros (parte dos quais também, posteriormente, vieram a se tornar Estados Membros da União Europeia). Assim, criou-se o Tribunal Europeu dos Direitos do Homem, em 1959 (Estrasburgo, França), responsável por apreciar as queixas dos cidadãos, grupos de cidadãos (mesmo que não nacionais de um dos Estados membros), ONGs ou pessoas jurídicas que aleguem violações da Convenção ou, ainda, por um Estado Membro com relação a outro.

> O TEDH examinou inúmeras situações relacionadas à proteção de dados, especialmente referentes à intervenção nas comunicações, várias formas de vigilância pelos setores público e privado e proteção em face da conservação de dados pessoais pelas autoridades públicas. Dado que o respeito pela privacidade não é um direito absoluto, quando o exercício do direito à privacidade pode prejudicar outros direitos - como a liberdade de expressão e acesso à informação e vice-versa - o Tribunal tentou encontrar um equilíbrio entre os diferentes direitos enfrentados. O Tribunal esclareceu que o artigo 8º da CEDH não apenas obriga os Estados a se absterem de praticar atos suscetíveis de violar este direito da Convenção como impõe também, em certos casos, uma obrigação positiva de garantir efetivamente o respeito pela vida privada e familiar...[32] (tradução livre).

---

[30] *Las Partes Contratantes tienen la obligación internacional de cumplir el CEDH. Todos los Estados miembros del CdE han incorporado o aplicado ya el CEDH en su legislación nacional, por lo que están obligados a actuar de conformidad con las disposiciones del Convenio*. Ou seja: Os Estados estão sujeitos a uma obrigação internacional de cumprimento da CEDH. Todos os Estados membros do CdE incorporaram ou deram cumprimento à CEDH no seu direito nacional, pelo que são obrigados a atuar em conformidade com as disposições da Convenção (tradução livre). CONSELHO EUROPEU. *Manual de Legislación Europea en Materia de Protección de Datos.* Edición de 2018, p. 26. *Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa.* Luxemburgo: *Oficina de Publicaciones de la Unión Europea, 2019.* Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 Acesso em 16/03/2021.

[31] Artigo 8°. Direito ao respeito pela vida privada e familiar. 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros. Disponível em: https://www.echr.coe.int/documents/convention_por.pdf Acesso em 14/03/2021.

[32] *El TEDH ha examinado numerosas situaciones relacionadas con la protección de datos, en particular referidas a la intervención de las comunicaciones, varias formas de vigilancia por parte de los sectores público y privado y la protección frente a la conservación de datos personales por los poderes públicos. Dado que el*

A Declaração Universal dos Direitos Humanos e a Declaração Europeia dos Direitos do Homem, como já mencionado, traçaram linhas gerais sobre a proteção à privacidade, sendo de extrema importância para sua época e primordiais para o esboço das primeiras noções sobre o direito a proteção de dados pessoais, adotadas antes mesmo do avanço da sociedade de informação.

Tais avanços significaram benefícios consideráveis para os cidadãos e a sociedade, que melhoraram sua qualidade de vida, eficiência e produtividade. Ao mesmo tempo, geram novos riscos ao direito ao respeito pela vida privada. Em resposta à necessidade de contar com regras que regulam especificamente a coleta e o uso de informações pessoais, surgiu um novo conceito de privacidade, conhecido em algumas jurisdições como 'privacidade de informações' e em outras, como o 'direito a autodeterminação' em matéria de informação. Este conceito ensejou na elaboração de normas jurídicas específicas para regulamentar a proteção de dados pessoais.

Assim, o Conselho da Europa[33], a partir da metade da década de 70, adotou várias Resoluções[34] sobre a proteção de dados pessoais fundamentadas no artigo 8º da Convenção Europeia dos Direitos do Homem e finalmente, em 1981, foi aberta para assinatura a Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, conhecida como Convenção 108 ou Convenção de Strasbourg,

---

respeto de la vida privada no es un derecho absoluto, cuando el ejercicio del derecho a la privacidad puede lesionar otros derechos — como la libertad de expresión y el acceso a la información y viceversa — , el Tribunal trata de alcanzar un equilibrio entre los distintos derechos enfrentados. El Tribunal ha aclarado que el artículo 8 del CEDH no solo obliga a los Estados a que se abstengan de realizar cualquier acción que pueda vulnerar este derecho del Convenio sino también a que, en determinadas circunstancias, bajo obligaciones positivas, garanticen activamente el respeto efectivo de la vida privada y familiar. Muchos de estos casos se describen con detalle en los capítulos correspondientes. CONSELHO EUROPEU. *Manual de Legislación Europea en Materia de Protección de Datos. Edición de 2018, p. 27. Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa. Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2019.* Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 Acesso em 23/03/2021.

[33] Artigo 16.o 1. O Conselho exerce, juntamente com o Parlamento Europeu, a função legislativa e a função orçamental. O Conselho exerce funções de definição das políticas e de coordenação em conformidade com as condições estabelecidas nos Tratados. (...) Artigo 26.o 1. O Conselho Europeu identifica os interesses estratégicos da União, estabelece os objetivos e define as orientações gerais da política externa e de segurança comum, incluindo em matérias com implicações no domínio da defesa. O Conselho Europeu adota as decisões necessárias. (...) 2. O Conselho elabora a política externa e de segurança comum e adota as decisões necessárias à definição e execução dessa política, com base nas orientações gerais e linhas estratégicas definidas pelo Conselho Europeu. (...) Tratado da União Europeia. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF. Acesso em 31/03/2021.

[34] O Tratado sobre o Funcionamento da União Europeia, ainda, prevê várias atribuições ao Conselho Europeu.

único instrumento internacional juridicamente vinculativo no domínio da proteção de dados até os dias atuais.

> A Convenção 108 se aplica a todo o processamento de dados realizado pelos setores público e privado, incluindo autoridades judiciais e forças de segurança. Protege as pessoas singulares contra os abusos que podem ser cometidos no tratamento de dados pessoais e procura, ao mesmo tempo, regular os fluxos transfronteiriços de dados pessoais. No que diz respeito ao tratamento de dados pessoais, os princípios estabelecidos na Convenção referem-se, em particular, à recolha e tratamento automático de dados de forma lícita e justa, para determinados fins legítimos. Isso significa que os dados não devem ser usados para fins incompatíveis com esses fins e que não devem ser mantidos por mais tempo do que o necessário. Também se referem à qualidade dos dados, que especificamente devem ser adequados, relevantes e não excessivos (proporcionalidade), além de precisos.[35] (tradução livre)

Instrumento inovador na área da proteção de dados, a Convenção 108 é considerada como o principal ícone de uma visão da matéria sob o ângulo dos direitos fundamentais, preconizando, já em seu preambulo[36], que a proteção de dados pessoais está diretamente ligada à proteção dos direitos humanos e das liberdades fundamentais.

A Convenção de Strasbourg trouxe, em seus 27 artigos, regras mais pormenorizadas para a preservação das pessoas através da proteção de seus dados pessoais, estabelecendo garantias e obrigações quanto ao tratamento de dados pessoais, devotando-se à segurança

---

[35] *El Convenio 108 se aplica a todo tratamiento de datos realizado por los sectores público y privado, incluidas las autoridades judiciales y los cuerpos de seguridad. Protege a las personas físicas contra los abusos que pueden llevarse a cabo en el tratamiento de datos personales, y busca, al mismo tiempo, regular los flujos transfronterizos de datos personales. En lo que respecta al tratamiento de datos personales, los principios establecidos en el Convenio se refieren, en particular, a la recopilación y el tratamiento automático de datos de manera lícita y leal, con fines legítimos especificados. Esto significa que los datos no deben utilizarse con propósitos incompatibles con estos fines y que no deben conservarse más tiempo del necesario. También se refieren a la calidad de los datos, que concretamente deben ser adecuados, pertinentes y no excesivos (proporcionalidad), además de exactos.* CONSELHO EUROPEU. *Manual de Legislación Europea en Materia de Protección de Datos.* Edición de 2018, p. 28. *Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa.* Luxemburgo: *Oficina de Publicaciones de la Unión Europea, 2019.* Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 Acesso em 16/03/2021.

[36]Consta do preâmbulo da Convenção 108: Os Estados membros do Conselho da Europa, signatários da presente Convenção: Considerando que a finalidade do Conselho da Europa é conseguir uma união mais estreita entre os seus membros, nomeadamente no respeito pela supremacia do direito, bem como dos direitos do homem e das liberdades fundamentais; Considerando desejável alargar a protecção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado; Reafirmando ao mesmo tempo o seu empenhamento a favor da liberdade de informação sem limite de fronteiras; Reconhecendo a necessidade de conciliar os valores fundamentais do respeito pela vida privada e da livre circulação de informação entre os povos, acordaram o seguinte:.... Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_protecao_pessoas_tratamento_automatizado_dados_caracter_pessoal.pdf Acesso em 16/03/2021.

destes e permitindo o processamento de dados sensíveis somente mediante a existência de garantias jurídicas adequadas. Conferiu, ainda, aos titulares de dados o direito ao conhecimento e, quando apropriado, a retificação dos mesmos, somente permitindo a limitação aos direitos nela estabelecidos quando conflitantes com interesses superiores, tais como a segurança ou defesa do Estado.

O novel instrumento, vinculativo para os Estados que o ratificaram, permitiu a livre circulação de dados pessoais entre os Contratantes, com limitações a serem observadas nos Estados onde a legislação não estabelece proteção equivalente.

> Deve-se notar que a Convenção 108 é vinculativa para os Estados que a ratificaram. Não está sujeita ao controle judicial do TEDH, mas foi levado em consideração na jurisprudência da TEDH, no contexto do artigo 8.º da CEDH. Ao longo do anos, o Tribunal determinou que a proteção de dados pessoais faz parte importante do direito ao respeito pela vida privada (Artigo 8) e tem sido regido por os princípios da Convenção 108 para determinar se houve ou não interferência na este direito fundamental.[37] (tradução livre)

O Conselho da Europa adotou, ainda, várias Recomendações, medidas não juridicamente vinculativas, visando irradiar os princípios e padrões contidos na Convenção 108 e que, efetivamente, influenciaram no desenvolvimento da legislação de proteção de dados na Europa. Uma das principais foi a Recomendação da Polícia[38] que, por muito tempo, foi o único instrumento na Europa a orientar a utilização de dados pessoais no setor policial e cujas diretrizes[39] tiveram forte influência na formulação da legislação europeia subsequente,[40] além de outras que dispõe sobre o tratamento de dados pessoais no setor do trabalho e nas comunicações eletrônicas.

---

[37] *Hay que señalar que el Convenio 108 es vinculante para los Estados que lo han ratificado. No está sujeto al control judicial del TEDH, pero se ha tomado en consideración en la jurisprudencia del TEDH en el contexto del artículo 8 del CEDH. A lo largo de los años, el Tribunal ha determinado que la protección de los datos personales es parte importante del derecho al respeto de la vida privada (artículo 8) y se ha regido por los principios del Convenio 108 para determinar si se ha producido o no injerencia en este derecho fundamental(...)* CONSELHO EUROPEU. *Manual de Legislación Europea en Materia de Protección de Datos. Edición de 2018, p. 28/29. Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa.* Luxemburgo: *Oficina de Publicaciones de la Unión Europea, 2019.* Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 Acesso em 16/03/2021.

[38] Conselho da Europa, Comitê de Ministros (1987), Recomendação Rec (87) 15 aos Estados Membros, destinada a regulamentar o uso de Dados de Pessoais no Setor Policial. Estrasburgo, 17 de setembro de 1987.

[39] Como exemplo, cite-se a padronização de meios de preservação dos arquivos de dados e de regras claras para acesso somente por pessoas autorizadas a tais arquivos.

[40] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, DO L 281, de 23 de novembro de 1995.

A Convenção 108 foi ratificada por todos os Estados Membros da União Europeia e, em 1999, foi alterada para que, então, também a União Europeia se tornasse parte nela[41].

Logo em seguida (2001), foi admitido um Protocolo Adicional à Convenção 108[42], inserindo normas sobre a obrigatoriedade da criação de autoridades de controle nacionais de proteção de dados, bem como sobre o fluxo de dados transfronteiriços a Estados que não eram partes na convenção (países terceiros):

> A Convenção 108 está aberta à adesão de Partes não Contratantes ao CoE. O potencial da Convenção como um padrão universal, juntamente com sua natureza aberta, poderia servir de base para a promoção da proteção de dados em todo o mundo. Até esta data, 51 países são partes da Convenção 108, entre os quais estão todos Estados membros do Conselho da Europa (47 países) mais o Uruguai, que foi o primeiro país não europeu a aderir em agosto de 2013, bem como as Ilhas Maurício, Tunísia e Senegal, que aderiram em 2016 e 2017[43] (tradução livre)

Recentemente foram ratificados os objetivos principais da Convenção coincidentes com o fortalecimento da proteção da privacidade na esfera digital e dos mecanismos de monitoramento da Convenção, fundamentado em consulta pública realizada no ano de 2011. Concluiu-se, assim, um processo de atualização da Convenção, resguardando-se o seu caráter universal e flexível e intensificando sua aptidão como instrumento global de regulação da proteção de dados com a edição de mais um protocolo adicional no ano de 2018, o Protocolo CETS 223.

Os trabalhos de atualização ocorreram em conjunto com a reforma das normativa europeia de proteção de dados que a União Europeia iniciou em 2012[44], buscando-se observar

---

[41] Conselho da Europa, Alterações à Convenção para a Proteção das Pessoas em relação ao processamento automatizado de dados pessoais (STCE no. 108) para permitir a adesão do Comunidades Europeias, adotada pelo Comitê de Ministros, em 15 de junho de 1999, em Estrasburgo; Artigo 23, parágrafo 2, da Convenção 108, conforme emendada.

[42] Conselho da Europa, Protocolo Adicional à Convenção para a Proteção das Pessoas no que diz respeito ao processamento automatizado de dados pessoais, no que diz respeito às autoridades de controle e fluxos de dados transfronteiriços, STCE No. 181, 2001.

[43] *El Convenio 108 está abierto para la adhesión de Partes no Contratantes del CdE. El potencial del Convenio como norma universal, junto con su carácter abierto, podría servir de base para promover la protección de datos a escala mundial. Hasta la fecha hay 51 países partes del Convenio 108, entre los que se encuentran todos los Estados miembros del Consejo de Europa (47 países) más Uruguay, que fue el primer país no europeo en adherirse en agosto de 2013, así como Mauricio, Túnez y Senegal, que se incorporaron en 2016 y 2017.* CONSELHO EUROPEU. *Manual de Legislación Europea en Materia de Protección de Datos.* Edición de 2018, p. 29-30. *Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa.* Luxemburgo: *Oficina de Publicaciones de la Unión Europea, 2019.* Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 Acesso em 17/03/2021.

[44] A Comissão Europeia propôs uma reforma abrangente das regras de proteção de dados da UE de 1995, para fortalecer os direitos de privacidade *online* e impulsionar a economia digital da Europa.

a compabitilidade entre os dois quadros jurídicos, ao mesmo tempo em que se operavam, também, reformas em outros instrumentos de proteção internacional de dados.

Além de confirmar importantes princípios, mencionada atualização também atribui novos direitos aos titulares de dados como, por exemplo, o direito a ter ciência do motivo pelo qual se realiza o tratamento de seus dados e de se opor a este tratamento, bem como de não se sujeitar a decisões automatizadas sem levar em conta suas próprias opiniões.

Dispõe, ainda, sobre a necessidade de prestação de contas, com o aumento das responsabilidades das entidades que processam dados pessoais, pretendendo, assim, amortecer a prática, em franca ascenção, da criação de perfis na *internet*.

A Convenção 108 modernizada erige como fundamental a estrita observância da normativa de proteção de dados pelas autoridades de controle independentes nos países signatários, enfatizando como primordial o exercício das atribuições de tais autoridades com absoluta indenpendência no cumprimento de seu mister.

2.1 PRINCIPAIS FONTES DO DIREITO DA UNIÃO EUROPEIA EM MATÉRIA DE PROTEÇÃO DE DADOS

O sistema de fontes do direito da União Europeia é inusitado, não guardando simetria no direito interno de qualquer dos Estados-membros ou no Direito Internacional, e nem em qualquer outro sistema jurídico.

2.1.1 Direito Originário

A principal fonte do Direito da União Europeia é o Direito Originário. Conforme leciona a professora Ana Maria Guerra Martins,

> A primeira fonte do Direito da União Europeia é, pois, o Direito Originário, o qual é o parâmetro de validade de todas as outras regras da União Europeia. O Direito Originário é, em primeira linha, constituído pelos Tratados Institutivos, inicialmente, das Comunidades Europeias e, atualmente, da União Europeia, bem como por todos aqueles que os

> modificaram, completaram ou adaptaram, cujo último expoente já não é o Tratado de Lisboa, mas antes o Tratado de Adesão da Croácia.[45]

Desde o início, este sistema sofreu uma permanente evolução[46], em consonância com a história da integração da Europa que, de razoavelmente simples em sua origem, passou a ter sua complexidade aumentada, ainda mais após a edição do Tratado de Maastrischt[47], que desenvolveu um outro quadro normativo a par do já existente nas Comunidades Europeias. Tal conjuntura, aliada a uma série de críticas havidas em razão da inexistência de uma hierarquia de normas e atos previstos no Tratado da União Europeia, culminou na edição do Tratado de Lisboa[48].

O Tratado da União Europeia[49] e o Tratado sobre o Funcionamento da União Europeia[5051] posicionam-se no topo da hierarquia das fontes do Direito da União e constituem

---

[45] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. Editora Almedina. Coimbra, 2017, p. 482.

[46] (...) ... os três Tratados originários são o Tratado da Comunidade Europeia do Carvão e do Aço, assinado em 18 de abril de 1951, entrou em vigor em 25/7/52, cuja validade expirou em 23 de julho de 2002, o Tratado da Comunidade Econômica Europeia, assinado em Roma, em 25 de março de 1957, que entrou em vigor em 1 de janeiro de 1958 e que foi substituído pelo Tratado sobre o Funcionamento da União Europeia aprovado em Lisboa, assinado em 13 e dezembro de 2007 e que entrou em vigor e m 1 de dezembro de 2009, e o Tratado da Comunidade Europeia de Energia Atomica assinado em Roma, em 25 de março de 1957, que entrou em vigor em 1º de janeiro de 1958 e que se mantém em vigor. Os tratados originários foram, ao longo da História da integração europeia, modificados inúmeras vezes, com ou sem observância do procedimento de revisão neles previsto. (...) (MARTINS, 2017, p. 482).

[47] O Tratado da União Europeia foi assinado em Mastrischt, em 07 de fevereiro de 1992, entrando em vigor em 1993. Daí também ser conhecido como Tratado de Maastricht.

[48] (...) o Tratado de Lisboa, por imposição do mandato da CIG 2007, limitou-se a modificar os anteriores Tratados da União Europeia e da Comunidade Europeia, sendo que este último se passou a denominar Tratado sobre o Funcionamento da União Europeia. A ideia de um texto único como base constitucional da União Europeia proveniente da Convenção sobre o Futuro da Europa e aceite pela CIG 2004 foi, por conseguinte, abandonada. Em seu lugar, surge o Tratado de Lisboa, o qual permite colocar a questão de saber se ele consubstancia a vitória daqueles que durante a Convenção sobre o Futuro da Europa defenderam a tese de que a União se deveria fundar em dois Tratados: um tratado que contivesse as bases e um outro que as desenvolvesse. O primeiro seria o TUE e o segundo seria o TFUE. Com efeito, o TUE apresentava algumas características de um tratado-base, na medida em que fixa as regras fundamentais da União, designadamente, as relativas aos objetivos, às atribuições, aos princípios democráticos, às instituições, às cooperações reforçadas e às condições de revisão dos Tratados e de adesão à União. Note-se, todavia, que o TUE também contém regras que dificilmente se enquadram num tratado-base, como é o caso do Título V relativo à PESC. A sua inserção neste tratado explica-se por razões que já atrás foram explicadas, mas o certo é que confere um caráter híbrido ao TUE. Acresce que o TUE e o TFUE tem o mesmo valor jurídico (artigo 1º, par. 3º, do TUE), o que significa que não se verifica qualquer relação de subordinação do TFUE ao TUE. Pode-se dizer que a Ordem Jurídica da União se funda em dois Tratados, sendo que nenhum deles é autossuficiente. Só juntos constituem o fundamento, o critério e o limite do Direito da União. O modo como se integram e organizam as disposições nos dois Tratados é mais influenciado pela anterior estrutura do TUE e do TCE do que por qualquer princípio segundo o qual as bases da União estariam reservadas ao TUE enquanto a implementação pormenorizada faria parte do TFUE. O Direito Originário ainda compreende os Tratados de adesão de novos Estados-membros (...) Por último, deve salientar-se que fazem parte integrante do Direito Originário os Protocolos e Anexos dos Tratados (artigo 51º do TUE). (MARTINS, 2017, p. 483-484).

[49] Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF Acesso em 21/04/2021.

o fundamento, o critério e o limite das suas atribuições normativas. Os Tratados Institutivos[52] imperam sobre todos os atos e normas de Direito Derivado e compõe o chamado 'bloco de constitucionalidade'.

Desde a edição do Tratado de Lisboa, os Tratados Institutivos não tem prazo determinado para vigência[53] e, via de regra[54], são aplicáveis a todos os Estados-membros[55].

> Assim, o TUE e o TFUE formam, desde a entrada em vigor do Tratado de Lisboa, o primeiro fundamento de todo o Direito da União Europeia. A esses dois Tratados há que se juntar a Carta dos Direitos Fundamentais da União Europeia. Embora estes textos tenham todos o mesmo valor jurídico, não está excluída a existência de uma certa hierarquia interna, uma vez que o TFUE se afigura como um tratado de desenvolvimento do TUE e dentro de cada um dos Tratados há disposições que têm um caráter mais fundamental do que outras. (MARTINS, 2017, p. 512)

Nas demais esferas, os atos adotados pelas instituições e pelos órgãos da União – direito derivado – devem respeitar todo o Direito Originário, bem como os princípios gerais do Direito, que também integram o 'bloco de constitucionalidade'.

O Direito Originário deve ser respeitado, ainda, nos acordos internacionais de que a União é parte, ante a possibilidade, inclusive, de controle jurisdicional preventivo e sucessivo (pela via dos atos de conclusão e aplicação) dos mesmos. Os acordos internacionais prevalecem, todavia, sobre o Direito Derivado, na medida em que eles vinculam os Estados-membros e as instituições da União, conforme disposto no Tratado sobre o Funcionamento da União Europeia[56].

---

[50] Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF Acesso em 21/04/2021.

[51] O Tratado sobre o Funcionamento da União Europeia surgiu da alteração do Tratado de Roma (que estabelecia a Comunidade Europeia, em 1957) pelo Tratado de Lisboa (que reformou os Tratados base da União e reorganizou suas instituições, em 2007).

[52] Inicialmente, das Comunidades Europeias e, atualmente, da União Europeia, bem como por todos aqueles que posteriormente os modificaram, completaram ou adaptaram.

[53] *Ex vi* o disposto nos artigos 53º do TUE e 356º do TFUE.

[54] Verifica-se, todavia, algumas situações derrogatórias em relação a Estados-membros, referentes a determinados domínios materiais, dentre eles a zona do euro, o espaço de Liberdade, Segurança e Justiça, o acervo Schengen e até mesmo a Carta dos Direitos Fundamentais da União Europeia. Ou seja, os Tratados não se aplicam de modo igual a todos os Estados-membros, o que significa que nem todas as normas dos Tratados se aplicam no território enunciado nos preceitos acima referidos. (MARTINS, 2017, p. 486).

[55] *Ex vi* o disposto nos artigos 52º do TUE e 355º do TFUE.

[56] Artigo 216.o 1. A União pode celebrar acordos com um ou mais países terceiros ou organizações internacionais quando os Tratados o prevejam ou quando a celebração de um acordo seja necessária para alcançar, no âmbito das políticas da União, um dos objetivos estabelecidos pelos Tratados ou quando tal celebração esteja prevista num ato juridicamente vinculativo da União ou seja suscetível de afetar normas comuns ou alterar o seu alcance. 2. Os acordos celebrados pela União vinculam as instituições da União e os Estados-Membros.

