A Proteção de Dados Pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia

INDRA SPIECKER GENANNT DÖHMANN[1]
Goethe-Universität Frankfurt, Alemanha.

RESUMO: O presente artigo tem como objetivo apresentar o direito sobre proteção de dados na Europa, expondo os seus conceitos, princípios e traços fundamentais. Como a efetivação foi tema de grande importância para a motivação do RGPD-UE, introduzem-se as estruturas da implementação, particularmente a importância das autoridades independentes de fiscalização, bem como o novo mecanismo de coerência mediante o qual atua o novo Comitê Europeu para a Proteção de Dados (*European Data Protection Board* – EDPB) (4). Conclui-se a contribuição com uma perspectiva referente a novos desafios e novas abordagens de regulação (5).

PALAVRAS-CHAVE: Proteção de dados pessoais; Regulamento Europeu de Proteção de Dados; autoridade independente de supervisão.

ABSTRACT: The paper presents the context of the data protection in Europe, highlighting its concepts, principles and fundamental features. As enforcement was a topic of great importance for the approval of the GDPR, the paper introduces the implementation structures of the regulation, particularly the importance of the independent supervisory authorities, as well as the new coherence mechanism. The article concludes with a perspective on new challenges and new regulatory approache.

KEYWORDS: Data protection; General Data Protection Regulation; independent supervisory authorities.

1 Orcid: <https://orcid.org/0000-0001-6023-929X>.

rior fora da União Europeia: adequação; 2.8 *Privacy by design* e *privacy by default;* 3 Estruturas de efetivação do RGDP; 3.1 As pessoas interessadas e seus direitos; 3.2 As autoridades independentes para a proteção de dados; 3.3 O *European Data Protection Board* (EDPB) e o mecanismo de coerência na *One-Stop-Shop;* 4 Perspectivas e conclusão: desafios e novas abordagens de regulação; 4.1 Decisão automatizada, algoritmos, inteligência artificial e aprendizado de máquina; 4.2 A globalização e a luta pela internet; 4.3 Última observação.

INTRODUÇÃO

Desde o dia 25 de maio de 2018, o tique-taque dos relógios na proteção de dados na Europa tem maior intensidade: com a entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia (RGPD-UE), o direito de proteção de dados é reposicionado mais uma vez, sendo dotado de maior efetividade e recebendo uma efetivação visível[2].

Paralelamente, foi aprovada, em caráter complementar – ainda que tenha sido objeto de bem menos atenção –, a chamada Diretiva sobre a Proteção de Dados na Polícia e no Judiciário (Diretiva [UE] nº 2016/680 – Diretiva JAI). Ela regula – em nível de diretiva – princípios comuns para tratamentos de dados dos Estados-membros na persecução penal e no Judiciário. Além disso, atualmente está sendo revisada a chamada Diretiva ePrivacy ([UE] 2002/58/CE), que regulava o tratamento de dados pessoais e a proteção da esfera privada na área da telecomunicação. Originalmente, pretendia-se que ela entrasse em vigor paralelamente ao RGPD e à Diretiva nº 2016/680; de fato, porém, sua aprovação ainda continua pendente. A mais recente decisão do Tribunal Europeu de Justiça (TEJ) sobre o consentimento efetivo com os chamados *cookies*[3] poderá exercer agora pressão sobre os parceiros de negociação da Comissão, do Conselho e do Parlamento da União Europeia.

A repercussão do RGPD-UE para além das fronteiras da Europa não deveria ser subestimada, pois ele oferece a possibilidade de estabelecer um *level playing field* em um mercado que já parece estar firmemente subdividido, com poucos fornecedores, e contrabalançar fenômenos de falha de mercado já existentes. Mencione-se apenas, a título de exemplo, que três das maiores democracias do mundo assumiram, por sua vez, elementos substanciais do RGPD-UE. O Japão reformou seu direito referente à prote-

2 No que se segue, são feitas, deliberadamente, apenas poucas indicações bibliográficas, particularmente de comentários e visões panorâmicas do assunto, para possibilitar ao leitor e à leitora um primeiro acesso; via de regra, essas indicações remetem a outros textos.

3 EuGH [Tribunal Europeu de Justiça] Rs. C-673/17 (Planet49), ECLI:EU:C:2019:801.

ção de dados em estreita sintonia com a UE, de modo que, no dia de sua aprovação por parte do Parlamento japonês, ocorreu a chamada resolução de adequação da Comissão Europeia e, com isso, pôde surgir o maior mercado europeu-asiático para dados – e isto sob condições de proteção de dados, privacidade e segurança[4]. Na Califórnia, o *Consumer Protection Act* (CCCPA)[5] estabeleceu direitos substanciais para usuários e obrigações para os agentes de tratamento de dados que guardam grande semelhança com as normas do RGPD-UE[6]. Além disso, em agosto de 2018, o Brasil aprovou uma lei geral de proteção de dados que, por sua vez, é moldada por muitos conceitos de proteção de dados também defendidas na Europa[7].

A contribuição que se segue apresenta um breve histórico do direito sobre proteção de dados na Europa com base nos princípios e traços fundamentais nele contidos (2), antes de apresentar os princípios essenciais do RGPD-UE (3). Como a efetivação foi tema de grande importância para a motivação do RGPD-UE, introduzem-se as estruturas da implementação, particularmente a importância das autoridades independentes de fiscalização, bem como o novo mecanismo de coerência mediante o qual atua o novo Comitê Europeu para a Proteção de Dados (*European Data Protection Board* – EDPB) (4). Conclui-se a contribuição com uma perspectiva referente a novos desafios e novas abordagens de regulação (5).

1 BREVE HISTÓRICO DO DIREITO EUROPEU DE PROTEÇÃO DE DADOS

1.1 Antecedentes e primórdios

É difícil situar o início do direito europeu de proteção de dados. Certamente o ano de 1970 pode ser considerado um marco, pois foi então que, no estado de Hesse, na Alemanha, foi aprovada a primeira lei de proteção de dados do mundo. Com a decisão de estatuir regras vinculantes para a forma de lidar com dados pessoais, o legislador reagiu à mudança radical que ocorria na tecnologia da informação, impulsionada principalmente pelo tratamento automatizado de dados[8]; ele reagiu, com isso, a exigências que

4 Veja quanto a isso a Resolução da Comissão Europeia nº 2019/419, de 23 de janeiro de 2019.

5 Disponível em: <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375>. Acesso em: 21 nov. 2019.

6 Veja quanto a isso, p. ex., Spies, ZD-Aktuell 2018, 06156 USA: Neues kalifornisches Datenschutzgesetz CCPA als Vorreiter.

7 Hornung; Spiecker gen. Döhmann. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.). *Datenschutzrecht*, 2019, Introdução nº 260, nº 614.

8 Simitis; Hornung; Spiecker gen. Döhmann. In: id. (Ed.), 2019, Introdução nº 1.

tinham sido manifestadas anteriormente na Alemanha e nos EUA referentes à forma de lidar com dados pessoais[9].

