LEI GERAL DE PROTEÇÃO DE DADOS

CADERNO ESPECIAL • NOVEMBRO • 2019

COORDENAÇÃO:
CARLOS AFFONSO SOUZA
EDUARDO MAGRANI
PRISCILLA SILVA

Ana Lara Mangeth
Caio Oliveira
Caitlin Mulholland
Carlos Affonso Souza
Chiara Spadaccini de Teffé
Daniel Bucar
Danilo Doneda
Filipe Fonteles
Giovana Carneiro
Gisela Sampaio
Henrique Cunha Souza Lima
Isabella Frajhof
Laura Schertel Mendes
Leonardo Heringer
Leonardo Parentoni
Marcel Leonardi
Mario Viola
Priscilla Silva
Rafael Zanatta
Renato Leite Monteiro
Vinicius Padrão

THOMSON REUTERS
REVISTA DOS TRIBUNAIS™

A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis

Laura Schertel Mendes

Professora Adjunta de Direito Civil da Universidade de Brasília (UnB). Professora do mestrado acadêmico em Direito Constitucional do Instituto Brasiliense de Direito Público (IDP). Doutora em Direito Privado pela Universidade Humboldt de Berlim.

1. Introdução

A[1] disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados *per se*, mas, sim, a pessoa que é titular desses dados.

Por diversas razões, tais como a ampliação da complexidade do sistema industrial, a burocratização dos setores público e privado e a transformação das ciências sociais, o certo é que nos tornamos a sociedade que mais gerou dados pessoais na história da humanidade, o que pode ser demonstrado pelas dezenas de bancos de dados nos mais variados setores: registros de nascimento e casamento, registros escolares, dados do censo, registros militares, dados de passaporte, registros de empregados e de servidores públicos, registros do

1. O presente texto atualiza capítulo do livro "Privacidade, proteção de dados pessoais e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014", de modo a adaptá-lo à recém-aprovada Lei Geral de Proteção de Dados (Lei 13.709/2018).

Mendes, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. Caderno Especial LGPD. p. 35-56. São Paulo: Ed. RT, novembro 2019.

serviço de saúde, registros da defesa civil, registros de seguros, registros financeiros, registros de dados telefônicos, entre outros[2].

Tendo em vista que as informações pessoais constituem-se em intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito[3]. Por se constituírem em uma parcela da personalidade da pessoa, os dados merecem tutela jurídica, de modo a assegurar a sua liberdade e igualdade.

O modelo jurídico adotado por diversos países para a proteção dos dados pessoais consiste em uma proteção constitucional, por meio da garantia de um direito fundamental e, na concretização desse direito, por meio de um regime legal de proteção de dados, na forma de uma lei geral sobre o tema.

O regime legal de proteção de dados pessoais pode ser compreendido como a legislação ordinária, geralmente fundamentada na Constituição, cuja finalidade é a de regular o tratamento de dados pessoais na sociedade. É, portanto, o exercício do poder do Estado para intervir no processamento de dados, buscando estabelecer fluxos adequados de informação na sociedade, de modo a proteger tanto a coletividade como os direitos fundamentais dos cidadãos[4]. Essa regulação constitui, além do controle do Estado sobre a economia ou sobre a sociedade, o controle sobre os seus próprios órgãos que realizam tratamento de dados pessoais.

Muito embora existam diversas formas de se regulamentar a privacidade, como por meio de previsões constitucionais, *privacy torts*, mecanismos contratuais determinados legalmente, nos últimos 30 anos, as leis gerais de proteção de dados pessoais se firmaram como umas das formas mais eficazes de se proteger a privacidade nos países desenvolvidos[5].