2.1.1.1 Os Tratados Institutivos

A União Europeia é uma comunidade baseada na lei e que, através dela, segue no encalço de seus objetivos. O Direito da União, base do sistema institucional, rege a convivência econômica e os direitos sociais dos povos dos Estados-Membros.

> Só o Direito da União pode dar vida e cumprir a 'Constituição' da UE que acabamos de descrever, em particular, os seus valores fundamentais. Por esta razão, a UE é de dois pontos de vista um fenômeno de direito: é uma criação da lei e uma comunidade baseada na lei. Esta é a novidade decisiva em relação às tentativas anteriores para a unificação da Europa nos meios utilizados para tanto, que agora não são mais a violência e a submissão, mas a força da lei. O Direito deve criar o que sangue e armas não conseguiram em séculos, já que apenas uma unidade que repouse em uma decisão livre tem chance de durar. Uma União baseada em valores fundamentais, como liberdade e igualdade, e que seja preservada e realizada por meio da direita. Esta é a base subjacente aos Tratados fundadores, como atos criadores da União Europeia.[57] (tradução livre)

[57] *Solamente el Derecho de la Unión puede dar vida y realizar la «Constitución» de la UE que acabamos de describir, en particular sus valores fundamentales. Por esa razón, la UE es desde dos puntos de vista un fenómeno del Derecho: es una creación del Derecho y una comunidad basada en el Derecho. Esta es la novedad decisiva que la caracteriza respecto a los intentos anteriores de lograr la unidad de Europa: los medios utilizados no son la violencia y la sumisión, sino la fuerza del Derecho. El Derecho debe crear lo que la sangre y las armas no lograron en siglos, ya que solo una unidad que repose en una decisión libre tiene posibilidades de perdurar. Una Unión que se base en los valores fundamentales, como la libertad y la igualdad, y que sea preservada y realizada a través del Derecho. Esta es la base subyacente a los Tratados constitutivos, como actos creadores de la Unión Europea. (...) Sin embargo, la UE no es tan solo una creación del Derecho, sino que también persigue sus objetivos utilizando exclusivamente el Derecho. Es una comunidade basada en el Derecho. No es la fuerza del poder la que rige la convivencia económica y social de los pueblos de los Estados miembros, sino el Derecho de la Unión. El Derecho de la Unión es la base del sistema institucional. Establece los procedimientos para la adopción de decisiones de las instituciones de la Unión y regula las relaciones entre ellas. Pone en sus manos una serie de instrumentos jurídicos en forma de reglamentos, directivas y decisiones que permiten adoptar actos jurídicos con efectos vinculantes para los Estados miembros y sus ciudadanos. De esta forma, también el individuo se convierte en soporte de la Unión. El ordenamiento jurídico de esta influye en su vida cotidiana de forma cada vez más directa. Le concede derechos y le impone obligaciones, de forma que el individuo, ciudadano de su país y de la Unión, está sometido a ordenamentos jurídicos de diferentes niveles, como los que observamos en las constituciones de los Estados federales. Al igual que cualquier ordenamiento jurídico, el de la UE dispone de un sistema completo de tutela jurídica para resolver los litigios em torno al Derecho de la Unión y para velar por su cumplimiento. El Derecho de la Unión determina igualmente la relación entre la UE y los Estados miembros; estos últimos deben adoptar todas las medidas apropiadas para cumplir las obligaciones derivadas de los Tratados o de los actos de las instituciones de la Unión. Les corresponde ayudar a la Unión a llevar a la práctica su misión y abstenerse de todo lo que pueda poner en peligro la realización de los objetivos de los Tratados. Los Estados miembros son responsables ante los ciudadanos de la Unión de todos los perjuicios provocados por las infracciones del Derecho de la Unión.* Ou seja: No entanto, a UE não é apenas uma criação da lei, mas também persegue os seus objetivos utilizando exclusivamente a lei. É uma comunidade com base na lei. Não é a força do poder que rege a convivência econômica e direitos sociais dos povos dos Estados membros, mas sim o Direito da União. O direito da União é a base do sistema institucional. Estabelece os procedimentos de tomada de decisão das instituições da União e regula as relações entre elas. Coloca em suas mãos uma série de instrumentos legais na forma de regulamentos, diretivas e decisões que permitem a adoção de atos jurídicos com efeito vinculantes para os Estados-Membros e os seus cidadãos. Dessa forma, o indivíduo também se torna um apoiador da União. O ordenamento jurídico

Assim, o Tratado da União Europeia[58] e o Tratado sobre o Funcionamento da União Europeia fundamentam a criação da União Europeia[59] e juntos inauguram a disciplina sobre a proteção de dados em nível de direito primário, eis que não se verifica precedentes de forma explícita sobre o tema em tratados anteriores. O tema vem disposto no artigo 39º do TUE[60] e no artigo 16º do TFUE[61].

Com relação ao artigo 39 Tratado da União Europeia, cabe consignar que

> Este artigo é uma inovação, não tendo um preceito correspondente em anteriores versões dos Tratados. O mandato de 26 de junho de 2007 para a Conferência Inter-Governamental continha uma referência à necessidade de se adotar uma base jurídica específica para a proteção de dados pelos EM.
> O artigo 39º constitui uma base jurídica especial, relativamente à base jurídica geral consagrada no artigo 16º do TFUE. Em derrogação do nº 2

influencia em sua vida diária de forma cada vez mais direta. Isso lhe concede direitos e impõe obrigações, de forma que o indivíduo, cidadão de seu país e da União, está sujeito às ordenamentos jurídicos de diferentes níveis, como os que observamos nas constituições dos estados federais. Como em qualquer ordenamento jurídico, a UE dispõe de um sistema completo de tutela jurídica para resolver litígios em torno do Direito da União e garantir o seu cumprimento. O direito da União também determina a relação entre a UE e os Estados-Membros; estes devem tomar todas as medidas necessárias para cumprir as obrigações decorrentes dos Tratados ou dos atos das instituições da União. É sua responsabilidade ajudar a União a cumprir sua missão e abster-se de tudo o que possa comprometer a realização dos objectivos dos Tratados. Os Estados-Membros são responsáveis ante os cidadãos da União por todos os prejuízos decorrentes das infrações ao Direito da União (tradução livre).(BORCHARDT, 2011, p. 85-86)

[58] TÍTULO I Disposições Comuns ARTIGO 1.º Pelo presente Tratado, as ALTAS PARTES CONTRATANTES instituem entre si uma UNIÃO EUROPEIA, adiante designada por "União", à qual os Estados-Membros atribuem competências para atingirem os seus objectivos comuns. O presente Tratado assinala uma nova etapa no processo de criação de uma união cada vez mais estreita entre os povos da Europa, em que as decisões serão tomadas de uma forma tão aberta quanto possível e ao nível mais próximo possível dos cidadãos. A União funda-se no presente Tratado e no Tratado sobre o Funcionamento da União Europeia (a seguir designados "os Tratados"). Estes dois Tratados têm o mesmo valor jurídico. A União substitui-se e sucede à Comunidade Europeia. Tratado da União Europeia, que instituiu a União Europeia. Disponível em: https://www.parlamento.pt/europa/Documents/Tratado_Versao_Consolidada.pdf. Acesso em 20/03/2021.

[59] O Tratado da União Europeia foi assinado em Mastrischt, em 07 de fevereiro de 1992, entrando em vigor em 1993. Daí também ser conhecido como Tratado de Maastricht.

[60] ARTIGO 39.º Em conformidade com o artigo 16.º do Tratado sobre o Funcionamento da União Europeia e em derrogação do n.º 2 do mesmo artigo, o Conselho adopta uma decisão que estabeleça as normas relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de actividades relativas à aplicação do presente capítulo, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. Tratado da União Europeia (Versão Consolidada). Disponível em: https://www.parlamento.pt/europa/Documents/Tratado_Versao_Consolidada.pdf. Acesso em 21/03/2021.

[61] Artigo 16.o (ex-artigo 286.o TCE) 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.o do Tratado da União Europeia. Tratado sobre o Funcionamento da União Europeia (Versão Consolidada). Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF. Acesso em 03/04/2021.

> deste último preceito, ou seja, em derrogação do processo legislativo ordinário, o Conselho adotará, por unanimidade, uma decisão que estabeleça as normas relativas à proteção de pessoas singulares no que diz respeito ao tratamento dos dados pessoais pelos EM, no âmbito da PESC. O artigo 39º refere-se apenas ao tratamento de dados pessoais pelos EM: todos os outros tratamentos de dados pessoais efetuados pelas Instituições da União, inclusivamente os que se situam na área da PESC, cabem na previsão do artigo 16º do TFUE.
> O artigo 39º remete para o princípio geral do artigo 16º, nº 1, do TFUE, relativo à proteção de dados pessoais de caráter pessoal, aliás configurado como um verdadeiro direito subjetivo. O artigo 8º da CDFUE proclama formalmente este direito, especificando ainda um direito de acesso aos dados pessoais e um direito à retificação de dados incorretos. O nº 3 do artigo 8º refere, à semelhança do artigo 16 do TUE e do artigo nº 16 do TFUE, o controle por uma autoridade independente de supervisão.
> No momento atual, a proteção de dados pessoais possui uma disciplina própria quanto às áreas correspondentes ao ex-primeiro pilar e ao ex-terceiro pilar. No primeiro caso, trata-se essencialmente da Diretiva 95/46/CE, adotada com base no ex-artigo 95 do TCE e, no segundo caso, trata-se essencialmente da Decisão Quadro do Conselho 2008/977/JAI, de 27 de novembro de 2008 (...)[62]

Digno de nota é que a citação acima transcrita foi lavrada antes da edição da nova legislação europeia sobre a proteção de dados, inserida no ordenamento jurídico União Europeia em 2018. A Diretiva 95 e a Decisão Quadro 977 foram substituídas, respectivamente, pelo Regulamento 2016/679/CE e pela Diretiva 2016/680/EU, verdadeira evolução de tais instrumentos normativos.

Quanto ao artigo 16 do Tratado sobre o Funcionamento da União Europeia, cabe lançar algumas considerações, tendo em vista que

> O regime europeu de proteção de dados pessoais, considerado um dos mais avançados a nível mundial, veio a ser consideravelmente reforçado com a consagração do artigo 16º no TFUE. Este artigo estabelece pela primeira vez uma base jurídica expressamente aplicável ao "tratamento de dados pessoais (...) pelos EM". Tal constitui um progresso relativamente ao regime constante do TCE, em que apenas o seu artigo 286º se ocupava expressamente da matéria, para determinar a aplicabilidade aos tratamentos efetuados pelas instituições, órgãos e organismos da União" dos atos comunitários relativos aos tratamentos de dados de caráter pessoal e à sua livre circulação.

[62] SOARES, Miguel de Serpa. Tratado de Lisboa Anotado e Comentado. Almedina: Coimbra, janeiro/2012. Disponível em: https://www.amazon.com.br/Tratado-Lisboa-Manuel-Lopes-Porto/dp/9724046133/ref=asc_df_9724046133/?tag=googleshopp00-20&linkCode=df0&hvadid=379815867332&hvpos=&hvnetw=g&hvrand=11120421614727122636&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1001541&hvtargid=pla-986299319217&psc=1. Acesso em 20/03/2021.

> Quanto aos tratamentos efetuados pelos Estados Membros, o direito derivado prévio ao TFUE foi adotado, no âmbito do regime da harmonização da legislação do mercado interno, com base no artigo 95º do TCE.
> A proteção de dados pessoais transcende muito a mera dimensão econômica do mercado interno. Hoje em dia, a base jurídica do direito derivado nesta matéria – o artigo 16º do TFUE – encontra-se integrada na Parte I, intitulada Os Princípios, sob o Titulo II, que consagra as Disposições de Aplicação Geral, do TFUE, estabelecendo um verdadeiro regime geral de proteção de dados aplicável à totalidade da ação da UE, com exceção da PESC, campo em que se aplica o artigo 39º do TUE. Foi também consagrado um direito autônomo à proteção de dados no artigo 8º da CDFUE, que, como é sabido, em virtude do artigo 6º do TUE, passou a ter força vinculativa idêntica à dos tratados.[63]

2.1.1.2 A Carta dos Direitos Fundamentais da União Europeia

A Comunidade Econômica Europeia surgiu como uma organização regional visando buscar a integração econômica regional e a criação de um mercado comum, razão pela qual os tratados originais das comunidades europeias não traziam qualquer menção aos direitos humanos ou a sua proteção. Assim, diferentemente do Conselho da Europa, os tratados da União Europeia, originalmente, não incluíam disposições expressas em matéria de direitos fundamentais.

> No entanto, o TJUE fez interpretações importantes dos Tratados em decisões proferidas nos casos que julgou em relação a alegadas violações dos direitos humanos em matérias reguladas pelo direito da UE. Para conceder proteção às pessoas, os direitos fundamentais foram incorporados aos chamados princípios gerais do direito europeu. De acordo com o TJUE, estes princípios gerais refletem o conteúdo da proteção dos direitos humanos que incluem constituições nacionais e tratados de direitos humanos, em particular, o CEDH. O TJUE declarou que garantiria o cumprimento da legislação da UE com estes princípios.[64] (tradução livre)

---

[63] GALVÃO, Luís Neto. Tratado de Lisboa Anotado e Comentado. Almedina: Coimbra, janeiro/2012. Disponível em: https://www.amazon.com.br/Tratado-Lisboa-Manuel-Lopes-Porto/dp/9724046133/ref=asc_df_9724046133/?tag=googleshopp00-20&linkCode=df0&hvadid=379815867332&hvpos=&hvnetw=g&hvrand=3811724672327266600&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1001541&hvtargid=pla-986299319217&psc=1. Acesso em 20/03/2021.

[64] *Sin embargo, el TJUE realizó importantes interpretaciones de los Tratados a raíz de los asuntos que juzgó en relación con presuntas violaciones de los derechos humanos en materias reguladas por la legislación de la UE. Para conceder protección a las personas físicas, se incorporaron los derechos fundamentales a los denominados principios generales del Derecho europeo. Según el TJUE, estos principios generales reflejan el contenido de la protección de los derechos humanos que recogen las constituciones nacionales y los tratados de derechos humanos, en particular, el CEDH. El TJUE declaró que velaría por el cumplimiento del Derecho de la UE con estos principios.* CONSELHO EUROPEU. *Manual de Legislación Europea en Materia de Protección de Datos.* Edición de 2018, p. 29-30. *Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa.* Luxemburgo: *Oficina de Publicaciones de la Unión Europea, 2019.* Disponível em:

Ante a repercução de suas políticas na proteção dos direitos humanos e buscando maior proximidade com os cidadãos, a União Europeia editou, no ano 2000, a Carta de Direitos Fundamentais da União Europeia[65]. Inicialmente tida como um documento político, com o tempo passou a ser juridicamente vinculante como direito primário da União Europeia[66], graças a entrada em vigor do Tratado de Lisboa, em 2009.

No capítulo que trata das liberdades, a Carta dispõe, dentre outros, sobre a proteção à vida privada e familiar (artigo 7º). Logo em seguida, estabelece o direito à proteção de dados pessoais (artigo 8º), erigindo, assim, o nível de tal proteção ao de um direito fundamental no direito da União Europeia[67], a ser observado pelos Estados-membros, instituições e órgãos da União Europeia[68].

---

https://op.europa.eu/pt/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 Acesso em 17/03/2021.

[65] A Carta, dirigida aos organismos e instituições da União Europeia, vinculados à observância dos direitos nela estabelecidos no exercício de suas funções, bem como aos Estados Membros, no que diz respeito a aplicação do direito da União Europeia, constitui a síntese das tradições constitucionais e obrigações internacionais comuns aos Estados Membros. Os direitos descritos na Carta são organizados em 6 capítulos, intitulados Dignidade, Liberdade, Igualdade, Solidariedade, Cidadania e Justiça, abarcando, assim, todos os direitos civis, políticos, econômicos e sociais dos cidadãos europeus.

[66] Artigo 6.o (ex-artigo 6.o TUE) 1. A União reconhece os direitos, as liberdades e os princípios enunciados na Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, com as adaptações que lhe foram introduzidas em 12 de dezembro de 2007, em Estrasburgo, e que tem o mesmo valor jurídico que os Tratados. De forma alguma o disposto na Carta pode alargar as competências da União, tal como definidas nos Tratados. Os direitos, as liberdades e os princípios consagrados na Carta devem ser interpretados de acordo com as disposições gerais constantes do Título VII da Carta que regem a sua interpretação e aplicação e tendo na devida conta as anotações a que a Carta faz referência, que indicam as fontes dessas disposições. 2. (...) Tratado da União Europeia. Disponível em https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF. Acesso em 22/03/2021.

[67] Título II Das Liberdades Artigo 6º (...) Artigo 7º Respeito pela vida privada e familiar. Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. Artigo 8º Proteção de dados pessoais. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. Carta dos Direitos Fundamentais da União Europeia. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso em 22/03/2021.

[68] Artigo 51º Âmbito de aplicação 1. As disposições da presente Carta têm por destinatários as instituições, órgãos e organismos da União, na observância do princípio da subsidiariedade, bem como os Estados-Membros, apenas quando apliquem o direito da União. Assim sendo, devem respeitar os direitos, observar os princípios e promover a sua aplicação, de acordo com as respetivas competências e observando os limites das competências conferidas à União pelos Tratados. 2. A presente Carta não torna o âmbito de aplicação do direito da União extensivo a competências que não sejam as da União, não cria quaisquer novas atribuições ou competências para a União, nem modifica as atribuições e competências definidas pelos Tratados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso em 22/03/2021.

Elaborada anos após a Diretiva de Proteção de Dados[69], a Carta incorpora, em seu artigo 8º, a legislação já existente na União Europeia sobre a matéria vez que, além de apontar textualmente o direito à proteção de dados, também enuncia os princípios básicos de proteção de dados cuja aplicação estará subordinada ao controle de uma autoridade independente.

Assim, incontestável é que

> A adoção do Tratado de Lisboa é um marco na evolução das leis sobre proteção de dados, não só porque dá à Carta o status de um documento juridicamente vinculativo, ao nível do direito primário, mas também porque estabelece o direito à protecção dos dados pessoais. Este direito é especificamente referido no artigo 16º do TFUE, na parte dedicada aos princípios gerais da UE. O artigo 16 também cria uma nova base jurídica, pela qual é concedida à UE o poder de legislar sobre protecção de dados. Isto é um avanço importante, porque os regulamentos de proteção de dados da UE - em particular, o Diretiva de proteção de dados - baseava-se, em princípio, na base jurídica do mercado interno e a necessidade de harmonizar as legislações nacionais para não limitar o fluxo livre de dados na União Europeia. Artigo 16 do TFUE agora estabelece uma base jurídica independente para uma formulação moderna e proteção abrangente de dados, cobrindo todas as questões da competência da UE, incluindo a cooperação policial e judiciária em matéria penal. O referido artigo do TFUE também afirma que o cumprimento das normas para a proteção de dados adotados de acordo com ela devem estar sujeitos ao controle das autoridades de supervisão independente. O artigo 16 serviu de base jurídica para a adoção da reforma abrangente dos regulamentos de proteção de dados em 2016, ou seja, do Regulamento geral de proteção de dados e a Diretiva sobre a proteção de dados para autoridades policiais e de justiça criminal[70] (...) (tradução livre).

---

[69] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados.

[70] *La adopción del Tratado de Lisboa es un hito en la evolución de las leyes sobre protección de datos, no solo porque confiere a la carta el estatuto de documento jurídico vinculante, al nivel del Derecho primario, sino también porque establece el derecho a la protección de los datos personales. Este derecho está específicamente contemplado en el artículo 16 del TFUE, en la parte dedicada a los principios generales de la UE. El artículo 16 también crea una nueva base jurídica, por la que se otorga a la UE la facultad de legislar en materia de protección de datos. Este es un avance importante, porque la normativa de protección de datos de la UE —en particular, la Directiva sobre protección de datos— se basó en principio en el fundamento jurídico del mercado interior y en la necesidad de armonizar las legislaciones nacionales para no limitar la libre circulación de datos en la Unión Europea. El artículo 16 del TFUE establece ahora una base jurídica independiente para una formulación moderna (27) UE (2012), Carta de los Derechos Fundamentales de la Unión Europea, DO 2012 C 326. (28) Véanse Comunidades Europeas (2012), versiones consolidadas del Tratado de la Unión Europea (TUE), y del Tratado de Funcionamiento de la Unión Europea (TFUE), DO 2012 C 326. 33 Contexto y antecedentes de la legislación europea en materia de protección de datos e integral de la protección de datos, que comprenda todas las materias de competencia de la UE, incluida la cooperación policial y judicial en materia penal. Dicho artículo del TFUE también afirma que el cumplimiento de la normativa de protección de datos adoptada en virtud del mismo debe estar sujeta al control de autoridades de supervisión independientes. El artículo 16 sirvió de base jurídica para la adopción de la reforma integral de la normativa de protección de datos en 2016, es decir, del Reglamento general de protección de datos y de la Directiva sobre protección de datos para las autoridades policiales y de justicia penal (...)* CONSELHO EUROPEU. *Manual de Legislación Europea en Materia de Protección de Datos. Edición de 2018,* p. 32-33. *Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa.* Luxemburgo: *Oficina de*

2.1.2 Direito Derivado

No que respeita ao Direito Derivado[71], ao abrigo da competência que lhes foi atribuída pelos Tratados, as instituições da União Europeia adotam regulamentos, diretivas, decisões, recomendações e pareceres[72].

Os Regulamentos tem caráter geral, abstrato e obrigatório em todos os seus elementos (diferente de outros atos obrigatórios somente quanto a alguns elementos, como as diretivas, e de outros atos não vinculativos, como recomendações e pareceres). São diretamente aplicáveis, estando apto a conferir direitos e impor obrigações aos Estados-membros, aos seus órgãos e aos particulares, à semelhança da lei nacional. Colocam-se como se fosse direito nacional, não necessitando da interposição do poder normativo nacional. É o instrumento normativo da União que mais se assemelha à lei, a nível interno.

Diretivas são normas adotadas pela Comissão e pelo Parlamento Europeu que vinculam os Estado-membros destinatários quanto ao resultado a alcançar, cabendo às instâncias nacionais disciplinar a forma e os meios para alcançar tal objetivo[73]. Diferentemente dos regulamentos, que são diretamente aplicáveis na ordem jurídica interna dos países da União Europeia após a sua entrada em vigor, a diretiva deve ser objeto de transposição para o direito

---

Publicaciones de la Unión Europea, 2019. Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 Acesso em 02/04/2021.

[71] Artigo 289º. 1. O processo legislativo ordinário consiste na adoção de um regulamento, de uma diretiva ou de uma decisão conjuntamente pelo Parlamento Europeu e pelo Conselho, sob proposta da Comissão. Este processo é definido no artigo 294º. 2. Nos casos específicos previstos pelos Tratados, a adoção de um regulamento, de uma diretiva ou de uma decisão pelo Parlamento Europeu, com a participação do Conselho, ou por este, com a participação do Parlamento Europeu, constitui um processo legislativo especial. 3. Os atos jurídicos adotados por processo legislativo constituem atos legislativos. 4. Nos casos específicos previstos pelos Tratados, os atos legislativos podem ser adotados por iniciativa de um grupo de Estados-Membros ou do Parlamento Europeu, por recomendação do Banco Central Europeu ou a pedido do Tribunal de Justiça ou do Banco Europeu de Investimento.

[72] Dispõe o Tratado sobre o Funcionamento da União Europeia, no artigo 288: Para exercerem as competências da União, as instituições adoptam regulamentos, directivas, decisões, recomendações e pareceres. O regulamento tem carácter geral. É obrigatório em todos os seus elementos e directamente aplicável em todos os Estados-Membros. A directiva vincula o Estado-Membro destinatário quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios. A decisão é obrigatória em todos os seus elementos. Quando designa destinatários, só é obrigatória para estes. As recomendações e os pareceres não são vinculativos.