Além disso, uma grande importância para o desenvolvimento do Direito Europeu de Proteção de Dados cabe a uma decisão do Tribunal Constitucional Federal (TCF) alemão de 1983, em que se atribuiu pela primeira vez à proteção de dados uma dimensão relacionada ao direito constitucional e aos direitos humanos[10] e em que se fixaram pedras angulares da proteção de dados que desempenham um papel central também na legislação europeia atual.

O Tribunal fundamentou seu procedimento com base em uma argumentação construída em múltiplos níveis interligados a que se pode, ainda hoje, recorrer no tocante aos princípios e que pode servir de fundamento para a proteção de dados. O ponto de partida foi a reflexão de que só pode avaliar de modo confiável as consequências de seu comportamento a pessoa que souber quem sabe o que e a que tempo sobre ela. Por conseguinte, um dos efeitos da proteção de dados consiste em assegurar a democracia: se esse conhecimento não existir, o cidadão possivelmente abriria mão, em face da insegurança a respeito do conhecimento de que disporia a outra parte, do exercício de liberdades protegidas por direitos fundamentais, particularmente, p. ex., a liberdade de reunião e de associação[11]. Portanto, o que atualmente se chama de *chilling effect*[12] foi, já naquela época, um motivo essencial para a fundamentação da proteção de dados por parte do TCF. A democracia necessita de uma implementação dos direitos fundamentais não sujeita a impedimentos e sem temor de sanções. Além disso, argumenta-se que um procedimento restritivo se faz imperativo em face dos efeitos imprevisíveis do tratamento automatizado[13]. Com isso se retoma um princípio do direito sobre a tecnologia segundo o qual uma tecnologia nova deve ser acompanhada regulatoriamente de acordo com o princípio da prevenção[14]. E, por fim, expressa-se – também em função da conexão dogmática da proteção da dignidade humana a partir do art. 1º, § 1, da Constituição alemã com o direito fundamental de proteção da personalidade a partir do art. 2º, § 1, da mesma Constituição – uma perspectiva individualista: a liberdade e a autonomia do indivíduo exigem uma proteção das condições informacio-

9 Ibid.; cf. também Tinnefeld; Buchner; Petri. *Einführung in das Datenschutzrecht*. 5. ed., 2012, p. 69.
10 BVerfGE [Decisões do Tribunal Constitucional Federal] 65, 1 – decisão sobre o censo populacional.
11 BVerfGE 65, 1 (43).
12 Dix. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, art. 23, nº 13.
13 BVerfGE 65, 1 (46).
14 Röthel. In: Schulte; Schröder (Ed.). *Handbuch des Technikrechts*, 2011, p. 214s.

nais gerais sob as quais possam se desenvolver. Um controle total do indivíduo que impeça seu desenvolvimento e sua autonomia deve ser rejeitado. Isso é assegurado pela autodeterminação informacional que se manifesta na proteção de dados. Em consonância com isso, o TCF alemão também não fala primordialmente de um direito fundamental à proteção de dados, e sim de um direito fundamental à autodeterminação informacional. Esta consiste em determinar por conta própria a respeito da entrega dos dados[15].

Em sua decisão, o Tribunal Constitucional Federal alemão fixou traços essenciais de um direito sobre proteção de dados que acabaram sendo assumidos no RGPD-UE. Com base em elementos centrais do direito fundamental, o TCF definiu que interferências necessitam de uma regulação legal (específica para a respectiva área), que a pessoa interessada pode dispor sobre seu direito mediante consentimento, que para justificar interferências no novo direito fundamental só interesses gerais preponderantes seriam suficientes e que todo e qualquer uso de dados pessoais está vinculado à finalidade predeterminada para isso. Além disso, o Tribunal reconheceu já em 1983 que uma implementação do direito à proteção de dados somente por parte do indivíduo não está garantida[16]. Por isso, haveria necessidade de medidas complementares do direito processual e organizacional, como direitos de receber informações da pessoa interessada, bem como de controle adicional por parte de autoridades de fiscalização independentes[17].

Todas essas garantias encontram-se também na concepção europeia atual do direito referente à proteção de dados no marco do RGPD e da Diretiva JAI.

1.2 Artigos 7º e 8º da Carta dos Direitos Fundamentais da União Europeia e artigo 16, § 2º, do Tratado sobre o Funcionamento da União Europeia

Garantias centrais de direitos humanos no tocante à proteção de dados no nível do direito primário europeu encontram-se, desde o Tratado de Lisboa, como autêntica vinculação aos direitos fundamentais[18], tanto nos arts. 7º e 8º da Carta dos Direitos Fundamentais da União Europeia (CDF) quanto no art. 16º do Tratado sobre o Funcionamento da União Europeia (TFUE). Enquanto o art. 8º da CDF trata da proteção de dados, o art. 7º abor-

15 BVerfGE 65, 1 (42).
16 BVerfGE 65, 1 (46).
17 BVerfGE 65, 1 (46).
18 Schiedermair. In: Simitis; Hornung; Spiecker gen. Döhmann (ed.), 2019, Introdução nº 167, 177.

da o respeito pela vida privada e a liberdade de comunicação. O art. 16º, § 2, do TFUE contém, ainda, um fundamento homogêneo de competências para regulações na área do direito sobre proteção de dados em favor da UE. Em consequência disso, o que se encontra em primeiro plano do direito secundário baseado nessas normas – como, p. ex., é possível depreender do art. 1º, § 2, do RGPD-UE – não é mais uma estruturação e harmonização do mercado interno, e sim, de fato, a realização dos direitos fundamentais[19].

Até agora, a jurisprudência do TEJ não vem fazendo uma distinção substancial entre os dois direitos fundamentais. Em decisões anteriores, aceita-se a concorrência ideal[20], mas, em decisões mais recentes, a relação entre ambos também é deixada em aberto[21]. Não se deve esperar que no futuro próximo o Tribunal enxergue razões para tematizar mais de perto uma possível diferença de privacidade e proteção de dados.

Isso não altera o fato de haver uma distinção entre essas duas concepções: a privacidade pode ir além do direito à proteção de dados em sua exigência de proteção, e a proteção de dados também pode ir além da privacidade. Isso se mostra principalmente a partir do fato de que, segundo a compreensão europeia do Direito, também existe uma proteção de dados pessoais na esfera pública, portanto, p. ex., em praças públicas, ou na escola, ou no local de trabalho[22]. Inversamente, os obstáculos, p. ex., para intervenções policiais na privacidade, p. ex. na moradia ou em anotações pessoais, são claramente maiores do que os obstáculos para intervenções policiais em dados pessoais. Por conseguinte, a privacidade e a proteção de dados podem se fortalecer e complementar mutuamente; o direito protetivo que seja mais forte em cada caso define o padrão de proteção.

1.3 Diretiva de Proteção de Dados da União Europeia (95/46/CE)

Já antes da consagração da proteção de dados como direito fundamental na CDF ou no art. 16 do TFUE foi promulgada a Diretiva de Proteção de Dados da UE (DPD), que entrou em vigor em 1995. Ela ainda se baseava, por falta de uma norma sobre competências comparável ao art. 16º, § 2, do TFUE, nos antigos tratados sobre a Comunidade Europeia sob a chamada

19 Hornung; Spiecker gen. Döhmann. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, art. 1, nº 22.

20 Cf. também Schiedermair. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, Introdução, nº 167; EuGH, C-92/09 (Schecke), Slg 2010, I-11063 Rn 47, 52; EuGH, Rs. C-468/10 (ASNEF), Slg 2011, I-12181 Rn. 41s.; EuGH, Rs. C-291/12 (Schwarz), ECLI:EU:C:2013:670 Rn 26.

