Recebido em: 24/06/2019
Aprovado em: 06/08/2019

A CIBERSEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS: A CHAVE-DE-OURO PARA EFETIVIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS (LEI N.º 13.709/2018)

CYBERSECURITY IN PERSONAL DATA PROCESSING: THE GOLDEN-KEY TO EFFECTIVENESS OF THE BRAZILIAN GENERAL DATA PROTECTION LAW (13.709/2018)

Mártin Marks Szinvelski
Mestre em Direito Público pela Universidade do Vale do Rio dos Sinos (UNISINOS). Graduado em Ciências Jurídicas e Sociais pela Universidade do Vale do Rio dos Sinos (UNISINOS/BR).

Taynara Silva Arceno
Mestre em Direito Público pela UNISINOS. Graduada em Direito pela Universidade do Vale do Rio dos Sinos - UNISINOS. Assessora de Juiz de Direito no TJRS.

de Proteção de Dados: mecanismos de segurança e confiança na proteção de dados. Considerações finais. Referências.

RESUMO: A recente *Lei Geral de Proteção de Dados* – LGPD surge no contexto em que a segurança dos dados é valorizada e fator de atribuição de confiança pelos titulares de informações. Em boa parte seguidas pela LGPD, as regulamentações no âmbito comunitário europeu reforçam a necessidade de adotar mecanismos técnicos e administrativos, ainda pouco utilizados, como as certificações ou selos de qualidade na proteção de dados e os códigos de conduta (apresentados no artigo), a serem normatizados pela Autoridade Nacional de Proteção de Dados – ANPD, instrumentos que fomentam a *responsabilização proativa* dos responsáveis pelo tratamento de dados.

PALAVRAS-CHAVE: Proteção de Dados. Autoridade Nacional de Proteção de Dados. Privacidade. Cibersegurança. Regulação. Certificação em Proteção de Dados. Códigos de Conduta.

ABSTRACT: The Brazilian General Data Protection Law - LGPD arises in the context in which data security is valued and a factor of trust attribution by the holders of information. To a large extent followed by the LGPD, regulations in the European community reinforce the need to adopt technical and administrative mechanisms, still little used, such as certifications or quality seals in data protection and codes of conduct (presented in the article), which will be regulated by the National Data Protection Authority (ANPD), instruments that foster the accountability of those responsible for the processing of data.

KEYWORDS: Data Protection. National Data Protection Authority (ANPD). Privacy. Cybersecurity. Regulation. Certifications in Data Protection. Codes of Conduct.

INTRODUÇÃO

O *Regulamento de Proteção de Dados da União Europeia (RGPD – UE 2016/679)* é, reconhecidamente, o *standard* regulatório seguido pela normatização brasileira em matéria de proteção de dados (*Lei Geral de Proteção de Dados – LGPD*). A adoção de uma regulamentação que discipline a coleta, o tratamento e os direitos do titular surge como imposição tácita do mundo interconectado por meio da internet. O comércio eletrônico e a *digitalização da vida* tornaram necessária a presença de instrumentos que guarnecessem segurança jurídica e conferissem legitimidade às operações inerentes ao tratamento de dados pessoais de pessoas singulares pelas empresas controladoras de banco de dados. O dado pessoal ocupa, à luz da metáfora, a função de *ouro negro* das economias digitais e, por que não, das organizações estatais.

A proteção de dados estrutura-se sob a base do respeito aos princípios reitores ou direitos específicos previstos em regras comunitárias e nacionais[1]. Não se deve olvidar, porém, que o antecedente lógico da adequada tutela dos dados passa pela atribuição de densidade ao princípio da segurança no tratamento de dados pessoais ou, como preferimos, das *medidas de seguridade*[2], o qual se traduziria na capacidade de resistência do sistema informático a eventos acidentais de vazamento de dados ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais conservados em bancos de dados ou em transmissão.

Nesse aspecto, surgem fatores diferenciadores e convergentes[3]: o elemento divergente reside na ausência de autonomia do direito à proteção de dados no ordenamento brasileiro, em razão da finalidade da *Lei Geral de Proteção de Dados* ser a tutela específica dos direitos de liberdade e de privacidade. De outra parte, a convergência está na importância destinada à *segurança da informação*,

1 Por via distinta, mas convergente, é o que defende Paul Bernal, sustentando que existiram quatros direitos básicos a serem respeitados na formulação de regulamentações em torno da trafegabilidade na rede: *(i)* o direito de navegar na internet com privacidade, *(ii)* o direito de monitorar quem monitora, *(iii)* o direito de excluir dados pessoais e *(iv)* o direito de proteger a identidade online (BERNAL, 2014, p.15).

2 Adiantamos, desde logo, que a escolha da expressão passa pela noção de que é impossível a garantia da *segurança absoluta* na proteção de dados por meio de sistemas informatizados. De outra parte, todos os responsáveis pelo tratamento de dados devem adotar medidas concretas de proteção dos sistemas informatizados, isto é, *medidas de seguridade*, motivo pelo qual adotamos a terminologia indicada.

3 O contraste está no desenvolvimento da proteção de dados no *velho continente* o qual germina na década de setenta e que, após, são consolidadas na *Diretiva Europeia 95/46*. A Carta dos Direitos Fundamentais da União Europeia (Carta de Nice), que ocupa *status constitucional* e prevê a proteção de dados pessoais como *direito fundamental*, inovou no cenário europeu, implicando na reelaboração técnica do instrumento jurídico responsável por conferir segurança jurídica aos tratamentos de dados pessoais.

incorporada no *Regulamento da União Europeia* no considerando trinta e nove e no artigo 5.º, alínea "f", no sentido de que "(...) os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade", o qual encontra paralelo na regulação brasileira no princípio da segurança, conceituado como a "(...) utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". Deveras, não existiria proteção de dados pessoais sem a concreção de mecanismos de segurança, os quais se ajustariam à destinação (princípio da finalidade) do dado coletado e o nível de proteção requerido (princípio da adequação), sob pena de colocar-se em *dúvida* a própria ideia de proteção de dados.