[73] Antes da década de 90, havia uma tendência em se redigir as Diretivas de modo tão mais preciso e determinar cada vez mais minuciosamente as modalidades da matéria nelas tratada que a escolha dos meios pelos Estados acabava por ser bastante restringida ou nem existir, limitando-os a mera transposição da Diretiva para seu âmbito interno. Tal situação que foi solucionada com a introdução do princípio da subsidiariedade pelo Tratado de Maastrischt.

nacional.[74] É dever dos Estados-membros transpor a diretiva para o direito interno, cabendo-lhes a escolha do tipo do ato legislativo destinado a implementá-la, de acordo com cada sistema jurídico nacional. As diretivas são destinadas aos Estados-membros: para serem aplicadas aos particulares, necessitam ser transpostas para o direito interno. Assim, é a norma interna e não a norma da União que será aplicada aos particulares. A não realização do processo de transposição de uma diretiva ou sua transposição tardia impede ou retarda o exercício de direitos pelos indivíduos residentes naquele Estado-membro, que "ficariam desprotegidos e em desigualdade de circunstâncias com os nacionais de outros Estados-membros, por força de um incumprimento imputável ao Estado, com o qual tem alguma conexão, (nacionalidade, residência, etc.), sem que nada pudessem fazer."[75]

As decisões também são diretamente aplicáveis e obrigatórias, em todos os seus elementos; porém, somente para as partes específicas envolvidas, sejam elas Estados-membros, indivíduos ou empresas (diferentemente das diretivas, que tem um texto com aplicação geral em todos os países da União Europeia). Após o Tratado de Lisboa, podem consubstanciar-se num ato legislativo ou não[76].

As recomendações e pareceres são atos não vinculativos e podem ser emitidos por diversas instituições europeias, anunciando posições sobre determinadas questões ou orientando comportamentos a serem adotados ou evitados, cujos destinatários são os Estados-membros e os particulares determinados ou indeterminados. Resultam da função orientadora dos órgãos da União, a eles atribuída pelos Tratados.

---

[74] A diretiva é adotada na sequência de um processo legislativo. Trata-se de um ato legislativo adotado pelo Conselho e pelo Parlamento no quadro de processos legislativos ordinários ou especiais. Assim, para que uma diretiva produza efeitos a nível nacional, os países da UE têm de adotar uma lei com vista à sua transposição. Esta medida nacional deve prosseguir os objetivos definidos pela diretiva. As autoridades nacionais devem comunicar estas medidas à Comissão Europeia. Os países da UE dispõem de margem de manobra neste processo de transposição. Esta margem permite-lhes ter em conta as especificidades nacionais. A transposição tem de ser efetuada no prazo fixado aquando da adoção da diretiva (regra geral, no prazo de dois anos). Caso um país não proceda à transposição de uma diretiva, a Comissão pode dar início a um processo por infração e intentar uma ação contra o país em causa junto do Tribunal de Justiça da UE (a não execução do acórdão poderá, nesta ocasião, conduzir a uma nova condenação, que por sua vez poderá resultar na aplicação de sanções pecuniárias). República Portuguesa. Direção-Geral das Atividades Econômicas. Disponível em: https://www.dgae.gov.pt/servicos/assuntos-europeus/transposicao-de-diretivas.aspx#:~:text=Transposi%C3%A7%C3%A3o%20de%20Diretivas&text=O%20artigo%20288%C2%BA%20do%20Tratado,%C3%A0%20forma%20e%20aos%20meios Acesso em 21/03/2021.

[75] (...) para impedir esta situação, o TJ considerou que, verificados certos requisitos, as normas das diretivas podem produzir efeitos em relação aos indivíduos, mesmo antes da sua transposição. O efeito direto resulta, portanto, da necessidade de proteger os cidadãos contra a inércia do Estado. (MARTINS, 2017, p. 500).

[76] Da decisão, tal como está prevista no artigo 288º do TFUE, há que distinguir outro tipo de decisões, que se destinavam a completar os Tratados, como foi ocaso da Decisão do Conselho relativa à eleição do PE por sufrágio direto e universal e da Decisão de criação do Tribunal de Primeira Instância, hoje revogada, bem como as decisões com alcance meramente interno ou orgânico ou instruções internas. (MARTINS, 2017, p. 500).

Por fim, cabe mencionar também a existência de outros atos diversos daqueles contidos no artigo 288 do TFUE e que emanam das instituições e de outros órgãos da União, previstos em disposições avulsas dos Tratados ou até sem qualquer previsão, como é o caso das resoluções, conclusões, programas de ação, comunicações e códigos de conduta. Apesar de não terem força vinculativa do ponto de vista jurídico, na prática produzem efeitos jurídicos. Trata-se de um conjunto de atos provenientes tanto dos órgãos da União como dos Estados-membros que, mesmo não sendo obrigatórios, produzem alguns efeitos práticos e, muitas vezes, preparam o terreno para atos posteriores obrigatórios.

2.1.2.1 O Novo Regulamento Geral de Proteção de Dados – Regulamento 2016/679/CE e a extinta Diretiva de Proteção de Dados – Diretiva 95/46/CE

Por mais de 20 anos, a Diretiva 95/46/CE[77] do Parlamento Europeu e do Conselho foi o principal instrumento jurídico da União Europeia em matéria de proteção de dados.

A Diretiva de Proteção de Dados foi concebida numa época em que diversos Estados Membros já tinham suas próprias leis de proteção de dados[78]. Pretendia-se, com a edição de dita diretiva, harmonizar as legislações nacionais para garantir a livre circulação de dados entre os diferentes Estados-Membros, necessária para a livre circulação de bens e serviços, capitais e pessoas no mercado interno e que só poderia ser alcançada se os Estados-Membros pudessem contar com um nível elevado e uniforme de proteção de dados.

> A Diretiva de Proteção de Dados refletiu os princípios de proteção de dados já contidos nas leis nacionais e na Convenção 108, embora em muitos casos ela os tenha ampliado. Aproveitou a possibilidade prevista no artigo 11 da

[77] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados (Diretiva de Proteção de Dados).

[78] *El estado alemán de Hesse adoptó la primera ley del mundo sobre protección de datos en 1970, que solo era de aplicación en ese estado. Suecia adoptó la Datalagen en 1973; Alemania la Bundesdatenschutzgestez en 1976; y Francia la Loi relative à l'informatique, aux fichiers et aux libertés en 1977. En el Reino Unido, la Data Protection Act se adoptó en 1984. Por último, los Países Bajos adoptaron los Wet Persoonregistraties en 1989.* Ou seja: Em 1970, o estado alemão de Hesse adotou a primeira lei mundial sobre proteção de dados, que, todavia, só se aplicava nesse estado. A Suécia adotou o *Datalagen*, em 1973; a Alemanha, o *Bundesdatenschutzgestez*, em 1976; e a França, a *Loi relative à l'informatique, aux fichiers et aux libertés*, em 1977. No Reino Unido, a Lei de Proteção de Dados foi adotada em 1984. Finalmente, os Países Baixos adotaram o *Wet Persoonregistraties*, em 1989. (tradução livre). CONSELHO EUROPEU. *Manual de Legislación Europea en Materia de Protección de Datos. Edición de 2018,* p. 33, em nota de rodapé. *Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa.* Luxemburgo: *Oficina de Publicaciones de la Unión Europea, 2019.* Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 Acesso em 29/03/2021.

> Convenção 108, de acrescentar instrumentos de proteção. Em particular, a introdução na Diretiva do controle independente como um instrumento para melhorar o cumprimento das normas de proteção de dados provou ser uma importante entrada para o funcionamento eficaz da legislação europeia em matéria de proteção de dados. Consequentemente, essa característica foi incorporada ao Direito do CoE em 2001, por meio do Protocolo Adicional à Convenção 108. É uma ilustração da estreita interação e da influência positiva de ambos os instrumentos ao longo do anos.[79] (tradução livre)

A Diretiva 95/46/CE instaurou um regime abrangente e detalhado de proteção de dados no âmbito da União Europeia, sujeitando os legisladores dos Estados-membros a aprovar normas de acordo com seu conteúdo normativo. Todavia, importa observar que tal espécie normativa[80], existente no regime jurídico da União Europeia, necessita ser transposta para ingressar no ordenamento jurídico dos Estados-Membros, o que confere ao legislador nacional de cada Estado Membro uma certa 'margem de discricionariedade' ao realizar tal processo (de transposição). Assim, por não serem as diretivas diretamente aplicáveis, o que se verificou pragmaticamente foi a adoção de diferentes interpretações, definições e regras sobre a proteção de dados em cada uma das legislações nacionais, em toda a União Europeia, fator de grande relevância a ser observado no contexto da época. Ainda, diferentes níveis de controle de sua aplicação e da severidade das sanções também foram utilizados nos diversos Estados-Membros, dificultando, assim, a concretização de seu objetivo inicial de alcançar a harmonização e nível de proteção totais.

Tais circunstâncias, aliadas às novas tecnologias de informação em frenética evolução desde a redação da Diretiva, ocorrida em meados de 1990, deixaram clara a importância de se proceder a uma reforma da legislação da União Europeia em matéria de proteção de dados que, após anos de intensas discussões, resultou na edição do Regulamento 2016/679/CE – Regulamento Geral de Proteção de Dados[81].

---

[79] *La Directiva sobre protección de datos reflejaba los principios de protección de datos que ya contenían las leyes nacionales y el Convenio 108, aunque en muchos casos los ampliaba. Aprovechaba la posibilidad, contemplada en el artículo 11 del Convenio 108, de añadir instrumentos de protección. En particular, la introducción en la Directiva del control independiente como instrumento de mejora del cumplimiento de las normas de protección de datos demostró ser una importante aportación al funcionamiento efectivo de la legislación europea en materia de protección de datos. En consequencia, esta característica fue incorporada al Derecho del CdE en 2001 através del Protocolo adicional al Convenio 108. Esto es ilustrativo de la estrecha interacción y positiva influencia de ambos instrumentos entre sí a lo largo de los años.* CONSELHO EUROPEU. *Manual de Legislación Europea en Materia de Protección de Datos. Edición de 2018,* p. 33/34. *Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa.* Luxemburgo: *Oficina de Publicaciones de la Unión Europea, 2019.* Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 Acesso em 29/03/2021.

[80] Já tratado anteriormente no item 2.1.2 deste trabalho.

[81] (...) *Los debates sobre la necesidad de modernizar la normativa de protección de datos de la UE comenzaron en 2009, cuando la Comisión puso en marcha una consulta pública sobre el marco jurídico futuro para el derecho fundamental a la protección de los datos personales. La propuesta de Reglamento fue publicada por la*

Tem-se, a partir deste novo instrumento legislativo, uma atualização da legislação da União Europeia em matéria de proteção de dados, ajustando-a para proteger os direitos fundamentais na era digital.

O Novo Regulamento preserva e desenvolve princípios e direitos dos titulares de dados já contidos na Diretiva de Proteção de Dados, bem como inaugura novas regras que, dentre outros, obrigam aqueles que realizam tratamento de dados a aplicar as normas de proteção de dados desde o projeto e por padrão, a respeitar o direito à portabilidade dos dados e, ainda, a nomear um encarregado de proteção de dados em determinadas situações.

Uma vez que os regulamentos tem aplicação imediata, não necessitando de transposição nacional, a partir da edição do RGPD criou-se uma normativa de proteção de dados uniforme e coerente em todo o território da União Europeia, estabelecendo-se, assim, um ambiente de segurança jurídica.

Com a adoção do novel instrumento legal, imprescindível é a atualização da legislação nacional em vigor em matéria de proteção de dados em cada Estado-Membro, a fim de que se adequem ao contido no Regulamento para além de aplicar a margem de discricionariedade para a adoção das disposições específicas previstas no considerando 10 [82].

Comisión en enero de 2012, como inicio de un largo proceso legislativo de negociación entre el Parlamento Europeo y el Consejo de la UE. Tras su adopción, el Reglamento general de protección de datos contemplaba un periodo de transición de dos años. Su plena entrada en vigor se produjo el 25 de mayo de 2018, momento en que se derogó la Directiva sobre protección de datos. (...) As discussões sobre a necessidade de modernizar os regulamentos de proteção de dados da UE começaram em 2009, quando a Comissão lançou uma consulta pública sobre o futuro quadro jurídico do direito fundamental à proteção de dados pessoais. A proposta de regulamento foi publicada pela Comissão em janeiro de 2012, no início de um longo processo legislativo de negociação entre o Parlamento Europeu e o Conselho da UE. Após sua adoção, o Regulamento Geral de Proteção de Dados contemplou um período de transição de dois anos. A sua plena entrada em vigor é ocorreu em 25 de maio de 2018, momento em que a Diretiva de Proteção de Dados foi revogada. (tradução livre) CONSELHO EUROPEU. *Manual de Legislación Europea en Materia de Protección de Datos.* Edición de 2018, p. 34. *Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa.* Luxemburgo: *Oficina de Publicaciones de la Unión Europea, 2019.* Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 Acesso em 29/03/2021.

[82] Considerando 10: A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. No que diz respeito ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento. Em conjugação com a legislação geral e horizontal sobre proteção de dados que dá aplicação à Diretiva 95/46/CE, os Estados-Membros dispõem de várias leis setoriais em domínios que necessitam de disposições mais específicas. O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»). Nessa medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais. Regulamento

Arrojada inovação também trazida pelo Regulamento é no tocante às disposições sobre o âmbito territorial, eis que se aplica a empresas sediadas na União Europeia, bem como aos que tratam dados pessoais fora da União e que oferecem produtos ou serviços a titulares de dados na União Europeia ou, ainda, aos que apenas observem o seu comportamento. Considerando que muitas empresas internacionais de tecnologia têm participação significativa no mercado interno da União Europeia e lá, consequentemente, milhões de clientes, é imprescindível que tais empresas estejam sujeitas às normativas de proteção de dados da União Europeia, a fim de garantir a proteção de pessoas singulares e da concorrência em igualdade de condições.

2.1.2.2 A Diretiva sobre a Proteção de Dados na Seara Criminal – Diretiva 2018/680/UE e a extinta Decisão Quadro 2008/977/JAI

O Novo Regulamento Geral de Proteção de dados trouxe um regime de proteção ainda mais abrangente que o já contido na extinta Diretiva 95/46/CE, eis que a diretiva revogada se limitava tão somente às atividades realizadas no mercado interno e às atividades de autoridades públicas outras, que não as responsáveis pela aplicação da lei.

Visando atingir o equilíbrio necessário entre a proteção dos direitos dos titulares de dados e outros interesses igualmente legítimos, bem como para resolver problemas em setores específicos, tornou-se imprescindível a adoção de instrumentos legais especiais, como é o caso das normas que regulam o tratamento de dados pessoais pelos órgãos de segurança.

Adotada simultaneamente ao Regulamento Geral de Proteção de Dados (que estabelece disposições gerais para proteger as pessoas em relação ao tratamento de seus dados pessoais e garante a livre circulação desses dados na UE), a Diretiva sobre a Proteção de Dados para as Autoridades de Aplicação da Lei e da Justiça Criminal – Diretiva 2016/680/EU[83] revogou a Decisão-Quadro 2008/977/JAI[84], do Conselho da Europa, e estabeleceu um sistema

---

2016/679/CE. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em 30/03/2021.

[83] Directiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa a proteção de pessoas físicas no que diz respeito ao tratamento de dados pessoais por das autoridades competentes para fins de prevenção, investigação, detecção ou processo de ofensas criminais ou execução de sanções criminais, e para a livre circulação de tais dados.

[84] O primeiro instrumento jurídico da União Europeia a regulamentar esta matéria foi a Decisão-Quadro 2008/977/JAI do Conselho, sobre o tratamento de dados pessoais realizados no âmbito da cooperação policial e judiciária em matéria penal. Suas disposições aplicavam-se exclusivamente ao intercâmbio de dados policiais e

abrangente para a proteção de dados pessoais no âmbito da segurança pública, reconhecendo as particularidades do tratamento de dados nesta área e fixando disposições específicas, inclusive para a proteção de dados pessoais nas áreas de cooperação judicial em matéria penal e cooperação policial.[85]

Restou suprida, desta forma, a lacuna existente por ocasião da vigência da Decisão-Quadro 2008/977/JAI, eis que o âmbito de aplicação da Diretiva 2016/680 abrange o tratamento de dados pessoais a nível nacional pelas autoridades responsáveis pela aplicação da lei, não se limitando, tão somente, ao intercâmbio desses dados entre os Estados-Membros, como ocorria outrora.

A Diretiva 2016/680 reconhece e respeita o direito à proteção dos dados pessoais e os princípios fundamentais pelos quais o tratamento dos dados pessoais deve ser regido, bem como as disposições e princípios consagrados no Regulamento Geral de Proteção de Dados, ambicionando, assim, encontrar um equilíbrio entre os direitos das pessoas singulares e os objetivos legítimos do tratamento de dados na seara criminal. À título exemplificativo, cite-se, em relação à segurança das informações, a proteção de dados desde a concepção e por defeito e as notificações de violação de dados pessoais, que refletem direitos dos titulares e obrigações impostas àqueles que tratam dados, contidos no Regulamento Geral de Proteção de Dados.

Com relação às novas realidades trazidas pela tecnologia, a Diretiva 2016/680 também delas se ocupou, proibindo a utilização, pelos que tratam dados na área criminal, de certas técnicas que possam trazer efeitos demasiadamente graves às pessoas, como a criação de perfis, o uso de decisões automatizadas e, ainda, a utilização de dados sensíveis, determinando que tal tratamento de dados não deve levar à discriminação de qualquer indivíduo.

> Esta diretiva também contém disposições destinadas a garantir a prestação de contas pelos responsáveis pelo tratamento. Eles devem nomear um encarregado de proteção de dados responsável por monitorar o cumprimento dos regulamentos de proteção de dados, para informar e aconselhar a entidade e os colaboradores que realizam o tratamento sobre as suas obrigações e cooperar com a autoridade supervisora. O tratamento de dados pessoais no setor policial e de justiça criminal está sujeito, agora, ao controle de autoridades de supervisão independentes. Tanto o regime jurídico geral de proteção de dados quanto o regime especial de proteção de dados para as

judiciais entre os Estados-Membros, excluindo de seu ambito de aplicação o tratamento de dados pessoais realizados pelos órgãos de segurança a nível nacional.

[85] Assim, quando uma autoridade competente tratar dados pessoais para fins de prevenção, investigação, detecção ou repressão de infrações penais, será aplicável a Diretiva 2016/680. Quando um autoridade competente trata os dados pessoais para fins diferentes dos mencionados acima, o regime geral estabelecido pelo Regulamento Geral de Proteção de Dados.

> forças de segurança e a justiça penal, devem igualmente cumprir os requisitos estabelecidos na Carta dos Direitos Fundamentais da União Europeia.[86] (tradução livre)

A Diretiva (UE) 2016/680, portanto, visa equilibrar o direito à proteção de dados com a prevenção, investigação e/ou repressão de infrações penais na UE

[86] *Esta Directiva también contiene disposiciones destinadas a garantizar la rendición de cuentas de los responsables del tratamiento. Deben nombrar un delegado de protección de datos responsable de controlar el cumplimiento de las normas de protección de datos, de informar y asesorar a la entidad y los empleados que lleven a cabo el tratamiento acerca de sus obligaciones y de cooperar con la autoridad de control. El tratamiento de datos personales en el sector de la policía y la justicia penal está sujeto ahora al control de autoridades de supervisión independientes. Tanto el régimen jurídico general de protección de datos como el régimen especial de protección de datos para los cuerpos de seguridad y la justicia penal deben cumplir por igual con los requisitos previstos en la Carta de los Derechos Fundamentales de la Unión Europea.* CONSELHO EUROPEU. *Manual de Legislación Europea en Materia de Protección de Datos.* Edición de 2018, p. 37. *Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa*. Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2019. Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1. Acesso em 11/04/2021.

3. PECULIARIDADES DO REGIME DE PROTEÇÃO DE DADOS NA ESFERA CRIMINAL: ANÁLISE COMPARATIVA ENTRE ASPECTOS DA DIRETIVA 2016/680/UE E DO REGULAMENTO 2016/679/EU

3.1. BREVES CONSIDERAÇÕES. OBJETIVOS DA DIRETIVA 680

Tal como a Diretiva 95/46/CE[87] que, no passado, com fundamento no artigo 16 do Tratado sobre o Funcionamento da União Europeia[88], foi a primeira legislação substantiva a regular a matéria da proteção de dados na União Europeia, a Decisão Quadro 2008/977/JAI[89] dispunha sobre a proteção de dados pessoais tratados no âmbito criminal. Aliada à uma série de outros instrumentos legais também aplicáveis à matéria, a União Europeia ostentava uma legislação fragmentada e, não raro, confusa sobre qual o instrumento legal adequado a aplicar em cada caso concreto.

Em 2016, a Diretiva 95/46/CE foi substituída pelo Regulamento 2016/679/UE – *General Data Protection Regulation* (GDPR)[90], que excluiu expressamente de seu âmbito de aplicação (artigo 2º, 2, *d*) o tratamento de dados efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública[91].

---

[87] Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046 Acesso em 22/06/2021.

[88] Artigo 16.o (ex-artigo 286.o TCE) 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.o do Tratado da União Europeia. Tratado sobre o Funcionamento da União Europeia. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF Acesso em 17/05/2021.

[89] Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal. Disponível em: https://www.google.com/search?q=decis%C3%A3o+quadro+2008%2F977%2Fjai%22+pdf&rlz=1C1GCEU_pt-BRBR914BR914&oq=&aqs=chrome.1.69i59i450l8.6481549566j0j15&sourceid=chrome&ie=UTF-8 Acesso em 17/05/2021.

[90] Regulamento Geral sobre a Proteção de Dados. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-pt/format-PDFA1A Acesso em: 22/06/2021.

[91] Artigo 2.o Âmbito de aplicação material 1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados. 2. O presente regulamento não se aplica ao tratamento de dados pessoais: a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União: b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2,

Assim, inaugurando um novo ordenamento jurídico em matéria de proteção de dados, juntamente com o Regulamento 679, visando suprir mencionada lacuna deixada por este novel instrumento adotado para regular a proteção de dados em geral na União Europeia, foi publicada também a Diretiva 2016/680/EU – *Law Enforcement Directive* (LED)[92], destinada a regular o tratamento de dados na seara criminal, revogando expressamente a Decisão Quadro 2008/977/JAI, com efeitos a partir de 6 de maio de 2018 (artigo 59 da LED).

Evocando o artigo 8º, nº 1, da Carta dos Direitos Fundamentais da União Europeia[93], bem como o já referido artigo 16, nº 1, do Tratado sobre o Funcionamento da União Europeia, a Diretiva 2016/680/EU assinala que o direito à proteção de dados se trata de um direito fundamental e anuncia que todas as pessoas tem direito à proteção dos dados de caráter pessoal que lhes diga respeito (considerando 1). Ainda, que tal proteção se aplica independentemente da nacionalidade ou do local de residência destas pessoas, ao mesmo tempo em que pretende contribuir para a realização de um espaço de liberdade, segurança e justiça (considerando 2).

Assim como o Regulamento 2016/679/UE, do Parlamento Europeu e do Conselho, relativo a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, também a Diretiva 2016/680/UE, relativa às pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeito de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, visa proteger a pessoa no que diz respeito ao tratamento de dados pessoais, embora ambas as espécies normativas se apliquem em situações diversas.

Sobre o assunto, Emmanuel Salami Akintunde, em artigo onde discute o impacto da Diretiva 680 no tratamento de dados pessoais realizado pelas autoridades competentes na seara criminal e a livre circulação de tais dados, em relação ao regime de privacidade existente, apregoa que

---

do TUE; c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Diretiva 2016/680/UE. Disponível em: https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-_protecao_de_dados.pdf. Acesso em 18/05/2021.

[92] Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680. Acesso em 22/06/2021.

[93] Carta dos Direitos Fundamentais da União Europeia. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em 22/06/2021.