21 EuGH, Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317; EuGH, verb. Rs. C-203/15, C-698/15 (Conservação de dados II), ECLI:EU:C:2016:970.

22 Karg. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, art. 4, nº 1, nº 31.

competência de mercado interno no art. 95º do Tratado constitutivo da Comunidade Europeia. A promulgação da DPD foi, aliás, para vários Estados-membros da UE, o ensejo para promulgar pela primeira vez regulações sobre a proteção de dados[23]. A DPD previa uma regulamentação abrangente dos tratamentos de dados pessoais tanto para a esfera privada quanto para a pública[24]. Ela já continha as estipulações essenciais em termos de conteúdo que também se encontram no RGPD. Delas faz parte, p. ex., a necessidade de justificar um tratamento de dados mediante o consentimento ou um fundamento jurídico; a vinculação do tratamento de dados a diversos princípios, como a vinculação à finalidade, a responsabilidade do agente de tratamento dos dados e a minimização de dados; a instituição de autoridades de fiscalização independentes, bem como a garantia da proteção de dados mediante diversos direitos da pessoa afetada, como, p. ex., informação, retificação, oposição e remoção.

Até a promulgação do RGPD, a DPD só sofreu pequenas complementações; de modo algum se pode dizer que tenha havido uma legislação europeia que tenha acompanhado a digitalização. Como complementação cautelosa, deve-se mencionar, primordialmente, a chamada Diretiva ePrivacy nº 2002/58/CE ou a Diretiva Complementar nº 2009/136/CE sobre o emprego de *cookies* para a área da telecomunicação. Ela continha regulações especiais ou específicas em comparação com o RGPD, que continua sendo considerado *lex generalis*, como, p. ex., elementos constitutivos de permissão e regras de tratamento para dados de tráfego e de localização, sobre medidas de segurança técnico-organizacionais das operadoras e obrigações de fornecer informações, bem como sobre *cookies*[25].

2 PRINCÍPIOS BÁSICOS DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UNIÃO EUROPEIA

Desde 25 de maio de 2018, o RGPD substitui a DPD pregressa; paralelamente a isso, a Diretiva ePrivacy também deveria ser transformada em um Regulamento ePrivacy modernizado. Sua aprovação, entretanto, continua pendente.

23 Simitis; Hornung; Spiecker gen. Döhmann. In: id. (Ed.), 2019, Introdução, nº 143.
24 Ibid., Introdução, nº 138.
25 Cf. Hornung; Spiecker gen. Döhmann. In: ibid., Introdução, nº 222.

2.1 Classificação em abordagens de regulamentação

O RGPD carrega a marca de várias abordagens de regulamentação. Elas estão sendo empregadas paralelamente, mas com isso também surgem ocasionalmente fricções. Em parte, elas já são provenientes dos primórdios do direito de proteção de dados, mas em alguns poucos casos também só se tornaram visíveis por causa do RGPD. Todas reagem ao fato de que o tratamento automatizado do maior número possível de dados pessoais contém um considerável potencial de perigo – associado a ele – de um controle permanente e de um direcionamento – ao menos indireto – da conduta dos cidadãos interessados[26]. Pretende-se criar uma contraposição a desigualdades de poder que possam surgir por meio da informação e seu aproveitamento.

Um elemento central é a classificação do direito de proteção de dados como um direito referente à tecnologia[27]: visa-se acompanhar juridicamente um campo tecnológico repleto de inseguranças de tal modo que os riscos da tecnologia sejam percebidos em tempo hábil e juridicamente limitados. Dessa maneira, as oportunidades podem ser aproveitadas. Com isso se parafraseia o princípio da prevenção que permeia o direito referente à tecnologia (e, em sua sequência, também o direito ambiental)[28]: não se conhecendo a evolução posterior, cabem ao Estado amplas competências para restringir e regular uma tecnologia nova[29].

Além disso, o direito de proteção de dados é um direito de proteção da personalidade[30]: ele pretende preservar a autonomia, liberdade e autodeterminação do indivíduo também sob condições de um amplo aproveitamento de informações sobre o indivíduo. Com isso, o direito referente à proteção de dados promove diretamente a democracia e a liberdade, como já destacou o Tribunal Constitucional Federal em 1983[31]: os direitos de liberdade só são implementados quando seu exercício não acarrete o temor de se sofrer desvantagens por causa disso[32]. Com esse direcionamento, o direito sobre proteção de dados do RGPD encontra-se em uma tradição individualista e liberal do iluminismo. Com isso, ele se contrapõe particularmente a esforços de, mediante uma ampla definição de perfis, classificar

26 Cf. Simitis; Hornung; Spiecker gen. Döhmann. In: ibid., Introdução, nº 13.
27 Hornung; Spiecker gen. Döhmann. In: ibid., art. 1, nº 4.
28 Röthel. In: Schulte; Schröder (Ed.), 2011, p. 214 ss.
29 Veja quanto a isso também ibid., p. 205.
30 Veja quanto a isso também Spiecker gen. Döhmann. In: Campos; Abboud; Nery Jr. (Ed.). *Proteção de dados e regulação*, 2020.
31 Veja *supra* seção 2.1.
32 Cf. BVerfGE 65, 1 (43).

o indivíduo em agrupamentos e, com base nisso, avaliá-lo e possibilitar-lhe participação e acesso tanto na área privada quanto na estatal.

O direito de proteção de dados é, além disso, direito de regulamentação econômica[33]. Muitas das inovações possibilitadas pelo tratamento automatizado de dados têm um potencial econômico enorme. As maiores empresas do mundo têm seu núcleo preponderantemente na área de prestação de serviços informacionais ou, em todo caso, baseiam-se consideravelmente na disponibilização de serviços e bens digitalizados. Sua regulamentação é, muitas vezes, ao mesmo tempo uma regulamentação do mercado porque elas se tornam necessárias em função de diversos efeitos que fazem com que mercados informacionais sofram falhas de mercado. Disso fazem parte as propriedades particulares das informações como bens comunitários (*common goods*, nos termos da teoria econômica) e como bens de experiência (*experience goods*). Além disso, normalmente o valor das informações não se deriva delas mesmas, e sim das decisões subsequentes. A partir destas, porém, não se pode perceber em que informações elas estão baseadas.

Por fim, nos últimos anos, o direito de proteção de dados também vem se transformando cada vez mais em um direito de defesa do consumidor[34]. Com isso se visa compensar desvantagens estruturais de consumidores na demanda de bens e serviços baseados na informação.

Um conhecimento dessas diversas abordagens de regulamentação permite, por um lado, explicar aparentes contradições nas regulações do RGPD e compreendê-las de um ponto de vista integral. Por outro lado, isso possibilita argumentos e avaliações importantes que se devem à respectiva abordagem explicativa.