A abrangência dessas normas e o seu âmbito de aplicação variam de país para país, conforme o seu próprio processo político. É possível, no entanto, observar semelhanças e tendências. Como visto, embora o início das legislações de proteção de dados pessoais tenha ocorrido em razão do temor do poder de processamento de dados pelo Estado, logo se viu que riscos semelhantes

2. WESTIN, Alan. *Privacy and Freedom*. Nova York: Atheneum, 1970. p. 158 e 159.
3. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.
4. BENNET, Colin; RAAB, Charles. *The governance of privacy*, cit., p. 125.
5. Ibidem, p. 126.

também existiam no setor privado. Desse modo, a Diretiva Europeia 95/46/CE[6] orientou os países a promulgarem leis abrangentes que compreendessem tanto o setor público quanto o setor privado. Esse movimento acabou por influenciar também países como Canadá e Austrália, que buscaram, cada um dentro de sua estrutura federativa, abarcar também a regulamentação do setor privado[7].

Neste contexto, a legislação sobre proteção de dados – entendida como o marco jurídico para a proteção individual em face do tratamento de dados e informações pessoais por terceiros – encontra-se atualmente no centro da discussão econômica, social e política no mundo e também no Brasil.

2. Contexto internacional: o desenvolvimento das gerações de leis de proteção de dados pessoais

A primeira geração das normas de proteção de dados pessoais surgiu, na década de 70, como reação ao processamento eletrônico de dados nas Administrações Públicas e nas Empresas Privadas, bem como às ideias de centralização dos bancos de dados em gigantes bancos de dados nacionais. São exemplos de normas da primeira geração as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Todas essas normas podem ser consideradas de primeira geração pela sua estrutura e linguagem[8].

O impulso para o surgimento dessas normas foi o contexto generalizado do Estado Social, que requeria, para o funcionamento de sua burocracia, de planejamento sofisticado, o que, por sua vez, somente poderia ser alcançado por meio da coleta e do processamento dos dados dos cidadãos. Como exemplos do grande interesse das burocracias governamentais pela coleta desses dados nesse período, podem-se citar a proposta feita pelo Parlamento da Suécia, em 1960, de fundir todas as informações fiscais e os registros civis aos dados do censo, bem como o Comitê criado pelo governo alemão para viabilizar a conexão entre os bancos de dados municipais, estaduais e federal[9].

6. Diretiva Europeia 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
7. BENNET, Colin; RAAB, Charles. *The governance of privacy*, cit., p. 130.
8. Ibidem, p. 221.
9. Ibidem, p. 222.

Nos EUA, pode-se citar como exemplo o caso do *National Data Center*, projeto que nunca saiu do papel, em razão da grande reação da população. Como relata Simson Garfinkel, o *National Data Center* foi proposto em 1965 pelo *Bureau of Budget*, órgão competente para administrar o orçamento, e visava à redução de custos pelo Estado[10]. O conceito do projeto era a de que um único centro de dados nacional eximiria os demais órgãos do governo de investirem em informática e em tecnologia de armazenamento. À medida que o projeto evoluiu, chegou-se à ideia de que o centro deveria conter dados de todos os cidadãos americanos em relação à data de nascimento, cidadania, registros escolares, serviço militar, registros de impostos, benefícios da previdência social, registro do espólio e, eventualmente, registros criminais. Procederam-se a inúmeras discussões nos meios de comunicação e a diversas audiências no Congresso. Esses debates culminaram em um debate público acerca dos potenciais danos que tal centralização de dados poderia causar, principalmente em razão do grande poder que ele conferia ao Estado sobre a vida de todos os cidadãos, ameaçando gravemente a tradição liberal americana[11]. Assim, o *National Data Center* nunca chegou a ser construído.

Como se vê, a reação dos cidadãos contra as tentativas dos governos de utilizar a tecnologia existente para ampliar a coleta e o processamento dos dados foi extremamente forte, por causa do temor do poder de controle de uma burocracia automatizada e desumanizada. A reivindicação da opinião pública voltava-se prioritariamente no sentido de se controlar a tecnologia, o que acabou por influenciar as legislações de proteção de dados. Grande parte das leis da década de 70 tem uma perspectiva funcional e busca controlar os bancos de dados de forma *ex ante*, condicionando o seu funcionamento à licença prévia ou ao registro nos órgãos competentes[12]. Ademais, ao priorizar o controle rígido dos procedimentos, as normas desse período deixavam para segundo plano a garantia do direito individual à privacidade, o que pode ser percebido a partir do próprio jargão técnico utilizado nas normas.