Em razão da ausência de um contorno legislativo que aponte para a autonomia do direito à proteção de dados, será analisado, na primeira parte do artigo, a *mutação da privacidade*; seguindo-se com a construção da autodeterminação informativa, especialmente em torno da possibilidade de controle dos dados pessoais; e, logo após, a perspectiva do consentimento livre e informado como medida preventiva de segurança. Após, expõe mecanismos de segurança e confiança na proteção de dados que a *LGPD* dispõe a serem implementados pelos setores públicos e privados: a certificação e a adoção de códigos de conduta setoriais.

1. A MUTAÇÃO DA PRIVACIDADE: O COLORIDO DA SOCIEDADE DIGITALIZADA

O escândalo revelado pelo jornal britânico *The Guardian*[4] reascendeu o debate sobre a necessidade da uniformização da proteção de dados em torno de instrumentos regulatórios sólidos e que confiram padrões mínimos de segurança e de confiabilidade na utilização de dados pelos controladores, nos limites do

4 A empresa *Cambridge Analytica* coletou os dados de mais de cinquenta milhões de usuários da rede social *Facebook*, os quais foram utilizados na campanha de Donald Trump à presidência dos Estados Unidos. As informações sobre o caso foram contadas ao *The Guardian* por *Christopher Wylie*, ex-funcionário da *Cambridge Analytica*. A coleta dos dados foi feita por intermédio de um aplicativo, dentro da plataforma *Facebook*, no ano de 2014, que realizava testes de personalidade com os usuários. Com as informações colhidas, a empresa traçou um perfil psicográfico comportamental de cada usuário da rede, o que permitiu que fossem fornecidas propagandas políticas adequadas para cada perfil, influenciado diretamente em seus votos. O número expressivo de dados vazados se deu pelo fato de que o aplicativo não coletava apenas os dados daquele usuário que realizava o teste, aceitando as condições de uso, mas sim, de toda a sua rede de contatos dentro da rede social. O vazamento teria ocorrido por conta de uma política flexível da rede social *Facebook* em relação ao fornecimento de informações pessoais a aplicativos de terceiros dentro da rede social. Poucos dias após divulgação do acontecido, o *Facebook* já havia perdido aproximadamente de 50 bilhões de dólares de seu valor no mercado. (CADWALLARD; GRAHAM-HARRISON, 2018) e (FOLHA DE SÃO PAULO, 2018).

consentimento do usuário. Pensar que o incidente passou ao largo da realidade brasileira é um equívoco: o episódio de vazamento de dados atingiu cerca de 500 mil cidadãos brasileiros, participantes da rede social. O desnudamento dos efeitos do relacionamento entre tecnologia e cidadãos, põe forma ao poder simbólico do *processo de aceleração dos rumos da história*. Embora os contornos apresentam-se, ainda, indefinidos, torna presente a conclusão de que está-se diante do fenômeno da *reinvenção da privacidade*, ressignificada pelo *devir tecnológico* e o corolário da (re)construção contínua da identidade da pessoa. O tempo pauta-se em milissegundos – não mais em horas e minutos – e a dependência crescente dos modelos da sociedade do consumo e da cultura cosmopolita assenhoram-se do sujeito (RODOTÀ, 2014, p.293-294; LIMBERGER, 2016).

No entanto, convém notar que a preocupação com a tutela do direito à privacidade que é própria da contemporaneidade alcança as atuais características somente no final do século XIX (DONEDA, 2006, p.8). Perez Luño (2012, p. 1) registra que a *metamorfose* apresenta-se dupla maneira: *(i)* do original direito de estar só para o aspecto *de estar no âmbito social e coletivo* e *(ii)* desde o *direito da personalidade* ao deslocamento para a *esfera patrimonial*. Significa afirmar, portanto, que na sociedade de informação e de consumo, a intimidade se transformou em mercadoria. A intimidade de cada pessoa, dessa forma, possui valor singular, especialmente nos meios de comunicação e de publicidade, que estão dispostos a pagar para obtê-la e publicizá-la. Assim sendo, a característica tradicional do direito à intimidade se mantém como direito personalíssimo somente para os absolutamente incapazes, os quais gozam de forma plena, já que para os civilmente capazes o grau de exposição pessoal pode ser objeto de transação, renúncias e cessões, com finalidade exclusiva de exploração econômica. Diante disso, conclui-se que, no que afeta a maioria da sociedade, a intimidade reposicionou-se da dimensão de direito da personalidade para o âmbito dos direitos patrimoniais (PÉREZ LUÑO, 2012, p.121).

Os dados pessoais assumem inquestionável transcendência na sociedade contemporânea: o *tsunami digital*[5] repercute em organismos públicos e privados. As repercussões superam a face individual e coletiva, chegando a fomentar o debate sobre o futuro da democracia no contexto tecnológico, como alerta Rodotà, quando afirma que "*o fim da privacidade não representaria somente um risco para as liberdades individuais: ele pode efetivamente conduzir ao fim da democracia*" (2008, p.144), dado que a construção das identidades

5 A expressão é de autoria de Stefano Rodotà (2014, p. 298).

restaria conduzida, guiada, por poderes "invisivelmente" constituídos[6]. Por essa via, a presença da perspectiva do *panóptico eletrônico* é inegável, querendo significar que nossas vidas estariam permanentemente expostas a monitoramento ou, conforme alerta Castells, "[...] como vivemos existências compósitas, essa exposição pode nos levar a *um eu esquizofrênico*, divididos entre o que somos *off-line* e a imagem que temos de nós mesmos online, que assim internaliza a censura"[7]. À luz da contextualização, sustenta-se como relevante a adoção de mecanismos jurídicos que norteiem a proteção de dados e a noção de segurança nos sistemas informatizados.