2.2 Esfera de aplicação

O RGPD reivindica vigência essencialmente sob duas condições, a saber, que dados pessoais sejam tratados (1) e que o tratamento de dados afete interesses europeus e seja, por isso, territorialmente aplicável (2).

2.2.1 Dados pessoais

O conceito de dado pessoal, no art. 4º, § 1, do RGPD, é substancialmente idêntico à regulação que o antecedeu, a Diretiva sobre Proteção de

33 Veja quanto a isso também Spiecker gen. Döhmann, 2020.

34 Veja quanto a isso também ibid.

Dados (DPD). Basta a possibilidade de identificação de uma pessoa, isto é, também uma informação que aparentemente se refere a um objeto pode se enquadrar no RGPD se ela puder ser relacionada a uma pessoa concreta[35].

O que se torna problemática é a questão de quem depende o conhecimento adicional necessário para isso: o próprio agente de tratamento dos dados precisar dispor sobre isso, o tratamento deve ocorrer justamente com vistas à referência à pessoa ou basta que esse conhecimento adicional se encontre em um lugar qualquer e junto a um alguém qualquer? O Tribunal Europeu de Justiça (TEJ) achou uma solução conciliatória: segundo ela, para se supor a existência de uma informação objetiva como dado relacionável a uma pessoa, é suficiente que se possa, com um esforço não injustificável e com meios legais – entre os quais também contam meios de terceiros – produzir a ligação com uma pessoa[36]. Já se pode depreender de decisões anteriores do TEJ que dados pessoais que sequer são tratados por causa de sua referência a pessoas ainda assim se enquadram no RGPD[37].

No raciocínio em contrário, isso significa que o RGPD não é aplicável quando os dados não permitem a identificabilidade de uma pessoa[38]. Em especial, dados anonimizados ou dados estatísticos que não admitem uma desanonimização podem, portanto, ser tratados sem as vinculações do RGPD.

2.2.2 Princípio do estabelecimento e princípio do local do mercado

A segunda grande condição a ser cumprida para se enquadrar no RGPD refere-se à sua aplicabilidade territorial: quando, afinal, o RGPD é aplicável a um processo de tratamento de dados? A resposta a essa pergunta encontra-se no art. 3º do RGPD.

Como já era o caso da DPD, o RGPD conhece o chamado princípio do estabelecimento segundo seu art. 3º, § 1: quem mantém um estabelecimento na UE e procede a tratamentos de dados "no contexto desse estabelecimento" deve aplicar o Direito Europeu de Proteção de Dados. Na decisão sobre Google Spain, o TEJ elucidou que uma conexão econômica é suficiente para a ligação do estabelecimento e do tratamento de dados: se um tratamento de dados só pode ocorrer porque uma filial – juridicamente independente – disponibiliza as fontes de financiamento para isso, p. ex.,

35 Karg. In: Simitis; Hornung; Spiecker (ed.), 2019, art. 4, Nr. 1, nº 46.
36 EuGH, Rs. C-582/14 (Breyer), ECLI:EU:C:2016:779.
37 EuGH, Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317.
38 Karg. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, art. 4, Nr. 1, nº 19 s.

através de *marketing* e contratos de publicidade, existe tal tratamento "no contexto" e, portanto, o direito da UE é aplicável[39].

Por outro lado, o que é novo é o chamado princípio do local do mercado segundo o art. 3º, § 2, do RGPD. Ele substitui o chamado princípio da territorialidade[40], até agora vigente sob a DPD, segundo o qual o tratamento de dados tinha de ocorrer no território da UE. A partir de agora, uma de duas alternativas pode desencadear a aplicabilidade. Ou um agente de tratamento de dados oferece bens ou serviços na UE, ou então realiza uma análise de comportamento voltada para pessoas na UE. No primeiro caso, o que é decisivo para a avaliação é a forma concreta da oferta, p. ex., se existe um endereço de caixa postal do fornecedor na UE pelo qual se pode fazer contato, se são feitas ofertas em uma língua que só é essencialmente usual na UE, ou também se é oferecida uma expedição para a UE[41]. Expressamente não está previsto que o bem ou serviço implique pagamento (art. 3º, § 2, alínea *a*, do RGPD. A segunda alternativa, segundo o art. 3º, § 2, alínea *b*, do RGPD, vai mais longe: o Regulamento já encontra aplicação quando se pesquisa um comportamento na UE. Neste ponto, reconhecem-se as diferentes abordagens de regulamentação: a garantia de proteção da personalidade por parte da UE não termina em suas fronteiras, porque as condições do mercado são consideravelmente definidas pela disponibilidade de dados pessoas em um mundo globalizado. Ao mesmo tempo se apela, com isso, ao cânone de valores do direito da personalidade da UE: o efeito promotor da liberdade e da democracia do direito referente à proteção de dados tem uma vigência ampla. Por isso, essas normas também se aplicam aos estrangeiros na UE.

2.3 Princípio da proibição

Se o RGPD é aplicável, seu princípio básico determinante é o chamado princípio da proibição já contido na DPD[42]: segundo ele, todo tratamento de dados carece de justificação[43]. Isso pode acontecer ou por meio de um consentimento do titular dos dados (art. 7º, art. 4º, n. 11, art. 6º, § 1, alínea *a*, do RGPD) ou com base em um fundamento jurídico (art. 6º, § 1, alíneas *a* até *e* do RGPD). Com isso, pode perfeitamente haver interesses que se so-

39 EuGH, Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317.

40 Hornung. In: Simitis; Hornung; Spiecker gen. Döhmann, 2019, art. 3, nº 5.

41 Ibid., art. 3, nº 53.

42 Hornung; Spiecker gen. Döhmann. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, Introdução, n. 212.

43 Ibid., Introdução, nº 236.

breponham à proteção de dados[44]. Esse princípio da proibição também deve ser sempre entendido no sentido de que o tratamento lícito para determinadas finalidades e de determinada maneira não significa necessariamente que qualquer outro tratamento segundo a vontade do agente de tratamento dos dados fosse admissível. O titular dos dados continua sendo o ponto de referência para todo e qualquer tratamento adicional. Por conseguinte, devem-se recusar concepções como, p. ex., a da "soberania sobre os dados", que considera suficiente uma justificação inicial para a primeira transmissão de dados por parte do titular deles, ou de uma transparência substitutiva referente a todos os outros tratamentos de dados sem outras restrições. Elas esvaziariam o direito da proteção de dados por transformarem o titular dos dados em joguete dos interesses do agente de tratamento de dados. Em contraposição a isso, o RGPD visa a um equilíbrio adequado dos interesses, como já ilustra seu objetivo – elaborado de diversas formas – de mercado de dados e proteção de dados no art. 1º, § 1, do RGPD.