É interessante ressaltar que os planos estatais ambiciosos de construção de um banco de dados centralizado não se concretizaram. Isso, no entanto, se deve menos às reivindicações sociais e mais à transformação tecnológica que

10. GARFINKEL, Simson. *Database Nation*, cit., p. 13.

11. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, cit., p. 189.

12. MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe*, cit., p. 223.

possibilitou que unidades organizacionais pequenas do governo e da iniciativa privada utilizassem processamento de dados eletrônicos de forma descentralizada[13]. Tal fato ocasionou a proliferação da quantidade de bancos de dados existentes e, consequentemente, expôs a fragilidade da regulamentação das normas de primeira geração que estabeleciam procedimentos em detrimento de direitos.

Desse modo, surgiu a necessidade de alteração legislativa e abriu-se espaço para a segunda geração das normas de proteção de dados pessoais. Tais normas buscavam tratar prioritariamente do direito à privacidade, ao invés de procedimentos. A temática da proteção de dados pessoais passa a se associar diretamente ao direito à privacidade, às liberdades negativas e à liberdade individual em geral. Como consequência, a privacidade informacional é inserida nos textos das Constituições da Áustria, da Espanha e de Portugal.

O temor por um banco de dados único e centralizado passa a ser substituído, então, pelo temor da existência de milhares de bancos de dados espalhados pelo mundo, conectados em rede e gerenciados por organizações públicas e por empresas privadas[14]. Nesse contexto, entendeu-se que o melhor seria que os cidadãos lutassem pela preservação de sua privacidade a partir de direitos fortes e, em alguns casos, protegidos constitucionalmente. São exemplos de normas da segunda geração as leis da Áustria, da França, da Dinamarca e da Noruega[15]. Outra mudança significativa dá-se no âmbito institucional, com a ampliação dos poderes das autoridades administrativas encarregadas da proteção de dados.

A segunda geração de normas de proteção de dados pessoais suscita uma controvérsia bastante interessante, relacionada à efetividade do consentimento do cidadão e do real exercício de sua liberdade de escolha, em um contexto no qual a não disponibilização dos dados pode acarretar a sua exclusão social. Por um lado, no âmbito do Estado Social, é muito difícil assegurar-se a liberdade informacional sem comprometer as funções dessa complexa burocracia que necessita de dados dos cidadãos para planificar. Por outro, também na relação entre privados, é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca de suas informações pessoais.

13. Ibidem, p. 225.

14. HASSEMER, Winfried. *Datenschutz: die Aufgaben der nächsten Jahre*, cit., p. 131.

15. Ibidem, p. 227.

Mayer-Schönberger observa de forma crítica e precisa o custo social que o indivíduo tem de pagar para exercer o seu direito à privacidade e à proteção dos dados pessoais:

> "A proteção de dados pessoais como liberdade individual pode proteger a liberdade do indivduo. Ela pode oferecer ao indivíduo a possibilidade de não conceder informações a seu respeito que lhe são solicitadas. Mas qual será o custo que se tem de pagar por isso? É aceitável que a proteção de dados pessoais possa ser exercida apenas por eremitas?"[16]

A terceira geração de normas de proteção de dados pessoais é marcada pela decisão do Tribunal Constitucional alemão[17], de 1983, que declarou a inconstitucionalidade de parte da Lei do Censo. Na ocasião, o Tribunal reinterpretou a lei federal de proteção de dados pessoais alemã à luz da Lei Fundamental de Bonn e declarou que os cidadãos possuem o direito à autodeterminação informativa, radicalizando a ideia do controle do indivíduo no processamento de seus dados.

Nessa formulação de um direito à autodeterminação informativa, o Tribunal reconheceu uma carga participativa muito maior que a reconhecida pelas interpretações das normas de proteção de dados pessoais em períodos anteriores. A principal diferença em relação à segunda geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como a opção entre "tudo ou nada".