A *Lei Geral de Proteção de Dados – LGPD (Lei n.º 13.709/2018)* segue a tendência global de estabelecer parâmetros de legitimidade para o tratamento de dados pessoais, tanto que novas políticas vêm sendo adotadas por grandes empresas cujas plataformas de negócio situam-se na *internet*, em razão dos efeitos da inspiração protecionista-equilibrada da normatização europeia[8]. As regras vigentes na União Europeia, em boa medida, são seguidas pela LGPD[9]

6 Nesse sentido, Piñar Mañas, em recente artigo, pontua um fenômeno que está destinado a expandir, haja vista o incremento de dados gerados automaticamente, uma vez que " (...) poder de los algoritmos puede configurar la identidad de la persona, una identidad controlada, diseñada y vigilada. Lo que pone en cuestión el propio derecho al libre desarrollo de la personalidad. Una identidad cuya configuración puede limitarse, en base al modo en que se reconducen e incluso definen los gustos o prioridades de las personas. Se puede perfilar con facilidad a las personas y puede limitarse el marco de su desarrollo personal en un proceso difícil de identificar y ante el que puede resultar aún más difícil resistirse, pues en definitiva el algoritmo va a adecuar procesos a nuestros gustos, por lo que no será fácil objetar las indicaciones que de ello se deriven." (2017, p.69).

7 Manuel Castells (2013, p. 143-149) sustenta a possibilidade do "fim da privacidade" na *internet*, trabalhando a questão da exposição exacerbada nas redes e programas de vigilância governamentais. Adverte que o ânimo com a liberdade trazida pela *internet* foi elevada, ao ponto de tornarem distantes da memória coletiva as práticas autoritárias de vigilância no próprio ambiente de trabalho. Castells afirma que o problema gira em torno da troca de dados pelo privilégio de acesso a determinados sites. A maior parte dos indivíduos abre mão do direito à privacidade para ter condições de acesso à *internet*.

8 O *Facebook*, que após pedidos de desculpas de seu fundador Mark Zuckerberg, disponibilizou uma ferramenta que permite que os usuários participantes da rede social baixem um arquivo com todas as suas informações coletadas e armazenadas, a fim de que tenham um maior controle sobre os seus dados pessoais. Essa ampliação da possibilidade de controle por parte do usuário, representa um avanço do *Regulamento Europeu*, conforme salienta Enrique Pérez-Luño, filho do consagrado Catedrático da Universidade de Sevilha, na medida em que " (...) se refuerzan también las garantías de los titulares de los datos personales frente a nuevas formas de agresión a los equipos informáticos que pudieran redundar en una vulneración de los datos que les conciernen". (ROBLEDO, 2019, p.218).

9 A *LGPD* trabalha com o princípios reconhecidos no âmbito comunitário europeu e nos países em que há regulação de proteção de dados, entre os quais encontra-se a prevenção (artigo 6.º, inciso VIII) e a responsabilização (artigo 6.º, inciso X), sendo que este último é conceituado pelo legislador como sendo a " (...) demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". (BRASIL, 2018).

especialmente pela necessidade de demonstração de adequação ao padrão europeu de proteção de dados. Nessa linha de raciocínio, a *responsabilidade proativa* é utilizada como mecanismo para a afirmação da lógica da prevenção. Em contraste com a orientação prevista na *Diretiva 95/46/CE* e, por exemplo, na antiga Lei de Proteção de Dados Espanhola (LOPD), que recorriam ao modelo regulação reativo e passivo, o *Regulamento Europeu* propõe o dever de atuação positiva do responsável pelo tratamento de dados, de modo que ele adote medidas técnicas e organizativas de acordo com a *(i)* natureza dos dados protegidos, *(ii)* o contexto tecnológico e *(iii)* o risco de violação a direitos e liberdades fundamentais. Além disso, prevê-se um modelo fluído de organização, em que as técnicas de proteção de dados devam ser atualizadas quando houver necessidade ou mutação tecnológica, introduzindo a noção de *reflexividade* no tratamento de dados, no sentido de avaliação permanente dos riscos de vulneração de sistemas informatizados.

O modelo implica tornar o responsável não somente o cumpridor de normas prefixadas, mas um agente pautado pela previdência e diligência, que visualize a possibilidade de descumprimento de normas por meio de expedientes típicos da tradição do direito anglo-saxão (REIGADA, 2016). Nesse sentido, o modelo global de proteção de dados que se desenha passa pelo equilíbrio entre a livre circulação de dados (desenvolvimento tecnológico e econômico) e a proteção da esfera privada dos cidadãos, o qual se efetiva pela adoção de medidas de proteção que atuam como forma de outorgar densidade ao princípio da segurança no tratamento dos dados pessoais[10].

2. PROTEÇÃO DE DADOS E AUTODETERMINAÇÃO INFORMATIVA: POSSIBILIDADE DE CONTROLE DOS DADOS

Em 1981, Vittorio Frosini publicava, na *Rivista Informatica* e *diritto*, notas de reflexão a respeito do que, na época, representava a *jovem dimensão*

10 A introdução de elementos da cultura jurídica dos países de tradição anglo-saxã, como as noções de autorregulação, desregulamentação e responsabilidade, oferecem maior flexibilidade ao procurar soluções para casos concreto e específicos e permite a adaptação rápida às futuras mudanças tecnológicas. Todavia, a escolha implica maior incerteza jurídica para os responsáveis habituados à extensa regulação característica do modelo legal continental, seguido no Brasil. Nesse sentido, Pinãr Mañas salienta que não está correta a noção de "(...) de que es suficiente el cumplimiento formal de las obligaciones que fijan la ley y el reglamento ha de quedar definitivamente superada. Ya no basta (nunca ha sido así, por lo demás) con inscribir los ficheros, adoptar el documento de seguridad, implementar las medidas de seguridad y redactar las clausulas informativas en materia de protección de datos; obligaciones éstas, por lo demás, claramente definidas en las normas. A partir de ahora será necesario adoptar decisiones propias en función de los tratamientos de datos que se lleven cabo y de la naturaleza de éstos. Algo que va a estar mucho más al alcance de las grandes compañías y Administraciones públicas, pero no tanto de las pymes y pequeños organismos públicos" (PIÑAR MAÑAS, 2016, p.15).

da liberdade individual informática. A contextualização evidenciava as perspectivas do renomado filósofo italiano: não por menos que os efeitos do uso das calculadoras eletrônicas (ou computadores) na tutela dos dados pessoais era objeto de investigação científica naquele momento. A aprovação em janeiro daquele ano da *Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (UNIÃO EUROPEIA, Convenção 108, 1981)* pelo *Conselho da Europa* representou, não o passo precursor[11], mas o decisivo para a construção da tutela da proteção de dados que se desenvolveu na União Europeia nas décadas que seguiram. Passou-se, na década seguinte, com a *Diretiva 95/46/CE*, à unificação da regulação comunitária e, recentemente, com o Regulamento Geral sobre a Proteção de Dados UE 2016/679 – RGPD ou *Regulamento Europeu*, à normatização cada vez mais especializada e atenta à velocidade das comunicações informatizadas por meios eletrônicos e da necessidade de tutela jurídica eficiente[12].