2.3.1 Consentimento

Segundo a definição legal do art. 4º, n. 11, do RGPD, o consentimento é a "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento". Exige-se, portanto, a presença cumulativa de todos os elementos constitutivos (voluntariedade, ato personalíssimo, informação, concreticidade, caráter inequívoco)[45]. Quando isso acontece concretamente, é uma questão controvertida e não pode ser esboçado aqui em detalhes[46]. Atualmente é problemática, por exemplo, a forma como uma informação compreensível sobre os tratamentos previstos de dados pode ocorrer e se, para isso, é possível empregar símbolos como, p. ex., um sistema de semáforos[47] ou um procedimento com vários níveis[48]. Além disso, é controvertido

44 Cf. Simitis; Hornung; Spiecker gen. Döhmann. In: id. (Ed.), 2019, Introdução, nº 34.

45 Klement. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, art. 7, nº 5.

46 Detalhes quanto a isso em ibid., art. 7, nº 1 ss.

47 Neste caso, p. ex., atribui-se um serviço na internet que faça o tratamento de dados pessoais uma avaliação geral no tocante ao cumprimento do direito de proteção de dados, que – p. ex., usando as cores "vermelho" ou "verde" – visa orientar o usuário na concessão de seu consentimento. Neste caso, naturalmente, muitas informações sobre detalhes não são levadas em consideração, o usuário não tem uma noção individual do que acontece com seus dados e atitudes individuais para com a proteção de dados não podem ser expressas em imagens.

48 Neste caso se dão ao usuário informações adicionais – p. ex., através de *links* em que se pode clicar –, em caso de necessidade individual. Assim, p. ex., no primeiro nível só se poderia comunicar que dados são transferidos para o exterior, no segundo nível se poderia indicar o país a que eles se destinam e no terceiro, então, concretamente o destinatário deles.

até que ponto existem situações em que uma voluntariedade não é possível por causa de uma desvantagem estrutural do titular dos dados, p. ex., no caso de contratos de aluguel ou de trabalho[49]. Por fim, ainda se disputou, até uma decisão bem recente do TEJ[50], se sob determinadas condições um "*opt-out*" deveria ser possível, ou seja, que o titular dos dados não precisaria consentir ativamente antes da utilização dos dados, mas só teria a possibilidade de rejeitar *a posteriori* o consentimento "dado" por predefinição[51]. O Regulamento ePrivacy poderá criar para isso novas regulações para o consentimento *on-line*.

2.3.2 Fundamento jurídico

As normas contidas no art. 6º, § 1, alíneas *b* até *e*, do RGPD criam os demais fundamentos jurídicos para o tratamento de dados pessoais. Nisso se enquadram, na esfera do tratamento privado de dados, principalmente a necessidade desse tratamento de dados para a celebração ou o cumprimento de contrato (alínea *b*), bem como a cláusula de ponderação, segundo a qual o tratamento só é inadmissível em caso de preponderância dos interesses do titular dos dados (alínea *f*). Para o tratamento estatal de dados, aplicam-se principalmente os fundamentos jurídicos para o tratamento de dados com base em obrigação jurídica (alínea *c*), bem como para o tratamento de dados por interesse público (alínea *e*). Neste último caso, deve-se levar em conta que, no art. 6º, §§ 2 e 3, do RGPD, está contida uma chamada cláusula de abertura. Nessas cláusulas de abertura, existe – contrariando o caráter do RGPD como decreto segundo o art. 288º, § 2, do TFUE –, para os Estados-membros, a possibilidade de uma legislação divergente, especial ou, em todo caso, própria. Isso está expressamente previsto para o tratamento estatal de dados, de modo que sua justificação é objeto de regulações em Estados-membros. Por isso, neste caso – assim como no âmbito da Diretiva JAI –, as normas nacionais são vinculantes; na Alemanha, p. ex., a Lei Federal de Proteção de Dados (LFPD) e as leis estaduais de proteção de dados como leis aplicáveis em casos omissos, bem como um grande número de regulações especiais e normas avulsas.

Deve-se observar, porém, que o emprego de cláusulas de abertura não invalida as demais normas do RGPD; ou seja, elas continuam em vi-

49 Klement. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, art. 7, nº 65; cf. também o considerando 43 do RGPD.

50 EuGH, Rs. C-673/17 (Planet49), ECLI:EU:C:2019:801.

51 Hansen. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, art. 25, nº 8.

gor, sem alterações, e também precisam ser levadas em conta pelo Poder Público.

2.4 Princípio da vinculação à finalidade

O art. 1º, § 1, alínea *b*, do RGPD contém um princípio básico essencial do direito referente à proteção de dados desde seus primórdios, que tem uma conexão estreita com o princípio da proibição: em princípio, dados só podem ser tratados e utilizados pela instância responsável para a finalidade para a qual foram captados[52]. Ou em outras palavras: o tratamento de dados está vinculado a que ocorra para uma finalidade determinada, e isto se aplica a todos os seus passos. A finalidade define e limita o tratamento de dados a essa finalidade. Caso os dados sejam tratados em um passo adicional ou sejam, mais tarde, tratados para uma outra finalidade, faz-se necessária uma justificativa nova e à parte[53]. A vinculação à finalidade é um dos princípios centrais do direito de proteção de dados e adquire uma importância decisiva, levando em consideração a possibilidade de concatenação e recombinação aleatória de dados em tempos de *Big Data* e de uma captação quase ilimitada de dados[54].

Portanto, justamente não é possível inferir da presença – legal – de dados pessoais junto ao agente de tratamento de dados que, em consequência disso, qualquer tratamento adicional desses dados seja admissível, como o tentam formular, p. ex., a concepção de soberania sobre os dados, de doação de dados ou ainda abordagens relacionadas ao direito de propriedade.

Neste contexto, o art. 5º, § 1, alínea *b*, do RGPD, em associação com o art. 6, § 4º, do mesmo Regulamento, representa uma particularidade: dele se pode inferir que uma outra finalidade não exige uma nova justificativa e o tratamento de dados para uma nova finalidade ainda está coberto pela justificativa do tratamento original de dados se a nova finalidade for compatível ("*compliant*") com a finalidade original[55]. Segundo o art. 6º, § 4, do RGPD, para a avaliação se deve recorrer, entre outros, ao critério de quão estreita é a conexão entre a antiga e a nova finalidade, de quais as consequências que se devem esperar do tratamento ampliado de dados e outros semelhantes.

52 Hornung; Spiecker gen. Döhmann. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, Introdução, nº 36 s.

53 Veja detalhes quanto a isso em Roßnagel. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, art. 5, nº 96.

54 Simitis; Hornung; Spiecker gen. Döhmann. In: id. (Ed.), 2019, Introdução, nº 36; Spiecker gen. Döhmann, *Spektrum der Wissenschaft*, 2017, p. 56 ss; Hornung, *Spektrum der Wissenschaft*, 2017, p. 62 ss.

55 Roßnagel, 2019, art. 5, nº 97.

2.5 Princípio da minimização de dados

O princípio da parcimônia/minimização de dados do art. 5º, § 1, alínea *c*, do RGPD encontra-se, por sua vez, em estreita conexão com a vinculação à finalidade do art. 5º, § 1, alínea *b*, do mesmo Regulamento: justamente com referência à vinculação à finalidade a captação e o tratamento dos dados devem ser limitados em termos quantitativos e qualitativos. Os dados só são adequados à finalidade quando forem necessários para alcançar a finalidade[56]. Em termos bem fundamentais, esse princípio obriga os agentes de tratamento de dados a só captar e tratar dados quando outras possibilidades de consegui-los não são viáveis.