Também o contexto tecnológico sofreu alteração na década de 80, na medida em que novas tecnologias de rede e de telecomunicações ampliaram a capacidade e a velocidade de transmissão de dados. Nesse sentido, não é mais possível localizar fisicamente os bancos de dados, pois esses estão armazenados em redes e não mais em uma central identificável de processamento, podendo ser transferidos em segundos[18].

São exemplos dessa fase as leis dos Estados alemães posteriormente à decisão do Tribunal Constitucional, a emenda à lei federal de proteção de dados

16. MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe*, cit., p. 228.
17. BVefGE 65, 1, Volkszählung – grifo nosso. Ver MARTINS, Leonardo (Org.). *Cinqüenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005. p. 233 a 245.
18. MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe*, cit., p. 230.

pessoais alemã de 1990, a emenda da lei da Áustria de 1986, a alteração da lei da Noruega e a previsão constitucional da proteção de dados pessoais da Holanda.

No entanto, mais uma vez, pode-se dizer que o ideal participativo dos cidadãos no controle das informações pessoais, consubstanciado na ideia de autodeterminação informativa, provou-se não ser factível no mundo real. Isso porque, semelhante ao que ocorreu com a segunda geração das normas de proteção de dados pessoais, os cidadãos não estavam dispostos a arcar com os altos custos monetários e sociais de exercer o seu direito e, por consequência, serem privados do acesso a bens e serviços ou a benefícios[19].

Ademais, tendo em vista que o consentimento do indivíduo autorizava o processamento dos dados pessoais, em caso de violação ao seu direito à privacidade, não teria ele condições de lutar pela reparação daquela violação, na medida em que tinha consentido para o tratamento de seus dados.

A quarta geração de normas buscou resolver esses problemas apresentados nos períodos anteriores por meio de duas soluções. Primeiramente, algumas das normas visaram fortalecer a posição dos indivíduos, tornando mais efetivo o seu autocontrole sobre os dados pessoais. Isso foi possível, por exemplo, a partir da previsão de *no fault compensation* para reclamações individuais a respeito da violação à proteção de dados pessoais, que se deu na Alemanha, com a emenda à Lei Federal de Proteção de Dados alemã, dado que norma semelhante já existia na legislação da Noruega em menor extensão[20].

Em outros casos, as normas retiraram da esfera do controle do indivíduo determinados assuntos, por compreenderem que alguns temas relativos aos dados pessoais são tão relevantes para o cidadão que merecem ser extremamente protegidos, não podendo estar na esfera de disposição individual. Tal pode ser observado na proibição, total ou parcial, imposta para o tratamento dos dados pessoais considerados sensíveis, que são aqueles cujo tratamento tem grande potencial de acarretar discriminação, tais como os dados relativos à etnia, opção sexual, opinião política e religião[21].

19. Ibidem, p. 232.

20. Ibidem, p. 233.

21. SIMITIS, Spiros. Revisiting Sensitive Data. *Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 24-26 November 1999. Acessível em: [www.coe.int/t/dghl/standardsetting/dataprotection/Reports_and_studies_en.asp]. Acesso em: 29.02.2012.

Outra característica bastante interessante da quarta geração de normas de proteção de dados pessoais consiste no fato de que, em diversos países, normas gerais sobre a proteção de dados são complementadas com normas setoriais. Tal fato tem como finalidade ampliar a proteção do indivíduo nos diversos setores em que é possível o tratamento dos seus dados pessoais, de modo que a legislação possa contemplar as diversas especificidades setoriais existentes[22]. Assim, na maioria dos países europeus, percebe-se a existência de uma regulamentação geral sobre proteção de dados, mas com códigos de conduta setoriais suplementares.

Conforme afirma Mayer-Schönberg, a Diretiva Europeia sobre proteção de dados pessoais de 1995 reflete a evolução geracional, pela qual passou a disciplina da proteção de dados pessoais na Europa[23]. Isso porque está no seu cerne a participação do indivíduo no processo de tratamento dos dados pessoais. Além disso, em caso de tratamento de dados sensíveis, a Diretiva determina que esse está condicionado ao consenso expresso e informado do indivíduo.