O direito à autodeterminação informativa, tese doutrinária de origem alemã elaborada para explicar as primeiras implicações entre dados informatizados e a respectiva proteção da pessoa, consiste em garantir ao cidadão os direitos de informação, acesso, retificação e supressão de dados pessoais, e antecede a autonomia do direito à proteção de dados prevista na Carta da União Europeia (LIMBERGER, 2007). No Brasil, a autodeterminação informativa apresenta-se como um dos fundamentos da *Lei Geral de Proteção de Dados*. Pressupõe, portanto, o controle, o conhecimento e o consentimento da utilização-destinação dada pelo responsável pelo tratamento de dados.

Nessa linha de ideias, convém observar que o tratamento dos dados pessoais se submete a *padrões de proteção*, elaborados ou certificados pela Autoridade Nacional de Proteção de Dados – ANPD. Com base nessa lógica, o *Regulamento Europeu* e a *LGPD*, tendo no horizonte a ideia motriz de conferir maiores responsabilidades ao responsável pelo tratamento, coloca o *consentimento do titular dos dados* como fator determinante à

11 O Convênio Europeu para Proteção de Direitos Humanos – CEDH previu o direito à vida privada, no sentido de resguardar o desenvolvimento da personalidade sem influências externas. A Convenção 108, no âmbito de uma definição normativa de dado pessoal, apresenta-o como qualquer informação relacionada à pessoa natural identificada ou identificável, definição que sobrevive e está presente na *LGPD*.

12 Convém notar a distinção entre proteção de dados e privacidade tecida por Rodotà: "La protección de datos, por el contrario, fija normas sobre las modalidades de tratamiento de datos, se concreta en poderes de intervención: la tutela es dinámica, y sigue a los datos durante su circulación" (2003, p.17).

legitimidade do processo de tutela das informações[13]. Não apenas isso: o *Regulamento Europeu* inova ao trazer os princípios da proteção de dados desde a concepção (*privacy by design*) e por defeito (*privacy by default*)[14], identificando a proposta do novo sistema com a *autorregulação*, própria da incorporação de ferramentas do direito anglo-saxão. As empresas, as organizações e o setor público, dessa forma, deverão configurar ou programar os produtos, serviços ou processos que utilizam sistemas informatizados de maneira a estabelecer o nível mais elevado de segurança da informação (segurança desde a concepção) e adotar medidas que prestigiem a *segurança por defeito*, no momento de eventual *ciberataque*, de modo a resguardar a proteção de dados pessoais. Vale dizer, constituem-se de medidas técnicas e administrativas que deverão ser adotadas para efetivar a proteção dos dados pessoais, especialmente ações preventivas como função de dar eficácia à *responsabilidade proativa* (REIGADA, 2018).

3. O CONSENTIMENTO LIVRE E INFORMADO: MEDIDA PREVENTIVA DE SEGURANÇA EM MATÉRIA DE PROTEÇÃO DE DADOS PESSOAIS?

O direito à proteção de dados pessoais, que representa o aspecto dinâmico-evolutivo da tutela da privacidade, confere ao sujeito o direito de escolher o que está disposto a revelar aos outros (NIGER, p.150). Dessa forma, o *consentimento do titular* é o primeiro passo para que se inicie o tratamento de dados pessoais. A *LGPD* define o consentimento como *"(...) manifestação livre, informada e inequívoca pela qual o titular concorda com*

13 "Se sustancia habilitando a la persona física a ejercer el control sobre sus datos de carácter personal y explica la recurrente denominación del derecho fundamental a la protección de datos personales como derecho a la 'autodeterminación informativa'". (LOMBARTE, 2017, p. 654). Além disso, outro princípio relevante em matéria de proteção de dados é o da licitude, pelo qual o responsável pelo tratamento de dados deve comportar-se conforme as regras do Estado de Direito, de modo que não viole arbitrariamente o que deveria proteger. (PIÑAR MAÑAS, 2016, p. 56-58).

14 No Brasil, o respeito aos princípios está previsto no art. 46, §2.º da LGPD. O conceito de privacidade desde a concepção da tecnologia (desde o design) está baseado numa postura pró-ativa e não reativa da vulneração do direito à privacidade. Com relação à proteção de dados, a privacidade desde o design estaria relacionada com a diminuição dos riscos e, nesse caso, poderia ser uma manifestação do princípio da precaução, levando-se em conta a natureza, o âmbito, o contexto e os fins do tratamento. Um segundo sentido do princípio da privacidade desde o design seria a adoção de processos, procedimentos e políticas, que seriam medidas protetoras da privacidade, voltadas para avaliação dos riscos e da segurança e as avaliações de impacto na proteção de dados pessoais. A proteção de dados desde a concepção da tecnologia está prevista no parágrafo 1 do artigo 25 do Regulamento. O conceito de privacidade desde a concepção da tecnologia culmina no conceito de proteção da privacidade por defeito na tecnologia. A privacidade por defeito garante que mesmo que o usuário não tome as cautelas para proteger seus dados, o sistema da própria arquitetura de software, baseada na privacidade, garantiria a confidencialidade de toda a informação de caráter pessoal. O parágrafo 2.º do artigo 25 do regulamento afirma que o responsável aplicará medidas técnicas e de organização para que, em caso de defeito, os dados não sejam acessíveis. (CALÉS, 2016, p. 305).

o tratamento de seus dados pessoais para uma finalidade determinada"[15]. A manifestação, portanto, é ato positivo e claro. *Al fine*, o titular dos dados pessoais estará anuindo com o tratamento de dados e, *em tese*, conhecendo o quanto sua informação está segura e a extensão do risco da cessão do uso do dado pessoal (princípio da finalidade)[16]. Vale dizer, o aceitará, ao aderir ao contrato em que cede os dados pessoais, às formas de tutela de segurança da informação que a empresa responsável utiliza no processo de tratamento[17]. O consentimento deverá ser prestado de forma a abranger a integralidade do tratamento que contenha a finalidade idêntica, nas hipóteses de múltipla cessão de dados pessoais.

