ALGUMAS REFLEXÕES EM TORNO DO RGPD, EM ESPECIAL QUANTO AO CONSENTIMENTO, COM ALUSÕES À LGPD (UM EXERCÍCIO INTERPRETATIVO)

Regina Linden Ruaro

Doutora em Direito pela Universidad Complutense de Madrid (1993 com título revalidado pela UFRGS em 1993). Pós-Doutora pela Universidad San Pablo – CEU de Madri. Professora titular da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Membro da Comissão Coordenadora do Programa de Pós-Graduação em Direito da Faculdade de Direito da PUCRS. Procuradora Federal/AGU (aposentada). Compõe o Grupo Internacional de Pesquisa "Protección de datos, transparencia, seguridad y mercado". *Lattes*: http://lattes.cnpq.br/8023231740817826.

Resumo: O novo Regulamento (União Europeia – UE) 2016/679, agora simplesmente RGPD, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, reforça e harmoniza as regras de proteção dos direitos e liberdades de privacidade dos indivíduos no ambiente europeu e, em determinadas condições, fora do território da UE. Este novo marco normativo prolonga e atualiza o acervo da UE da anterior Diretiva de proteção de dados 95/46/CE. O RGPD fixa as regras gerais aplicáveis a qualquer tipo de processamento de dados pessoais e regras específicas aplicáveis ao processamento de categorias especiais de dados pessoais. Este ensaio tem como objetivo fornecer uma visão geral do RGPD, no que diz com o consentimento e com a autodeterminação informativa. Também menciona, ainda que brevemente, a Lei brasileira de Proteção de Dados, aqui apenas LGPD (Lei nº 13.709/2018).

Palavras-chave: RGPD. LGPD. Consentimento. Autodeterminação. Dados. Processamento.

1 Introdução

Após um longo período sem norma específica versando acerca do direito à proteção de dados pessoais no Brasil, em 2018, finalmente, foi promulgada a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais – LGPD, que trata da matéria e que entrará em vigor no ano de 2020.

Em um cenário em que a coleta e o tratamento de dados que conjugados propiciam a formação de perfis e *big data* a partir do uso das tecnologias de informação e comunicação (TIC), impõe-se uma modificação no pensar e agir da sociedade em geral. É que, com o advento da Lei Geral de Proteção de Dados Pessoais – LGPD, surge a necessidade de uma tomada de consciência acerca de todas as questões relativas à privacidade, à autodeterminação informativa, ao livre desenvolvimento da personalidade na perspectiva de que todas as ações que os envolvem deve ser norteada a partir de fundamentos que visam à dignidade da pessoa humana, princípio basilar do Estado Democrático de Direito. Todavia, ainda em *vacatio* (entra em vigor em 2020), *mas ao lado* do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27.4.2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, a partir de agora simplesmente RGPD.[1]

Neste artigo se busca refletir sobre o tema do processamento e da proteção de dados de modo amplo e simplificado, partindo-se do consentimento. Proteção de dados, a (nova) estrutura legal e processamento baseado em consentimento. O direito fundamental à proteção de dados é atualmente no ambiente europeu (entre outros instrumentos) regido pelo RGPD e suas implementações e similares de muitas nações em todas as latitudes do planeta. Este novo quadro jurídico traz muitas alterações para a proteção de dados na União Europeia, agora simplesmente EU e demais países ocidentais identificados com o Estado de Direito. Na Europa, especialmente, e em primeiro lugar, porque agora se trata de um regulamento em vez de uma diretiva, o que tem grandes implicações de ordem instrumental pela sua compulsoriedade.

Um dos fundamentos legais para o processamento legal de dados pessoais que é alterado é o consentimento. O processamento baseado no consentimento pode ser considerado como processamento baseado na permissão do indivíduo cujos dados são processados. O consentimento como base para o processamento desempenhou papel importante nas concepções de proteção de dados e privacidade. De fato, a maioria diária, ordinária das atividades de processamento que nos cercam utilizam o consentimento como base legal.

1.1 Problema de pesquisa: consentir agora e depois

O uso do consentimento como base para o processamento de dados pessoais é considerado problemático por não fornecer proteção de dados adequado em

[1] O Regulamento Geral de Proteção de Dados (RGPD, pelo acrônimo em português) entrou em vigor em 25.5.2018 (Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT) (*link* permanente).

ambientes *on-line*. O consentimento de serviços é, em muitos casos, em grande parte teórico, não tendo significado prático, uma vez que a maioria das pessoas apenas concorda com algo que não leu ou entendeu.

Devemos distinguir uma série de razões práticas para isso. Primeiro de tudo, há uma "transação sobre o consentimento". Há simplesmente muitos pedidos de consentimento para que os indivíduos considerem, ver o efeito psicológico de ser confrontado com uma transação de consentimento. Em segundo lugar existe uma "sobrecarga de informação", o que significa que aos indivíduos são apresentadas informações muitas vezes difíceis e altamente legalistas em "transações de consentimento". De acordo com o caso em particular, *sites* "gratuitos", como o Facebook, têm todo o incentivo para fazer avisos de privacidade já que seu produto é o acesso a pessoas que tenham ingressado de modo informal no tráfego de informações. Em terceiro lugar, os indivíduos não têm realmente uma escolha significativa quando recebem pedido de consentimento, e são deixados com um cenário não negociável – "pegar ou largar". Koops menciona a este respeito que não existe alternativa realista a esta prática, pois a maioria dos prestadores de serviços aplica as mesmas práticas.[2] Além disso, relativo a esta ausência de escolha significativa, Hull escreve que se tornará cada vez mais difícil resistir à informação e divulgação com mais e mais movimentos de vida *on-line*. Hull menciona que o Facebook, *site* de rede, por exemplo, tem sido amarrado ao "capital social dos estudantes universitários" por anos, e que pedir a um aluno para deixar o Facebook em favor de sua privacidade teria um preço alto.[3] Por causa das três razões práticas mencionadas anteriormente, Schermer, Custersand e Hof falam do "consentimento dessensibilização": os usuários deixam de fazer escolhas ativas e informadas quando confrontados com situação de consentimento, mas apenas optar por fornecer consentimento quando solicitado.[4]

Solove aprofunda o assunto e afirma que a atual ideia de gestão da privacidade, com o consentimento sendo a sua implementação, não proporciona às pessoas controle significativo sobre seus dados, uma vez que diversos problemas afetam a noção de gestão.[5] De acordo com Solove, a autogestão da privacidade implica problemas cognitivos que dizem respeito a desafios causados pela forma

[2] KOOPS, Bert-Jaap. The Trouble with European Data Protection Law (August 29, 2014). International Data Privacy Law. Forthcoming. *Tilburg Law School Research*, Paper 1, 04/2015. Disponível em: https://ssrn.com/abstract=2505692 (*link* permanente).

[3] HULL, G. Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics Inf Technol*, v. 17, n. 2, p. 89-101, 2015.

[4] SCHERMER, B. W.; CUSTERSAND, B.; VAN DER HOF, S. The crisis of consent: how stronger legal protection may lead to weaker consent. *Data Protection, Ethics & Information Technology*, v. 16, n. 2, p. 171-182, 2014.

[5] SOLOVE, Daniel J. Conceptualizing privacy. *California Law Review*, v. 90, p. 1087-1155, 2002.

como os humanos tomam decisões, e problemas estruturais sobre os desafios decorrentes de como as decisões de privacidade são tomadas.[6] Como Koops, Schermer, Custersand e Hof escreveram, um dos problemas (cognitivos) é que os indivíduos são frequentemente desinformados porque não leem aquilo com o qual consentem.[7] Uma possível explicação para isso de acordo com Solove é que os avisos de privacidade são longos e difíceis de compreender. Segundo o autor, também há um problema mais difícil com propostas de avisos aprimorados, como tornar os avisos mais simples e mais fáceis de entender com informação completa aos indivíduos. Outro problema cognitivo é o problema de tomada de decisão distorcida. Mesmo que os indivíduos leiam e entendam as "condições de proteção da privacidade", eles não teriam a experiência necessária para avaliar plenamente as consequências, concordando com esses textos. Isso ocorre porque as pessoas têm "racionalidade limitada", o que significa que eles lutam para aplicar seus conhecimentos em situações complexas.[8]

No entanto, mesmo que os indivíduos sejam informados e racionais, o sistema ainda enfrenta problemas estruturais. O primeiro problema é que há muitas entidades coletando dados, o que pode fazer do consentimento um misto de decisões impossíveis de serem manipuladas pelos indivíduos. Um segundo problema é o problema de agregação. Os indivíduos lutam para avaliar como seus dados podem ser agregados no futuro. A razão para isto é que "pedaços" de dados[9] (considerados insignificantes) que são coletados agora, no futuro, combinem-se e revelem informações sensíveis. Uma terceira dificuldade diz respeito ao fato de que as pessoas têm dificuldade em avaliar os danos (futuros). O motivo para isso é que a privacidade é uma questão de longo prazo, enquanto a maioria das decisões de consentimento está vinculada a benefícios de curto prazo.