Embora não abrangida temporalmente no texto de Mayer-Schönberger, atualmente, já se fala em uma quinta geração de proteção de dados pessoais. Isso se dá em razão de novos desenvolvimentos nessa seara, tais como a revisão pela OCDE das Diretrizes relativas à proteção de dados pessoais e ao fluxo de dados transfronteiriços de 2013, a edição do Regulamento Geral de Proteção de Dados na Europa em 2016, que entrou em vigor em 25 de maio de 2018, assim como a recém-aprovada Lei de Proteção de Dados da Califórnia.

Característica da geração atual de normas de proteção de dados, que começa a se desenvolver, é a aposta em um sistema de corregulação, amparado no princípio da *accountability*[24], isto é, passa-se a entender que a efetividade da proteção de dados não reside mais apenas em ampliar o controle do indivíduo, mas também em atribuir responsabilidade a toda a cadeia de agentes de tratamento de dados pelos riscos do processamento de informações. Isso porque se compreende que tais agentes têm mais condições de implementar medidas técnicas e organizativas capazes de proteger os dados pessoais do titulares. Nesse contexto, as mais recentes legislações, das quais se destaca o Regulamento Geral de Proteção de Dados europeu, passam a prever novos mecanismos que

22. BENNET, Colin; RAAB, Charles. *The governance of privacy*, cit., p. 131-132.

23. MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe*, cit., p. 233.

24. BENNETT, Colin; RAAB, Charles. *Revisiting 'The Governance of Privacy': Contemporary Policy Instruments in Global Perspective*, 2018. Disponível em: [https://ssrn.com/abstract=2972086]. Acesso em: 16.05.2019.

não estavam presentes nos marcos anteriores, tais como relatórios de impacto, códigos de boas condutas, certificações, programas de governança, bem como normas que incentivam a implementação do conceito de *privacy by design*[25].

Do exposto, percebe-se que o intenso processamento de dados pelo setor público e privado a partir da década de 70 enseja a evolução do direito à privacidade, que passa a abarcar uma dimensão de proteção de dados pessoais, na qual se destaca o controle do indivíduo sobre o fluxo de suas informações na sociedade. O próximo passo desta pesquisa consiste em investigar como essa evolução se deu na prática jurídica brasileira.

3. O contexto normativo brasileiro e a edição da Lei Geral de Proteção de Dados

Ao se analisar as gerações das legislações de proteção de dados na Europa, percebe-se que a evolução desse tema deu-se de forma bastante diversa no Brasil.

O primeiro instrumento normativo relacionado às modernas preocupações de tratamento de dados no nosso ordenamento é o *habeas data*, garantia constitucional estabelecida no rol de direitos fundamentais (art. 5°, LXXII) , que determina o seguinte:

> "LXXII – conceder-se-á "habeas data":
>
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
>
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;"

É certo que a doutrina há tempos já descreveu as limitações do *habeas data*, derivadas tanto da sua forma (o fato de constituir uma garantia processual e não um direito material expresso) quanto de sua origem (instrumento concebido da passagem da ditadura para a democratização.) No entanto, a despeito dessas limitações, é preciso destacar a modernidade desse instrumento, na medida em que ele reconhece a informação pessoal como um objeto merecedor de proteção constitucional.

No plano infraconstitucional, a primeira lei que tratou da privacidade e da proteção de dados pessoais de forma moderna e com vistas a lidar com as novas

25. Idem.

tecnologias de processamento de dados foi, certamente, o Código de Defesa do Consumidor (Lei 8.078/1990). O art. 43 do referido Código, ao regular os bancos de dados e cadastros de consumidores, autorizou o funcionamento dos bancos de dados e cadastros de consumidores, desde que atendidos determinados preceitos para a proteção da privacidade dos consumidores, quais sejam: a) possibilidade de acessar todas as informações existentes sobre o consumidor (direito de acesso); b) os dados arquivados devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão (princípio da qualidade dos dados); c) necessidade de comunicação da abertura de cadastro ou registro de dados pessoais de consumo (princípio da transparência); d) obrigação de banco de dados de corrigir os dados de forma imediata (direito de retificação e cancelamento); e e) limite temporal para o armazenamento de dados pessoais (princípio do esquecimento).