A perspectiva da *responsabilidade* e da *prevenção de danos* como medida de segurança pode ser verificada, de igual forma, na proibição de se reputar consentido o tratamento de dados resultante de previsões contratuais omissas ou de opções pré-validadas que autorizem o tratamento de dados pessoais, uma vez que *não é válido o consentimento prestado de forma genérica*. A *LGPD*, ao estabelecer regras sobre a forma pela qual é prestado o consentimento, protege todos os envolvidos, dado que confere legalidade e legitimidade ao tratamento. O controlador dos dados, por exemplo, deve demonstrar que o *consentimento do titular* foi obtido de *forma válida*, quando solicitado por autoridades administrativas e judiciais.

No âmbito da noção de autodeterminação informativa, consistente no controle dos dados pessoais pelo próprio titular, é admitida a possibilidade de revogação do consentimento, por declaração de vontade, sem provar a existência de causa justificadora ou de expor motivos para a revogação. Os efeitos da revogação operarão de forma irretroativa (*efeitos ex nunc*), de modo a não afetar a licitude dos dados que já foram tratados quando o *consentimento*

15 A definição legal está contida no inciso XII, artigo 5.º, da LGPD (BRASIL, 2018).

16 Questão relevante refere-se à ocorrência de *incidente de segurança* nos sistemas de dados, que pode ser entendida como *a ocorrência ou a potencial ocorrência de vazamento de dados (risco)*. O artigo 48 da LGPD impõe o dever de comunicação tanto ao titular do dado potencialmente em risco ou afetado, quanto à ANPD. Do ponto de vista comparativo, o *Regulamento Europeu* determina que, na hipótese de ocorrência de incidente de segurança, o controlador deve informar a autoridade em, no máximo, *setenta e duas horas* ou apresentar justificativa, caso isso não ocorra. No Brasil, não há prazo especificado na legislação, de modo que será a ANPD o órgão normativamente competente para fixá-lo. Um fator que não pode ser desconsiderado é que a LGPD faz referência ao fato de que as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, no *site* do responsável pelo tratamento de dados.

17 Cabe referir, quanto à forma, que o consentimento do titular de dados pode ser escrito ou oral. A forma eletrônica é admitida, de modo que não existe impedimento legal para que o consentimento ocorra por meio de vídeo ou áudio eletronicamente produzido e armazenados. Se o consentimento tiver de ser dado por via eletrônica, esse pedido tem de ser *claro* e *conciso*, de modo a ser apresentado sem afetar a utilização do serviço para o qual é fornecido.

do titular ainda estava vigorando. Dessa forma, o consentimento expresso é inequívoco. Não significa, entretanto, que o consentimento inequívoco será expresso[18]. De um lado, o consentimento do usuário representa a única condição ao acesso e à utilização de dados pessoais e, por outro lado, confere o poder ao titular de controlar a circulação na rede, a fim de determinar os limites de intervenção na sua vida privada.

A *cibersegurança* não se apresenta apenas como contingência tecnológica: o comportamento humano é fator determinante. Dessa forma, a informação do quanto os titulares de dados pessoais estão expostos a ameaças, e adoção de medidas simples de rotina que minimizam a exposição aos riscos decorrentes de *ciberameaças*, tendem a minimizar os episódios de vazamentos ou de exposições não-autorizadas. É nesse sentido que podemos inferir a importância do consentimento – e da revogação dele - quando detectado pelo cidadão a possibilidade de risco à segurança de seus dados pessoais.

4. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: MECANISMOS DE SEGURANÇA E CONFIANÇA NA PROTEÇÃO DE DADOS

Franchini (1996) e Amato (1997) destacavam, na década de noventa, o crescimento dos debates em torno das autoridades independentes, modelo de autoridade responsável pela supervisão da eficácia de regras de setores específicos, pautadas pela noção de neutralidade e imunidade às influências oriundas do poder político e do econômico. Tratava-se, no primeiro momento, da consolidação conceitual em torno dos critérios de qualificação de uma autoridade como independente; e, no segundo, da

18 Joana Mota (2018, p.4) procura demarcar a diferença entre as duas proposições em três exemplos. *Exemplo 1.* Na hipótese de contrato celebrado entre fornecedor e cliente, em que cláusula de declaração de consentimento do cliente para tratamentos específicos de dados pessoais, sendo que o pedido de consentimento está claramente distinto das demais cláusulas do contrato. Neste caso, fica claro que o consentimento é explícito e inequívoco. *Exemplo 2.* Admitindo-se hipoteticamente o contexto de ambiente laboral, em que os trabalhadores são avisados de que em determinado local da empresa serão fotografados, sendo essas fotografias publicadas na *intranet* da empresa. Se os trabalhadores, que foram informados de forma *transparente* sobre o evento, venham a se dirigir referido local da sessão de fotos, estão a consentir na captação de sua imagem, uma vez que essa autorização é auferida pela sua conduta. Nessa perspectiva, o consentimento é *inequívoco*, mas *não é expresso. Exemplo 3.* Como terceiro modelo de entendimento, deve-se admitir uma página de rede social que solicita que os usuários forneçam um conjunto de informações pessoais para que tenham acesso ao conteúdo. Na política de privacidade a ser consentida pelo usuário ao navegar pela página, está à disposição que ao acessar aos conteúdos ofertados, estará a consentir que seus dados sejam tratados por empresas terceiras para efeitos de *marketing*. Neste contexto, o consentimento *não é válido*, levando em consideração que a inatividade não pode consubstanciar no *consentimento inequívoco ou expresso*. Os referidos exemplos visam ilustrar que o consentimento, para ser válido, nem sempre necessita ser expresso. Haverá sempre que se proceder a análise *caso a caso* do contexto do tratamento dos dados.

especificação funcional e estrutural – administrativa, financeira e jurídica –, por meio da qual a autoridade desempenharia suas funções.