Os pontos acima mencionados deixam claro que o processamento de dados pessoais pode ser baseado quando o consentimento é o caminho que é tomado pelo controlador ou processador de dados, e o consentimento pode não retratar os desejos do indivíduo. Moerel e Prins anotam a esse respeito um "procedimentalismo mecânico", em que os responsáveis pelo tratamento de dados notificam os indivíduos e solicitam consentimento de maneira mecânica, sem oferecer proteção efetiva de dados. De acordo com eles, o consentimento é em muitos casos tornado sem sentido porque as empresas antecipam que as pessoas

6 SOLOVE, Daniel J. A taxonomy of privacy. *University of Pennsylvania Law Review*, v. 154, n. 3, jan. 2006; *GWU Law School Public Law Research*, Paper 129. Disponível em: https://ssrn.com/abstract=667622 (*link* permanente).

7 Cf., notas n. 2 e 4, *retro*.

8 Cf., SOLOVE, Daniel J. Conceptualizing privacy. *California Law Review*, v. 90, p. 1087-1155, 2002.

9 Isto é, fragmentos de dados coletados nos diferentes percursos do processamento.

rotineiramente dão seu consentimento.[10] Dado o fato de que o consentimento era e ainda parece ser uma importante maneira de legitimar o processamento de dados pessoais, essas críticas são preocupantes.

As críticas significam que o processamento de dados atual baseado no consentimento pode ser falho. Ao invés de capacitar indivíduos e conceder-lhes mais controle sobre seus dados pessoais, pode oferecer muito pouco controle na prática, como indivíduos podem apenas consentir de vez em quando, sem escolha adequada e/ou pensamento reflexivo. No entanto, o consentimento está presente no RGPD. O uso continuado do consentimento levanta algumas questões. Uma primeira pergunta é quais são as mudanças. Outra questão que levanta é porque nós atribuímos o consentimento como um papel proeminente como um meio de legitimar o processamento de dados que insistimos em continuar a usar.

Para a elaboração dessas breves reflexões utilizamos como metodologia o método indutivo e de interpretação jurídica pautado na coleta e análise bibliográficas e legislativas. Salienta-se que o presente ensaio está ancorado na linha de pesquisa Direito, Ciência, Tecnologia & Inovação e no Projeto de Pesquisa, A proteção dos dados pessoais na sociedade de vigilância: o direito fundamental a privacidade do Programa de Pós-Graduação em Direito da PUCRS, bem como dentro de um Projeto maior, internacional, da Universidade San Pablo de Madrid (Espanha) financiado pelo Ministério Espanhol de Economia e Competitividade, Referência DER2016-79819-R.

2 Consentimento legal para o processamento de dados pessoais

O processamento de dados pessoais não pode ser feito livremente sem consequências, pois existe o direito à privacidade e o direito à proteção de dados, em particular. O processamento de dados pessoais é, além disso, permitido apenas de acordo com certos princípios. Estes princípios importantes podem ser encontrados em várias fontes, quase idênticas. Eles afirmam (entre outras coisas importantes) que o ato de processar dados pessoais tem que ser legal e justo, que os dados pessoais são coletados apenas para fins específicos, explícitos e legítimos e que os dados recolhidos são adequados, relevantes e não excessivos em relação ao objetivo para o qual são processados. Além disso,

[10] MOEREL, E. M. L.; PRINS, Corien. *Privacy for the homo digitalis*: proposal for a New regulatory framework for data protection in the light of big data and the internet of things. 2016. Disponível em: http://dx.doi.org/10.2139/ssrn.2784123 (*link* permanente).

os dados coletados devem ser precisos e não podem ser mantidos por mais do que o necessário para a finalidade para a qual os dados são coletados.[11] Os princípios são, no entanto, muito gerais por natureza, o que deixa espaço para interpretação e discussão em situações concretas. Devido a esta margem de interpretação, exige-se para a proteção dos dados lançados no mercado regras mais pormenorizadas, como as da EU e, agora as do Brasil, grafadas na Lei Geral de Proteção de Dados (a seguir apenas LGPD).

A UE adotou, por conseguinte, regras mais concretas no RGPD, assim como o Brasil, que expressou, de modo rígido, o consentimento: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5º, XII da Lei nº 13.709/18). Regras importantes que foram criadas são regras sobre a legalidade do processamento. Essas regras limitam o número de motivos pelos quais os dados podem ser legalmente processados, oferecendo uma base para processar dados pessoais de forma legal. Isso é importante como limitação dos direitos fundamentais (como o direito à privacidade), isto, no entanto, não parece significar que toda atividade de processamento de dados deve ser vista automaticamente como uma interferência porque as atividades de processamento de dados diferem enormemente em ambos os tipos e impacto na privacidade.

Cada atividade de processamento de dados deve ter uma base legal. De acordo com a legislação de regência para que uma atividade de processamento seja permitida, ela deve estar de acordo com os princípios e as regras sobre a legalidade do processamento. A conexão entre os princípios, por um lado, e as regras, por outro lado, podem ser descritas da seguinte forma: os princípios afirmam que os dados devem ser processados legalmente, enquanto as regras estabelecem que os dados pessoais só são lícitos e na medida em que pelo menos uma das bases jurídicas aplica-se. Essa conexão, no entanto, não é explicitamente declarada tanto no RGPD como na LGPD.

2.1 As mudanças no consentimento

As mudanças em relação ao consentimento como base legal para o processamento de dados pessoais serão agora discutidas. Além de introduzir algumas coisas novas para consentir, isto é, para o procedimento do consentir, as regras atuais relativas ao consentimento também são esclarecidas através dos

[11] Cf., nesse sentido, MENDES, Laura Schertel Ferreira. *Privacidade, proteção de dados e defesa do consumidor* – Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2017.

considerandos e *artigos* do RGPD e em menor medida na LGPD. O RGPD trouxe algumas alterações aos requisitos de um consentimento válido, introduziu o direito de retirar o consentimento, introduziu um "ônus da prova" para os controladores de dados provarem que um indivíduo consentiu, e formulou regras especiais relativas ao consentimento de menores. Digno de nota é o fato de que tornar o consentimento mais estrito, usando uma interpretação restrita do conceito e adicionando mais requisitos formais, por si só, não melhorou a proteção de dados dos indivíduos. Segundo Purtova, o consentimento, que é um dos mais importantes direitos de controle, perde significância como fundamento do processamento legal quando os requisitos formais são reforçados para consentir e difíceis de cumprir.[12] Além disso, Schermer, Custersand e Hof explicam que neste contexto o consentimento perde o seu valor na prática quando é realizado de modo mais rigoroso no sentido de que é sempre necessário ser explícito (uma mudança proposta que [felizmente] não foi incluída no texto final do RGPD). Por conseguinte, continua a ser uma questão em aberto se as alterações ao consentimento melhoram a proteção dos dados dos indivíduos.

2.2 O ato de consentir sob o RGPD

Muitas das mudanças que o RGPD traz dizem respeito aos requisitos de um consentimento válido. O RGPD esclarece os já conhecidos conceitos e especifica que o consentimento deve ser dado por uma declaração ou afirmação de ação. Além disso, ele afirma que o silêncio, de "caixas" (nos formulários) previamente preenchidas, a inatividade, a falta de *opt-out* ou aquiescência passiva não constituem consentimento válido.[13] Como resultado disso, consentimento passivo ou *opt-out* é, portanto, oficialmente declarado impossível, e somente o consentimento por ação afirmativa é permitido. No entanto, esta alteração não parece significar que o consentimento implícito é excluído pelo RGPD. De acordo com o regulamento, o consentimento pode ser dado por qualquer declaração ou conduta que indique claramente, neste contexto, a aceitação da pessoa do processamento proposto. A razão para esta mudança pode muito provavelmente ser encontrada no desejo de esclarecer e possivelmente harmonizar todas as leis

[12] PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 40-81, 2018. Disponível em: https://bit.ly/2w3iKFu (*link* permanente).

[13] O termo *opt-out* refere-se a vários métodos pelos quais os indivíduos podem evitar receber informações não solicitadas sobre produtos ou serviços. Essa capacidade é geralmente associada a campanhas de *marketing* direto, como *marketing* por *e-mail* ou mala direta.

do estado-membro da EU, outros aspectos da proteção de dados, beneficiando o mercado interno da UE e oferecendo uma opção de proteção de dados. Isto porque o grupo de trabalho (do RGPD) já tinha uma opinião semelhante em relação ao consentimento passivo. Além disso, o silêncio total para entregar um consentimento válido foi considerado, também, como impossível na literatura.

2.3 Consentimento livre dado sob o RGPD

Uma segunda diferença diz respeito ao fato de que o consentimento deve ser dado livremente. De acordo com o RGPD não se deve fornecer uma base legal válida para o processamento de dados pessoais caso exista um claro desequilíbrio entre o titular dos dados e o responsável pelo tratamento, lembrando sempre que o controlador de dados é uma autoridade pública. Isso pode implicar que o consentimento não deve mais ser considerado um bom fundamento jurídico para certas atividades de tratamento entre autoridades e cidadãos ou empregadores e empregados, pois nesses contextos há um desequilíbrio inerente entre as partes. A proposta original para o RGPD feita pela Comissão incluiu a relação empregado *vs.* empregador em seu texto inicial, no entanto, parece ter desaparecido na versão definitiva.[14] No entanto, o consentimento em contextos de emprego é geralmente considerado inadequado. Segundo o grupo de trabalho, é enganador se um empregador procura legitimar o processamento dos dados de seu empregado por meio do consentimento, em alguns contextos de emprego, no entanto, o consentimento pode ter seus usos, desde que haja garantia de que o consentimento é realmente livre. Mas também fora dessas situações de autoridade pública *vs.* cidadão ou empregador *vs.* consentimento do empregado, pode não ser uma boa base para o processamento de dados, como o regulamento fala de um claro desequilíbrio entre uma pessoa em causa e um responsável geral. Se esta adição é boa ou não é discutível.