> Em 5 de maio de 2016, o parlamento da UE exerceu os seus poderes legislativos nos termos do artigo 16.º, n.º 2, do Tratado sobre o Funcionamento da União Europeia (TFUE), promulgando a Diretiva (UE) 2016/680 que revogará, a partir de sua vigência, revogar a Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal. A intenção do parlamento da UE era garantir que a UE adotasse uma abordagem abrangente para fins de proteção de dados, levando em consideração os avanços tecnológicos, para a regulamentação de todas as esferas da comunidade da UE, incluindo a aplicação da lei e a prevenção do crime. Portanto, a Diretiva (UE) 2016/680 visa equilibrar o direito à proteção de dados com a prevenção, investigação e/ou repressão de infrações penais na UE. (...) A essência desta legislação é, entre outras coisas, a livre circulação de dados na UE para efeitos do objetivo da presente Diretiva (UE) 2016/680[94] (tradução livre).

Ao contrário do Regulamento 2016/679/UE, que dispõe sobre o tratamento de dados em geral, os principais objetivos da Diretiva 2016/680/UE, por sua vez, residem no aumento do nível de proteção dos direitos fundamentais no domínio da polícia e da justiça criminal e na melhoria do compartilhamento de dados pessoais entre as autoridades competentes nos Estados-Membros, vez que poderão se apoiar em regras uniformes de proteção de dados [95].

Oportuno, também, colacionar as lições trazidas por Maria Belén Sanchez Domingo neste sentido, em publicação em que aborda a proteção de dados no âmbito da cooperação judiciária penal, em face a Diretiva 680, em que esta menciona que

---

[94] *On the 5th May 2016, the EU parliament exercised its legislative powers pursuant to Article 16(2) of the Treaty on the Functioning of the European Union (TFEU) by enacting the Directive (EU)/2016/680 which will, upon its applicability, repeal the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The intention of the EU parliament was to ensure that the EU adopts a comprehensive approach for the purpose of data protection, taking into cognizance the technological advancements, for the regulation of all spheres of the EU community including law enforcement and crime prevention. Therefore, the Directive (EU)/2016/680 intends to balance the right to data protection with the prevention, investigation and/or prosecution of criminal offences in the EU. (...) The essence of this legislation among other things is the free flow of data in the EU for the purpose of the objective of this Directive (EU) 2016/680.* AKINTUNDE, Salami Emmanuel. *The Impact of Directive (EU) 2016/680 on the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and on the Free Movement of Such Data on the Existing Privacy Regime.* Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2912449 Acesso em 20/06/2021.

[95] Artigo 1.o Objeto e objetivos 1. A presente diretiva estabelece as regras relativas 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, incluindo a salvaguarda e prevenção de ameaças à segurança pública. 2. Nos termos da presente diretiva, os Estados-Membros asseguram: a) A proteção dos direitos e das liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção dos dados pessoais; e b) Que o intercâmbio de dados pessoais entre autoridades competentes na União, caso seja previsto pelo direito da União ou do Estado-Membro, não seja limitado nem proibido por razões relacionadas com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais. 3. A presente diretiva não obsta a que os Estados-Membros prevejam garantias mais elevadas do que as nela estabelecidas para a proteção dos direitos e liberdades do titular dos dados no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes.

> A Diretiva, tal como definida na sua própria redação e no Considerando (6), substitui a Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008 ("DQ"), ambas as quais partilham características comuns, embora difiram em alguns outros aspectos. Os dois instrumentos têm a mesma estrutura; embora a Diretiva esteja articulada num vasto número de artigos (sessenta e cinco), sendo os considerandos igualmente mais amplos (cento e sete). Ao mesmo tempo, importa sublinhar que a Diretiva em questão segue o mesmo tom da Convenção 108, do Conselho da Europa, fruto da importante atividade desenvolvida pelo Conselho da Europa em matéria de proteção de dados pessoais. (...) Por sua vez, a Convenção visa harmonizar as legislações dos Estados-Membros em matéria de proteção de dados pessoais, convidando todos os Estados não membros do Conselho da Europa a aderirem. A Convenção continua a fazer parte da legislação europeia em matéria de proteção de dados pessoais, conforme determinado pela própria Diretiva no Considerando (68). (....) A própria Diretiva serve este objetivo, em consonância com o Considerando (2), pela prevenção a criminalidade e pela cooperação entre as autoridades judiciárias e policiais em matéria de proteção de dados pessoais. Assim, a Diretiva, por um lado, protege os direitos e liberdades fundamentais das pessoas naturais, em particular o direito à proteção dos dados pessoais. Por outro lado, procura garantir um elevado nível de segurança pública, facilitando o intercâmbio de dados pessoais entre as autoridades competentes para efeitos de prevenção, investigação e repressão da criminalidade, bem como para a aplicação de sanções penais. É um instrumento que promove a confiança entre as autoridades policiais e judiciárias dos diferentes Estados-Membros da União, no intercâmbio de informações entre as várias autoridades dos Estados-Membros no que diz respeito à proteção de dados pessoais, garantindo simultaneamente a segurança jurídica e pública[96] (tradução livre).

Também no mesmo sentido, em análise à Diretiva 680, Sajfert e Quintel, compartilham o entendimento de que

[96] *The Directive, as set out in its own wording and in Recital (6), replaces Council Framework Decision 2008/977/JHI of 27 of November 2008 ("FD"), both of which share common features, although they differ in some other respects. The two instruments have the same structure; although the Directive is articulated in an extensive number of Articles (sixty-five) the Recitals being equally broader (one hundred and seven). At the same time, it should be stressed that the Directive in question follows the same tone as Council of Europe Convention 108,[19] the result of the important activity carried out by the Council of Europe regarding the protection of personal data. (...) In turn, the Convention aims at harmonizing the laws of the Member States on the protection of personal data, inviting all non-Member States of the Council of Europe to accede to it. The Convention continues to form part of European legislation on the protection of personal data, as determined by the Directive itself in Recital (68).(...) The Directive itself serves this purpose, in line with Recital (2), by preventing crime and by cooperation between judicial and police authorities on the protection of personal data. Thus, the Directive, on the one hand, protects the fundamental rights and freedoms of natural persons, in particular, the right to protection of personal data. On the other hand, it seeks to ensure a high level of public security by facilitating the exchange of personal data between competent authorities for the purposes of the prevention, investigation and prosecution of crime, as well as for the enforcement of criminal penalties. It is an instrument that promotes trust between the police and judicial authorities of different Member States of the Union, in the exchange of information between the various authorities of the Member States with regards to the protection of personal data, while ensuring legal and public security.* Domingo, Maria Belén Sanchez (2019). *The protection of personal data in the field of judicial cooperation in criminal matters: special reference to Directive (EU) 2016/680 of the European Parliament and of the Council.* Unio - EU Law Journal. 5. 92-102. 10.21814/unio.5.2.2295.

> Tal como o Regulamento 679, a Diretiva 680 foi adotada em maio de 2016, constituindo um grande passo em frente no estabelecimento de um regime abrangente de proteção de dados da UE, como o primeiro instrumento horizontal e juridicamente vinculante que estabelece as regras para o tratamento nacional e transfronteiriço de dados pessoais na área da aplicação da lei. Além disso, a *Law Enforcement Directive* é um instrumento moderno, projetado para o tratamento de dados pessoais pelas autoridades de polícia e justiça criminal, na Era Digital. Como segunda parte do pacote de reforma da proteção de dados que estava em discussão há quatro anos, a Diretiva recebeu muito menos atenção do que o RGPD. No entanto, dois objetivos principais da Diretiva são demasiado importantes para serem negligenciados: o aumento do nível de proteção dos direitos fundamentais no domínio da polícia e da justiça criminal e a melhoria do compartilhamento de dados pessoais entre os Estados-Membros, uma vez que poderão se apoiar em regras uniformes de proteção de dados (Artigo 1.º, n.º 2). A Diretiva é a sucessora da Decisão-Quadro de 2008, que tinha um âmbito de aplicação muito mais limitado e se aplicava exclusivamente ao tratamento transfronteiriço de dados entre os Estados-Membros. As regras da Diretiva, que tiveram de ser transpostas para as legislações nacionais de todos os 28 Estados-Membros e dos quatro Estados do Espaço Schengen (Noruega, Islândia, Suíça e Lichtenstein) até maio de 2018, beneficiaram da atenção dada ao RGPD, uma vez que algumas das soluções do regulamento poderiam simplesmente ser copiadas. No entanto, várias disposições foram desenvolvidas especificamente para a Diretiva[97]. (tradução livre)

A *Law Enforcement Directive* pretendeu, também, consolidar as várias regras sobre o tratamento de dados realizado pelas autoridades de polícia e justiça criminal adotadas no âmbito do antigo terceiro pilar e as regras para as Agências de Justiça e Assuntos Internos da União Europeia sobre o tratamento de dados pessoais pelas autoridades policiais e de justiça criminal (artigo 62, 6, da Diretiva 680)[98].

---

[97] *Like the GDPR, the LED was adopted in May 2016, constituting a major step forward in establishing a comprehensive EU data protection regime, as the first horizontal and legally binding instrument laying down the rules for national and cross-border processing of personal data in the area of law enforcement. Moreover, the LED is a modern instrument, designed for LEAs processing personal data in the Digital Age. As the second part of the data protection reform package that had been under discussion for four years, the Directive received way less attention than the GDPR. However, two main objectives of the Directive are too important to be neglected: the increased level of fundamental rights protection in the area of police and criminal justice, and the improved sharing of personal data between the Member States, as they will be able to rely on uniform data protection rules (Article 1(2)). The Directive is the successor to the 2008 Framework Decision 2008, which had a much more limited scope and solely applied to cross-border data processing between the Member States. 12 The rules of the Directive, which had to be transposed into the national laws of all 28 Member States and the four Schengen Area States (Norway, Iceland, Switzerland and Lichtenstein)13 by May 2018 benefited from the attention given to the GDPR, as some of the Regulation's solutions could simply be taken over. However, a number of provisions were developed specifically for the Directive.* SAJFERT, Juraj e QUINTEL, Teresa, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities* (December 1, 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873. Acesso em 25/06/2021.

[98] Artigo 62.o Relatórios da Comissão (...) 6. Até 6 de maio de 2019, a Comissão reexamina outros atos jurídicos adotados pela União que regulam o tratamento pelas autoridades competentes para efeitos do artigo 1.o, n.o 1, designadamente os referidos no artigo 60.o, a fim de avaliar a necessidade de os harmonizar com a presente

As novas técnicas investigativas, incluindo sistemas que identificam pessoas ou locais suspeitos de crimes, sistema de vigilância para monitorar área de risco e sistemas de pesquisa para minerar dados em busca de pistas investigativas ou para desenvolver redes de inteligência de dados úteis para grupos ou comunidades contribuíram para o incremento do interesse dos estudiosos pela matéria.

No que toca aos estudos sobre as regulamentações existentes quanto ao tratamento de dados pessoais realizados pelas autoridades criminais, até a pouco tempo escassos, estes tomaram corpo rapidamente, dentre outros motivos, ante o aumento da criminalidade *on line,* cujos vestígios digitais deixados pelos autores da prática delitiva auxiliam as *law enforcement authorities*[99] nas tarefas de prevenção e apuração de crimes, favorecendo a coleta e o intercâmbio de dados que assumiram vital importância para o êxito do trabalho policial.

A intenção do parlamento da União Europeia de garantir um elevado nível de proteção de dados, assegurando também que o mesmo não iniba o livre fluxo de dados no domínio da investigação e repressão do crime, concretizou-se, pois, com a adoção da Diretiva 680.

3.2. ÂMBITO DE APLICAÇÃO DA LEI E CONCEITOS GERAIS

Inicialmente, é de se lançar luz no fato de que, diversamente do Regulamento 2016/679/EU, que tem aplicabilidade imediata em todos os Estados-Membros da União Europeia, o diploma legal que dispõe sobre o tratamento de dados no âmbito criminal na União trata-se de uma diretiva[100] e, em assim sendo, necessita ser transposta pelos Estados-Membros. Conforme já tratado anteriormente no presente trabalho (capítulo xxx), para ingressar e produzir efeitos em cada ordenamento jurídico nacional, as diretivas necessitam de uma lei de transposição editada por cada um dos Estados-Membros, no âmbito local, o que não ocorre com os Regulamentos que, já de pronto, são aplicáveis aos Estados-Membros, conferindo grande uniformidade ao tratamento da matéria a que se referem.

---

diretiva e apresenta, se for caso disso, as propostas necessárias à alteração desses atos de forma a assegurar uma abordagem coerente da proteção de dados pessoais no âmbito da presente diretiva.

[99] Autoridades de polícia e de justiça criminal. Em inglês, a expressão *law enforcement,* literalmente 'aplicação da lei', possui conotação eminentemente ligada à área do direito penal e da segurança pública, diversamente do que ocorre no Brasil, onde a expressão 'aplicação da lei' possui conotação mais ampla, abrangendo, também, atividades meramente administrativas.

[100] Concomitantemente ao Regulamento 2016/679/EU, a Diretiva 2016/680/UE foi publicada no Diário Oficial da União Europeia nº 119, em data de 04 de maio de 2016 (páginas 89-131).

Tal circunstância, por si só, já tem potencial para suscitar uma série de divergências na disciplina do tratamento de dados pessoais adotada pelos Estados-Membros, já que cada um deles, embora observando os parâmetros constantes da Diretiva, realiza a transposição de acordo com as peculiaridades locais. Assim, não raro se encontra diferenças interpretativas no tratamento dos dados pessoais utilizados pelas forças de segurança nos diversos Estados-Membros[101].

Tanto o Regulamento 679 como a Diretiva 680 visam proteger a pessoa no que diz respeito ao tratamento dos seus dados pessoais, embora com âmbito de aplicação diferenciado.

O Regulamento 679 disciplina o tratamento de dados em geral[102]. Além das disposições coincidentes com a Diretiva 680, o Regulamento 679 estabelece regras detalhadas quanto ao objeto, objetivos (artigo 1º) e âmbitos de aplicação material (artigo 2º) e territorial (artigo 3º), inclusive no que tange ao tratamento de dados realizado fora da União, pertencentes a titulares que se encontrem em seu território, cujos responsáveis pelo tratamento e/ou subcontratantes deverão às suas regras se curvar[103].

Por sua vez, a Diretiva 680, já no início, traz um de seus dispositivos de maior relevância[104] (artigo 2º, 1), que determina a aplicação desta ao tratamento de dados efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública (artigo 1º, 1), realizado por meios total ou parcialmente

---

[101] Todavia, esta foi a solução encontrada pelo bloco Europeu para concretizar o pacote de medidas legislativas no tocante à proteção de dados, cuja tramitação se iniciou no ano de 2012 e, até a conclusão, em 2016, contou com 3999 modificações no texto inicialmente proposto.

[102] O Regulamento 679 exclui expressamente de sua incidência determinadas atividades de tratamento de dados (artigo 2º), como as relativas à Política Externa e de Segurança Comum da União (*b*), no âmbito pessoal ou doméstico (*c*), pelas autoridades criminais – Diretiva 2016/680/UE – (*d*) e em relação ao comércio eletrônico – Diretiva 2000/31/CE – (item 4). Assim como a Diretiva 680 (artigo 2º, 3, *a* e *b*), o Regulamento 679 também exclui de sua incidência os tratamentos efetuados no exercício de atividades não sujeitas à aplicação do Direito da União (*a*) e efetuados por instituições, órgãos e organismos ou agências da União (item 3).

[103] Um dos mais relevantes dispositivos do Regulamento 679 é o que trata de sua aplicação extraterritorial (artigo 3º) e que determina sua incidência, também, sobre as entidades que, mesmo não estabelecidas na União Europeia, tratem dados pessoais de titulares que se encontram no seu território, quando o tratamento se relacionar à oferta de bens ou serviços, remunerados ou não, ou ao controle do seu comportamento, desde que ocorrido na União Europeia.

[104] Artigo 2.o Âmbito de aplicação 1. A presente diretiva aplica-se ao tratamento de dados pessoais pelas autoridades competentes para os efeitos estabelecidos no artigo 1.o, n.o 1. 2. A presente diretiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento de dados pessoais contidos num ficheiro ou a ele destinados por meios não automatizados. 3. A presente diretiva não se aplica ao tratamento de dados pessoais: a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União; b) Efetuado pelas instituições, organismos, serviços e agências da União.

automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados (artigo 2º, 2).

Nos termos da Diretiva 680, são protegidos os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais (artigo 1º, 2, *a*), bem como assegurado o intercâmbio de dados pessoais entre autoridades competentes na União, garantindo que este não seja limitado nem proibido por razões relacionadas com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais (artigo 1º, 2, *b*). Poderão os Estados-Membros, ainda, prever garantias mais elevadas aos titulares de dados que as já estabelecidas pelas autoridades competentes (artigo 1º, 3).

Digno de nota, também, quanto às leis de proteção de dados em estudo, são as peculiaridades existentes na parte conceitual do Regulamento 679 (artigo 4º) e da Diretiva 680 (artigo 3º).

Além das 15 definições comuns existentes em ambos os diplomas legais, o Regulamento 679 traz também as definições de: a) terceiro (item 10); b) consentimento do titular dos dados (item 11); c) estabelecimento principal (item 16); d) representante (item 17); e) empresa (item 18); f) grupo empresarial (item 19); g) regras vinculativas aplicáveis às empresas (item 20); h) autoridade de controlo interessada (item 22); i) tratamento transfronteiriço: (item 23); j) objeção pertinente e fundamentada (item 24); k) serviços da sociedade da informação (item 25).

Todavia, mais importante ainda é a definição de responsável pelo tratamento, contida em ambas as legislações, porém com conotações diversas.

O Regulamento 679 (artigo 4º) elege como responsável pelo tratamento a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais (item 7).

Já para Diretiva 680 (artigo 3º), responsável pelo tratamento é a autoridade competente que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento dos dados pessoais (item 8), apontando a 'autoridade competente' como sendo: a) uma autoridade pública competente para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; ou b) qualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para exercer a autoridade pública e os poderes públicos para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou

execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública (item 7).

3.2.1. A extensão do conceito de 'autoridade competente' como definidor da aplicação da Diretiva 680 ou do Regulamento 679

A definição de 'autoridade competente' consiste em inovação trazida pela lei que regula o tratamento de dados pelas forças de segurança, eis que não se vislumbra precedentes na legislação anterior que tratava da matéria.

No que toca às atividades desenvolvidas por tais autoridades, vale considerar que a vertiginosa evolução tecnológica e a globalização deram origem à novos desafios em matéria de proteção de dados, ante o aumento exponencial na partilha e recolha de dados pessoais que resultou no acréscimo, também, numa escala nunca antes experimentada, do tratamento dos dados utilizados no exercício das atividades de prevenção, investigação, detecção ou repressão de infrações penais, e na execução de sanções penais (considerando 3).

Ao passo em que a Diretiva 680 dispõe que deverá ser facilitada a transferência de dados a países terceiros, que não fazem parte da União, bem como a organizações internacionais, também exige que se assegure um nível elevado de proteção dos dados pessoais, que obriga ao estabelecimento de um regime de proteção de dados pessoais sólido e coerente na União, com rigorosa aplicação das regras específicas na matéria (considerando 4).

A livre circulação de dados é referida já desde o início pela *Law Enforcement Directive* que, quando anuncia à que vem, menciona não só a proteção que confere às pessoas no que diz respeito ao tratamento dos seus dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais e a execução de sanções penais, incluindo a salvaguarda e a prevenção à segurança pública a nível da União, mas também preconiza a livre circulação destes dados entre tais autoridades.

Essas autoridades competentes podem incluir não só as autoridades públicas (polícia, autoridades judiciárias ou outras autoridades de aplicação da lei penal), mas também outros organismos e entidades designadas pelo direito dos Estados Membros para o exercício da autoridade e dos poderes públicos para efeitos do contido na Diretiva.

Caso esses organismos ou entidades tratem dados pessoais para efeitos que não sejam os da Diretiva 680, é aplicável o Regulamento 679, o que ocorre, também, nos casos em que um organismo ou uma entidade recolhe dados pessoais para outros efeitos e, em seguida, os trata, a fim de dar cumprimento a uma obrigação legal a que está sujeito. Este pode ser o caso das

instituições financeiras quando retêm, para efeitos de investigação, detecção ou repressão de infrações penais, certos dados pessoais por si tratados, e os fornecem apenas às autoridades nacionais competentes, em casos específicos e nos termos do direito dos Estados-Membros.

Esses organismos ou entidades que tratam dados pessoais em nome das autoridades competentes no âmbito da Diretiva 680 deverão estar vinculados por contrato ou por outro ato jurídico e pelas disposições aplicáveis aos subcontratantes nos termos nela previstos, sem prejuízo da aplicação do Regulamento 679 ao tratamento de dados pessoais pelo subcontratante não abrangido pela Diretiva (considerando 11).

A facilitação no intercâmbio de dados entre as autoridades competentes dos Estados-Membros visa assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial. Para tanto, o nível de proteção dos direitos e liberdades individuais, no que tange ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais e a execução de sanções penais, incluindo a salvaguarda e a prevenção à segurança pública, deverá ser equivalente em todos os Estados-Membros. A proteção eficaz dos dados pessoais na União exige não só que sejam reforçados os direitos dos titulares dos dados e as obrigações de quem trata dados pessoais, mas também que haja reforço dos poderes equivalentes para controlar e assegurar a conformidade com as regras de proteção dos dados pessoais nos Estados-Membros (considerando 7).

Além das atividades de prevenção, investigação, detecção e repressão de infrações penais, as funções da polícia e das outras autoridades da justiça criminal incluem também as atividades policiais sem conhecimento prévio de que um incidente constitui ou não uma infração penal, inclusive a adoção de medidas coercitivas tais como as atividades da polícia em manifestações, grandes eventos desportivos e distúrbios. Tais funções incluem também a manutenção da ordem pública enquanto atribuição da polícia ou de outras autoridades de aplicação da lei, quando necessárias para salvaguarda e prevenção de ameaças à segurança pública e aos interesses fundamentais da sociedade protegidos por lei, e à prática de infrações penais. Os Estados membros podem atribuir às autoridades competentes, ainda, outras funções que não as descritas no artigo 1º, 1, da LED, sendo o tratamento de dados para outros efeitos abrangido pelo âmbito de aplicação do GDPR (considerando 12).

Sobre o assunto, Maria Belén Sanchez Domingo compartilha o seguinte entendimento:

> No que se refere às "autoridades competentes", a que se referem as alíneas a) e b) do artigo 3º, 25 pode-se dizer que são juízes, procuradores e mesmo

> membros das Forças de Segurança do Estado no exercício de funções que lhes são atribuídas como autoridade pública. Este é provavelmente um dos pontos mais problemáticos da Diretiva, especificamente no caso de membros das Forças de Segurança do Estado decidirem aplicar uma medida repressiva a uma manifestação que represente uma ameaça à segurança pública. Tal ação está relacionada à prevenção ou investigação de infrações criminais. Como é sabido, esta atividade é atribuída à Polícia, cabendo às Forças de Segurança do Estado e ao Corpo de Segurança a manutenção da ordem pública. A própria Diretiva estabelece que as medidas coercivas para reprimir uma manifestação ou motim são consideradas atividades policiais centradas na detenção ou prevenção de ameaças à segurança pública (Considerando 12). Por conseguinte, de acordo com a interpretação literal do artigo 3.º da Diretiva e as funções atribuídas a uma autoridade competente, esta deve poder efetuar a livre circulação de dados pessoais entre as autoridades responsáveis pela aplicação da lei para investigações judiciais[105]. (tradução livre).