A *Diretiva 95/46/CE* preconizava o modelo de autoridade de proteção de dados totalmente independente, embora não tenha esclarecido o conteúdo da independência. O *Regulamento Europeu*, em contraste, expressamente estabeleceu as garantias de independência das autoridades de controle a serem observadas pelos países da União Europeia. Ao seu turno, no Brasil, a *Medida Provisória n.º 869*, de 27 de dezembro de 2018, recentemente transformada na Lei n.º 13.853, de 8 de julho de 2019, pelo Congresso Nacional, veio a suprir a lacuna de organização administrativa relativa ao vício formal que ensejou o veto da criação da Autoridade Nacional de Proteção de Dados - ANPD. Apesar de constituí-la, não se conferiu à autoridade brasileira as garantias estruturais e substanciais que caracterizam o modelo europeu consolidado pelo *Regulamento* em vigor. Cabe destacar, no entanto, que a autoridade brasileira é tratada como órgão central de interpretação e fiscalização do cumprimento da *LGPD* e torna-se a entidade responsável pela manutenção da *confiança* e *seriedade* do sistema brasileiro e, nesse sentido, a ausência de uma independência reforçada – com garantias institucionais firmes – tenderia a acarretar dificuldades de organização da tutela da proteção de dados no país (SCHERTEL; DONEDA, p. 45).

Está-se a afirmar, com Cláudia Lima Marques, que *"(...) o direito encontra legitimidade justamente no proteger as expectativas legítimas e de confiança (Vertrauen) dos indivíduos"* (2004, p.31). Nesse sentido, a proteção de dados, a fiabilidade e a segurança dos sistemas informáticos são essenciais para as atividades desenvolvidas em rede, de modo que o esforço das autoridades competentes deve levar em conta, por um lado, a supervisão ex post, no sentido da adoção de mecanismos reativos e que permitam a avaliação do risco e fomento à prevenção de danos, por diferentes instrumentos; e, de outro, dar publicidade aos incidentes comunicados, como forma de equilibrar o interesse do público e individual do cidadão em ser informado acerca das ameaças aos dados pessoais que titulariza e os eventuais danos dos prestadores de serviços digitais, no tocante à reputação e prejuízos econômicos.

A competência regulamentar e fiscalizatória dos mecanismos de segurança adotados pelos prestadores de serviços digitais deverá ser regulamentada pela ANPD, o que, a título comparativo, é desempenhado pelas autoridades independentes europeias designadas para esse propósito, no âmbito de cada país, e, no âmbito comunitário, pela Agência da União

Europeia para a Segurança das Redes e da Informação – ENISA, que fixa regras gerais a serem observadas pelos países integrantes ao bloco[19].

A seguridade digital na transferência internacional de dados pessoais por meio de sistemas informatizados deve ser vista com atenção, em razão da crescente utilização do comércio eletrônico transfronteiriço e da possibilidade de não-autorização de transferências de dados para países que não possuam níveis de seguridade de dados compatíveis com o previsto na União Europeia. A ANPD, nesse sentido, exercerá função desafiadora, dada a ausência de independência total preconizada pela regulação comunitária, mas é possível encontrar na *LGPD* mecanismos alternativos aptos a garantir os padrões de segurança. Conforme dito anteriormente, a tendência verificada, no sentido de unificação das possibilidades jurídicas de proteção de dados e resguardo da segurança, reside na introdução de mecanismos de *autorregulação*[20] ou mecanismos que denotem uma postura ativa por parte do responsável. Nessa linha, o *Regulamento Europeu* prevê a possibilidade de adoção de selos e certificados de qualidade (art.42) e de adoção de códigos de conduta pelos responsáveis pelo tratamento (art.40)[21].

A certificação aplicada à proteção dos dados pessoais, além de servir como elemento de demonstração do cumprimento do *Regulamento Europeu*, foi incorporado na *LGPD* como possibilidade de auxílio na formação da confiança do titular de dados pessoais ao utilizar diferentes produtos e serviços[22]. De maneira objetiva, a certificação ou a conferência de selo de qualidade significa que os responsáveis pelo tratamento podem, com a intervenção prévia de organismo especializado e independência necessária, obter determinado certificado atestando que foram submetidos a um rigoroso e metodológico processo de avaliação, conforme as normas e padrões estabelecidos em matéria de segurança na proteção de dados, e que suas práticas atendem aos requisitos estabelecidos pela legislação vigente. Portanto, a certificação vai além da demonstração de cumprimento das regras de proteção de dados, vinculando-se ao tratamento seguro de dados

19 Criada pelo Regulamento n.º 460/2004, apresenta como objetivo desenvolver a cultura de segurança nas redes em benefício dos cidadãos, dos consumidores, das empresas e das administrações públicas. O Regulamento que vigora atualmente é o Regulamento UE n.º 2019/881.

20 Os instrumentos citados possuem afinidade com a denominada autorregulação regulada, de modo a ser dinâmica, flexível e baseada no consenso (MOREIRA NETO, 2009).

21 A LGPD não escapa ao padrão identificado, apresentando disposições semelhantes e sujeitando a regularidade dos instrumentos à fiscalização da ANPD

22 Veja-se, por exemplo, o avanço da indústria de automóveis autônomos, de dispositivos de aplicação médica interconectados com banco de dados, os sistemas de controle da automação industrial ou de redes inteligentes guiadas por inteligência artificial.

pessoais, conforme padrões técnicos de seguridade digital (SÁNCHEZ; GAYO, 2016, p.414).

Assim como preconizado pelo Regulamento n.º 2019/881, relativo à certificação da *cibersegurança* das tecnologias da informação e comunicação na União Europeia, a certificação da *cibersegurança* cumpre a função de assegurar ao titular dos dados que os produtos e serviços certificados estão de acordo com os padrões e requisitos estabelecido na rotina de certificação, com o intuito de proteger a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados, transmitidos ou tratados. Não é possível definir requisitos de *cibersegurança* globais aplicáveis em todas as circunstâncias, em razão da ampla variedade de produtos produzidos e diferentes tecnologias, porém é possível estabelecer o nível de segurança da informação utilizado, escalonados em *nível básico, nível substancial* e *nível elevado*, cada qual compatível com determinados padrões de segurança e com o risco de vulnerabilidade.