Outro aditamento que o regulamento traz pode ser encontrado no *Considerando* 43 do RGPD,[15] no qual se presume que o consentimento não é dado livremente se não permitir que seja dado em diferentes operações de processamento de dados pessoais, apesar de ser apropriado no caso, ou se a execução de um

[14] Cf., Texto 52012PC0011 – Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados). COM/2012/011 final – 2012/0011 (COD). Considerando 34.

[15] Cf., Considerando 43 de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

contrato depender do consentimento, apesar de que tal consentimento não é necessário para esse desempenho. Especialmente esta última frase requer alguma atenção. De acordo com o regulamento, quando a execução de um contrato, incluindo a prestação de um serviço, não requer o processamento dos dados dos indivíduos, mas mesmo assim é solicitado, presume-se que o consentimento não tenha sido dado livremente. Isto é enfatizado não apenas nos *Considerandos*, mas também nos artigos do próprio regulamento (art. 7 (4)). O consentimento não deve, portanto, ser empacotado com outros contratos. Finalmente, o consentimento de acordo com o regulamento não deve ser considerado gratuito, caso a pessoa em causa não tenha uma escolha genuína ou livre ou não possa recusar ou retirar o consentimento sem prejuízo.[16] Esta última frase contém a essência de um consentimento dado livremente e é provavelmente formulado para esclarecer o que constitui um livre consentimento. O motivo por trás dessas mudanças pode muito provavelmente ser encontrado no desejo de harmonizar condições de um consentimento válido. A Comissão referiu na sua avaliação de impacto (obrigatória) que o requisito de "livre consentimento" precisava de esclarecimento. Segundo a Comissão, o Grupo de Trabalho emitiu pareceres sobre este assunto, mas isto não resolveu o problema de abordagens nacionais divergentes.[17] Ao harmonizar estas regras sobre o consentimento, um uniforme (elevado) nível de proteção de dados na UE é assegurado, e o mercado interno da UE é salvaguardado.

2.4 Consentimento informado sob o RGPD

O consentimento informado recebeu mais clareza também sob o RGPD. De acordo com o regulamento, uma declaração de consentimento pré-formulada deve ser fornecida de forma inteligível e de fácil acesso. O formulário deve utilizar linguagem clara e simples e não deve conter termos injustos. Para orientação sobre o que exatamente pode ser visto como linguagem clara ou um termo injusto, a Diretiva 93/13/CEE pode ser consultada.[18] Esta diretiva parece ter sido a fonte de inspiração para esta obrigação. Além disso, de acordo com a Comissão, a transparência é essencial para proporcionar às pessoas controle sobre seus dados e garantia de proteção efetiva dos dados pessoais. Provavelmente, como

[16] Cf., Considerando 42 de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

[17] Cf., COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu e ao Conselho*. Proteção, novas oportunidades – Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018/FMT. Bruxelas: Comissão Europeia, 2018. Disponível em: https://bit.ly/2LVxhOe (*link* permanente).

[18] Cf., Disponível em: https://eur-lex.europa.eu/eli/dir/1993/13/oj (*link* permanente).

resultado disso, a transparência também pode ser encontrada como um novo princípio no RGPD; esse princípio exige que qualquer informação ou comunicação relacionada com o processamento de dados dos indivíduos tem que ser facilmente acessível e fácil de entender. Como resultado, o princípio cria um ambiente de processamento de dados de confiança. Esta confiança é importante de acordo com a Comissão para o desenvolvimento de uma economia digital no mercado interno. O regulamento, além disso, afirma que a pessoa em causa deve também ser informada, pelo menos, da identidade do controlador de dados, e as finalidades para as quais os dados pessoais são destinados.[19]

De acordo com o regulamento, estes tópicos devem, pelo menos, ser endereçados para um consentimento para ser informado. Isso serve apenas como um mínimo, e mais informações podem ser necessárias em determinadas situações. De acordo com o regulamento, as pessoas naturais devem estar cientes dos riscos, regras, salvaguardas e direitos em relação ao processamento de dados pessoais e como exercer os direitos em relação a tal processamento.[20] Isso, no entanto, parece parte de uma obrigação geral de informar os indivíduos, não necessariamente um requisito para criar um consentimento informado. O regulamento também menciona que, se o consentimento do titular de dados for dado após uma solicitação por via eletrônica, o pedido deve ser claro, conciso e não desnecessariamente perturbador para o uso do serviço para o qual é fornecido.[21] Na realidade *on-line*, a informação é geralmente dada ao indivíduo por políticas e avisos de privacidade, aos quais o indivíduo tem de dar aceitação. Essas políticas e avisos, no entanto, nem sempre são claras, dificultando muitas vezes a compreensão pelos indivíduos em dar seu consentimento informado. Essa mudança pode provavelmente ser vista como uma tentativa de abordar essas práticas. Além disso, essa frase faz com que se repense lei de *cookies* atual, que adiciona *pop-ups* enormes bloqueando páginas inteiras, sendo assim desnecessariamente perturbador. Estas adições ao consentimento informado no regulamento parecem abordar tanto o requisito de qualidade da informação como a acessibilidade e visibilidade informações. Isso é importante porque os indivíduos têm que estar bem informados para tomar boas decisões sobre seus dados pessoais.

[19] Cf., Considerando 42 de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

[20] Cf., RGPD. Considerando 39 e art. 7 (3) de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

[21] Cf., Considerando 32 de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

2.5 O direito de retirar o consentimento

De acordo com o regulamento, o titular dos dados terá o direito de retirar o seu consentimento a qualquer momento e tal fato não afetará a legalidade do processamento com base no consentimento antes de sua retirada.[22] Isso significa que a retirada do consentimento só é efetiva para processamento de dados futuros após esse fato. Esta é uma diferença importante com o "direito de ser esquecido" (também, "direito ao esquecimento"), que é adicionado ao quadro de proteção do RGPD. Este direito permite que informações antigas sejam apagadas após invocá-las.[23] A ideia sobre a possibilidade de retirar o consentimento não é nova, assim, pode-se dizer que essa mudança é mais uma afirmação de regras (implícitas) já existentes. A razão para essa mudança, portanto, parece basear-se principalmente na harmonização, tentando nivelar a proteção de dados na UE.

O regulamento parece adicionar algo novo. Uma novidade que pode ser observada é a obrigação de que a retirada do consentimento seja tão fácil quanto dar o consentimento. Isso pode implicar que a retirada do consentimento pode estar a meros cliques. Da perspectiva do indivíduo, esta regra parece acrescentar muito à sua proteção de dados pessoais. Oferece-lhe mais controle sobre o processamento de seus dados pessoais, permitindo-lhe parar o processamento de seus dados se desejar mais tarde. Isso pode ser valioso quando, após o consentimento, os dados processados ou seus efeitos provam ser indesejáveis. Do ponto de vista do controlador de dados essa adição ao direito de retirar o consentimento é susceptível de tornar o consentimento um terreno menos preferido para basear o processamento de dados pessoais. A razão para isso é que o consentimento pode se tornar opção insegura, pois ele pode ser retirado a qualquer momento e por qualquer motivo.

2.6 Demonstração do consentimento e consentimento de menores

Outra mudança pode ser encontrada no art. 7 (1) do RGDP, pois segundo esta norma o controlador deve ser capaz de demonstrar que o titular dos dados consentiu no processamento de seus dados pessoais. Essa mudança pode estar

[22] Cf., Art. 7 (3) de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

[23] Cf., Art. 17 de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente). Também, ESPANHA. Tribunal de Justicia. *ECJ C-131/12 Google Espanha vs. AEPD*. Disponível em: https://bit.ly/2OKMoHs (*link* permanente), onde o direito ao esquecimento foi articulado.

ligada ao "princípio da responsabilidade", um novo princípio encontrado no RGPD. De acordo com este princípio, a simples observância das regras de proteção de dados não é suficiente.

Uma menção deve ser feita no que diz respeito ao consentimento no caso de menores, pois merecem proteção extra. Eles merecem essa proteção, pois podem ser menos conscientes dos riscos, assim como as consequências e salvaguardas em causa e dos seus direitos em relação ao tratamento de dados pessoais.[24] Regras sobre outros grupos de indivíduos que são incapazes de dar um consentimento válido não parecem ter sido abordadas no regulamento. A proteção extra para menores pode ser encontrada no art. 8º (1) do RGPD. O regulamento exige que o consentimento de uma criança em relação aos serviços seja autorizado por seus representantes legais (que na maioria dos casos são os pais). De acordo com o regulamento, esta autorização é necessária até que a criança tenha pelo menos 16 anos de idade. Além disso, a legislação de um estado- membro da UE pode prever um requisito de idade ainda menor, desde que não abaixo de 13 anos. O regulamento estabelece uma exceção à autorização obrigatória: não é necessário em caso de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança. Para determinar se uma autorização é necessária, o significado de serviços em uma sociedade da informação pode ser encontrado entre as definições deparadas no regulamento. Como definido no art. 1 (1) (b) da Diretiva 2015/1535, "serviço significa qualquer serviço da sociedade da informação, isto é, qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrônica e mediante pedido individual de um destinatário de serviços".[25] Isso implica que praticamente todo serviço comercial *on-line* é afetado, como os *sites* de redes sociais sempre populares. Para determinar se a autorização é exigida em determinado caso, os controladores de dados são obrigados a fazer um esforço razoável se o consentimento de uma criança é autorizado pelo representante legal, levando em consideração a tecnologia disponível.[26] Esta regra parece muito dinâmica e capaz de suportar progresso tecnológico, garantindo assim que a verificação da idade permaneça sólida.[27]

[24] Cf., Considerando 39 de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

[25] Cf., PARLAMENTO EUROPEU E CONSELHO. *Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação*. Disponível em: https://bit.ly/2EhG1b0 (*link* permanente).