Por conseguinte, o princípio da minimização de dados estabelece um limite para tentativas de continuar guardando dados já tratados – de modo perfeitamente admissível – para além da finalidade original porque eles poderiam eventualmente ser usados para finalidades posteriores, atualmente ainda não definíveis. Isso também inclui coletas abrangentes de dados para o tratamento em *Big Data*, mas também métodos como o armazenamento e a conservação de dados na persecução penal. Neste tocante, o TEJ esclareceu repetidamente que a coleta de dados precisa ser limitada[57].

2.6 Princípio da transparência: deveres de prestar informações, direitos de acesso e dever de documentação

O princípio da transparência, contido em essência no art. 5º, § 1, alínea *a*, do RGPD, tem dois elementos que o concretizam e encontraram fundamentos próprios em diversas passagens do Regulamento para além da formulação genérica: por um lado, o titular dos dados deve ter condições de proceder a um controle próprio da forma como se lida com os dados. Para isso, são consagrados diversos direitos no RGPD. Por outro lado, porém, o responsável pelo tratamento também deve ser obrigado a proceder a uma verificação prospectiva da licitude do tratamento de dados, acompanhada de um dever de documentação.

Os direitos do titular dos dados de ter acesso ou obter informações, já previstos na DPD, são regulamentados, por um lado, pelo art. 15º do RGPD e, por outro, os deveres de prestar informações por parte do responsável pelo tratamento o são pelos arts. 13º e 14º do mesmo Regulamento, que cor-

56 Simitis; Hornung; Spiecker gen. Döhmann, 2019, Introdução, nº 37.

57 EuGH, verb. Rs. C-293/12, C- 594/12 (Digital Rights Ireland), ECLI:EU:C:2014:238; EuGH, verb. Rs. C-203/15, C-698/15 (Tele2 Sverige), ECLI:EU:C:2016:970.

respondem a um respectivo direito à informação. Por isso, as duas posições jurídicas encontram-se em estreita conexão; o direito de acesso estende-se ao menos às informações que precisam ser disponibilizadas de qualquer modo. Os arts. 13º e 14º do RGPD exigem do responsável pelo tratamento dos dados que disponibilize ativamente uma série de informações quando os dados são levantados por ele mesmo ou por um terceiro. Isso compreende informações sobre o responsável, as finalidades e o fundamento jurídico do tratamento, eventualmente interesses legítimos do responsável ou de terceiros, destinatário, intenção de transferência para países terceiros e garantias previstas (§ 1 em cada caso). Além disso, o responsável pelo tratamento dos dados deve disponibilizar à pessoa interessada as informações necessárias para garantir a ela um tratamento equitativo e transparente (§ 2 em cada caso: p. ex., duração do armazenamento, decisões automatizadas em casos avulsos, fonte dos dados, existência de um direito de reclamação junto a uma autoridade de fiscalização)[58]. Essas informações é que dão ao titular dos dados condições de avaliar a licitude do tratamento de dados e, eventualmente, recorrer a direitos contrários.

Inversamente, porém, o responsável pelo tratamento dos dados também tem o dever de assegurar – para além da mera prestação de informações e de acesso – transparência no sentido de que pode comprovar, de acordo com o art. 24º, § 1, alínea *1*, do RGPD, que o tratamento dos dados ocorreu de maneira lícita. Isso implica – o que vai claramente além do que previa a DPD – que o agente de tratamento dos dados está *de fato* sujeito a deveres de documentação e verificação, pois a comprovação só será bem-sucedida se os problemas jurídicos referentes à proteção de dados forem identificados, analisados e levados em consideração. Medidas concomitantes como a possibilidade ou até a obrigação de contratar um encarregado da proteção de dados na empresa (art. 37º do RGPD) apoiam essa preocupação do legislador europeu. Essa transparência diz respeito não apenas ao titular dos dados, mas também se aplica às autoridades que lidam com a proteção de dados: elas podem exigir o cumprimento da transparência e também exigir que a documentação seja entregue, p. ex., para poder avaliar a gravidade de uma violação do RGPD no marco de um processo que envolva uma multa.

58 Scholz. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, art. 4, nº 4, nº 12.

2.7 Transferência de dados para o exterior fora da União Europeia: adequação

Há muito tempo o tráfego de dados ocorre de forma globalizada. Por isso, o RGPD também regula – dando continuidade à DPD – de que maneira e sob que condições dados podem ser transferidos para países estrangeiros fora da UE. A reflexão básica é, inicialmente, que com o RGDP se cria um mercado interno de dados, de modo que dentro da UE dados pessoais podem ser transferidos livremente – dentro dos limites do Regulamento. Agora um tratamento de dados feito na Lituânia, na Áustria ou em Portugal está sujeito a regras jurídicas idênticas. Essa era uma preocupação central do RGPD com a uniformização, que vai claramente além da harmonização visada pela DPD.

A situação é outra no que diz respeito à transferência de dados para um país situado fora da UE. Nesse caso, vale inicialmente o princípio de que uma transferência de dados não é permitida. O livre mercado de dados termina na fronteira da EU para o exterior. Entretanto, em casos excepcionais, existe a possibilidade de uma transferência de dados. Para isso, é necessário que haja uma chamada adequação em relação ao país destinatário (art. 44º do RGPD). Essa adequação pode concernir a todo o âmbito do direito no país destinatário, mas também a um setor da indústria ou a um âmbito parcial.

A adequação pode ser constatada de três formas: ou os envolvidos chegam a um acordo quanto a "*corporate binding rules*" (art. 47º do RGDP), ou se sujeitam a "*standard contractual rules*" (art. 46º do RGPD), ou a Comissão Europeia tomou uma chamada decisão de adequação (art. 45º do RGPD). Portanto, o Regulamento possibilitou um acesso diferenciado, que concede às partes de uma transferência de dados possibilidades de estruturação. Visto que também se pode lançar mão de condições contratuais, os agentes de tratamento de dados envolvidos também podem prever regulações e garantias próprias independentemente da situação jurídica no país terceiro fora da UE.

Existe uma adequação quando no país destinatário um nível comparável de proteção de dados estiver garantido. Não obstante, o padrão de proteção não precisa ser idêntico. O que ainda não está claro, entretanto, é quais são as exigências mínimas para se poder supor que haja adequação. O TEJ formulou primeiras referências a esse respeito em sua decisão sobre

a troca de dados com os EUA[59]: segundo ela, é necessário um acesso irrestrito e incondicionado aos tribunais, sendo que mecanismos alternativos de resolução de litígios também podem estar incluídos; além disso, não pode haver garantia de acesso ilimitado – também não por parte de autoridades – aos dados; pelo contrário, a vinculação à finalidade precisa ser mantida, e precisa haver um controle eficaz. Mecanismos de autorregulamentação são perfeitamente possíveis. É preciso esperar para ver se o TEJ concretizará suas exigências mais ainda. O ensejo para isso é oferecido por um outro processo que está no TEJ[60] contra o fundamento para a troca de dados com os EUA, o chamado *Privacy Shield*[61]. Nesse caso, possivelmente a questão de até que ponto possibilidades de acesso a dados por parte das autoridades deverão ser incluídas na verificação da adequação também seja tematizada.