Gabriele Rugani (2019), quando discorre sobre a criticidade do âmbito de aplicação do GDPR e da LED, em razão da diversidade da abrangência do conceito de autoridade competente em cada Estado-Membro, aponta que, além das inúmeras regras específicas sobre proteção de dados contidas nos instrumentos anteriores não terem sido eliminadas, outro ponto crítico da Diretiva (UE) 2016/680 diz respeito à delimitação entre o âmbito de aplicação da diretiva e o do GDPR. De acordo com o artigo 2.º, n.º 1, a Diretiva aplica-se ao tratamento de dados pessoais pelas autoridades competentes para os fins referidos no artigo 1.º, n.º 1, ou para efeitos de prevenção, investigação, detecção e repressão de crimes ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública. É então o artigo 3º, dedicado às definições, que no nº 7) define o conceito de "autoridade competente" como "a) Uma autoridade pública competente para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; ou b) Qualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para

[105] *With regard to "competent authorities", referred to by the Article 3, a) and b), it can be said that they are judges, prosecutors and even members of the State Security Forces in the exercise of functions attributed to them as public authority. This is probably one of the most problematic points of the Directive, specifically in case members of the State's Security Forces decide to apply a repressive measure to a demonstration posing a threat to public security. Such action is related to the prevention or investigation of criminal offences. As is well known, this activity is conferred on the police, since it is the responsibility of the State Security forces and Corps to maintain public order. The Directive itself states that, coercive measures to repress a demonstration or a riot shall be considered as police activities focused on the detention or prevention of threats to public security (Recital 12). Therefore, in accordance with the literal interpretation of Article 3 of the Directive and the tasks assigned to a competent authority, it shall be able to carry out the free movement of personal data between law-enforcement authorities for judicial investigations.* Domingo, Maria Belén Sanchez (2019). *The protection of personal data in the field of judicial cooperation in criminal matters: special reference to Directive (EU) 2016/680 of the European Parliament and of the Council.* Unio - EU Law Journal. 5. 92-102. 10.21814/unio.5.2.2295.

exercer a autoridade pública e os poderes públicos para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública". Da leitura desta disposição, pode-se ver que, no final, prevaleceu uma definição muito ampla de "autoridade competente", sobretudo a pedido do Conselho. No entanto, segundo a AEPD, teria sido adequado que esta noção permanecesse tão limitada quanto possível. As autoridades tradicionais de aplicação da lei (autoridades policiais e de justiça criminal) estão indubitavelmente incluídas na letra a); no entanto, a definição referida na alínea a) também inclui outras autoridades públicas, como Unidades de Inteligência Financeira. Além disso, a letra b) também inclui organizações e entidades privadas, como, a título de exemplo, empresas de segurança privada (*private security contractors*). Um âmbito de aplicação tão amplo torna incerto o limite entre a Diretiva (UE) 2016/680 e o GDPR.

Prossegue Rugani (2019), ainda, apontando que, em primeiro lugar, a alínea a) do artigo 3.º, inclui não só as autoridades policiais e judiciárias, mas também outras autoridades públicas: a este respeito, importa referir que os Estados-Membros definem as atividades das respetivas autoridades, como ações de aplicação da lei ou puramente administrativas, de forma diferenciada de acordo com as próprias tradições; consequentemente, as mesmas operações de tratamento poderiam ser regidas num país membro pelo Regulamento (UE) 2016/679, noutro pelas regras nacionais de implementação da Diretiva. Por exemplo, pode-se notar que em alguns Estados as Unidades de Inteligência Financeira estabelecidas em cumprimento à Diretiva Anti-Lavagem de Dinheiro são autoridades administrativas, enquanto em outros são consideradas autoridades policiais: a diferença não é insignificante, uma vez que os tratamentos no contexto das infrações administrativas é abrangido pelo âmbito de aplicação do GDPR, ao passo que os tratamentos no contexto das infrações penais são abrangidos pelo da diretiva. Esta situação, por sua vez, mostra-se particularmente problemática uma vez que os dois instrumentos não são consistentes entre si. Tal como o Grupo de Trabalho do artigo 29.º também afirma, por um lado, seria necessária uma maior coerência entre a directiva e o regulamento e, por outro lado, uma maior clareza no que se refere à definição de "autoridades competentes". No que diz respeito ao artigo 3.º, alínea b), teria sido adequado que organizações e indivíduos não públicos desempenhassem funções de combate ao crime não fossem abrangidos pelo âmbito de aplicação da diretiva, mas sim pelo Regulamento, conforme também afirmado pela AEPD. Por exemplo, as companhias aéreas e os operadores de telecomunicações, obrigados por lei a recolher e fornecer dados, nunca

devem ser sujeitos à disciplina da Diretiva: o objetivo principal e original da coleta de tais dados, na verdade, é completamente diferente da prevenção, investigação, detecção ou repressão de crimes.

E ainda conclui Rugani (2019) que, para além da definição ampla de "autoridade competente", existe outro elemento que pode causar uma extensão indevida do âmbito de aplicação da Diretiva (UE) 2016/680: o fato de o artigo 1.º, n.º 1 incluir "a salvaguarda e prevenção de ameaças à segurança pública". Este aspecto, que não era abrangido pelo âmbito de aplicação da Decisão-Quadro 2008/977/JAI e que nem sequer estava previsto na proposta original de diretiva da Comissão, foi acrescentado por iniciativa do Conselho, apesar do parecer contrário da AEPD. O considerando 12, já citado no presente trabalho, apresenta alguns exemplos, tais como "atividades da polícia em manifestações, grandes eventos desportivos e distúrbios". Desta forma, alarga-se a aplicabilidade da Directiva no que diz respeito ao cerne fundamental das atividades de combate ao crime, uma vez que manifestações, grandes eventos desportivos e distúrbios apenas em alguns casos conduzem à prática de crimes. Esta extensão ocorre, mais uma vez, em detrimento do GDPD e, sobretudo, determina, ainda neste caso, uma situação de incerteza quanto à correta legislação a ser aplicada.

Por fim, anote-se que, buscando garantir o mesmo nível de proteção às pessoas no âmbito da União e evitar divergências que criem obstáculos ao intercâmbio de dados pessoais entre as autoridades competentes, cabe à Diretiva 680 prever regras harmonizadas para a proteção e a livre circulação de dados pessoais tratados para os efeitos descritos no artigo 1º, 1. A aproximação das legislações dos Estados-Membros tem por objetivo garantir o elevado nível de proteção dos dados pessoais na União, que inclusive poderão prever garantias mais elevadas que as constantes da Diretiva 680 no que diz respeito à proteção de dados pessoais tratados pelas autoridades competentes (considerando 15).

Para efeitos de prevenção, investigação ou repressão de infrações penais, é necessário que as autoridades competentes tratem os dados pessoais, recolhidos no contexto da prevenção, investigação, detecção ou repressão de infrações penais específicas para além desse contexto, a fim de obter uma melhor compreensão das atividades criminais e de estabelecer ligações entre as diferentes infrações penais detectadas (considerando 27).

3.3. PRINCÍPIOS SOBRE A PROTEÇÃO DE DADOS PESSOAIS

No que toca aos princípios em matéria de proteção de dados pessoais, tanto a Diretiva 680 (artigo 4º) quanto o Regulamento 679 (artigo 5º) elencam os mesmos princípios a serem observados por aqueles que tratam dados pessoais de outrem, divergindo, todavia, em alguns pontos de interpretação dos mesmos.

Ambos os diplomas legais dispõe que os dados devem ser objeto de tratamento lícito e leal (princípios da licitude e lealdade), recolhidos para finalidades determinadas, explícitas e legítimas, com as quais devem ser tratados de forma compatível (princípio da finalidade). Ainda, tais dados devem ser adequados, pertinentes e limitados ao mínimo necessário (princípio da minimização dos dados), bem como exatos e atualizados (princípio da exatidão), conservados apenas durante o período necessário para alcançar a finalidade para a qual foram coletados (princípio da limitação da conservação) e tratados de forma segura, seja com relação à proteção quanto ao tratamento não autorizado ou ilícito ou quanto a eventuais acidentes – perda, destruição ou dano acidentais, mediante a adoção das medidas técnicas ou organizativas adequadas (princípio da segurança).

Já insculpido no artigo 8º da Carta dos Direitos Fundamentais da União Europeia[106], a lealdade de tratamento, que constitui um dos princípios da proteção de dados, orienta que as pessoas singulares deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos seus dados pessoais, bem como para os meios de que dispõem para exercer os seus direitos relativamente ao tratamento desses dados. Em especial, os efeitos específicos do tratamento deverão ser explícitos e legítimos, e deverão estar determinados no momento da recolha dos dados pessoais (considerando 26).

Também os dados pessoais deverão ser adequados e relevantes para o tratamento a que se destinam, garantindo-se que os dados recolhidos não sejam excessivos nem conservados durante mais tempo do que o necessário, para os efeitos para os quais são tratados. Os dados pessoais só deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. Visando assegurar que os dados são conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar prazos para o seu apagamento ou revisão periódica. Por fim, deverão ser previstas garantias adequadas

[106] Artigo 8.o Proteção de dados pessoais 1. Todas as pessoas tem direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas tem o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. Carta dos Direitos Fundamentais da União Europeia. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em 10/07/2021.

aplicáveis aos dados pessoais conservados durante períodos mais longos, a fim de fazerem parte de arquivos de interesse público ou de serem utilizados para fins científicos, estatísticos ou históricos (considerando 26).

Com relação ao princípio da finalidade, note-se que os dados pessoais deverão ser recolhidos para finalidades determinadas, explícitas e legítimas abrangidas pelo âmbito de aplicação da Diretiva 680, e não deverão ser tratados para fins incompatíveis com os da prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais — nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública. Se os dados pessoais forem tratados, pelo mesmo ou por outro responsável pelo tratamento, para uma finalidade abrangida pelo âmbito de aplicação da presente diretiva que não aquela para a qual foram recolhidos, esse tratamento deverá ser permitido, na condição de que esse tratamento seja autorizado em conformidade com as disposições legais aplicáveis e necessário e proporcionado para a prossecução dessa outra finalidade (considerando 29).

Ainda no que toca à finalidade, cumpre ressaltar que o Regulamento 679 permite o tratamento posterior, com finalidade diversa da inicialmente prevista, para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, que não é considerado incompatível com as finalidades iniciais – limitação das finalidades (artigo 5º, 1, *b*). Ainda, da mesma forma estabelece, quanto à conservação dos dados pessoais, que podem ser conservados durante períodos mais longos para as finalidades acima descritas, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados – limitação da conservação (artigo 5º, 1, *e*). Assim, no GDPR, para tratamento de dados com fins diversos da coleta, não tendo sido feita esta com base no consentimento e nem no direito da União ou dos Estados membros, o responsável pelo tratamento deve analisar a compatibilidade das finalidades da coleta e do tratamento posterior, tendo em conta alguns parâmetros (artigo 6º, item 4).

Já a Diretiva 680 permite o tratamento pelo mesmo ou por outro responsável pelo tratamento para as finalidades previstas no seu artigo 1º, nº 1, diferentes da finalidade para a qual os dados pessoais foram recolhidos, em determinadas situações, quais sejam: a) o responsável pelo tratamento esteja autorizado a tratar esses dados pessoais com essa finalidade, nos termos do direito da União ou dos Estados-Membros; e b) o tratamento seja necessário e proporcionado para essa outra finalidade, nos termos do direito da União ou dos Estados-Membros (artigo 4º, 2). O tratamento pelo mesmo ou por outro responsável pelo

tratamento pode incluir o arquivo de interesse público e a utilização científica, estatística ou histórica dos dados para as finalidades previstas no artigo 1º, nº 1, sob reserva de garantias adequadas dos direitos e liberdades do titular dos dados (artigo 4º, 3). Em assim sendo, será aplicado o Regulamento 679, o mesmo se verificando se as autoridades tiverem outras atribuições diversas das descritas no artigo 1º, nº 1 (artigo 9º, 1 e 2).

No que pertine ao princípio da exatidão dos dados, é conveniente observá-lo tendo em conta a natureza e a finalidade do tratamento em causa. Especialmente quando se trata de processos judiciais, as declarações que contêm dados pessoais são baseadas em percepções subjetivas da pessoa singular e nem sempre são verificáveis. Este princípio não deverá, por conseguinte, aplicar-se à exatidão da própria declaração, mas simplesmente ao facto de tal declaração ter sido feita (considerando 30).

Neste viés, a Diretiva 680 determina a distinção entre os dados pessoais que são baseados em fatos e os que são baseados em apreciações pessoais, bem como que as autoridades competentes tomem todas as medidas razoáveis para assegurar que os dados pessoais inexatos, incompletos ou desatualizados não possam ser transmitidos nem disponibilizados. Ainda, que, antes da adoção destas medidas, verifiquem a qualidade dos dados, fornecendo, na medida do possível, as informações necessárias para que a autoridade competente que as recebe possa apreciar até que ponto os dados são exatos, completos e fiáveis, e estão atualizados. Se houver transmissão de dados inexatos ou de forma ilícita o destinatário será avisado, caso em que os dados pessoais são retificados ou apagados, ou o tratamento é limitado nos termos do artigo 16º (artigo 7º da LED).

Ao contrário, o Regulamento 679 não faz distinção entre os dados pessoais que são baseados em fatos e os que são baseados em apreciações pessoais.

Ainda, as autoridades competentes deverão assegurar que não sejam transmitidos nem disponibilizados dados pessoais incorretos, incompletos ou desatualizados. A fim de assegurar a proteção das pessoas singulares e a exatidão, exaustividade ou atualidade e fiabilidade dos dados pessoais transmitidos ou disponibilizados, as autoridades competentes deverão acrescentar, na medida do possível, as informações necessárias em todas as transmissões de dados pessoais (considerando 32).

Sajfert e Quintel comentam sobre algumas diferenças existentes em relação aos princípios na lei geral de proteção de dados e na lei que disciplina o tratamento de dados efetuado pelas forças de segurança:

> No Capítulo II, já ao nível dos princípios de tratamento definidos no Artigo 4 encontram-se algumas diferenças importantes em relação ao RGPD. Em primeiro lugar, a Diretiva não se refere ao tratamento posterior [*further processing*], mas, em vez disso, introduz a noção de tratamento posterior pelo mesmo ou por outro responsável pelo tratamento nos n.ºs 2 e 3. No contexto da aplicação da lei penal, esse tratamento é geralmente considerado compatível com as finalidades do recolhimento inicial dos dados pessoais (se o recolhimento também tiver sido efetuado para as finalidades da Diretiva), se autorizada por lei e se necessário e proporcional à nova finalidade, na medida em que a nova finalidade continue a ser abrangida pelo âmbito de aplicação da Diretiva. Outra diferença notável é o princípio da minimização dos dados (artigo 4.º, n.º 1, alínea *c*)). Nos termos da Diretiva, os dados pessoais devem ser adequados, pertinentes e limitados ao mínimo necessário, em vez de adequados, pertinentes e limitados ao que é necessário, conforme estipulado no artigo 5.º, n.º 1, alínea *c*), do RGPD. Ambos os princípios conferem mais flexibilidade às autoridades de polícia e justiça criminal no desempenho de suas tarefas em comparação com os requisitos das disposições correspondentes do RGPD (tradução livre) [107].

Digno de nota, também, são as lições trazidas por Maria Belén Sanchez Domingo sobre o assunto:

> Por sua vez, a Diretiva especifica os princípios relativos ao tratamento de dados pessoais para efeitos de investigação, prevenção ou detecção de infrações penais nos artigos 4.º e seguintes, princípios que coincidem com os especificados na Convenção 108, na Diretiva 95/46/CE e na Decisão-Quadro 2008/977/JAI, embora com uma formulação mais precisa do que a apresentada pelos textos normativos acima mencionados. A Diretiva estabelece, portanto, que os Estados-Membros devem prever que os dados pessoais sejam tratados de forma lícita, justa e transparente em relação às pessoas em causa e que sejam efetuados apenas para os efeitos específicos previstos na lei. No Considerando (26), especifica-se que os dados pessoais devem ser adequados e relevantes em relação às finalidades para os quais são tratados, ou seja, para a prevenção, investigação e repressão de infrações penais ou sanções, o que exige uma garantia de que o os dados coletados não devem ser excessivos ou mantidos por mais tempo do que o estritamente necessário para a finalidade do tratamento. Além disso, sublinha que os dados pessoais só podem ser tratados se a finalidade do tratamento não puder

[107] *In Chapter II, already at the level of principles of processing defined in Article 4 are some important differences compared to the GDPR. Firstly, the Directive does not refer to further processing, but instead introduces the notion of subsequent processing by the same or another controller in paragraphs 2 and 3. In the law enforcement context, such processing is generally deemed compatible with the purposes of the initial data collection (if the collection was also carried out for the purposes of the Directive), if authorized by law and if necessary and proportionate to the new purpose, to the extent that the new purpose remains within the scope of the Directive. Another notable difference is the principle of data minimisation (Article 4(1)(c)). Under the Directive, personal data should be adequate, relevant and not excessive, rather than adequate, relevant and limited to what is necessary, as stipulated under Article 5(1)(c) GDPR. Both principles grant more flexibility to LEAs in the performance of their tasks compared to the requirements of the corresponding provisions under the GDPR.* SAJFERT, Juraj e QUINTEL, Teresa, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities* (December 1, 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873. Acesso em 25/06/2021.

> ser obtido por outros meios. Os fins específicos para os quais se destina o tratamento de dados pessoais, para efeitos de prevenção, investigação ou ação penal, devem ser explícitos e legítimos (Considerando 29), devendo estar determinados no momento da recolha dos dados pessoais objeto do tratamento.
>
> Por último, no que se refere ao princípio da exatidão dos dados pessoais, a Diretiva impõe às autoridades competentes uma obrigação, dada a natureza e a finalidade do tratamento dos dados pessoais, que os dados incorretos, incompletos ou desatualizados não sejam transmitidos ou disponibilizados (Considerando 32). Além disso, as autoridades devem adicionar as informações necessárias em todas as transmissões de dados pessoais. Há também a obrigação de manter os dados armazenados em um formato que permita a identificação dos titulares dos dados por um período não mais longo do que o necessário para as finalidades para os quais são tratados (Artigo 4, 1, e)[108] (tradução livre).

Ao contrário do que se verifica no Regulamento 679 (artigo 5º, 1, *a*), a Diretiva 680 não menciona expressamente o princípio da transparência na parte em que dispõe sobre os princípios relativos ao tratamento de dados pessoais (artigo 4º). Entretanto, dito princípio vem descrito na parte introdutória da lei que regula o tratamento de dados efetuado pelas forças de segurança, em que orienta que o tratamento de dados pessoais tem de ser feito de forma lícita, leal e transparente para com as pessoas singulares em causa, e exclusivamente para os efeitos específicos previstos na lei.

Cabe anotar que a adoção de tal princípio não obsta, por si só, a que as autoridades de aplicação da lei exerçam atividades tais como investigações encobertas ou de videovigilância. Estas atividades podem ser executadas para efeitos de prevenção, investigação, detecção ou

---

[108] *In turn, the Directive details the principles relating to the processing of personal data for the purposes of the investigation, prevention or detection of criminal offences in Articles 4 et seq., principles which coincide with those specified in Convention 108, Directive 95/46/EC and Framework Decision 2008/977/JHA, albeit with a more precise wording than that presented by the abovementioned normative texts. The Directive thus states that Member States shall provide for personal data to be processed lawfully, fairly and transparent in relation to the persons concerned and shall only be carried out for the specific purposes laid down by law. In Recital (26), it is specified that personal data shall be adequate and relevant in relation to the purposes for which they are processed, that is, for prevention, investigation and prosecution of criminal offences or sanctions, which requires a guarantee that the personal data collected shall not be excessive or kept for longer than strictly necessary for the purposes for which they are processed. Furthermore, it stresses that personal data may only be processed if the purpose of the processing cannot be obtained by other means. The specific purposes for which the processing of personal data is intended, for prevention, investigation or prosecution purposes, should be explicit and legitimate (Recital 29), with the obligation to be agreed at the time of collection of the personal data subject to processing. Finally, with regard to the principle of accuracy of personal data, the Directive imposes an obligation on the competent authorities, given the nature and purpose of the processing of personal data, that data which are inaccurate, incomplete or no longer up to date may not be transmitted or made available (Recital 32). Also, authorities should add necessary information in all transmissions of personal data. In addition, there is also an obligation to keep the data stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed (Article 4, 1, e).* Domingo, Maria Belén Sanchez (2019). *The protection of personal data in the field of judicial cooperation in criminal matters: special reference to Directive (EU) 2016/680 of the European Parliament and of the Council.* Unio - EU Law Journal. 5. 92-102. 10.21814/unio.5.2.2295.

repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, desde que estejam previstas na lei e constituam uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os interesses legítimos da pessoa singular em causa (considerando 26).

Discorrendo sobre as garantias básicas da transferência e tratamento de dados pessoais na cooperação judiciária penal, Maria Izabel Gonzales Cano, em referência aos princípios descritos lei que regula o tratamento de dados efetuado pelas forças de segurança, leciona que

> A Diretiva 2016/680 refere-se, portanto, ao tratamento de dados pessoais exatos e atualizados, devidamente armazenados e tratados de forma segura, no domínio da investigação criminal e da ação penal. Um tratamento lícito, justo e transparente, adequado e não excessivo, e realizado exclusivamente de acordo com os fins legais preestabelecidos (art. 4.1). Isto implica que a medida que envolve o tratamento de dados pessoais deve responder aos seguintes pressupostos: a) Estar previsto em lei, ser necessário, adequado, útil, pertinente e proporcionado para efeitos de investigação ou repressão de determinado crime. Assim, deve ser justificada a sua relevância para os fins prosseguidos, devendo ser garantido que os dados em questão não sejam excessivos para o que se está a investigar, nem que se conservem mais tempo do que o necessário para os fins prosseguidos, ou seja, para concluir uma investigação ou ação penal contra um crime específico contra uma pessoa específica, investigada ou processada. b) Ser objecto de informação ao sujeito, nomeadamente sobre os seus direitos e as vias de defesa, ou para os fazer valer em relação ao caso concreto. c) E, para ter finalidades específicas e legítimas, a determinar no momento da recolha ou recolha de dados.
>
> Nesse sentido, o art. 8 estabelece os pressupostos da legalidade do tratamento de dados, que são a necessidade fundamentada nos fins de investigação ou ação penal, e a justificativa de seu objetivo, de forma que os Estados devem prever em seus ordenamentos jurídicos, pelo menos, os objetivos do tratamento, os dados pessoais que serão objeto dos mesmos e os fins do tratamento.
>
> Ora, se esta é a regra geral, a Diretiva também estabelece vários regimes de exceções à lista de direitos que ela consagra, e que, não esqueçamos, remetem a um suspeito, investigado ou indiciado em processo penal.
>
> Assim, o princípio norteador é que os dados pessoais são coletados para fins específicos, explícitos e legítimos (art. 4.1), e que, fora do caso específico, a confidencialidade deve prevalecer, impedindo o acesso não autorizado aos dados. No entanto, isso não impede que esses dados sejam usados para outros fins, desde que não sejam incompatíveis com os relativos à investigação e ação penal.
>
> Neste sentido, o artigo 4.2 da Diretiva 2016/680, permite o tratamento de dados pessoais, para efeitos do art. 1.1 (investigação e ação penal) diversa daquela para a qual foram recolhidos, ou seja, para a investigação ou repressão de outros atos criminosos imputáveis à mesma pessoa ou a outra pessoa ainda não investigada. Ou seja, um tratamento dos dados com a mesma finalidade, mas em um processo penal diferente. E isso será possível se o responsável pelo tratamento for autorizado, e se necessário e

> proporcional a essa outra finalidade ou ação penal. Este é, portanto, o regime excepcional do princípio da especialidade, ou regime de disponibilidade ampliada da diretiva[109] (tradução livre).