[26] Cf., Art. 8 (2) de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

[27] Relativamente à LGPD, a norma brasileira, no seu art. 14 §1º, exige como obrigatório o consentimento dos responsáveis legais para o tratamento de dados pessoais para todos os menores de 18 anos, entendidos como menores nos termos do Estatuto da Criança e do Adolescente – ECA.

2.7 Impacto do RGPD no consentimento já dado

O consentimento é uma maneira importante de legitimar o processamento de dados pessoais. Isso levanta a questão sobre o que as mudanças no consentimento significam para as já existentes. Felizmente, o RGPD oferece uma resposta a essa pergunta. De acordo com o regulamento, os consentimentos dados anteriormente à vigência do regulamento permanecerão válidos desde que já estejam de acordo com as condições do regulamento.[28] Isso significa que quando um consentimento é à prova de GPDR, um controlador de dados pode continuar com suas operações de processamento de dados, e nenhuma ação extra é necessária.

3 Repensando as afirmações acima articuladas

O RGPD tem por objetivo garantir um alto nível de proteção de dados e alcançar o mercado interno na EU, com efeitos ultramarinos. Devido à redação do RGPD e a consequente adição de direitos individuais em uma regulamentação mais rigorosa, pode-se argumentar que o RGPD melhora significativamente a proteção de dados dos indivíduos. Concernente aos requisitos para um consentimento válido, o quadro regulamentar recebeu algumas alterações. Uma mudança importante é que consentimento passivo é descartado no regulamento, afirmando que uma ação afirmativa é necessária e o silêncio, "caixas" pré-assinaladas, inatividade etc. não constituem um consentimento válido. Outra mudança é que o RGPD agora declara que o consentimento não deve ser usado em situações nas quais há um claro desequilíbrio entre o controlador de dados e o indivíduo, como no governo *versus* cidadão e relações empregador *versus* empregado. Além disso, o RGPD presume não ter sido livremente dado se o uso do consentimento para uma operação de processamento de dados for obrigatório empacotado com diferentes operações de processamento de dados, ou se o consentimento for usado para um contrato, enquanto não é realmente necessário para essa finalidade. Além dessas mudanças, o consentimento informado também recebeu o imperativo da "clareza". De acordo com as mudanças nas declarações de consentimento, essas devem ser formuladas e fornecidas de forma facilmente acessível, com linguagem simples. Além disso, se o consentimento for solicitado *on-line*, a solicitação deve ser clara e não desnecessariamente perturbadora para o uso do serviço para o qual o consentimento é solicitado. Isso significa que *políticas de privacidade* excessivamente longas e pouco claras devem ser uma coisa do passado.

[28] Cf., Considerando 71 de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

Além dos requisitos para um consentimento válido, o RGPD também traz alterações em relação a outros tópicos relacionados ao consentimento. Uma primeira mudança é a introdução do direito de retirar o consentimento. Em primeiro lugar, a adição da regra de que retirar o consentimento deve ser tão fácil quanto dá-lo. Uma segunda mudança é que a retirada do consentimento deve ser sem prejuízo, proibindo assim "punições" para a retirada do consentimento. Uma terceira mudança é que para os dados os controladores são obrigados a demonstrar a existência de consentimento, caso solicitado. Isso significa reunir provas de que determinado consentimento se tornou crucial. Uma terceira mudança diz respeito ao consentimento dado por menores. Ao prestar serviços da sociedade da informação a crianças com menos de 16 anos autorização (parental) é necessária. Além disso, os controladores de dados precisam tomar medidas para verificar a idade dos indivíduos para determinar se a autorização é necessária.

Para concluir, as mudanças discutidas no consentimento parecem algumas vezes adicionar novos conceitos, tais como as regras relativas à autorização parental e as regras relativas à obrigação de demonstrar consentimento, mas em muitos casos esclarecer conceitos conhecidos.

3.1 A lógica subjacente ao consentimento

A lógica por trás do consentimento será discutida, para explicar por que o consentimento é considerado um importante meio de legitimar as operações de processamento de dados.

3.2 O nascimento da autodeterminação informacional em (partes da) Europa

A lógica por trás do consentimento está intimamente ligada ao foco e à lógica das leis de proteção de dados, em geral. As leis de proteção de dados foram adotadas pela maioria das nações europeias.[29] A tecnologia e a proteção de dados, entretanto, não ficaram paradas desde então, a proteção de dados não permaneceu a mesma. Esta mudança de foco se fundamenta no aumento

[29] MCCARTY-SNEAD, Steven S.; HILBY, Anne Titus. Research Guide to European Data Protection Law. *Legal Research Series*, Paper 1, 2013. Disponível em: http://scholarship.law.berkeley.edu/leg_res/1 (*link* permanente).

da ênfase em privacidade em documentos posteriores de proteção de dados e, finalmente, o RGPD e seu o direito dos indivíduos de controlar seus dados pessoais.

4 Legislação inicial de proteção de dados

No final da década de 1960, o aumento da automação no processamento eletrônico de dados estimulou os pedidos para regular o processamento de dados pessoais. Em 1970, o primeiro ato de proteção de dados do mundo foi adotado no estado alemão de Hessen;[30] a Suécia em 1973 edita sua lei de proteção de dados. A Lei Sueca de 1973 só cobriu o processamento de dados pessoais em registros informatizados tradicionais. O ato não contém muitas disposições materiais sobre quando e como os dados devem ser processados, ou princípios gerais de proteção de dados.[31] No caso da Suécia, por exemplo, o seu ato legislativo inicial (sendo o primeiro ato nacional no mundo) pode ser explicado pelo fato de que a informatização aconteceu cedo. A razão para isso é que a população relativamente pequena combinada com um alto padrão de vida favoreceu o desenvolvimento das TIC na Suécia. Além disso, a Suécia era um bom lugar para começar registradores automáticos, pois as autoridades públicas já mantinham muitos registros com informações de cidadãos suecos. A criação desses registros ou bancos de dados, no entanto, não aconteceu sem resistência pública. Os cidadãos temiam uma burocracia automatizada e desumanizada, com a tecnologia sendo problema. Na Suécia, por exemplo, o debate sobre a privacidade iniciou-se após a (informatizada) população sueca e censo de habitação de 1970, que foi surpreendente como consensos semelhantes tinham ocorrido mais cedo em 1960 e 1965. O computador parecia ser o problema, e o uso de computadores tinha que ser regulado e controlado. Como resultado disso, a maioria das primeiras normas pode ser vista como uma resposta a esses problemas. Elas não se concentram na proteção da privacidade individual (se entendida como controle), mas na função de processamento de dados na sociedade. De acordo

[30] A Hessische Datenschutzgesetz (Lei de Proteção de Dados Hessiana) de 1970 foi a primeira lei de proteção de dados na Alemanha e no mundo. Respondeu à crescente automação do processamento de dados. Para poder controlar o cumprimento das regras de proteção de dados, esta lei criou a instituição do Supervisor de Proteção de Dados da Hessian (uma cópia da lei original pode ser consultada em: HESSISCHE DATENSCHUTZGESETZ (LEI DE PROTEÇÃO DE DADOS HESSIANA) DE 1970. Disponível em: http://starweb.hessen.de/cache/GVBL/1970/00041.pdf#page=1 [*link* permanente]).

[31] ÖMAN, Sören. Implementing data protection in law. *Stockholm Institute for Scandianvian Law 1957-2010*. Disponível em: http://www.scandinavianlaw.se/pdf/47-18.pdf (*link* permanente).

com as normas de proteção de dados, na perspectiva de Mayer-Schönberger, elas foram entendidas como parte de uma tentativa de "domar" a tecnologia: o uso do processamento de dados regulado para garantir que estava de acordo com os objetivos da sociedade. Como consequência, a maioria dessas regras de proteção de dados não visava à garantia para os indivíduos na sua conformidade, mas em vez disso, em instituições especiais que tinham de supervisionar a conformidade dos controladores de dados.[32]

Em 1971, na Alemanha surge o primeiro projeto de uma lei federal de proteção de dados, tendo a *Bundesdatenschutzgesetz* (BDSG) entrado em vigor em 1º.1.1978. Nos anos seguintes, quando a BDSG tomava forma na prática, houve um desenvolvimento técnico no processamento de dados, pois o computador tornou-se cada vez mais importante tanto no trabalho quanto no setor privado. Houve também mudanças significativas no campo jurídico.[33] Com o *Volkszählungsurteil* (Julgamento do Recenseamento) de 15.12.1983, o Tribunal Constitucional desenvolveu o direito à autodeterminação da informação.[34] A sentença confirmou que os dados pessoais estão constitucionalmente protegidos na Alemanha. Isto significa que os indivíduos têm o poder de decidir quando e até que ponto as informações pessoais podem ser publicadas.