O procedimento adotado pelo Japão causou uma certa sensação: o direito japonês de proteção de dados foi desenvolvido com forte inspiração do RGPD, de modo que a Comissão da UE constatou, pouco tempo depois da aprovação da nova lei japonesa sobre proteção de dados, a adequação para o país todo, inaugurando, com isso, o maior espaço geográfico e virtual para transferência de dados entre a Europa e a Ásia[62].

2.8 Privacy by design e privacy by default

O fato de o direito referente à proteção de dados ser um direito de regulamentação de tecnologia marcado pelo princípio da precaução acarreta uma estruturação e programação tecnológica orientada pela proteção de dados. O que se encontra por trás disso é a noção da chamada *privacy by design* e *privacy by default* segundo o art. 25º do RGPD. O ponto de partida dessas concepções é que a melhor maneira de implementar as noções jurídicas sobre a proteção de dados se dá caso esta última já esteja integrada na programação e concepção arquitetônica dos processos de tratamento de dados e da tecnologia destes[63]. Por conseguinte, ao menos com essa norma também o desenvolvedor e o programador são, ao menos indiretamente, incluídos nas obrigações previstas no RGPD, pois o Regulamento não se

59 EuGH, C-362/14 (Schrems), ECLI:EU:C:2015:650.

60 EuGH, Rs. C-311/18 (Schrems II).

61 Veja uma visão panorâmica dessa questão em Hornung; Spiecker. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, Introdução, nº 261.

62 EU-Commission. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/de/IP_19_421>. Acesso em: 21 nov. 2019.

63 Hornung; Spiecker gen. Döhmann. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, Introdução, nº 245; Hartung. In: Kühling; Buchner (Ed.), *Datenschutz-Grundverordnung*, 2. ed., 2018, art. 25, nº 11.

dirige a eles, colocando a responsabilidade sobre o agente de tratamento de dados que utiliza o tratamento automatizado deles. Em última análise, essa norma possivelmente repercuta sobre o direito contratual, pois deve-se refletir sobre a eventual existência de uma violação contratual no relacionamento entre desenvolvedor do produto e o agente de tratamento de dados quando o produto informacional adquirido não cumprir as exigências do RGPD.

3 ESTRUTURAS DE EFETIVAÇÃO DO RGDP

Como já se mencionou, um dos ensejos para a reforma do Direito europeu referente à proteção de dados por meio do RGPD foi a existência de uma considerável deficiência em termos de efetivação[64]. O direito de proteção de dados existente sob a DPD não era implementado e cumprido ou não o era de modo eficaz. Faz-se frente a esse problema por meio de diversas estruturas de efetivação.

3.1 As pessoas interessadas e seus direitos

O ponto de partida da efetivação continua sendo o titular de dados. O RGPD concede-lhe uma série de posições jurídicas individuais. Elas visam servir para que as exigências jurídicas de proteção de dados sejam implementadas e a pessoa interessada mantenha o controle sobre os dados e as decisões neles baseadas. A maioria desses direitos encontra-se nos arts. 12º e seguintes do RGPD.

Deles fazem parte os já mencionados deveres de prestar informações do responsável pelo tratamento dos dados a partir dos arts. 12º, 13º e 14º do RGPD, aos quais corresponde um respectivo direito à informação[65]. Central é, além disso, o direito de obter informações da pessoa interessada consoante o art. 15º do RGPD, segundo o qual ela pode pedir informações, p. ex., sobre os dados tratados, as finalidades do tratamento, os destinatários aos quais os dados são revelados, bem como a duração prevista da armazenagem.

Visto que não pode bastar que o titular de dados tenha ciência das formas de tratamento, os direitos à informação são secundados por uma série de outros direitos, que podem restringir consideravelmente o agente de

64 Hornung; Spiecker gen. Döhmann. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, Introdução, nº 209.

65 Scholz, 2019, art. 4, nº 4, nº 12.

tratamento em sua utilização ulterior dos dados. O que tem maior alcance é o direito ao apagamento ou remoção dos dados a partir do art. 17º, que ocasionalmente é chamado de maneira enganosa de "direito a ser esquecido"[66]. Ele é complementado por um dever de prestar informações a partir do art. 17º, § 2, do RGPD: segundo ele, quem tornou públicos os dados sobre uma pessoa interessada precisa tomar medidas para informar outras instâncias responsáveis que essa pessoa está pedindo a remoção de todos os *links* para esses dados, bem como de cópias deles. Com isso, a posição da pessoa interessada é consideravelmente melhorada justamente no tocante a publicações na internet[67].

De menor alcance, mas ainda assim eficazes são os direitos de retificação segundo o art. 16º do RGPD, correspondente ao princípio da exatidão dos dados a partir do art. 5º, § 1, alínea *d*, do mesmo Regulamento, bem como o direito de oposição segundo o art. 21º para levar em consideração circunstâncias particulares. E também os direitos à indenização, no art. 82º do RGPD – agora também por danos chamados imateriais no art. 82º, § 1, do mesmo Regulamento –, bem como à reclamação às autoridades de fiscalização independentes segundo o art. 77º, fortalecem a posição do titular dos dados. De modo geral, com isso a probabilidade de implementação aumenta, os custos para os agentes de tratamento de dados que os processam contrariando o RGPD tornam-se mais altos e a probabilidade de que as normas sejam cumpridas fica maior.

3.2 As autoridades independentes para a proteção de dados

Desde os primórdios do direito referente à proteção de dados, já estava claro que uma implementação desse direito unicamente por parte do titular de dados não seria suficiente por causa das propriedades específicas das informações e das estruturas específicas. Lembremos que, frequentemente, dados podem ser usados muitas vezes e que dados passam a fazer parte de decisões sem que se possa depreender isso das próprias decisões. Por isso, já na decisão do Tribunal Constitucional Federal alemão sobre o censo populacional, a salvaguarda através de procedimentos e da organização foi elevada à condição de princípio[68].

66 Cf. Dix. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, art. 17, nº 1.
67 Quanto a isso, veja ibid., art. 17, nº 26 ss.
68 Cf. BVerfGE 65, 1 (44).

Um elemento central dessa proteção concomitante através do direito procedimental e organizacional é a institucionalização de autoridades de fiscalização independentes nos Estados-membros (art. 51º e seguintes do RGPD). O RGPD amplia e complementa as competências e os deveres pregressos (cf. arts. 57º e 58º do Regulamento) e, além disso, torna mais precisas as normas procedimentais. Com isso, ele retoma as diretrizes do art. 3º, § 3, da Carta dos Direitos Fundamentais, segundo o qual a instituição de instâncias independentes de controle está prescrita para o cumprimento das diretrizes do art. 8º, § 1, 2, da Carta. Uma alteração substancial introduzida pelo RGPD é a competência das autoridades de fiscalização para aplicar multas (art. 83º do Regulamento).

O postulado de independência rigorosa é valorizado e tornado ainda mais preciso com base na jurisprudência pregressa e ainda em vigor[69] do TEJ[70]. Os Estados-membros devem garantir que essas autoridades sejam adequadamente equipadas (art. 52º, § 4, do RGPD). Já agora se pode perceber que os esforços de efetivação por parte dos Estados-membros aumentaram consideravelmente.