O *Regulamento Europeu* define que a certificação poderá ser realizada por uma entidade independente das partes interessadas, que se manifesta se uma organização, produto, processo ou serviço, cumpre os requisitos definidos em uma norma específica ou técnica. Além disso, prevê que as empresas de certificação devem reunir vários requisitos para atuação, inclusive perícia experiência necessárias para a realização das avaliações e que desfrutem de prestígio devidamente reconhecido perante o mercado. A certificação, no âmbito europeu, tem validade de três anos, podendo ser renovada, desde que os requisitos ainda estejam presentes. (UE, 2016). No Direito brasileiro[23], ainda não se tem, de forma minuciosa, regras sobre os *mecanismos de certificação em proteção de dados*. Entretanto, de forma genérica, a *LGPD* dispõe que empresas poderão buscar a certificação de que seus produtos ou serviços atendem aos requisitos de segurança de tratamento estabelecidos pela norma. A *LGPD* determina ainda, que a certificação deverá ser feita pela ANPD, podendo esta designar organismo de certificação diverso, que permanecerá sob sua fiscalização (BRASIL, 2018).

As soluções relacionadas à certificação em matéria de proteção de dados caracterizam-se pela flexibilidade, em razão da busca contínua por

23 Mesmo antes da vigência do RGPD – UE 2016/679, a Argentina havia recebida da União Europeia certificação quanto ao nível de segurança no tratamento das informações. O país foi o precursor na América do Sul na edição de uma lei geral de proteção de dados, recebendo o "selo europeu de qualidade", em razão de sua amplitude. A Lei nº 25.326/00 – AR, promulgada no mês de outubro do ano 2000, estabelece direitos e deveres, cria os órgãos de supervisão de proteção de dados e estabelece sanções em caso de descumprimento.

adequação dos sistemas às novas vulnerabilidades, e a rapidez com que os sistemas de proteção ficam desatualizados. Desse modo, percebe-se que a certificação proporciona as seguintes vantagens no que concerne à proteção de dados: *(i)* demonstração do cumprimento da *LGPD*; *(ii)* transparência nos processos de tratamento; *(iii)* aumento da competitividade entre organizações que realizam o tratamento de informações pessoais; e (iv) incremento da confiança individual e da reputação da organização pública ou privada.

Além da certificação, os códigos de conduta também servem para demonstrar o cumprimento das regras constantes nas legislações de proteção de dados. O *Regulamento Europeu* e a *LGPD* trazem disposições para incentivar que agentes de tratamento de dados editem seus próprios códigos ou adotem códigos de determinados setores do mercado, adequando-os à realidade de atuação e às necessidades específicas do setor. Na verdade, o código de conduta será um manual a ser seguido pela organização para fins de adequação dos padrões de segurança e tratamento de dados, especialmente no concerne às medidas e procedimentos de segurança a serem adotados no caso de vazamento de dados ou incidentes informáticos. Para que determinado código de conduta não seja uma simples declaração de intenções, existem procedimentos de supervisão e controle de seu cumprimento efetivo. Essa supervisão será feita pela ANPD ou por um ente habilitado por ela para exercer tal função. Gómez (2016, p. 405) questiona se os códigos de conduta podem ser caracterizados como uma *autorregulação* ou *autorregulação regulada*, e soluciona a questão explicando que os códigos de conduta são aprovados e fiscalizados por um órgão do poder público, não podendo, desta maneira, serem considerados autorregulação em sentido estrito, mas, sim, como uma manifestação de *corregulação*.

5 CONSIDERAÇÕES FINAIS

A proteção de dados pessoais apresenta-se como consequência do desenvolvimento e especificação do direito à vida privada (privacidade), de modo a permitir que o titular de dados desempenhe a autodeterminação informativa, consistente na faculdade de controlar o uso dos dados pessoais que titulariza. O consentimento para utilização de dados pessoais desempenha função importante no processo de tratamento de dados pessoais, por conferir legitimidade à utilização das informações por organizações públicas e privadas. Mas, para além disso, a revogação do consentimento é outro mecanismo de destaque, este que pode ser promovido, sem a apresentação de justificativas pelo titular de dados.

A relevância da temática do consentimento assume relevância no debate acerca da segurança das redes e dos sistemas informatizados dos responsáveis pelo tratamento de dados. A *Lei Geral de Proteção de Dados – LGPD (Lei n.º 13.709/2018)* propõe o resguardo da segurança e da confidencialidade dos dados pessoais, de modo a tornar obrigatória a utilização de medidas contendoras, técnicas e administrativas, de incidentes de vazamento. Nesse sentido, preconizou a observância dos princípios da proteção de dados desde a concepção (*privacy by design*) e por defeito (*privacy by default*), identificando a proposta do novo sistema com a autorregulação, própria da incorporação de ferramentas do direito anglo-saxão. Vale dizer, adotou, aos moldes do *Regulamento Europeu* a noção de segurança dos dados desde a concepção do produto ou serviço e, além disso, a busca de contenção dos danos em eventual falha da segurança da aplicação.

A perspectiva global da proteção de dados indica a aposta das regulamentações em mecanismos de *responsabilização proativa*, no sentido de romper com a lógica das empresas que *meramente cumprem normas de segurança*, para a visão antecipatória dos riscos e vulnerabilidades com adoção de medidas preventivas.

Embora não seja possível definir requisitos de *cibersegurança* globais aplicáveis em todas as circunstâncias, em razão da ampla variedade de produtos produzidos e diferentes tecnologias, a adoção de certificados ou selos de qualidade de proteção de dados torna possível o controle dos padrões de segurança, escalonados em *nível básico*, *nível substancial* e *nível elevado*, categorizados conforme o risco de vulnerabilidade. Trata-se de uma possibilidade que a *LGPD* permite às organizações públicas e privadas, ainda pouco utilizada, mas que garante flexibilidade dos sistemas informáticos às mutações tecnológicas, no tocante à adequação a padrões de segurança. Os códigos de conduta assumem função complementar, nessa linha de raciocínio, na medida em que permitem a previsão objetiva dos procedimentos a serem adotados no tratamento e das medidas emergenciais na hipótese de *ciberincidentes*.