Os pesquisadores das primeiras leis de proteção de dados dedicaram-se à análise do papel dos bancos de dados centralizados, mas de modo muito primário dadas as ferramentas instrumentais que dispunham naquele momento. Todavia surge um novo fenômeno, que pode ser atribuído à oposição dos cidadãos, porque a tecnologia se desenvolveu em outra direção. Assim surgem os denominados minicomputadores, que permitiram alguma forma de relacionamento com o governo ou com organizações para aplicar processamento eletrônico de dados. A razão para isto pode ser encontrada no fato de que os minicomputadores eram menores, menos poderosos, mas também menos caros do que computadores de *mainframe*; na verdade, eles foram projetados para atrair pequenas e médias empresas e organizações. A quantidade relativamente pequena de possíveis violadores de proteção de dados cresceu exponencialmente em uma enorme abundância de potenciais violadores, e, como resultado disso, levando a uma mudança na discussão sobre proteção de dados. Um número crescente de

[32] Cf., para aprofundamento, MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Philip E.; ROTENBERG, Marc. *Technology and privacy*: the new landscape. Cambridge: MIT Press, 1998. p. 219-272. Também, BENNETT, Colin J. *Regulating privacy*: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992. p. 60 e ss.; 121 e ss.

[33] A Bundesdatenschutzgesetz (BDSG) pode ser consultada em: https://bit.ly/30yYXvh (*link* permanente).

[34] Cf., *BVerfG*, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

cidadãos europeus queria não apenas a legislação destinada a tentar controlar a tecnologia de processamento de dados, mas também privacidade individual e os direitos de proteção dos dados.[35]

4.1 Maior ênfase na privacidade individual

O desejo acima mencionado levou a uma segunda geração de normas de proteção de dados. A perspectiva então voltava-se para a proteção de dados imediatamente conectada ao direito de privacidade e, consequentemente, a proteção de dados era vista como o direito do indivíduo e da sociedade em termos pessoais. As regras da segunda geração parecem semelhantes às da primeira geração, mas com algumas diferenças. O jargão técnico foi removido, as definições tornam-se abstratas (tecnologia neutra) e os direitos individuais existentes foram aperfeiçoados. Segundo Mayer-Schönberg, os estatutos de proteção de dados francês, austríaco, dinamarquês e norueguês podem ser vistos como o início desta segunda geração de proteção de dados na legislação.[36] Além disso, durante a primeira geração de regras, os indivíduos tinham o direito de acessar e corrigir seus dados pessoais, mas estes foram interpretados funcionalmente, em outras palavras, eles foram instalados para melhorar a precisão dos dados processados. Assim, poderia fazer algo sobre os dados, mas não interromper completamente o processamento deles.

No entanto com a vinda da segunda geração os indivíduos começaram a falar no artifício de processamento de dados. O consentimento às vezes se tornou uma pré-condição para processamento de dados pessoais, os indivíduos poderiam, em alguns casos, permitir ou não o processamento de dados, por exemplo, na Lei de Dados da Noruega, foi estabelecido que os indivíduos poderiam recusar o processamento de dados para *marketing* direto ou pesquisa de mercado.[37]

[35] Cf., MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Philip E.; ROTENBERG, Marc. *Technology and privacy*: the new landscape. Cambridge: MIT Press, 1998. p. 219-272. Também, BENNETT, Colin J. *Regulating privacy*: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992. p. 219-272.

[36] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Philip E.; ROTENBERG, Marc. *Technology and privacy*: the new landscape. Cambridge: MIT Press, 1998. p. 219-272. Também, BENNETT, Colin J. *Regulating privacy*: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992, notadamente, p 226.

[37] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Philip E.; ROTENBERG, Marc. *Technology and privacy*: the new landscape. Cambridge: MIT Press, 1998. p. 219-272. Também, BENNETT, Colin J. *Regulating privacy*: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992, notadamente p. 227.

Além disso, durante esta geração, a proteção de dados deixou de ser vista como um ensaio de tecnologia, mas tornou-se uma liberdade individual dos cidadãos.

Essa mudança, no entanto, não alcançou maiores desenvolvimentos. Os cidadãos e a sociedade estão tão conectados que a resistência aos pedidos de informação é impossível ou possível, mas com um grande custo social. Consequentemente, na realidade, o indivíduo realmente não tem a oportunidade de decidir se ele participou ou permaneceu dentro ou fora da sociedade. A questão de saber se este curso de eventos foi o caminho a percorrer e que levou a uma nova geração de normas de proteção de dados.

4.2 O direito à autodeterminação informacional

E assim chegou o fim da segunda geração, após a qual veio uma nova geração. Uma terceira, que modificou a proteção de dados de uma liberdade individual (informativa) para afastar invasões de privacidade. Agora, pretende-se um direito participativo à autodeterminação informacional.[38]

Em vez da pergunta sobre se o indivíduo quer participar em processos informacionais, a questão agora muda para como o indivíduo quer participar, o que se torna mais importante. Essa visão corresponde à ideia de Westins de privacidade. Segundo ele:

> [...] Privacidade é a reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e até que ponto as informações sobre eles são comunicadas aos outros. Visto em termos da relação do indivíduo com a participação social, a privacidade é a retirada voluntária e temporária de uma pessoa da sociedade em geral por meios físicos ou psicológicos, seja em estado de solidão ou intimidade de pequenos grupos ou, quando entre grupos maiores, em condição de anonimato ou reserva.[39]

Novos desenvolvimentos tecnológicos e seus desafios legais afetaram a lei de proteção de dados durante a segunda e terceira geração; por causa disso, os

[38] Cf., nota 31 *retro*.

[39] Cf., WESTIN, Alan F. *Privacy & Freedom*. London, Sydney, Toronto: The Bodley Head, 1967. p. 7. No original: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve".

legisladores retiraram-se da regulação ativa da tecnologia. Em vez de persistir ao longo de um difícil caminho de adaptação contínua da legislação que dá forma à tecnologia, os políticos escolheram se concentrar em mais "liberdades individuais e direitos de participação".[40] Consequentemente, a terceira geração de normas de proteção de dados enfatizou a participação e autodeterminação.

A autodeterminação na informação tem pronúncia pela primeira vez em aguda decisão do Bundesverfassungsgericht em 1983. Esse caso foi sobre uma tentativa alemã de realizar um censo populacional.[41] O ato que possibilitou

[40] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Philip E.; ROTENBERG, Marc. *Technology and privacy*: the new landscape. Cambridge: MIT Press, 1998. p. 219-272. Também, BENNETT, Colin J. *Regulating privacy*: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992, notadamente p. 230 e 231.

[41] Cf., BVERFGE, 65, 1 – Volkszählung. Disponível em: http://www.servat.unibe.ch/dfr/bv065001.html (*link* permanente). Ementa: "1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. 2. Einschränkungen dieses Rechts auf 'informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. 3. Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymer Form erhoben und verarbeitet werden, und solchen, die für statistische Zwecke bestimmt sind. Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. Der Informationserhebung und Informationsverarbeitung müssen aber innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen. 4. Das Erhebungsprogramm des Volkszählungsgesetzes 1983 (§2 Nr. 1 bis 7, §§3 bis 5) führt nicht zu einer mit der Würde des Menschen unvereinbaren Registrierung und Katalogisierung der PersönBVerfGE 65, 1 (1)BVerfGE 65, 1 (2) lichkeit; es entspricht auch den Geboten der Normenklarheit und der Verhältnismäßigkeit. Indessen bedarf es zur Sicherung des Rechts auf informationelle Selbstbestimmung ergänzender verfahrensrechtlicher Vorkehrungen für Durchführung und Organisation der Datenerhebung. 5. Die in VoZählG 1983 §9 Abs. 1 bis 3 vorgesehenen Übermittlungsregelungen (unter anderem Melderegisterabgleich) verstoßen gegen das allgemeine Persönlichkeitsrecht. Die Weitergabe zu wissenschaftlichen Zwecken (VoZählG 1983 §9 Abs. 4) ist mit dem Grundgesetz vereinbar". Tradução: "1. Nas condições modernas de tratamento de dados, a protecção das pessoas singulares contra a coleta, conservação, utilização e divulgação ilimitadas dos seus dados pessoais é abrangida pelo direito geral de personalidade do artigo 2º, nº 1, da GG, em conjugação com o artigo 1º, nº 1, da GG. A este respeito, o direito fundamental garante o direito do indivíduo de determinar a divulgação e utilização dos seus dados pessoais por si próprio. 2) As restrições deste direito à 'autodeterminação informativa' só são permitidas no interesse geral prevalecente. Exigem uma base jurídica constitucional, que deve corresponder à exigência de clareza normativa do Estado de direito. Nos seus regulamentos, o legislador deve igualmente respeitar o princípio da proporcionalidade. Deve também tomar precauções organizacionais e processuais para contrariar o perigo de violação do direito de personalidade. Nos requisitos constitucionais para tais restrições, deve ser feita uma distinção entre os dados pessoais coletados e tratados de forma individualizada e não anónima e os que se destinam a fins estatísticos. No caso da coleta de dados para fins estatísticos, não pode ser exigida uma limitação estreita e concreta da finalidade dos dados. A coleta e o tratamento da informação devem, contudo, ser contrabalançados por barreiras adequadas no âmbito do sistema de informação. (4) O programa de pesquisa da Lei do recenseamento de 1983 (§2 nos. 1 a 7, §§3 a 5) não conduz a um registo e catalogação de dados pessoais incompatíveis com a dignidade

o recenseamento da população não recebeu muita resistência, porém em forte contraste com isso o debate social em torno dele era enorme. Além disso, afora de um debate acalorado o ato também foi levado perante os tribunais alemães, em última análise, vindo antes do Tribunal Constitucional alemão. A decisão deste tribunal acabou por confirmar o objetivo do censo populacional, mas exigiu salvaguardas processuais e organizacionais adicionais para os direitos fundamentais dos cidadãos. O censo da população, no entanto, não foi interrompido, mas adiado até que um novo ato que permitiria que o censo da população fosse aprovado mais tarde, em 1987. No entanto, o julgamento do tribunal foi muito importante. Em seu julgamento, o tribunal afirmou que *o direito* à *autodeterminação da informação era um direito constitucional fundamental*. Além disso, era a implementação de um direito geral de personalidade, que era constituído pela proteção da dignidade e, por outro lado, a proteção pessoal em geral da liberdade. Ademais, o direito garantiu a capacidade do indivíduo de decidir ou determinar a liberação e o uso de seus dados pessoais.