3.3 O *European Data Protection Board* (EDPB) e o mecanismo de coerência na *One-Stop-Shop*

A efetivação do RGPD por parte de autoridades de fiscalização dos *Estados-membros* acarreta fundamentalmente a problemática de decisões divergentes. Isso podia ser observado em grau considerável sob a SPD. O RGPD faz frente a essa problemática mediante a introdução de um processo de colaboração que assegura uma coordenação uniforme e melhor entre as autoridades nacionais responsáveis pela implementação[71]. Isso acontece no chamado mecanismo de coerência, até agora desconhecido no direito da UE. Para isso se instituiu o Comitê Europeu de Proteção de Dados (*European Data Protection Board* – EDPB), em que cada País-membro está representado por uma autoridade de fiscalização e que decide, majoritariamente, segundo o princípio "*one-agency-one-vote*" (art. 68º ss. do RGPD). Com isso se garante que decisões importantes não possam ser tomadas pelas autoridades dos Estados-membros por conta própria, mas que agora se precise se-

69 Cf. quanto a isso Schiedermair. In: Simitis; Hornung; Spiecker gen. Döhmann (Ed.), 2019, Introdução, nº 169 ss.

70 EuGH, Rs. C-288/12 (Kommission/Ungarn), ECLI:EU:C:2014:237; EuGH, Rs. C-614/10 (Kommission/Österreich), ECLI:EU:C:2012:631; EuGH, Rs C-518/07 (Kommission/Deutschland), Slg 2010, I-1885; EuGH, Rs. C-230/14 (Weltimmo), ECLI:EU:C:2015:639.

71 Simitis; Hornung; Spiecker gen. Döhmann. In: id. (Ed.), 2019, Introdução, nº 90.

guir um caminho conjunto. Isso é secundado pelo fato de que, de agora em diante, também para os agentes do tratamento de dados só existe um interlocutor na forma de uma autoridade de fiscalização chamada "*lead authority*" (art. 56º do RGPD), de modo que, no marco dessa "*One-Stop-Shop*", haverá uma simplificação considerável para as empresas.

4 PERSPECTIVAS E CONCLUSÃO: DESAFIOS E NOVAS ABORDAGENS DE REGULAÇÃO

O RGPD trata-se uma série de problemas que estão surgindo para o Direito e a sociedade em função da digitalização. Ele faz isso sob um ângulo específico, a saber, a proteção de dados pessoais. Com isso, forçosamente, não aborda determinadas áreas ou só o faz de maneira limitada. Ainda assim, o RGPD, na qualidade de direito parcial[72] mais abrangente do direito informacional público e privado na atualidade, disponibiliza ao menos rudimentos de um tratamento normativo para algumas outras áreas de problemas.

4.1 Decisão automatizada, algoritmos, inteligência artificial e aprendizado de máquina

Tratamos aqui de outros desdobramentos de tecnologias já existentes, sem que se possa entrar em detalhes técnicos. Eles colocam uma série de exigências em relação à sua utilização, principalmente quanto à transparência do tratamento de dados que realizam, à avaliação e às decisões neles baseadas.

Embora o direito referente à proteção de dados não tenha aplicação a muitas formas de tratamento de dados nesse âmbito, já que, em geral, ocorre uma dissolução da referência a pessoas por causa da anonimização ou da integração em dados massivos, o RGPD manifesta-se, no art. 22º, sobre as decisões que os tomam por base: em princípio, ele exige que não se pode tomar uma decisão unicamente mediante um tratamento automatizado. As exceções a isso que se encontram no art. 22º, § 2, do RGPD permitem, ainda assim, que, em muitos casos, decisões possam ser tomadas de modo completamente automatizado. Além disso, a inclusão da definição de perfis (*profiling*), que usa muitas formas de inteligência artificial, é um dos casos previstos na legislação nos quais, por causa da existência de um risco especialmente elevado para o titular de dados, é necessária uma avaliação dos riscos segundo o art. 35º do RGPD. Afinal, uma das finalidades inerentes ao

72 O direito sobre telecomunicações e o direito da propriedade intelectual são, além de outras matérias jurídicas, áreas parciais importantes do direito da informação, mas ela são mais estreitas em seu âmbito de aplicação.

direito de proteção de dados é evitar discriminações[73]. Consequentemente, deve ser mais aconselhável realizar simulações do que treinar inteligência artificial com dados reais.

4.2 A globalização e a luta pela internet

O RGPD é um conjunto de regulações europeu. Entretanto, em face do fluxo ubíquo de dados que ultrapassa todas as fronteiras, principalmente por causa da forma de funcionamento da internet, ele deve ser levado em consideração em função do princípio do local do mercado (art. 3º, § 2, do RGPD) e do princípio do estabelecimento (art. 3º, § 1). Ainda que, em última análise, o TEJ tenha restringido a efetividade de direitos contrários de pessoas interessadas ao espaço europeu[74], as repercussões do RGPD são, não obstante, globais.

Por um lado, o princípio da adequação exige, quando da transferência de dados para o espaço jurídico fora da UE, uma harmonização em potencial. Por outro, não se deve subestimar o papel pioneiro desempenhado pela UE na regulamentação da utilização e do tratamento de dados pessoais, que até agora não têm sido objeto de uma regulamentação ampla. Com isso surge – passando ao largo das posições de supremacia ocupadas atualmente por algumas empresas – a possibilidade de um novo mercado para produtos e serviços que tenham uma atitude favorável para com a proteção de dados. Dessa maneira, um mercado supostamente já subdividido é redefinido de maneira nova e as regras de mercado são alteradas. Por conseguinte, as regulamentações do RGPD[75] – caracterizadas por liberalidade e proteção do indivíduo – estabelecem um novo marco jurídico que também repercute em nível internacional.

4.3 Última observação

Atualmente ainda está em aberto qual é a direção que o direito de proteção de dados na Europa irá tomar. Não resta dúvida, porém, de que, com isso, a UE deu um passo considerável para fortalecer a posição fática e jurídica do indivíduo, o chamado titular de direitos. Isso deve acontecer em uma relação de equilíbrio com outros direitos, como a liberdade de informação e de expressão. Mas, assim como essas liberdades, uma proteção de

73 Hornung; Spiecker gen. Döhmann, 2019, art. 1, nº 31.
74 EuGH, Rs. C-507/17 (Google LLC), ECLI:EU:C:2019:772.
75 Hornung; Spiecker gen. Döhmann, 2019, art. 1, nº 36.

dados funcional é imprescindível para assegurar a democracia e a liberalidade[76]. Neste sentido, o RGPD está criando um marco jurídico importante.

Sobre a autora:

Indra Spiecker genannt Döehmann | *E-mail*: czoik@jur.uni-frankfurt.de
W3-Chair of Public and Administrative Law, Information Law, Environmental Law and Legal Theory, Goethe University Frankfurt a.M., Director Research Center for Data Protection, Co-Director Research Institute on Environmental Law, Co-Director Institute of European Health Politics and Social Law (Ineges).

Data da submissão: 26 de junho de 2020.
Data do aceite: 6 de julho de 2020.

76 Cf. Spiecker gen. Döhmann, VVDStRL, 2018, 9 (55).