Gonzales Cano (2019) segue pontuando que a necessidade e a proporcionalidade da transferência dos dados para outro processo, bem como a outra 'finalidade não incompatível' em relação àquela para a qual os dados foram inicialmente recolhidos, a fim de tornar possível o compartilhamento de dados, hão que ser aferidos pelo responsável pelo tratamento. Diversamente da legislação que a antecede, a Diretiva 680 estabelece parâmetros mínimos, exigindo, para a transferência dos dados já coletados, uma finalidade genérica e única, ou seja, a investigação de um crime ou a ação penal, embora em outra causa e para fatos ou contra pessoas diferentes, e suscita a necessidade de regulamentação da matéria nas legislações nacionais, com base jurídica clara e precisa sobre os objetivos e finalidades do tratamento de dados pessoais, os procedimentos de manutenção da sua integridade e confidencialidade, bem como os necessários para a sua destruição, com garantias suficientes para evitar abusos e arbitrariedades. Neste sentido, cabe mencionar a legislação espanhola

---

[109] *La Directiva 2016/680 se refiere pues a un tratamiento de datos personales exactos y actualizados, conservados adecuadamente y tratados de manera segura, en el ámbito de la investigación y enjuiciamiento penal. Un tratamiento lícito, leal y transparente, adecuado y no excesivo, y llevado a cabo únicamente en función de los fines legales preestabelecidos (art. 4.1). Ello implica que la medida que conlleve el tratamiento de datos personales debe responder a los siguientes presupuestos. a) Estar prevista en la ley, resultar necesaria, adecuada, útil, pertinente y proporcionada a los fines de la investigación o del enjuiciamiento de un concreto delito. Así, debe justificarse su pertinência en cuanto a los fines que se persiguen, y garantizarse que los datos em cuestión no son excesivos para lo que se investiga, ni que se conservarán más tiempo del necesario para los fines que se persiguen, es decir para culminar una investigación o el enjuiciamiento de un delito concreto contra una persona determinada, investigada o encausada. b) Ser objeto de información al sujeto, especialmente en lo relativo a sus derechos y a los cauces para su defensa, o para hacerlos valer com relación al caso concreto. c) Y, contar con fines específicos y legítimos, a determinar en el momento de la recopilación u obtención de los datos. En tal sentido, el art. 8 establece los presupuestos de la licitud del tratamiento de los datos, que son la necesidad en función de los fines de investigación o enjuiciamiento, y la fundamentación de su objetivo, de manera que los Estados deberán prever en sus ordenamientos al menos los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento. Ahora bien, si esta es la regla general, la Directiva también dispone diversos regímenes de excepciones al elenco de derechos que consagra, y que, no lo olvidemos, vienen referidos a un sospechoso, investigado o encausado en un proceso penal. Así, el principio rector es que los datos personales se recogen con fines determinados, explícitos y legítimos (art. 4.1), y que fuera del caso concreto debe primar la confidencialidad, impidiendo accesos no autorizados a los datos. Sin embargo, ello no obsta para que estos datos puedan ser usados para otros fines, siempre que no sean incompatibles con los relativos a la investigación y el enjuiciamiento. En este sentido, el art. 4.2 de la Directiva 2016/680, permite el tratamiento de los datos personales, para fines del art. 1.1 (investigación y enjuiciamiento) distintos de aquel para el que se recogieron, es decir para la investigación o enjuiciamiento de otros hechos delictivos atribuibles a la misma persona o a otra hasta el momento no investigada. Es decir, un tratamiento de los datos con el mismo fin pero em distinta causa penal. Y ello será posible si el responsable del tratamento está autorizado, y si es necesario y proporcional con ese otro fin o causa penal. Este es pues el régimen excepcional del principio de especialidad, o régimen de disponibilidad ampliada de la Directiva.* GONZÁLEZ CANO, Mª Isabel. *Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680.* Revista Brasileira de Direito Processual Penal. Porto Alegre, vol. 5, n. 3, p. 1331-1384, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.279. Disponível em: http://www.ibraspp.com.br/revista/index.php/RBDPP/article/view/279/188. Acesso em: 03/07/2021.

que, no artigo 588, bis, k, da LECRIM, estabelece as regras aplicáveis à destruição e conservação dos registros eletrônicos informáticos utilizados nas investigações[110], em complementação aos artigos 4, 1, *d, e* e *f,* e também ao artigo 5º da Diretiva 680.

Estes princípios orientadores de finalidade, especialidade e proporcionalidade condicionam a obtenção de dados pessoais e a sua consequente transferência e tratamento para fins criminais, constituindo, assim, os pressupostos habilitadores das medidas de investigação que afetam ou limitam o direito fundamental da proteção de dados pessoais (CANO, 2019).

3.3.1. A livre circulação dos dados recolhidos pelas autoridades competentes como resposta aos fins pretendidos pela cooperação judiciária penal

Aliado ao arcabouço jurídico e teórico aventado até o momento, cumpre anotar que a troca de informações entre as autoridades que compõe as forças de segurança é medida essencial de inteligência para o controle social da atividade criminosa, ainda mais em razão da velocidade com que os dados se propagam na sociedade de informação, elemento facilitador da prática delitiva.

A livre circulação de dados entre as autoridades das forças de segurança, incluindo o acesso a órgãos públicos, para fins de investigação criminal, é medida que integra a própria essência da atividade investigatória, que confere celeridade às investigações, visando a

---

[110] *Artículo 588 bis k. Destrucción de registros. 1. Una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Se conservará una copia bajo custodia del secretario judicial. 2. Se acordará la destrucción de las copias conservadas cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal. 3. Los tribunales dictarán las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción contemplada en los anteriores apartados.* Artigo 588 bis k. Destruição de registros. 1. Terminado o procedimento por resolução definitiva, será ordenado o apagamento e eliminação dos autos originais que possam constar dos sistemas eletrónico e informático utilizados na execução da medida. Uma cópia ficará sob custódia do escrivão. 2. A destruição das cópias preservadas será acordada depois de decorridos cinco anos desde a execução da pena ou quando o crime ou pena tenha sido prescrito ou a livre demissão tenha sido decretada ou a absolvição final tenha sido emitida em relação ao investigado, desde que na opinião do Tribunal não seja necessária a sua conservação. 3. Os tribunais expedirão as ordens cabíveis à Polícia Judiciária para proceder à destruição a que se referem os números anteriores (tradução livre). Lei Orgânica 13/2015, de 5 de outubro, que altera a Lei de Processo Penal para o reforço das garantias processuais e a regulamentação das medidas de investigação tecnológica. Disponível em: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725 Acesso em 10/07/2021.

obtenção dos dados e informações sobre os fatos com maior rapidez e, com isto, preservando as provas e evidências do crime.

Clara se apresenta, assim, a necessidade da autoridade pública que investiga a persecução de um crime ter acesso a dados, essencial para o deslinde da investigação, que deverá, todavia, mantê-las sob sigilo.

De acordo com Gonzales Cano (2019), a Diretiva 680 responde a uma série de princípios gerais, que partem das linhas de atuação do Programa de Estocolmo[111] assim como dos critérios já adotados pelo TJUE na matéria. Esta nova regulação sobre o tratamento e análise de dados pessoais em causas penais, que já transcende o âmbito transfronteiriço e parece optar pela aproximação normativa visando facilitar a cooperação judiciária penal, tem suas bases nos primeiros trabalhos da Comissão Europeia (2009)[112], e que define uma política

---

[111] Disponível (PT): https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:pt:PDF Acesso em 11/07/2021.

[112] Sobre o Programa de Estocolmo, pertinente esclarecer que: *In this context, in order to strengthen prevention in the fight against terrorism, the Union provided, inter alia, the development of common rules on the protection of personal data. Thus, in the well-known multiannual programmes, such as the Hague Programme (2005-2009), its priorities include effectively combating terrorism and its causes. It contained proposals aimed at strengthening cooperation between the law enforcement authorities of the Member States, by improving the exchange of information between the various law enforcement and judicial authorities, as well as the objective of developing a European data protection framework. This objective was also reaffirmed in the Stockholm Programme (2010-2014), which already established the basic informing principles regarding the processing of personal data. At the same time, the European Agenda on Security (2015-2019), reiterates the need to achieve effective action in the framework of judicial cooperation, insists on the need to formulate measures that serve to address the main challenges facing the Union in the fight against terrorism and other forms of organized crime.* Ou seja: Neste contexto, a fim de reforçar a prevenção na luta contra o terrorismo, a União proporcionou, nomeadamente, o desenvolvimento de regras comuns em matéria de proteção de dados pessoais. Assim, nos conhecidos programas plurianuais, como o Programa de Haia (2005-2009), as suas prioridades incluem o combate eficaz ao terrorismo e às suas causas. Continha propostas destinadas a reforçar a cooperação entre as autoridades de aplicação da lei dos Estados-Membros, melhorando o intercâmbio de informações entre as várias autoridades de aplicação da lei e judiciárias, bem como o objetivo de desenvolver um quadro europeu de proteção de dados. Este objetivo foi também reafirmado no Programa de Estocolmo (2010-2014), que já estabeleceu os princípios básicos de informação relativos ao tratamento de dados pessoais. Paralelamente, a Agenda Europeia para a Segurança (2015-2019), reitera a necessidade de uma ação efetiva no âmbito da cooperação judiciária, e insiste na necessidade de formular medidas que sirvam para dar resposta aos principais desafios que a União enfrenta na luta contra o terrorismo e outras formas de crime organizado. E ainda: *Stockholm Programme: An open and secure Europe serving and protecting citizens, OJ of the EU No. C 115/1, 4 May 2010: "The Union must therefore respond to the challenge posed by the increasing exchange of citizens' personal data and the need to ensure the protection of privacy. The Union must secure a comprehensive strategy to protect citizens' data within the EU and in its relations with other countries. In those circumstances, it should promote the application of the principles set out in relevant Union instruments on data protection and the 1981 Council of Europe Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data as well as promoting accession to that Convention".* Ou seja: Programa de Estocolmo: Uma Europa aberta e segura que sirva e proteja os cidadãos, JO da UE n.º C 115/1, de 4 de maio de 2010: "A União deve, pois, responder ao desafio colocado pelo aumento do intercâmbio dos dados pessoais e à necessidade de assegurar a proteção da vida privada. A União deve assegurar uma estratégia global de proteção dos dados no âmbito da União e no âmbito das suas relações com países terceiros. Neste contexto, a União deverá promover a aplicação dos princípios enunciados nos instrumentos pertinentes da União em matéria de proteção de dados e na Convenção do Conselho da Europa de 1981 para a proteção das pessoas relativamente ao tratamento automatizado dos dados de carácter pessoal, bem como a adesão a esta convenção (tradução livre). DOMINGO, Maria Belén Sanchez (2019). *The protection of personal data in the field of judicial cooperation in criminal*

mais coerente e integradora do direito fundamental à proteção de dados pessoais em todos os contextos. Tais trabalhos resultaram nas propostas legislativas de 2012, que tramitaram até 2016 e, então, deram origem ao Regulamento 679 e a Diretiva 680. Por sua vez, o TJUE e suas linhas mestras sobre o princípio da legalidade e da proporcionalidade tiveram grande influência na elaboração da Diretiva 680, embora sem ignorar esta orientação de política criminal centrada no princípio da disponibilidade dos dados pessoais para fins criminais, buscando sempre conciliar um processo mais eficaz de investigação e repressão ao crime, e utilizando-se dos avanços tecnológicos, com respeito aos direitos fundamentais do titular dos dados pessoais sendo ele suspeito, investigado ou processado.

Ainda no que toca aos princípios adotados no tratamento de dados pessoais, desperta grande interesse a abordagem trazida pela mencionada autora, em referência aos avanços e desafios enfrentados pela Diretiva 680, no que tange à transferência e tratamento de dados pessoais no processo penal. Tratando sobre a disponibilidade e livre circulação de tais dados, leciona que

> A livre circulação de dados entre as autoridades competentes na investigação e repressão do crime deve ser facilitada no domínio da cooperação penal e como instrumento de criação e reforço do espaço europeu de liberdade, segurança e justiça, embora sempre num quadro de protecção sólida e consistente e de garantias adequadas e eficazes dos titulares dos dados pessoais. É, pois, claro que a própria eficácia da cooperação judiciária penal depende da criação prévia e da garantia de um nível uniforme e equivalente de protecção dos dados pessoais e do seu tratamento em todos os Estados-Membros.
>
> Embora seja verdade que o novo Regulamento Geral 2016/679, sobre proteção de dados, estabelece as regras gerais para a proteção das pessoas singulares em relação ao tratamento dos seus dados pessoais e para garantir a livre circulação de dados pessoais na UE, é também imprescindível a elaboração de um conjunto de normas específicas sobre proteção de dados e livre circulação dos mesmos no domínio da cooperação penal a que se refere o art. 16 do TUE, ou seja, para investigação e processamento de crimes pelas autoridades competentes (Juízes, Procuradores, Polícia) e, em geral, por qualquer órgão ou entidade encarregado do tratamento desses dados para tais fins.
>
> Recorde-se que o trabalho normativo da UE em matéria de protecção de dados teve início com a Directiva 95/46/CE, procurando reforçar a livre circulação de dados pessoais no âmbito do mercado único comunitário, prevendo para isso um quadro de protecção alargado aos dados contidos em suporte informático ou em qualquer tipo de suporte ou ficheiro idóneo ou idóneo ao seu tratamento. A partir daí, os avanços tecnológicos, por um lado,

---

matters: special reference to Directive (EU) 2016/680 of the European Parliament and of the Council. Unio - EU Law Journal. Vol. 5, nº 2 (2019), p. 92-102. Disponível em: https://revistas.uminho.pt/index.php/unio/article/view/2295/2410 e em: https://revistas.uminho.pt/index.php/unio/article/view/2295. Acesso em: 11/07/2021.

e, por outro, a necessidade de obtenção e tratamento de dados pessoais no âmbito da cooperação judiciária penal, deram origem, como afirma GALÁN MUÑOZ, à dupla via da proteção de dados pessoais, ou seja, via de garantia geral, de forma a preservar os direitos de informação, acesso, retificação, cancelamento e oposição face à livre circulação de dados pessoais; e, a via excepcional ou especial, aquela relativa à repressão, investigação e repressão do crime, que requer tratamento especial no que se refere aos meios de investigação e obtenção de fontes de prova pré-estabelecidas e, em última instância, de acusação. a imposição de consequências jurídicas sancionatórias de natureza penal.

Embora certamente os primeiros passos normativos foram dados no domínio geral e garantidor da protecção de dados pessoais num mercado único com livre circulação de serviços, bens e pessoas, o desenvolvimento legislativo mais importante ocorreu efectivamente no domínio da utilização de dados pessoais como material de investigação e pré-constituição de prova de acusação, como vimos nas páginas anteriores.

Trata-se, portanto, de garantir o mesmo nível de proteção neste âmbito da cooperação judiciária penal, normas harmonizadas e aproximação normativa que não devam contribuir para o enfraquecimento dos padrões de proteção dos Estados. Muito pelo contrário, os Estados, a partir do mínimo estabelecido, e independentemente da nacionalidade ou residência do titular dos dados (considerando 17 da Diretiva 2016/680), de que seja pessoa identificada ou identificável e de que se trate ou não de tratamento automatizado de dados (neutralidade tecnológica para evitar o risco de violação do padrão de proteção, de acordo com o considerando 18), poderão logicamente ter maiores garantias em seus ordenamentos jurídicos. Do mesmo modo, as normas processuais penais dos Estados-Membros podem conter as suas próprias prescrições sobre a obtenção e tratamento de dados pessoais em processos penais, bem como sobre dados de identificação, dados genéticos, relativos à saúde, económicos ou financeiros[113] (tradução livre).

---

[113] *La libre circulación de datos entre las autoridades competentes en la investigación y enjuiciamiento del delito, debe ser facilitada en el ámbito de la cooperación penal y como instrumento para la creación y fortalecimiento del espacio europeo de libertad, seguridad y justicia, aunque siempre en un marco sólido y coherente de protección y de garantías adecuadas y efectivas de los titulares de los datos personales. Es pues evidente que la propia eficacia de la cooperación judicial penal depende de que previamente se cree y asegure en todos los Estados miembros, un nivel uniforme y equivalente de protección de los datos personales y de su tratamiento. Si bien es cierto que el nuevo Reglamento general 2016/67924, de protección de datos, establece las normas generales para la protección de las personas físicas en relación con el tratamiento de sus datos personales, y para garantizar la libre circulación de datos personales en la UE, también lo es que resulta imprescindible la elaboración de una serie de normas específicas sobre protección de datos y libre circulación de los mismos en el ámbito de la cooperación penal a la que se refiere el art. 16 del TUE, es decir, en orden a la investigación y enjuiciamiento de delitos por autoridades competentes (Jueces, Fiscales, Policía), y en general por todo organismo o entidad que tenga encomendado el tratamento de estos datos a tales fines. Téngase presente que la labor normativa de la UE en materia de protección de datos comenzó con la Directiva 1995/46/CE, intentando reforzar la libre circulación de datos personales en el marco del mercado único comunitario25, dispensando para ello un marco de protección que se extendió a datos contenidos en soporte informático o en cualquier tipo de soporte o archivo adecuado o idóneo para su tratamiento. A partir de ahí, los avances tecnológicos por una parte y, por otra, la necesidad de la obtención y tratamiento de los datos personales en el ámbito de la cooperación judicial penal, han dado lugar, como afirma GALÁN MUÑOZ, a la doble vía de protección de los datos de carácter personal, es decir, la vía garantista general, en orden a preservar ante la libre circulación de datos personales, los derechos de información, acceso, rectificación, cancelación y oposición; y, la vía excepcional o especial, la relacionada com la represión, la investigación y el enjuiciamiento del delito, que requiere un tratamiento especial26 en cuanto se trata de medios de investigación y obtención de fuentes probatorias preconstituidas y, en definitiva, de prueba de cargo en orden a la imposición de consecuencias jurídicas sancionadoras de naturaleza penal. Aunque ciertamente los primeros pasos*

Neste viés, digno de nota, por fim, é ainda a disposição trazida pela Diretiva 680 possibilitando as tranferências de dados pela União à Interpol – Organização Internacional da Polícia Criminal, organização de que todos os Estados Membros fazem parte, mediante a promoção de um eficaz intercâmbio de dados pessoais e assegurando, ao mesmo tempo, o respeito pelos direitos e liberdades fundamentais no que se refere ao tratamento dos dados pessoais. No exercício das suas atribuições, a Interpol recebe, conserva e divulga dados pessoais, a fim de auxiliar as autoridades competentes na prevenção e no combate à criminalidade internacional (considerando 25).

3.4. DIFERENTES CATEGORIAS DE TITULARES DE DADOS E HIPÓTESES AUTORIZATIVAS PARA O TRATAMENTO DE DADOS

Inovação trazida pela lei que rege o tratamento de dados realizado pelas forças de segurança na seara criminal diz respeito à cisão dos titulares de dados em categorias distintas, regra esta não experimentada pela legislação antecedente.

Ao contrário do Regulamento 679, que nada menciona a este respeito, a Diretiva 680 (artigo 6º) distingue os titulares de dados em diferentes categorias, de acordo com o papel que desempenham na seara criminal: a) suspeitos da prática de crime ou em potencial; b) condenados; c) vítimas (reais ou potenciais); d) terceiros envolvidos na infração penal (testemunhas, informantes ou contactos dos suspeitos ou condenados).

---

normativos se dieron en el ámbito general y garantista de la protección de datos personales em un mercado único con libre circulación de servicios, bienes y personas, realmente el desarrollo legislativo más importante se ha producido en el ámbito de la utilización de datos personales como material de investigación y preconstitución probatoria de cargo, tal y como hemos visto en páginas anteriores. Se trata pues de garantizar un mismo nivel de protección em este ámbito de la cooperación judicial penal, normas armonizadas y aproximación normativa que no deben contribuir a debilitar los estándares de protección de los Estados. Muy al contrario, los Estados, partiendo de los mínimos que se establezcan, e independientemente de la nacionalidade o residencia del titular de los datos (Considerando 17 de la Directiva 2016/680), de que sea persona identificada o identificable, y de que se trate de tratamiento automatizado o no de los datos (neutralidad tecnológica para evitar el riesgo de elusión del estándar de protección, con arreglo al Considerando 18), podrán lógicamente disponer mayores garantias en sus ordenamientos. Igualmente, las normas procesales penales de los Estados miembros podrán contener sus propias prescripciones sobre obtención y tratamiento de datos personales en causas penales, así como sobre identificación, datos genéticos, relativos a la salud, económicos o financeiros. GONZÁLEZ CANO, Mª Isabel. *Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680.* Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1331-1384, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.279. Disponível em: http://www.ibraspp.com.br/revista/index.php/RBDPP/article/view/279/188. Acesso em: 03/07/2021.

O tratamento de dados pessoais nos domínios da cooperação judiciária em matéria penal e da cooperação policial implica necessariamente o tratamento de dados pessoais relativos a categorias diferentes de titulares de dados. Importa, portanto, estabelecer, se aplicável e tanto quanto possível, uma clara distinção entre dados pessoais de diferentes categorias de titulares de dados, tais como suspeitos, pessoas condenadas por um crime, vítimas e terceiros, designadamente testemunhas, pessoas que detenham informações ou contactos úteis, e os cúmplices de pessoas suspeitas ou condenadas, o que não impede. Tal não atinge, todavia, o direito à presunção de inocência, tal como garantido pela Carta e pela Convenção Europeia dos Direitos do Homem, de acordo com a interpretação da jurisprudência do Tribunal de Justiça e do Tribunal Europeu dos Direitos do Homem, respetivamente (considerando 31).

No que respeita ao fundamento legal para o tratamento dos dados pessoais, também flagrante divergência se verifica entre ambos os diplomas legais.

O Regulamento 679 (artigo 6º, 1, *a* a *f*) estabelece seis bases legais para o tratamento de dados pessoais (consentimento, execução de contrato, cumprimento de obrigação jurídica, defesa de interesses vitais do titular ou outrém, exercício de função de interesse público ou de autoridade pública pelo responsável e, por fim, legítimo interesse do responsável pelo tratamento ou de terceiro). Autoriza, ainda, aos Estados-Membros, a aplicação de disposições mais específicas e outras medidas destinadas a garantir a licitude e lealdade do tratamento (artigo 6º, item 2, do GDPR), inclusive para situações específicas do tratamento, conforme disposto no capítulo IX.

A lei que regula o tratamento de dados realizado pelas forças de segurança para fins penais, por sua vez, não prevê outro fundamento legal para o tratamento de dados, senão um: a lei.

Assim, na Diretiva 680, a base legal para o tratamento dos dados é o direito da União ou dos Estados-Membros (artigo 8º). Tal tratamento só é lícito se e na medida em que for necessário para o exercício de uma atribuição pela autoridade competente para os efeitos previstos no artigo 1º, nº 1, e tiver por base o direito da União ou de um Estado-Membro (item 1). Ainda, o direito de um Estado-Membro que rege o tratamento no âmbito da Diretiva 680 deve especificar, pelo menos, os objetivos do tratamento, os dados pessoais a tratar e as finalidades do tratamento (item 2).

Para ser lícito, o tratamento de dados pessoais, nos termos da Diretiva 680, deverá ser necessário para a execução de uma missão de interesse público por uma autoridade competente com base no direito da União ou dos Estados-Membros para efeitos de prevenção,

investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Estas funções deverão abranger a proteção dos interesses vitais do titular dos dados (considerando 35).

Tal previsão já tinha lugar na Carta dos Direitos Fundamentais da União Europeia (artigo 8º), que prevê que o tratamento de dados pessoais será realizado, dentre outros requisitos, com base no consentimento do sujeito ou, se for caso disso, sob outra base legal e legítima, como repressão, investigação e repressão do crime[114].

O exercício das funções de prevenção, investigação, detecção ou repressão de infrações penais conferidas institucionalmente por lei às autoridades competentes permite-lhes exigir que as pessoas singulares cumpram o que lhes é solicitado. Neste caso, o consentimento do titular dos dados, na acepção do Regulamento (UE) 2016/679, não deverá constituir a fundamento jurídico do tratamento de dados pessoais pelas autoridades competentes. Caso seja obrigado a cumprir uma obrigação legal, o titular dos dados não tem verdadeira liberdade de escolha, pelo que a sua reação não poderá ser considerada uma livre manifestação da sua vontade. Tal não deverá obstar a que os Estados-Membros prevejam, por lei, a possibilidade de o titular dos dados consentir que os seus dados pessoais sejam tratados para as finalidades previstas na presente diretiva, nomeadamente que sejam efetuados testes de ADN no âmbito de investigações penais ou controlada a sua localização por meio de etiquetas eletrônicas, tendo em vista a execução de sanções penais (considerando 35).