O direito à autodeterminação informativa não é absoluto, outros interesses devem ser equilibrados com este direito. Partes importantes da decisão formulada pelo Tribunal baseiam-se em ideias da teoria dos sistemas sociológicos, em particular os trabalhos de Niklas Luhmann.[42] O direito à autodeterminação da informação, tal como estabelecido, influenciou muito a legislação de proteção de dados em muitos países europeus, colocando o indivíduo em posição de determinar como ele participaria da sociedade. O que se pode dizer, no entanto, é que, devido ao direito à autodeterminação da informação, o conceito de consentimento ganhou importância. A razão para isso pode ser encontrada no fato de que o consentimento é uma forma, se não a mais importante, de controlar seus próprios dados pessoais. O consentimento, na perspectiva de inúmeros autores, pode ser visto como a "expressão genuína do direito à autodeterminação informativa".[43]

humana; cumpre igualmente os requisitos de clareza das normas e de proporcionalidade. No entanto, a fim de salvaguardar o direito à autodeterminação informativa, são necessárias disposições processuais suplementares para a implementação e organização da coleta de dados. (5) As regras de transmissão previstas no VoZählG 1983 §9 par. 1 a 3 (entre outros, comparação do registo de matrícula) violam o direito geral de personalidade. A transmissão para fins científicos (VoZählG 1983 §9 Abs. 4) é compatível com a Lei Fundamental".

42 Cf., LUHMANN, Niklas. Grundrechte als Institution: ein Beitrag zur politischen Soziologie. *In*: MEHNER, Ingo. *Schriften zum* öffentlichen *Recht*. Berlin: Duncker & Humblot, 1965. v. 24.

43 Cf., FRIEDEWALD, Michael; LAMLA, Jörn; ROßNAGEL, Alexander. *Informationelle Selbstbestimmung im digitalen Wandel*. [s.l.]: Springer-Verlag, 2017. Na literatura brasileira, cf., BIONI, Bruno R. *Autodeterminação informacional*: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016. Dissertação (Mestrado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016.

Enfatizando, a participação e controle, no entanto, acabaram por não ter os efeitos desejados. Mesmo com direitos de participação melhorados, os indivíduos não estavam dispostos a pagar o custo social do exercício de seu direito de autodeterminação informacional.[44] Como resultado da posição fraca dos indivíduos veio a quarta geração de normas de proteção de dados.

Esta quarta geração pode ser caracterizada por nova legislação setorial e normas que tentam fortalecer a posição do indivíduo contra as instituições de coleta de informações e intentam impedir a negociação de direitos relacionados à proteção de dados. Exemplos dessas normas são a introdução da compensação sem culpa para reclamações de proteção de dados, a proibição de processar dados (interrompendo assim a negociação do direito de processar esses dados) e a adição de novas instituições de aplicação.[45] Com a proteção de dados de quarta geração, o direito de autodeterminação da informação manteve o mesmo papel de antes, mas agora é reforçado, detalhado, complementado e apoiado, melhorando assim o conceito.

4.3 Autodeterminação da informação e estruturas internacionais de proteção de dados

Como vimos, o conceito de autodeterminação da informação tem prevalecido em algumas leis nacionais de proteção de dados por algum tempo. Neste parágrafo, a influência da autodeterminação da informação deve ser discutida sob a Convenção 108 do CoE, diretrizes da OCDE e as estruturas do RGPD.

4.3.1 Autodeterminação informacional, as diretrizes da OCDE e a Convenção do CoE 108 e do CoE 108+

A autodeterminação da informação não parece desempenhar um papel de maior destaque em ambas as Convenções 108/108+ e as Diretrizes da OCDE

[44] Cf., MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Philip E.; ROTENBERG, Marc. *Technology and privacy*: the new landscape. Cambridge: MIT Press, 1998. p. 219-272. Também, BENNETT, Colin J. *Regulating privacy*: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992, notadamente p. 232.

[45] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Philip E.; ROTENBERG, Marc. *Technology and privacy*: the new landscape. Cambridge: MIT Press, 1998. p. 219-272. Também, BENNETT, Colin J. *Regulating privacy*: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992, notadamente p. 233.

sobre a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais.[46] Estas diretrizes da OCDE fornecem regras básicas que governam a proteção de dados pessoais e privacidade, no entanto, seu escopo é limitado a dados pessoais que, devido à maneira que eles são processados, ou por causa de sua natureza, ou contexto em que são usados, representam um perigo para a privacidade e liberdades individuais, implicando uma condição de proteção de dados pessoais. Isso parece não estar de acordo com a ideia de autodeterminação informacional, que se revela na capacidade de decidir ou determinar a liberação e uso de seus dados pessoais. Ademais, não há muitos vestígios de consentimento, uma noção-chave de acordo com a autodeterminação informacional. As diretrizes da OCDE mencionam apenas consentimento em duas ocasiões, e elas estabelecem que o princípio de limitação de coleta deve dispor de limites para a coleta de dados pessoais, e que tais dados devem ser obtidos por meios legais e justos e, quando apropriado, com o conhecimento do consentimento a pessoa em causa. As diretrizes, no entanto, não deixam claro quando o consentimento é ou não requerido.[47]

As diretrizes da OCDE afirmam que os dados pessoais não devem ser utilizados para fins diferentes dos especificados em conformidade com o princípio da especificação do objetivo, exceto quando o consentimento do titular dos dados for obtido por autoridade de direito. Essas diretrizes não oferecem nenhum outro esclarecimento sobre o que exatamente constitui um consentimento e se/e quando o consentimento é necessário em outras situações. As diretrizes têm um princípio de participação individual, mas esse princípio visa fornecer aos indivíduos informações sobre as operações de processamento de dados e permitir eventuais correções nos dados sobre eles, não lhes concedendo o controle sobre quando e como seus dados são divulgados. Em suma, a autodeterminação informativa e o consentimento não têm muita atenção nas diretrizes da OCDE.

As convenções 108 e 108+ do CoE[48] também não se baseiam na ideia de autodeterminação da informação. As convenções mencionam o consentimento,

[46] Poucos meses antes de a Convenção nº 108 ser adotada, a OCDE adotou as Diretrizes de Privacidade que, embora não sejam vinculantes, também têm sido muito influentes, particularmente em países fora da Europa, como Estados Unidos, Canadá, Austrália e Japão. As Diretrizes implicam um conjunto de princípios básicos elaborados em estreita coordenação com o Conselho da Europa e, portanto, consistentes com os princípios de proteção de dados da Convenção 108 e 108+. Entretanto, também há diferenças sutis, mas significativas, entre elas.

[47] Cf., OECD. *OECD Privacy Guidelines*. Disponível em: https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm (*link* permanente).

[48] Cf., COUNCIL OF EUROPA. *Modernization of Convention 108*. Disponível em: https://www.coe.int/en/web/data-protection/convention108/modernised (*link* permanente). Para a Convenção 108+ consulte o texto em: COUNCIL OF EUROPA. *Convenção 108+*. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (*link* permanente).

nomeadamente no que diz da possibilidade de assistência a titulares de dados residentes no estrangeiro. Elas ainda não apresentam uma definição de consentimento. O que elas, no entanto, articulam, ao contrário das diretrizes da OCDE, é uma exigência de propósito legítimo e uma base legal para o processamento de dados. Isso, indiscutivelmente, é porque a OCDE está vindo de um ponto de vista econômico, enquanto o CoE está mais relacionado com CEDH,[49] vindo sob a perspectiva dos direitos fundamentais.

4.3.2 RGPD: aprimorando o controle do usuário

Com a adoção do RGPD, o quadro europeu de proteção de dados está mudando mais para a autodeterminação informativa, concedendo aos indivíduos controle sobre seus dados pessoais. Por conseguinte, propõe-se a determinar formas de clarificar e melhorar direitos relacionados ao controle, como o direito de acesso, retificação, eliminação ou bloqueio de dados. Além disso, complementa os direitos já existentes com um direito de portabilidade de dados.