REFERÊNCIAS

AGÊNCIA O GLOBO. *Facebook perde quase US$ 50 bilhões em dois dias*. [S.L]. 20 mar. 2018. Disponível em: <http://www.valor.com.br/empresas/5398017/facebook-perde-quase-us-50-bilhoes-em-dois-dias>. Acesso em 02 jun. 2019.

AMATO, Giuliano. Autorità semi-indipendenti ed autorità di garanzia. *Rivista trimestrale di diritto pubblico*, Milano, n. 3, p.645-664, jul./set., 1997.

ARGENTINA. *Lei n.º 25.326, de 4 de outubro de 2000*. Disponível em: <https://www.oas.org/juridico/PDFs/arg_ley25326.pdf>. Acesso: 24 jun. 2019.

BERNAL, Paul. *Internet privacy rights*: rights to protect autonomy. Cambridge: Cambridge University, 2014.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso: 24 jun. 2019.

CADWALLARD, Carole; GRAHAM-HARRISON, Emma. Revealed: *50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian. [S.L.]. 27 de mar. 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em 02 jun. 2019.

CALÉS, Rosario Duaso. Los principios de protección de datos desde el diseño y protección de datos por defecto. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos*. Madrid: Editora Reus, 2016. p.299-325.

CASTELLS, Manoel. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2013.

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

FOLHA DE S. PAULO. *Vazamento de dados do Facebook atinge 443.117 usuários brasileiros*. São Paulo. 5 abr. 2018. Disponível em: <https://www1.folha.uol.com.br/mundo/2018/04/vazamento-de-dados-do-facebook-atinge-443117-usuarios-brasileiros.shtml>. Acesso em 02 jun. 2019.

FRANCHINI, Claudio. Mito e realtà delle autorità indipendenti. *Impresa e Stato*, n. 35, p. 29-35, 1996.

FROSINI, Vittorio. La protezione della riservatezza nella società informatica. *Rivista Informatica e diritto*, v.7, n. 1, p. 5-14, 1981.

GÓMEZ, Alberto Díaz-Romeral. Los códigos de conducta en el reglamento general de protección de datos. In: PIÑAR MAÑAS, José Luis; GAYO,

Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos.* Madrid: Editora Reus, 2016. p.393-410

LIMBERGER, Têmis. *Cibertransparência informação pública em rede*: a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016.

LIMBERGER, Têmis. *O direito à intimidade na era da informática*: A necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

LOMBARTE, Artemi Rallo. De la "libertad informática" a la constitucionalización. De nuevos derechos digitales (1978-2018). *Revista de Derecho Político*, n. 100, p. 639-669, septiembre-diciembre, 2017.

MARQUES, Cláudia Lima. Confiança no Comércio Eletrônico e a Proteção do Consumidor: um estudo dos negócios jurídicos de consumo no comércio eletrônico. São Paulo: *Revista dos Tribunais*, 2004.

MOREIRA NETO, Diogo de Figueiredo. Crisis y regulación de mercados financieros. la autorregulación regulada: ¿una respuesta posible? *Revista de Administración Pública*, Madrid, n. 180, págs. 9-19, septiembre-diciembre, 2009.

MOTA, Joana. O consentimento no regulamento geral sobre proteção de dados. *Revista InforBanca*, Lisboa, n.112, p.4-10, fev., 2018.

NIGER, Sérgio. *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali.* Padova: CEDAM, 2006.

PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedade tecnológica.* Madrid: Universitas, 2012.

PIÑAR MAÑAS, José Luis. Sociedad, innovación y privacidad. Información Comercial Española, ICE: *Revista de economía*, Madrid, n. 897, p.67-76, jul./ago, 2017.

PIÑAR MAÑAS, José Luis. El objeto del reglamento. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos.* Madrid: Editora Reus, 2016. p.13-22.

REIGADA, Antonio Troncoso. Autoridades de control independientes. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos.* Madrid: Editora Reus, 2016. p.465-516.

REIGADA, Antonio Troncoso. *Del principio de seguridad de los datos al derecho a la seguridad digital.* Economía industrial, Madrid, [s.v.], n. 410, p.127-151, 2018.

ROBLEDO, Enrique Pérez-Luño. *La nueva normativa europea para la protección de los datos personales.* Derechos y libertades, Madrid, n. 40, p. 213-238, enero, 2019.

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

RODOTÀ, Stefano. *El derecho a tener derechos.* Madrid: Trotta, 2014.

RODOTÀ, Stefano. *Democracia y protección de datos. Cuadernos de Derecho Público*, Bogotà, n. 19-20, p.15-26, mayo-diciciembre, 2003.

SÁNCHEZ, Carlos Manuel Fernández; GAYO, Miguel Recio. Certificación en protección de datos personales. In: PIÑAR MAÑAS, José Luis; GAYO, Miguel Recio; CARO, María Álvarez (Org.). *Reglamento general de* protección de datos: hacia un nuevo modelo europeo de protección de datos. Madrid: Editora Reus, 2016. p.417-430.

SCHERTEL MENDES, Laura; DONEDA, Danilo. Reflexões gerais sobre a nova lei de proteção de dados. *Revista do Direito do Consumidor*, Brasília, v.120, p.469-483, nov./dez. 2018.

UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia.* Disponível: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf> Acesso em 24 jun. 2019.

UNIÃO EUROPEIA. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal* Data Disponíve em: Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37>. Acesso em 24 jun. 2019.

UNIÃO EUROPEI*A.* Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho da Europa, de 17 de abril de 2019. Disponível em: <https://eur-lex.

europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32019R0881&qid=1561376799525&from=PT#d1e4535-15-1>. Acesso em 24 jun. 2019.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho da Europa*, de 27 de abril de 2016. Disponível: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em 24 jun. 2019.