Sobre estes aspectos da Diretiva 680, Sajfert e Quintel mencionam que

> Além disso, o artigo 6º introduz uma obrigação específica para os responsáveis pelo tratamento abrangidos pela Diretiva estabelecerem uma distinção clara entre dados pessoais de diferentes categorias de titulares de dados (suspeitos, condenados, vítimas, testemunhas). As autoridades de polícia e justiça criminal têm, portanto, de categorizar e organizar adequadamente as suas bases de dados, de acordo com a jurisprudência do TEDH. Outro princípio específico da Diretiva é estabelecido no artigo 7º, que exige que os dados pessoais baseados em fatos sejam distinguidos dos dados pessoais baseados na apreciação pessoal. Além disso, a qualidade, exatidão, integridade e confiabilidade dos dados pessoais devem ser

[114] Artigo 8º Proteção de dados pessoais 1. Todas as pessoas tem direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas tem o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. Carta dos Direitos Fundamentais da União Europeia. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em 10/07/2021.

> verificadas e devidamente indicadas antes que a troca de dados com outras autoridades possa ocorrer.
>
> No que diz respeito ao fundamento da legalidade do tratamento, a Diretiva estabelece apenas um fundamento jurídico no artigo 8º (se necessário para o desempenho de uma tarefa desempenhada por uma autoridade competente para efeitos da Diretiva e com base no direito da União ou do Estado-Membro), enquanto o artigo 6º do RGPD prevê seis bases jurídicas diferentes. Obviamente, o legislador reconheceu que as autoridades de polícia e justiça criminal só podem realizar tarefas permitidas por lei e não processar dados para efeitos da Diretiva com base no consentimento, nas obrigações contratuais ou no interesse legítimo do responsável pelo tratamento[115] (tradução livre).

No mesmo viés, por sua vez, Salami Emmanuel Akintunde (2017), mencionando sobre a distinção entre dados pertencentes a suspeitos, condenados, vítimas e outras partes relevantes para o crime, como testemunhas, trazida pelo artigo 6º da Diretiva 680, lembra que esta é uma nova disposição não existente na Diretiva 95/46/CE, bem como que o grupo de trabalho recomendou que o tratamento de dados pessoais de não suspeitos fosse tratado com cautela e que sejam seguidas condições e salvaguardas específicas para evitar o tratamento indevido de pessoas não envolvidas no crime.

Por fim, quanto à novidade contida no artigo 6º, aponta que a distinção é diversa daquela contida no artigo 7º da mesma diretiva, que estabelece uma diferenciação entre os dados obtidos a partir de fatos e os obtidos com base em avaliações pessoais. Tal disposição também se afigura louvável, vez que distingue uma informação claramente correta dedutível de um conjunto de fatos de uma que possivelmente poderia ser tingida de incorreção, como resultado de uma avaliação pessoal sobre um conjunto de fatos.

---

115 *Furthermore, Article 6 introduces a specific obligation for controllers under the Directive to establish a clear distinction between personal data of different categories of data subjects (suspects, convicts, victims, witnesses). The LEAs therefore have to neatly tag and properly organise their databases, in line with the jurisprudence of the ECtHR[18]. Another principle specific to the Directive is laid down in Article 7, requiring personal data based on facts to be distinguished from personal data based on personal assessment. Additionally, the quality, accuracy, completeness and reliability of personal data have to be verified and properly indicated before data exchanges with other authorities may take place. 19 As regards the basis for the lawfulness of processing, the Directive lays down only one legal ground in Article 8 (if necessary for the performance of a task carried out by a competent authority for the purposes of the Directive and based on Union or Member State law), while Article 6 of the GDPR provides for six different legal bases. Obviously, the legislator recognized that LEAs may only carry out tasks permitted by law, and not process data for the purposes of the Directive on the basis of consent, contractual obligations or the controller's legitimate interest.* SAJFERT, Juraj e QUINTEL, Teresa, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities* (December 1, 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873. Acesso em 25/06/2021.

3.5. DIREITOS DO TITULAR

Também na Diretiva 680 os direitos conferidos aos titulares de dados vem descritos no Capítulo III.

Conforme lecionam Sajfert e Quintel (2019), em comparação aos artigos mais 'generalistas' do Capítulo III do Regulamento 679, a abordagem em relação aos direitos do titular dos dados e suas possíveis limitações ao abrigo do Capítulo III da Diretiva 680 é definida com mais detalhes, a fim de adaptar os meios de tratamento de dados pessoais às necessidades das autoridades de polícia e justiça criminal. Permanece o mesmo o conjunto básico de direitos (informação, acesso, retificação, apagamento, restrição de tratamento), que podem ser exercidos pelos titulares de dados junto ao responsável pelo tratamento, entregando-lhes diretamente seus pedidos (para acesso e posterior retificação, eliminação e restrição do tratamento)[116].

Há, todavia, outros pontos de convergências e divergências entre a Diretiva e o Regulamento dignas de nota, podendo-se relacionar as que seguem.

I) O artigo que inicia o Capítulo III (artigo 12 – numeração do dispositivo e do capítulo coincidentes em ambos os diplomas legais) é intitulado, na Diretiva 680, de 'Comunicação e regras de exercício dos direitos dos titulares dos dados' e, no Regulamento 679, de 'Transparência e regras de exercício dos direitos dos titulares dos dados'. A ausência de referência à transparência das informações dos titulares na Diretiva 680 (embora tal, como já mencionado, venha descrito na parte introdutória da lei – considerando 26), diversamente do que dispõe o GDPR, aliado ao descrito até o momento, leva a crer que, na lei que regulamenta o tratamento de dados realizado pelas forças de segurança, a transparência se coloca de certa

---

116 *Previously, the 2008 Framework Decision, in its Articles 17(1)(a) and 18(1) allowed Member States to choose whether they allow data subjects to either directly assert their rights against the controller or through the national supervisory authority as intermediary. Similar deference to Member State rules is provided for under the data protection rules applicable to the Second-generation Schengen Information System (SIS II), in particular under Article 41 of the SIS II Regulation and Article 58 of the SIS II Decision.* Ou seja: Anteriormente, a Decisão-Quadro de 2008, nos seus artigos 17.º, n.º 1, alínea a), e 18.º, n.º 1, permitia aos Estados-Membros escolherem se autorizam os titulares dos dados a fazer valer os seus direitos diretamente contra o responsável pelo tratamento ou por intermédio da autoridade de controle nacional. Uma deferência semelhante em relação às regras dos Estados-Membros está prevista nas regras de proteção de dados aplicáveis ao Sistema de Informação de Schengen de segunda geração (SIS II), em particular nos termos do artigo 41.º do Regulamento SIS II e do artigo 58.º da Decisão SIS II (tradução livre). SAJFERT, Juraj e QUINTEL, Teresa, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities* (December 1, 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873. Acesso em 25/06/2021.

forma mitigada, imprescindível ao exercício das atividades peculiares das forças de segurança na área criminal.

II) O Regulamento 679 dispõe sobre as informações a fornecer aos titulares de dados (artigo 12) quando estas são ou não recolhidas junto aos mesmos (artigos 13 e 14), o direito de acesso (artigo 15), retificação (artigo 16), apagamento (artigo 17), limitação do tratamento pelo responsável (artigo 18) e notificação do titular sobre estas 3 últimas situações (artigo 19), portabilidade de dados (artigo 20), direito de oposição (artigo 21), direito à não ficar sujeito a decisões individuais automatizadas (artigo 22) e limitação ao alcance das obrigações e direitos descritos na lei (artigo 23).

A Diretiva 680 orienta sobre as informações a facultar ou a fornecer aos titulares de dados (artigos 12 e 13), prevê o direito de acesso (artigo 14) e, em contrapartida, a limitação deste direito de acesso como restrição a ser determinada pelo responsável pelo tratamento (artigo 15), o direito a retificação, apagamento e limitação do tratamento (artigo 16), o direito a notificação à autoridade de origem no caso de retificação dos dados inexatos (artigo 16, item 5) e dos destinatários dos dados no caso de limitação, apagamento ou retificação (artigo 16, item 6).

Em suma, diversamente do Regulamento 679, a Diretiva 680 não traz previsão do direito de portabilidade dos dados e nem do direito de oposição a ser exercido pelo titular de dados; nela está contido, ainda, a possibilidade do responsável pelo tratamento limitar as informações a serem fornecidas ao titular dos dados (artigo 13), bem como o seu direito de acesso (artigo 15), de retificação e de apagamento (artigo 16), sendo que o Regulamento dispõe a este respeito somente de forma genérica (artigo 23).

III) Assim sendo, com relação às informações a serem fornecidas aos titulares dos dados (artigo 12 e 13), a Diretiva 680 prevê que tal deve ser feita de forma simples, inteligível e de fácil acesso, através dos meios adequados, em geral na mesma forma que o solicitado (artigo 12, 1). Tais disposições visam garantir o efetivo esclarecimento ao titular sobre o tratamento de dados realizado.

Ainda, que o responsável deverá facilitar o exercício dos direitos do titular dos dados (artigo 12, 2) e a este informar, por escrito e sem demora injustificada, sobre o seguimento dado ao seu pedido (artigo 12, 3), não prevendo prazos nem o procedimento para tanto.

Por sua vez, o Regulamento 679 dispõe, além de outros requisitos (em especial quando dirigido a crianças), que as informações sobre o tratamento (artigo 12) devem ser feitas ao titular de forma transparente (item 1), por escrito ou outros meios, inclusive oralmente, caso o titular assim solicitar. O exercício dos direitos será sempre facilitado pelo responsável (item 2), que só poderá negar seguimento ao pedido do titular se não estiver em condições de identificá-lo (artigo 11, 2). O Regulamento prevê, também, que o responsável deve informar ao titular sobre as medidas tomadas, descrevendo a forma e prazos para tanto (artigo 12, 3), bem como os prazos e a forma como deverá proceder nas hipóteses em que não der seguimento ao pedido apresentado pelo titular, quando deverá expor as razões que o motivaram e informar o titular sobre a possibilidade de reclamar a autoridade de controle ou buscar a via judicial (artigo 12, 4).

IV) Consta ainda do Regulamento 679 que o responsável pelo tratamento deve tomar as medidas 'adequadas' para fornecer ao titular informações sobre os dados tratados, diferenciando as informações a facultar ao titular em dois dispositivos diferentes (artigos 13 e 14) em função da coleta ter sido realizada ou não junto ao titular.

Na Diretiva 680, o responsável pelo tratamento deve tomar as medidas 'razoáveis' para fornecer ao titular informações sobre os dados tratados recolhidos junto ao titular a que se refere o artigo 13 (artigo 12). Neste diploma legal, não há diferenciação no tratamento conferido aos dados coletados junto ao titular em relação aos que foram recolhidos sem o consentimento deste mesmo porque, dado a natureza das atividades desenvolvidas pelas forças de segurança, não raro tal coleta ocorre sem a anuência do titular.

V) Quanto ao prazo para o fornecimento de informações ao titular, também ao contrário do Regulamento 679, que estabelece que, já no momento da recolha, o responsável pelo tratamento deve facultar informações ao titular dos dados (artigo 13, item 1), a Diretiva 680 não estabelece o momento adequado para o fornecimento das informações ao titular de dados.

VI) A Diretiva 680 prevê que o responsável pelo tratamento faculte ao titular de dados, 'em determinados casos', informações adicionais (artigo 13, item 2), como o fundamento jurídico e prazo de conservação e, se for o caso, as categorias de destinatários, inclusive em países terceiros e organizações internacionais, como também o fornecimento de informações adicionais, especialmente se forem recolhidos sem o conhecimento do titular. Tal orientação

não vem inicialmente descrita como informações a facultar/fornecer ao titular dos dados no artigo 13, item 1, diversamente do contido no Regulamento 679, que não faz qualquer diferenciação neste aspecto.

Referido dispositivo prevê também a possibilidade de se fornecer ao titular dos dados informações referentes aos responsáveis pelo tratamento, com o que há que se ter cautela, considerando o direito a proteção dos dados pessoais também do próprio responsável pelo tratamento. Ademais, há que se considerar que, na maioria das vezes, os titulares dos dados cujo tratamento é albergado por esta diretiva tratam-se de suspeitos ou condenados, sendo mais seguro para a vida dos responsáveis pelo tratamento estabelecer-se uma forma de contato impessoal com os titulares.

VII) A Diretiva 680 prevê, também (artigo 13, item 3), a possibilidade de adiamento, limitação ou não prestação das informações contidas no item 2 do artigo 13 aos titulares, ora mencionadas, a fim de: a) evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais; b) evitar prejudicar a prevenção, detecção, investigação ou repressão de infrações penais ou a execução de sanções penais; c) proteger a segurança pública; d) Proteger a segurança nacional; e) proteger os direitos e as liberdades de terceiros (artigo 13, item 3). Assim sendo, mediante lei, determinadas as categorias de tratamento poderão ser suscetíveis de serem abrangidas, total ou parcialmente, por uma das limitações contidas no artigo 13, item 3 acima descritas (artigo 13, item 4), não se verificando correspondência no Regulamento 679 a este respeito.

Neste ponto, parece clara a intenção da Diretiva de preservar o desempenho das atividades peculiares desenvolvidas pelas forças de segurança que, via de regra, necessitam de sigilo para a eluscidação dos delitos e consequente contenção da criminalidade.

Já o Regulamento 679, por sua vez, dentre as informações a serem fornecidas ao titular (artigo 13), além das coincidentes com a Diretiva, prevê que a ele seja informado o fundamento jurídico e especificado o legítimo interesse do responsável pelo tratamento, a justificar o tratamento de dados (item 1, *c* e *d*), caso tais bases legais sejam utilizadas, bem como sobre a eventual intenção do responsável pelo tratamento de transferir dados para um país terceiro ou organização internacional, a existência ou não de decisão de adequação ou de garantias adequadas e o meio de obter cópia destas (item 1, *f*). O Regulamento 679 dispõe, ainda, que ao titular de dados será informado sobre a existência de decisões automatizadas, incluindo a formação de perfis (item 2, *f*), bem como que, quando houver a intenção de

tratamento posterior dos dados para finalidade diversa da recolha, antes deste tratamento, o responsável deverá lhe fornecer informações sobre este fim e quaisquer outras pertinentes (item 3) e, ainda, que não se aplicam o disposto nos itens 1, 2 e 3 se o titular dos dados já tiver conhecimento das informações.

VIII) Como antes mencionado, o Regulamento 679 prevê diversas informações a facultar quando os dados pessoais não são recolhidos junto do titular (artigo 14). Há, também, previsão de limitação do exercício de tal direito (item 5, *a* a *d*), porém, em raras situações e muito diversas das contidas na Diretiva 680 (artigo 13, item 3).

Já a Diretiva 680, como também já dito, não diferencia as informações a facultar quando os dados pessoais são ou não recolhidos junto ao titular, considerando tal hipótese somente no artigo 13, item 2, *d*, quando dispõe que poderão ser fornecidas 'informações adicionais, especialmente se os dados pessoais forem colhidos sem o consentimento do seu titular'.

IX) Quanto ao direito a informações sobre destinatários a quem os dados foram ou eventualmente poderão ser divulgados ou transferidos, a Diretiva 680 não traz qualquer previsão a este respeito, diversamente do Regulamento 679, que prevê o acesso do titular à informações sobre destinatários ou categorias de destinatários a que os dados foram ou venham a ser divulgados futuramente (artigo 15, item 1, *c*).

X) A Diretiva 680 prevê também que ao titular dos dados será informado sobre as finalidades e o fundamento jurídico do tratamento (artigo 14, *a*), bem como os contactos da autoridade de controle (artigo 14, *f*) e, ainda, que ele será comunicado sobre os dados pessoais sujeitos a tratamento (artigo 14, *g*). Além das previsões coincidentes, o Regulamento prevê também a informação ao titular sobre as garantias adequadas, em caso de transferência internacional de dados (artigo 15, item 2), bem como que o responsável pelo tratamento fornecerá ao titular uma cópia dos dados pessoais em fase de tratamento (artigo 15, item 3), sem prejuízo dos direitos e as liberdades de terceiros, disposições estas não contidas na Diretiva.

Assim, as pessoas singulares deverão ter o direito de aceder aos dados recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de tomar conhecimento do tratamento e verificar a sua licitude. Por conseguinte, cada titular de dados deverá ter o direito de ser informado das finalidades a que se destina o tratamento dos

seus dados, da sua duração e de quem são os destinatários, inclusive em países terceiros. Nos casos em que essa comunicação inclua informações relativas à origem dos dados pessoais, tais informações não deverão revelar a identidade das pessoas singulares, em especial de fontes confidenciais. Para que esse direito seja respeitado, basta que o titular dos dados esteja na posse de um resumo completo desses dados num formulário inteligível, ou seja, um formulário que permita que o titular dos dados tome conhecimento desses dados e verifique a sua exatidão e o seu tratamento em conformidade com a presente diretiva, de modo a que possa exercer os direitos que esta lhe confere. Esse resumo poderá ser concedido por via de uma cópia dos dados pessoais sujeitos a tratamento (considerando 43).

XI) Nos mesmos moldes já referidos anteriormente no tocante às informações a facultar ao titular de dados (artigo 13, 3), outro dispositivo da Diretiva 680 dispõe que o responsável pelo tratamento pode limitar (artigo 15, 1) o direito de acesso do titular dos dados insculpidos no artigo 14, total ou parcialmente, quando necessário para: a) evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais; b) evitar prejudicar a prevenção, detecção, investigação ou repressão de infrações penais ou a execução de sanções penais; c) proteger a segurança pública; d) proteger a segurança nacional; e) proteger os direitos e as liberdades de terceiros.

Desta forma, os Estados-Membros poderão adotar medidas legislativas que visem atrasar, limitar ou recusar a informação prestada a titulares de dados ou restringir, total ou parcialmente, o acesso aos dados pessoais que lhes digam respeito, desde que tal constitua uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos da pessoa singular em causa, para não prejudicar os inquéritos, investigações ou procedimentos oficiais ou legais, procurar não prejudicar a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais, salvaguardar a segurança pública ou a segurança nacional ou, ainda, proteger os direitos e as liberdades de terceiros. O responsável pelo tratamento deverá avaliar, através de uma análise concreta de cada caso individualmente, se o direito de acesso deverá ser total ou parcialmente restringido (considerando 44).

O responsável pelo tratamento deverá informar ao titular dos dados sobre os casos e motivos que ensejaram sua decisão de limitação do acesso (artigo 15, item 3), disponibilizando tal informação também às autoridades de controle (item 4), bem como do

direito que assiste ao titular de apresentar reclamação à autoridade de controle ou de intentar uma ação judicial (item 3).

Todavia, o responsável pelo tratamento poderá omitir a informação de limitação ou recusa ao direito de acesso, bem como os motivos que a ensejaram (artigo 15, item 3), caso a sua prestação possa prejudicar uma das finalidades enunciadas no item 1 do artigo 15, acima descritas.

Assim, caso o responsável pelo tratamento recuse ao titular dos dados o direito à informação, o acesso aos dados pessoais ou a sua retificação ou apagamento ou a limitação do tratamento, o titular dos dados deverá ter o direito de solicitar que a autoridade nacional de controle verifique a licitude do tratamento. O titular dos dados deverá ser informado desse direito. Quando a autoridade de controle agir em nome do titular dos dados deverá, pelo menos, informá-lo de que foram realizadas todas as verificações ou revisões necessárias. A autoridade de controle deverá também informar o titular de dados do seu direito de intentar ação judicial (considerando 48).

Diferentemente da Diretiva 680, o Regulamento 679 não trata das limitações de cada direito em um artigo particular, referente a cada direito em seu artigo correspondente, mas de forma geral, no artigo 23, referindo-se a todos os direitos conferidos nos seus artigos de 12 a 22, 34 e 5º, quando menciona sobre limitações ao alcance das obrigações e direitos contidos na lei.

XII) A Diretiva 680 (artigo 16, 1 e 2) prevê o direito de retificação e apagamento dos dados pessoais em hipóteses semelhantes ao Regulamento 679 (dados sensíveis e ofensa aos princípios e bases legais), também aqui fixando limitações a estes direitos.

Assim, em vez de proceder ao apagamento, o responsável poderá limitar o tratamento (artigo 16, item 3) caso o titular conteste a exatidão dos dados pessoais e essa não possa ser apurada (o responsável pelo tratamento informará o titular dos dados antes de anular a limitação do tratamento, a exemplo do que ocorre no Regulamento – artigo 18, 3) ou quando os dados pessoais tenham de ser conservados para efeitos de prova (artigo 16, item 3).

O responsável pelo tratamento informará o titular dos dados, por escrito, de todos os casos de recusa da retificação ou do apagamento de dados pessoais ou da limitação do tratamento, e dos motivos da recusa.

Todavia, prevê a Diretiva também que, através de medidas legislativas, poder-se-á limitar, total ou parcialmente, a obrigação do responsável em fornecer tais informações para

evitar prejuízo ao trâmite de inquéritos policiais, investigações ou ações judiciais, para evitar prejuízo a prevenção, detecção, investigação ou repressão de infrações penais ou a execução de sanções penais e para proteger a segurança pública, nacional e direitos e liberdades de terceiros (artigo 16, item 4).

Assim, caso os dados pessoais sejam tratados no âmbito de uma investigação criminal ou de um processo judicial em matéria penal, os Estados-Membros deverão poder dispor que o exercício do direito à informação, ao acesso aos dados pessoais e à sua retificação ou apagamento, bem como à limitação do tratamento, seja feito nos termos das regras nacionais aplicáveis aos processos judiciais (considerando 49).

Conforme orientam os ensinamentos trazidos por Sajfert e Quintel (2019),

> Compreensivelmente, a Diretiva não prevê direitos previstos na RGPD que foram principalmente concebidos para serem exercidos contra operadores comerciais, como o direito de ser esquecido ou o direito à portabilidade de dados. O responsável pelo tratamento pode limitar o direito de fornecer informações específicas ao titular dos dados, o direito de acesso e o direito de obter informações sobre a possível recusa de retificação, apagamento ou restrição de tratamento de forma semelhante ao artigo 23.º do RGPD, ou seja, se existe uma medida legislativa que permite a limitação e se a limitação é necessária e proporcional. Os motivos para tais limitações são muito mais restritos do que ao abrigo do RGPD e estão intimamente ligados aos objetivos[117] da Diretiva.[118]

O Regulamento 679 (artigo 16 e 17), por sua vez, além das hipóteses comuns à Diretiva, possibilita a retificação ou apagamento (direito ao esquecimento) nos casos em que o titular

---

[117] *Articles 13(3), 15(3) and 16(4): Avoid obstructing official or legal inquiries, investigations or procedures; avoid prejudicing the prevention, detection, investigation, or prosecution of criminal offences or the execution of criminal penalties; protect public security; protect national security; protect the rights and freedoms of others.* Ou seja: Artigos 13 (3), 15 (3) e 16 (4): Evitar obstruir os inquéritos, as investigações ou os procedimentos oficiais ou judiciais; evitar prejudicar a prevenção, detecção, investigação ou repressão de infrações penais ou a execução de sanções penais; proteger a segurança pública; proteger a segurança nacional; proteger os direitos e as liberdades de terceiros (tradução livre). SAJFERT, Juraj e QUINTEL, Teresa, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities* (December 1, 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873. Acesso em 25/06/2021.

[118] *Understandably the Directive does not provide for GDPR rights that were primarily designed to be exercised against commercial operators, such as the right to be forgotten or the right to data portability. The controller may limit the right of specific information to be given to the data subject, the right of access and the right to obtain information about the possible refusal of rectification, erasure or restriction of processing in a similar way as under Article 23 GDPR, i.e. if there is a legislative measure allowing for the limitation and if the limitation is necessary and proportionate. The grounds for such limitations are much narrower than under the GDPR and closely linked to the purposes of the Directive.* SAJFERT, Juraj e QUINTEL, Teresa, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities* (December 1, 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873. Acesso em 25/06/2021.

oferece oposição ao tratamento[119], bem como quando os dados forem recolhidos no contexto da oferta de serviços da sociedade da informação referentes às crianças, hipóteses estas não contempladas na Diretiva.