A importância do controle é enfatizada no próprio regulamento. Em um dos primeiros *considerandos* afirma-se que as pessoas singulares devem ter o seu próprio domínio de dados.[50] Um par de novos direitos que o RGPD traz também adiciona controle para os indivíduos. Primeiro, há o "direito de ser esquecido".[51] Tecnicamente, este não é um direito novo, como foi desenvolvido anteriormente no Google Espanha, caso paradigmático julgado pelo TJUE. O direito de ser esquecido dá às pessoas em certas situações o direito de obter o apagamento de seus dados pessoais, como quando o indivíduo retira seu consentimento (que era a base legitimadora do processamento de dados) ou quando os dados não são mais necessários em relação à finalidade para a qual foram coletados ou caso processado. Além do direito de ser esquecido, há também o novo direito da portabilidade dados.[52] Este direito permite que os indivíduos, a seu pedido, recebam de um controlador de dados os dados pessoais relativos a ele que ele forneceu ao controlador de dados. Além disso, a informação deve ser dada em um formato estruturado, comumente habitual e legível por máquina.

---

[49] Cf., Para aprofundamento, COUNCIL OF EUROPA. *Human Rights Intergovernmental Cooperation*. Disponível em: https://www.coe.int/en/web/human-rights-intergovernmental-cooperation/ (*link* permanente).

[50] Cf., Considerando 7 de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

[51] Cf., Art. 17 de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

[52] Cf., Art. 20 de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

4.3.3 O RGPD e responsabilidade do controlador

O parágrafo anterior mostra que o "controle do usuário" está ganhando importância na proteção de dados na lei de proteção europeia. Outro desenvolvimento interessante, no entanto, é que a "responsabilidade do controlador" também está ganhando importância, a fim de garantir um alto nível de proteção de dados.

A ideia de responsabilidade do controlador pode ser observada nos princípios de proteção de dados. O princípio da legalidade, por exemplo, proporciona aos responsáveis pelo tratamento uma série de motivos legais que os obrigam a avaliar os interesses dos indivíduos, enquanto o princípio do processamento justo exige que os controladores de dados considerem os interesses dos indivíduos. No RGPD a ideia responsabilidade pelo tratamento de dados é reforçada pelos mecanismos de acompanhamento previstos no capítulo IV do RGPD. Uma condição que vai aumentar a responsabilidade do controlador é a provisão que requer que os controladores de dados tomem medidas organizacionais para implementar princípios de proteção de dados, pois ademais de proteger os indivíduos, devem garantir que apenas os dados necessários sejam processados por padrão.[53]

5 Considerações finais

A lógica do consentimento está relacionada ao foco da proteção de dados, que é a autodeterminação. O foco da proteção de dados nem sempre foi assim. Inicialmente a proteção de dados poderia ser mais bem descrita como uma maneira de "domesticar a tecnologia". Mais tarde, devido às transformações tecnológicas e sociais, isso mudou, e a proteção de dados tornou-se mais concentrada na proteção da privacidade das pessoas. Isso, por sua vez, evoluiu para a ideia de autodeterminação informacional. O principal influenciador desse desenvolvimento, como já afirmado, foi o Tribunal Constitucional alemão, com o caso de recenseamento da população em 1983.

Ao longo dos anos, a autodeterminação informativa continuou admirável. Com a vinda do RGPD, a noção de autodeterminação informacional parece ter se tornado mais importante. Isso pode ser demonstrado por todos os sinais de controle adicional para os indivíduos em relação aos seus próprios dados pessoais. Ademais, observando o regulamento, os próprios *considerandos* apontam para a importância do controle pelas pessoas sobre seus dados. Esta importância

[53] Cf., Art. 25 de PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Disponível em: https://bit.ly/2JQGtkb (*link* permanente).

também é reforçada pelo fato de que certos direitos foram adicionados ou estendidos para fornecer mais controle, como o direito de ser esquecido ou o direito de portabilidade de dados.

No entanto, o aumento do controle do usuário não parece significar que a autodeterminação informativa é o núcleo da proteção de dados no âmbito do RGPD. Uma maneira de observar isso é o fato de o regulamento não só permitir o processamento de dados com o consentimento dos indivíduos, mas em vários outros motivos lícitos. Além disso, também pode ser demonstrado pelo fato de que não apenas o controle do usuário é importante, mas também a responsabilidade do controlador. Esse último parece ter alcançado importância no âmbito do RGPD, devido, notadamente, à adição do princípio de responsabilização e seus mecanismos de acompanhamento.

O processamento de dados pessoais regular e adequado só é possível em conformidade com os princípios e regras de proteção de dados fixados pelo comando normativo. Uma dessas regras é que o processamento de dados deve ter uma base legal, com o consentimento sendo um deles, e o mais importante. Ao lado de declarar os requisitos para um consentimento válido, o RGPD esclarece no que consiste o consentimento e, ao mesmo tempo, intenta resolver problemas de harmonização, pois é um regulamento que não precisa ser implementado porque tem efeito direto em cada estado-membro da UE.

Relativamente à LGPD, o consentimento ganhou alta densidade, pois a manifestação de vontade precisa ser livre e inequívoca, bem como cultivada com ciência das informações indispensáveis para tal, o que alcança, por certo, a finalidade do tratamento de dados, ademais de ser cingida aos escopos exclusivos e determinados que foram previamente informados ao titular dos dados.

Aqui, fica evidenciado o acoplamento do consentimento com o princípio da finalidade, que ordena que "a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades", como dispõe o art. 6º, da norma de regência. Ademais, o §4º do art. 8º da LGPD robustece o princípio da finalidade, assentando que o "consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas". Importa acrescentar que a LGPD, a teor do seu inc. I do art. 7º c/c o art. 5º inc. XII, admite prova do consentimento por meio idôneo que demonstre a manifestação inequívoca do titular dos dados, devendo ser salientado que em nenhuma hipótese o consentimento pode ser obtido mediante omissão do titular dos dados.

Ainda que não expresso na Constituição de 1988 o direito fundamental da autodeterminação informativa (podendo apenas antecipá-lo como decorrência da

clausula constitucional de proteção da liberdade e da vida privada e intimidade fundadas na dignidade da pessoa humana), a LGPD no inc. II do art. 2º o elegeu como fundamento da proteção de dados pessoais, cuja fundamentalidade decorre do §2º do art. 5º da Carta Fundamental.

Como implicação da autodeterminação informativa, muitos outros direitos são conferidos como dispõe o art. 18 da lei. Em seu art. 18, a LGPD traz os direitos dos titulares de dados pessoais. Os titulares poderão solicitar, a qualquer momento: (a) direito à confirmação da existência de tratamento; (b) direito de acesso aos dados; (c) direito de correção de dados incompletos, inexatos ou desatualizados; (d) direito à anonimização, bloqueio ou eliminação de dados tratados em desconformidade com a LGPD; (e) direito de portabilidade dos dados a outro fornecedor de serviço ou produto; (f) direito de eliminação dos dados pessoais tratados; (g) direito à informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (h) direito à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; (i) direito de revogação do consentimento; (j) direito de revisão por pessoa natural de decisões automatizadas.

Finalmente, em um breve cotejo podemos elencar as principais diferenças entre a *LGPD* e o *RGPD*:[54]

(I) em relação ao tratamento de dados sensíveis:

- *LGPD* – A legislação brasileira prevê uma proteção especial para os dados sensíveis, que só podem ser tratados em casos expressamente previstos na lei. Sem equivalência no *RGPD*, também prevê que os dados sensíveis possam ser tratados independentemente do consentimento do titular nos casos em que sejam indispensáveis: (1) execução pela administração pública, tal como previsto nas disposições legislativas e regulamentares; (2) garantia da prevenção da fraude e a segurança do titular na identificação e autenticação do registro em sistemas eletrônicos.
- *RGPD* – A legislação europeia proíbe o tratamento de dados sensíveis, com algumas exceções à proibição. Duas delas não foram incorporadas à legislação brasileira: (1) dados publicados pelo proprietário; (2) dados sobre membros ou antigos membros de fundações, associações ou organizações sem fins lucrativos tratados para fins lícitos e com medidas de segurança adequadas.

(II) em relação ao tratamento de dados de menores:

[54] Cf., no mesmo sentido, DRZ – BUSINESS SOLUTION. Disponível em: https://www.drz.global/ (*link* permanente).

- *LGPD* – A legislação brasileira exige o consentimento dos pais ou responsáveis para o processamento de dados pessoais de qualquer pessoa menor de 18 anos, conforme definido pelo ECA (Estatuto da Criança e do Adolescente).
- *RGPD* – A legislação europeia aceita o consentimento de menores com pelo menos 16 anos de idade. Com idade inferior, o consentimento do progenitor, tutor ou responsável legal é obrigatório.

(III) em relação às políticas de proteção de dados:

- *LGPD* – A legislação brasileira trata da implementação de um programa de governança e proteção de dados como uma faculdade para os controladores de dados.
- *RGPD* – A legislação europeia, por outro lado, exige que os responsáveis pelo tratamento de dados tomem as medidas técnicas e organizativas adequadas para assegurar que o tratamento de dados seja efetuado em conformidade com a lei.

(IV) em relação aos representantes:

- *LGPD* – A regulamentação brasileira prevê que a empresa estrangeira será notificada e intimada de todos os atos processuais na pessoa do agente, representante ou pessoa responsável por sua filial, agência, estabelecimento ou escritório instalado no Brasil.
- *RGPD* – Contrariamente à legislação brasileira, nos termos da regulamentação europeia, a indicação de controlador ou processador deve ser constituída por escrito por um representante seu em um dos seus Estados-Membros.

(V) em relação à responsabilização dos agentes:

- *LGPD* – Têm três proposições em que o controlador/operador não é responsabilizado: (1) se a pessoa natural ou jurídica não estiver envolvida no tratamento dos dados; (2) se, apesar dos danos, o tratamento for efetuado de acordo com as disposições legais; (3) se os agentes provarem que o dano foi causado exclusivamente pela pessoa do titular dos dados, ou por terceiros.
- *RGPD* – A diferença em relação à legislação brasileira é que a legislação europeia contém apenas os pontos 1 e 2 a seguir descritos: (1) se a pessoa natural ou jurídica não se encontrar enredada no tratamento dos dados; (2) se, apesar dos danos, o tratamento for efetuado em conformidade com a lei.

(VI) em relação ao *marketing* direto:

- *LGPD* – A legislação brasileira aplica as regras gerais de consentimento, transparência e direito de oposição dos titulares de dados pessoais.

- *RGPD* – O regulamento europeu fornece previsões concretas. O titular dos dados tem o direito de se opor, a qualquer momento, ao tratamento dos seus dados pessoais, incluindo a definição de perfis, na medida em que esteja relacionado com o *marketing* direto.

(VII) relativamente à relação entre controlador e operador:

- *LGPD* – Enquanto a legislação brasileira exige que o operador processe os dados de acordo com as instruções do controlador, não há necessidade de formalização através de um contrato.
- *RGPD* – Diversamente, a legislação europeia prevê que o tratamento de dados efetuado por um operador deve ser regido por um contrato ou outro ato jurídico que vincule o responsável pelo tratamento ao operador.

(VIII) relativamente ao relatório de impacto:

- *LGPD* – A lei brasileira não deixou claro em quais situações o controlador será obrigado a realizar um relatório de impacto à proteção de dados pessoais, delegando a uma regulamentação posterior o tratamento desta matéria.
- *RGPD* – Na lei europeia está previsto que o controlador deve prover um relatório de impacto à proteção de dados pessoais, quando o tratamento resultar em um elevado risco para o direito e a liberdade das pessoas. O *RGPD* traz ainda uma detalhada descrição do que deve ser abordado neste relatório.

(IX) relativamente à transferência de dados:

- *LGPD* – A lei brasileira permite a transferência de dados pessoais para países ou órgãos internacionais que proporcionem grau de proteção de dados pessoais adequados ao previsto. A lei é breve quanto a este procedimento e elementos a serem considerados como adequados. A *LGPD* estabelece apenas diretrizes genéricas a serem observadas pelas autoridades nacionais.
- *RGPD* – A regulamentação europeia alega que a transferência internacional dos dados pode ser realizada independentemente de autorização específica caso a Comissão Europeia reconheça que o país terceiro assegure um nível de proteção adequado. Caso não, a transferência internacional estará condicionada a garantias adequadas, que devem ser asseguradas pelo agente. Todos os procedimentos e elementos que são levados em consideração pela Comissão para a autorização da transferência estão descritos na RGPD. E, finalmente,

(X) relativamente à fiscalização do cumprimento da lei:

- *LGPD* – O projeto de lei que originou a LGPD previa a criação da Autoridade Nacional de Proteção de Dados, seguindo a mesma linha do regulamento

europeu. Porém, os dispositivos que previam a sua criação e responsabilidades foram vetados, por incorrerem em inconstitucionalidade do processo legislativo.

- *RGPD* – Já a regulamentação europeia estabelece a criação do Comitê Europeu para Proteção de Dados, responsável por assegurar a aplicação coerente da RGPD.

Some reflections around RGPD, especially regarding consent, with allusions to LGPD (an interpretative exercise)

Abstract: The new Regulation [European Union (EU)] 2016/679, now simply the GDPR, on the protection of individuals with regard to the processing of personal data and on the free movement of such data strengthens and harmonizes the rules protecting the rights and freedoms of individuals in the European environment and, under certain conditions, outside the EU. This new legal framework extends and updates the EU acquis of the previous Data Protection Directive 95/46 / EC. The GDPR sets the general rules applicable to any type of processing of personal data and specific rules applicable to the processing of special categories of personal data. The aim of this essay is to provide an overview of the GDPR, with regard to consent and information self-determination. It also mentions, albeit briefly, the Brazilian Data Protection Law, here only BDPL (Law No. 13.709/2018).

Keywords: GDPR. LGPD. Consent. Self-determination. Data. Processing.

Referências

BENNETT, Colin J. *Regulating privacy*: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992.

BIONI, Bruno R. *Autodeterminação informacional*: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016. Dissertação (Mestrado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016.

BRASIL. *LGPD*. Diponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

BUNDESDATENSCHUTZGESETZ (BDSG). Diponível em: https://bit.ly/30yYXvh.

BVERFG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

BVERFGE, 65, 1 – Volkszählung. Diponível em: http://www.servat.unibe.ch/dfr/bv065001.html.

COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu e ao Conselho*. Proteção, novas oportunidades – Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018/FMT. Bruxelas: Comissão Europeia, 2018. Diponível em: https://bit.ly/2LVxhOe.

COUNCIL OF EUROPA. *Convenção 108+*. Diponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

COUNCIL OF EUROPA. *Human Rights Intergovernmental Cooperation*. Diponível em: https://www.coe.int/en/web/human-rights-intergovernmental-cooperation/.

COUNCIL OF EUROPA. *Modernization of Convention 108*. Diponível em: https://www.coe.int/en/web/data-protection/convention108/modernised.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006.

DRZ – BUSINESS SOLUTION. Diponível em: https://www.drz.global/.

ESPANHA. Tribunal de Justicia. *ECJ C-131/12 Google Espanha vs. AEPD*. Diponível em: https://bit.ly/2OKMoHs.

FRIEDEWALD, Michael; LAMLA, Jörn; ROßNAGEL, Alexander. *Informationelle Selbstbestimmung im digitalen Wandel*. [s.l.]: Springer-Verlag, 2017.

HESSISCHE DATENSCHUTZGESETZ (LEI DE PROTEÇÃO DE DADOS HESSIANA) DE 1970. Diponível em: http://starweb.hessen.de/cache/GVBL/1970/00041.pdf#page=1.

HULL, G. Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics Inf Technol*, v. 17, n. 2, p. 89-101, 2015.

KOOPS, Bert-Jaap. The Trouble with European Data Protection Law (August 29, 2014). International Data Privacy Law. Forthcoming. *Tilburg Law School Research*, Paper 1, 04/2015. Disponível em: https://ssrn.com/abstract=2505692.

LUHMANN, Niklas. Grundrechte als Institution: ein Beitrag zur politischen Soziologie. *In*: MEHNER, Ingo. *Schriften zum* öffentlichen *Recht*. Berlin: Duncker & Humblot, 1965. v. 24.

MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Philip E.; ROTENBERG, Marc. *Technology and privacy*: the new landscape. Cambridge: MIT Press, 1998.

MCCARTY-SNEAD, Steven S.; HILBY, Anne Titus. Research Guide to European Data Protection Law. *Legal Research Series*, Paper 1, 2013. Disponível em: http://scholarship.law.berkeley.edu/leg_res/1.

MENDES, Laura Schertel Ferreira. *Privacidade, proteção de dados e defesa do consumidor* – Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2017.

MOEREL, E. M. L.; PRINS, Corien. *Privacy for the homo digitalis*: proposal for a New regulatory framework for data protection in the light of big data and the internet of things. 2016. Disponível em: http://dx.doi.org/10.2139/ssrn.2784123.

OECD. *OECD Privacy Guidelines*. Diponível em: https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

ÖMAN, Sören. Implementing data protection in law. *Stockholm Institute for Scandianvian Law 1957-2010*. Disponível em: http://www.scandinavianlaw.se/pdf/47-18.pdf.

PARLAMENTO EUROPEU E CONSELHO. *Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação*. Diponível em: https://bit.ly/2EhG1b0.

PARLAMENTO EUROPEU E CONSELHO. *RGPD*. Diponível em: https://bit.ly/2JQGtkb.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 40-81, 2018. Disponível em: https://bit.ly/2w3iKFu.

SCHERMER, B. W.; CUSTERSAND, B.; VAN DER HOF, S. The crisis of consent: how stronger legal protection may lead to weaker consent. *Data Protection, Ethics & Information Technology*, v. 16, n. 2, p. 171-182, 2014.

SOLOVE, Daniel J. A taxonomy of privacy. *University of Pennsylvania Law Review*, v. 154, n. 3, jan. 2006; *GWU Law School Public Law Research*, Paper 129. Disponível em: https://ssrn.com/abstract=667622.

SOLOVE, Daniel J. Conceptualizing privacy. *California Law Review*, v. 90, p. 1087-1155, 2002.

WESTIN, Alan F. *Privacy & Freedom*. London, Sydney, Toronto: The Bodley Head, 1967.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

RUARO, Regina Linden. Algumas reflexões em torno do RGPD, em especial quanto ao consentimento, com alusões à LGPD (um exercício interpretativo). *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 14, n. 42, p. 219-249, jan./jun. 2020.

Recebido em: 28.05.2019
Pareceres: 13.06.2019, 26.07.2019, 03.09.2019
Aprovado em: 13.09.2019