Vale mencionar que o Regulamento também traz exceções, dispondo que não se aplica o direito ao apagamento (itens 1 e 2 do artigo 17) em algumas hipóteses em que o tratamento se revele necessário (exercício da liberdade de expressão e informação, cumprimento de obrigação legal ao exercício de função de interesse público ou de autoridade pública que esteja investido o responsável, por motivo de interesse público no domínio da saúde pública, arquivo de interesse e investigação científica, histórica e fins estatísticos e ainda para efeitos de declaração, exercício ou defesa de um direito num processo judicial – artigo 17, 3).

De forma semelhante, o Regulamento prevê também a comunicação aos destinatários a quem os dados tenham sido transmitidos em caso de retificação, apagamento ou limitação no tratamento (artigo 19), salvo se impossível ou depender de esforço desproporcionado, podendo fornecer informações sobre ditos destinatários ao titular.

XIII) A Diretiva 680 prevê que o responsável pelo tratamento notifique os destinatários a quem os dados tenham sido transmitidos para que estes retifiquem, apaguem ou limitem o tratamento dos dados pessoais sob sua responsabilidade (artigo 16, item 6), caso uma destas situações tenha ocorrido, como também que este comunique a retificação dos dados pessoais inexatos a autoridade competente que está na origem dos dados pessoais inexatos (artigo 16, item 5).

Tal previsão não guarda correspondência com nenhum dispositivo contido no Regulamento 679.

XIV) Em outras palavras, sobre as limitações do tratamento de dados, refere-se a Diretiva 680 (artigo 16) à limitação da obrigação ao fornecimento de informações pelo responsável pelo tratamento (artigo 13, 3), à limitação do acesso do titular aos dados tratados (artigo 15, 1) e à recusa pelo responsável em expor as razões pelas quais assim agiu (artigo 15, 3). Refere-se, ainda, à limitação ao tratamento pelo responsável como alternativa à retificação ou ao apagamento (artigo 16, 3), e também à recusa em expor as razões por ter assim agido (artigo 16, item 4).

[119] Como já mencionado, o direito de oposição não é previsto ao titular de dados na Diretiva 2016/680/UE.

O Regulamento 679 (artigo 23) refere-se à limitações ao alcance das obrigações e direitos previstos nos artigos 12 a 22 (direitos do titular), artigo 14, 5 (informações a facultar ao titular de dados, quando não são recolhidos junto ao titular) e artigo 34 (comunicação de violação de dados ao titular), bem como ao contido no artigo 5º (princípios), este último no que correspondam aos citados direitos e obrigações para assegurar, designadamente: a) A segurança do Estado; b) A defesa; c) A segurança pública; d) A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; e) Outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social; f) A defesa da independência judiciária e dos processos judiciais; g) A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas; h) Uma missão de controlo, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas a) a e) e g); i) A defesa do titular dos dados ou dos direitos e liberdades de outrem; j) A execução de ações cíveis.

XV) Encerrando o capítulo que trata dos direitos dos titulares de dados, prevê a Diretiva 680, no artigo 18, que, no âmbito das investigações e ações penais, os direitos previstos nos artigos 13, 14 e 16 (informações a facultar ou fornecer ao titular de dados, direito de acesso aos dados pelo titular e direito retificação e apagamento e limitação do tratamento) serão exercidos nos termos do direito dos Estados-Membros, se os dados constarem de uma decisão judicial ou registro criminal ou outro processo objeto de tratamento no âmbito de uma investigação ou ação penal.

Conforme pontuam Sajfert e Quintel (2019),

> Por último, o artigo 18.º permite que os Estados-Membros estabeleçam regras para o exercício dos direitos dos titulares de dados em processos penais, em conformidade com as disposições da legislação processual penal nacional. Isso significa que a Diretiva é plenamente aplicável aos processos penais, mas, caso os códigos de processo penal dos Estados-Membros já prevejam regras sobre informação, acesso, retificação, apagamento e restrição do tratamento, o dispositivo reconhece esses códigos como esforços de transposição corretos[120] (tradução livre).

[120] *Finally, Article 18 allows Member States to lay down rules for the exercise of data subject rights in criminal proceedings in accordance with the provisions of the national criminal procedural laws. That means that the Directive is fully applicable to criminal proceedings, but since Member States' criminal procedural codes*

Por sua vez, o Regulamento 679 (artigo 10), quanto ao tratamento de dados pessoais referentes a condenações criminais ou medidas de segurança, prevê que este só é realizado sob o controle de uma autoridade pública, ou com autorização do direito da União ou dos Estados Membros, com garantias adequadas para os direitos e liberdades dos cidadãos. Os registros completos das condenações penais só são conservados sob o controle das autoridades públicas.

O Regulamento prevê, também, agora no artigo 18, o direito do titular dos dados de solicitar ao responsável a limitação do tratamento por ele realizado (item 1), nas hipóteses em que o titular contestar a exatidão dos dados, o tratamento for ilícito, o responsável já não precisar mais dos dados e estes forem necessários ao titular para uso em processo judicial e, ainda, se o titular tiver se oposto ao tratamento (item 1, *a* a *d*), hipóteses em que, à exceção da conservação, os dados somente poderão ser objeto de tratamento com o consentimento do titular ou para uso em processo judicial ou defesa de direitos de outra forma, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro (item 2). Ainda, o titular é informado pelo responsável pelo tratamento antes de ser anulada a limitação ao referido tratamento (item 3).

Digno de nota, ainda, neste aspecto, é que o direito citado no parágrafo anterior – o direito do titular dos dados de solicitar ao responsável a limitação do tratamento por ele realizado – , albergado pela lei geral de proteção de dados, não traz correspondente na *law enforcement directive,* que trata a limitação ao tratamento como hipótese a ser exercida pelo responsável pelo tratamento, e não como direito do titular de dados.

XVI) Cabe anotar, por fim, que o Regulamento 679 (artigo 20) dispõe ainda que o titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, bem como o direito de transmitir esses dados a outro responsável pelo tratamento, sem a resistência de quem os detém (direito à portabilidade dos dados). Esse direito não se aplica ao tratamento necessário para o exercício de funções de

---

already provide for rules on information, access, rectification, erasure and restriction of processing, the provision recognises such codes as correct transposition efforts. SAJFERT, Juraj e QUINTEL, Teresa, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities* (December 1, 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873. Acesso em 25/06/2021.

interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.

Tal previsão não guarda correspondência com nenhum dispositivo na Diretiva 680.

3.5.1. Exercício indireto dos direitos do titular

Verdadeira inovação da Diretiva 680 vem insculpida no seu artigo 17, também constante do Capítulo III e ainda não tratado neste estudo, que prevê o 'exercício indireto' dos direitos dos titulares de dados que eventualmente tenham sido limitados pelo responsável pelo tratamento.

Assim sendo, em que pese a regra estabelecida pela Diretiva seja a aceitação direta pelo responsável dos pedidos formulados pelos titulares, nos casos referidos no artigo 13º, 3, no artigo 15º, 3 e no artigo 16º, 4, adotando os Estados-membros medidas que disciplinem tal circunstância, estes direitos poderão ser exercidos indiretamente, via autoridade de controle (artigo 17, item 1), disto sendo informado o titular dos dados (item 2) pela autoridade de competente, bem como sobre seu direito de intentar ação judicial (item 3).

Não se pode olvidar que a Diretiva 680 também tratou de preservar a realização das atividades próprias das forças de segurança, como já visto anteriormente, quando estabeleceu que os responsáveis pelo tratamento podem limitar não só os direitos, mas também a informação sobre a recusa da concessão de um determinado direito, permitindo-lhes, assim, não somente não fornecer os dados solicitados, mas também preservar os motivos da recusa e, ainda, a confirmação ou não sobre referido tratamento.

Eventual alegação de dificuldade na formulação de contestação por parte dos titulares dos dados, quanto à referida limitação, vem suprida por este dispositivo, já que o artigo 17 prevê uma revisão independente pela autoridade de controle e o exercício dos direitos do titular dos dados indiretamente, por intermédio desta, conforme acima enunciado.

Sobre o tema, muito elucidativos são os ensinamentos compartilhados por SAJFERT e QUINTEL, que esclarecem que

> Esta abordagem a dois níveis do exercício dos direitos das titulares de dados é uma novidade para quase todos os Estados-Membros, que até agora optaram por prever o exercício direto ou indireto dos direitos das titulares de dados. A nova abordagem, portanto, melhora significativamente a situação dos titulares dos dados cujos dados estão sendo processados pelas autoridades das forças de segurança, uma vez que introduz uma nova linha de verificações por uma autoridade de controle independente. Consequentemente, a nova abordagem da Diretiva terá um efeito indireto nas bases de dados da UE, como o SIS II, uma vez que as regras nacionais

referidas nos instrumentos do SIS II acima mencionados passarão a ser as leis nacionais de transposição da Diretiva.

(...)

O fundamento lógico deste novo sistema reside no necessário contrapeso à abordagem em três etapas para o exercício dos direitos das titulares de dados ao abrigo da Diretiva, que é ao mesmo tempo diferente e mais específica do que a do RGPD.

A primeira etapa é uma situação simples em que a autoridade competente decide conceder integralmente os direitos do titular dos dados. Nesse cenário, a polícia informará proativamente um titular de dados, de acordo com o Artigo 13 (2), que seus dados estão sendo processados, comunicará a base legal para o tratamento, divulgará o período de armazenamento aplicável, etc. Os titulares dos dados das diferentes categorias devem receber essas informações: vítimas, testemunhas, peritos, condenados e mesmo suspeitos em fases posteriores do processo, quando o fornecimento de tais informações não prejudique mais a investigação. Mediante pedido, a autoridade competente terá também de facultar ao titular dos dados o acesso aos seus dados pessoais em tratamento (artigo 14.º) e, eventualmente, retificar os dados inexatos que detém sobre ele (artigo 16.º, n.º 1).

A segunda etapa refere-se a uma situação mais complexa, que exige uma medida legislativa que permita uma limitação e uma avaliação da necessidade e proporcionalidade dessa limitação, após o que a autoridade competente limitará os direitos do titular dos dados. Por exemplo, a autoridade competente não fornecerá informações quanto à origem dos dados pessoais para proteger o informante (artigo 14.º, alínea g), em conjugação com o artigo 15.º, n.º 1). Nesses casos, a autoridade competente deve informar o titular dos dados sobre a recusa de fornecimento de informações relacionadas com a origem dos dados pessoais em questão e os motivos que levaram à recusa.

No entanto, em alguns casos, em particular quando as autoridades das forças de segurança lidam com pedidos especulativos de titulares de dados, o fornecimento de informações sobre a recusa de concessão de um determinado direito já pode apresentar demasiadas informações. Às vezes, a mera revelação de que certos dados são mantidos em um banco de dados da polícia pode colocar em risco as investigações em andamento contra um suspeito. A Diretiva, portanto, prevê uma terceira etapa, em que as autoridades competentes podem decidir não fornecer qualquer tipo de informação ao titular dos dados e, em vez disso, fornecer uma resposta neutra ao seu inquérito (Artigo 15 (3), segunda frase) – 'Nós não podemos confirmar nem negar que seus dados estão sendo tratados.' Essas respostas são frustrantes para os titulares dos dados e os deixam completamente no escuro.

Particularmente durante a segunda etapa, e ainda mais na terceira etapa, o papel das autoridades de controle nos termos deste artigo é crucial para garantir que os direitos do titular dos dados sejam plenamente respeitados[121] (tradução livre).

---

[121] *This two-level approach to the exercise of data subject rights is a novelty for almost all Member States, who have so far chosen to provide for either the direct or the indirect exercise of data subject rights. The new approach, therefore, significantly improves the situation of data subjects whose data are being processed by LEAs, as it introduces another line of checks by an independent supervisory authority. As a consequence, the new approach of the Directive will have a spill-over effect on the EU databases such as SIS II, as the national rules referred to in the abovementioned SIS II instruments will become the national laws transposing the Directive. (...) The rationale behind this novel system lies in the necessary counterbalance to the threestep*

Em suma, a depender de sua avaliação, as autoridades competentes podem conceder acesso total, retificar ou eliminar dados pessoais (etapa 1), podem limitar total ou parcialmente o pedido e fornecer uma explicação quanto aos motivos da limitação (etapa 2) ou podem dar uma resposta neutra ao titular dos dados (etapa 3). Se optarem por limitar os direitos do titular dos dados em conformidade com o passo 2 ou 3, a sua resposta deve informar o titular dos dados de que tem a possibilidade de exercer os seus direitos indiretamente, através do intermediário investido na autoridade de controle. Essas informações valiosas devem garantir que a possibilidade de um exercício indireto dos direitos do titular dos dados seja realmente utilizada na prática, resumem os citados autores.

O artigo 17 da Diretiva 680, assim, representa um avanço significativo nos direitos do titular dos dados, verdadeiro fortalecimento em comparação com as anteriores disposições da legislação da União Europeia na área de cooperação policial e cooperação judiciária em matéria penal, e não guarda correspondência com nenhum dispositivo do Regulamento 679.

---

approach to the exercise of data subject rights under the Directive, which is at the same time different and more specific than the one of the GDPR. The first step is a simple situation in which the competent authority decides to fully grant data subject rights. In that scenario, the police will proactively inform a data suspect, in accordance with Article 13(2), that his or her data are being processed, communicate the legal basis for processing, disclose the applicable storage period etc. Most of the categories of data subjects should receive such information: victims, witnesses, experts, convicts, and even suspects in later stages of proceedings, when provision of such information would not jeopardise the investigation anymore. Upon request, the competent authority will also have to provide the data subject with access to his or her personal data being processed (Article 14) and eventually rectify inaccurate data held about him or her (Article 16(1)). The second step refers to a more complex situation, which requires a legislative measure allowing for a limitation and a necessity and proportionality assessment of such limitation, after which the competent authority will limit data subject rights. For instance, the competent authority will not provide information as to the origin of the personal data in order to protect the informant (Article 14(g) in conjunction with Article 15(1)). In such cases, the competent authority should inform the data subject about the refusal to provide information relating to the origin of the personal data in question and the reasons that led to the refusal. However, in some cases, in particular when LEAs are dealing with speculative requests of data subjects, already providing information about the refusal to grant a certain right might present too much information. Sometimes the mere revelation that certain data are held in a police database might jeopardize ongoing investigations against a suspect. The Directive, therefore, envisages a third step, in which competent authorities may decide not to give any sort of information to the data subject and instead provide a neutral reply to his or her inquiry (Article 15(3) second sentence) - 'we can neither confirm nor deny your data is being processed'. Such replies are frustrating for data subjects and leave them completely in the dark. Particularly during the second step, and even more the third step, the role of the supervisory authorities under this Article is crucial in order to ensure that data subject rights are being fully respected. SAJFERT, Juraj e QUINTEL, Teresa, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities* (December 1, 2017). Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, Forthcoming, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873. Acesso em 25/06/2021.

CONCLUSÃO

Traçando um panorama geral desde as primeiras noções do direito à privacidade até a contemporânea legislação que trata sobre o direito à proteção de dados, necessário à compreensão da matéria em comento, porém longe de qualquer pretensão de exaurir as questões atinentes ao tema, o presente estudo tencionou verificar a existência e mapear as principais semelhanças e diferenças entre o Regulamento 2016/679/UE e a Diretiva 2016/680/UE, respectivamente, a lei geral de proteção de dados e a lei que regula o tratamento de dados realizado pelas forças de segurança, na União Europeia.

Referidos diplomas fazem parte do pacote europeu de proteção de dados e tem escopos distintos e complementares. Constituem, hoje, os principais instrumentos normativos sobre o tema na União Europeia, buscando o Regulamento 679 regular a proteção de dados em termos gerais e a Diretiva 680, a harmonia entre a preservação do direito à proteção de dados pessoais e a prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais e, ainda, a livre circulação desses dados.

A proteção dos dados pessoais, no âmbito penal, caracteriza-se por indiscutíveis peculiaridades. Imperioso, pois, observar o equilíbrio entre necessidades habitualmente opostas: de um lado, a garantia da proteção dos dados pessoais de indivíduos que não são somente suspeitos ou condenados, mas também vítimas, testemunhas ou terceiros e, de outro, o aumento gigantesco, nos últimos anos, dado à evolução tecnológica, de dados e informações armazenados em arquivos digitais e que podem circular, para fins de combate à criminalidade. A Diretiva 680 orienta, assim, que as novas tecnologias devem ser aproveitadas e a circulação da informação facilitada.

As particularidades referentes às atividades exercidas pelas autoridades das forças de segurança justificaram a adoção de regras específicas que diferiam da disciplina geral sobre proteção de dados. O que se pretendeu, com a edição de tal instrumento normativo, foi conferir aos Estados-membros maior flexibilidade considerando-se as especificidades locais, em especial no que tange ao tratamento de dados realizados no contexto do combate à criminalidade (à título exemplificativo, poderão as autoridades das forças de segurança tratar os dados por períodos superiores aos determinados pela normativa geral, ou mesmo perpetuamente).

Em cumprimento ao proposto no início deste estudo, conclui-se que tais normas de proteção de dados no âmbito geral e criminal convergem em muitos pontos, praticamente se repetindo.

As divergências verificadas entre a lei geral de proteção de dados e a lei que regula o tratamento de dados realizado pelas forças de segurança na União Europeia resulta das peculiaridades típicas características às atividades desenvolvidas pelas forças de segurança e comuns ao redor do mundo, ao menos minimamente.

Os três primeiros capítulos da Diretiva 680 (âmbito de aplicação e definições, princípios e direitos dos titulares) divergem fortemente de seus correspondentes no Regulamento Geral. Das diversas semelhanças e diferenças detectadas no decurso do presente estudo, algumas delas se afiguram mais marcantes e que merecem especial destaque.

Além do citado âmbito de aplicação diferenciado, já que o Regulamento 679 refere-se ao tratamento de dados pessoais no âmbito geral e a Diretiva 680, ao tratamento de dados realizado nas atividades desenvolvidas pelas forças de segurança em matéria criminal e de segurança pública, também diferem quanto às definições nelas relacionadas. Mais do que os conceitos comuns, o Regulamento 679 apresenta outras várias definições utilizadas no decorrer do diploma legal, inerentes à vasta gama de atividades a que se aplica e ausentes na Diretiva 680. Apesar de mais enxuta neste aspecto, a Diretiva 680 traz o conceito de autoridade competente, que é responsável pelo tratamento de dados pessoais no âmbito criminal e de segurança pública.

Os princípios insculpidos em ambos os instrumentos legais são os mesmos, somente divergindo quanto ao princípio da transparência. Elencado no Regulamento 679 e ausente na Diretiva 680, tal circunstância leva em consideração as necessidades típicas das autoridades das forças de segurança e a natureza particular de suas atividades de tratamento, conferindo mais flexibilidade às autoridades de polícia e justiça criminal no desempenho de suas tarefas em comparação com os requisitos das disposições correspondentes do Regulamento 679.

Inovação trazida pela diretiva 680 é a distinção que mencionada norma faz entre diferentes categorias de titulares de dados pessoais, relacionando-os como suspeitos ou condenados, vítimas ou terceiros envolvidos (testemunhas, informantes ou contatos dos suspeitos ou condenados), a ser considerada por ocasião do tratamento de dados realizado pelas autoridades criminais.

A Diretiva 680 distingue ainda os dados pessoais que são baseados em fatos dos que são baseados em apreciações pessoais, também inovando neste aspecto.

Tais distinções não guardam correspondência com nenhum dispositivo do Regulamento 679, eis que afetas às atividades desenvolvidas pelas forças de segurança, e nem precedentes nas legislações antecedentes.

O Regulamento 679 prevê seis hipóteses para o tratamento de dados pessoais, dentre elas o consentimento do titular. Diferentemente, a Diretiva 680 prevê somente uma base legal para tratamento de dados pessoais: o Direito da União ou dos Estados-Membros, só sendo lícito o tratamento se e na medida em que for necessário para o exercício de uma atribuição pela autoridade competente para fins de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública.

Com relação aos direitos do titular e às possíveis limitações a estes direitos, a abordagem na Diretiva 680 é mais detalhada que a contida no Regulamento 679 e os motivos para tais limitações estão intimamente ligados aos objetivos da Diretiva, justamente visando adequar os meios de tratamento de dados pessoais às necessidades das autoridades das forças de segurança.

Coincidem nas duas normas o direito à informação, acesso, retificação, apagamento e restrições de tratamento, e esses direitos podem ser exercidos diretamente contra o responsável pelo tratamento dos dados.

Poderá o responsável limitar as informações a fornecer ao titular dos dados, o direito de acesso do titular, de retificação e de apagamento dos dados, total ou parcialmente, quando o exercício de tais direitos vier a prejudicar as atividades investigatórias e/ou judiciais, próprias das forças de segurança no âmbito criminal. Sobre as razões de eventuais limitações, o responsável informará o titular. Todavia, poderá também a autoridade competente deixar de esclarecer ao titular os motivos que o levaram à recusa do exercício de tais direitos, quando tal revelação puder prejudicar as atividades desenvolvidas pelas autoridades no âmbito criminal, ou seja: para evitar prejuízo ao trâmite de inquéritos policiais, investigações ou ações judiciais, para evitar prejuízo a prevenção, detecção, investigação ou repressão de infrações penais ou a execução de sanções penais e para proteger a segurança pública, nacional e direitos e liberdades de terceiros.

A Diretiva 680 prevê o direito de retificação e apagamento dos dados pessoais em hipóteses semelhantes ao Regulamento 679 (dados sensíveis e ofensa aos princípios e bases legais). Todavia, o responsável poderá limitar o tratamento ao invés de apagar os dados caso o titular dos dados conteste a exatidão dos mesmos e a sua exatidão ou inexatidão não possa ser

apurada, bem como quando os dados pessoais tenham de ser conservados para efeitos de prova.

Por fim, quanto aos direitos dos titulares, cabe pontuar que a Diretiva 680, compreensivelmente, não prevê ao titular o direito de oposição e nem o de portabilidade dos dados.

Em contrapartida às limitações acima descritas, a Diretiva prevê também uma revisão independente e o exercício dos direitos limitados via autoridade de controle, outro avanço trazido pela Diretiva 680 e sem correspondente no Regulamento 679, bem como do exercício dos mesmos direitos através da via judicial, disto sendo informado o titular pelo responsável.

Digno de nota, ainda é que a Diretiva 680 prevê que os Estados membros podem estabelecer salvaguardas mais elevadas que as já nela contidas para a proteção dos direitos e liberdades das pessoas em causa, no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes. Com tal disposição resta clara a intenção do parlamento da União Europeia de assegurar que são aplicados padrões de alta qualidade para efeitos de proteção de dados de acordo com as disposições da Diretiva. Tal comando não tem precedente nas legislações antecedentes e nem guarda correspondência com qualquer dispositivo do Regulamento 679, sendo, portanto, mais uma inovação da *Law Enforcement Directive.*

Por derradeiro, como já apontado outras vezes neste estudo, da análise da Diretiva 680 percebe-se claramente que esta pretende preservar o direito dos indivíduos cujos dados pessoais são submetidos à tratamento pelas autoridades competentes para fins penais, sem olvidar, todavia, da sociedade como um todo.

Desde o título que a anuncia referida normativa enaltece o direito à proteção de dados do indivíduo em paralelo à livre circulação destes dados. Disto se percebe que não só o direito fundamental à proteção de dados é tutelado, mas também a sociedade em relação à segurança pública, já que se considera, no corpo da norma, as necessidades particulares das autoridades criminais e de segurança pública no exercício de suas funções, bem como as peculiaridades das atividades desenvolvidas pelas forças de segurança que atuam para a elucidação dos delitos objetivando a contenção da criminalidade, em busca de uma sociedade mais segura para todos.