No contexto da evolução das normas de proteção de dados no Brasil, diversos outros diplomas que também contemplaram a proteção de dados pessoais, como o Código Civil (10.406/2002), a Lei do Cadastro Positivo (Lei 12.414/2011), a Lei de Acesso à Informação Pública (Lei 12.527/2011) e o Marco Civil da Internet (Lei n. 12.965/2014).

Como se percebe, até a edição da LGPD no ano de 2018, o Brasil não dispunha de uma regulamentação geral sobre proteção de dados pessoais. O tema era regulado por diversas leis setoriais, formando uma verdadeira "colcha de retalhos normativa", o que suscitava inúmeras críticas, seja pela fragilidade da proteção do titular de dados pessoais, seja pela insegurança jurídica à qual se submetiam empresas que tinham como um dos pilares de seus negócios o tratamento de dados.

Nesse sentido, há tempos se ouviam vozes na academia brasileira[26] e de atores de diferentes setores[27] defendendo a edição da uma lei geral, apta a formar um sistema coerente de regras e parâmetros mínimos para o tratamento de dados no país. A aprovação da Lei Geral de Proteção de Dados pode ser

26. Cf: MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. In: *Revista de Direito Civil Contemporâneo*, v. 9, 2016. BIONI, Bruno Ricardo. A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. In: *Direitos e novas tecnologias*: XXIII Encontro Nacional do Conpedi, Florianópolis: Conpedi, 2014. v. 1, p. 59-82.

27. Cf. Manifesto de proteção de dados assinado por diversos atores. disponível em: [https://brasscom.org.br/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais/].

vista, assim, como um resultado, em parte, desse reconhecimento interno da academia e *steakholders* brasileiros. Não obstante, importantes fatores externos contribuíram de forma decisiva também para o processo de aprovação dessa legislação, podendo se citar a entrada em vigor o Regulamento Geral sobre Proteção de Dados (UE 2016/679) na Europa, em 25 de maio de 2018, bem como os acontecimentos relacionados à empresa Cambridge Analytica acerca da utilização de dados do *Facebook* para *microtargeting* na campanha eleitoral americana de 2016, em violação às normas de proteção de dados[28].

3.1. Novo paradigma

A sanção da Lei 13.709/2018, em 14 de agosto de 2018, instituiu de forma inédita no país um regime geral de proteção de dados, consolidando e complementando o marco normativo da sociedade da informação em desenvolvimento no Brasil. A Lei Geral de Proteção de Dados (LGPD) inaugura um modelo *ex ante* de proteção de dados, fundado na ideia de que não existem mais dados irrelevantes em face do processamento automatizado e ubíquo de dados na sociedade da informação. Na medida em que os dados pessoais são um meio de representação da pessoa na sociedade, qualquer tratamento de dados pode afetar a sua personalidade e liberdade. Essa é a razão pela qual a tutela jurídica dos dados pessoais – nos moldes da LGPD – realiza-se de forma horizontal, aplicando-se a todos os setores econômicos e também ao setor público.

A grande inovação que a LGPD operou no ordenamento jurídico brasileiro pode ser compreendida na instituição de um modelo *ex ante* de proteção de dados, baseado no conceito de que não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação[29]. Os dados pessoais são projeções diretas da personalidade e como tal devem ser considerados. Assim, qualquer tratamento de dados, por influenciar na representação da pessoa na sociedade, pode afetar a sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais.

---

28. A penalidade aplicada pela Autoridade de Proteção de Dados do Reino Unido aos envolvidos pode ser encontrada no seguinte documento: [https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf].

29. A constatação foi feita pelo Tribunal Constitucional alemão na decisão que consagrou a autodeterminação informativa (ver nota de rodapé 2). Cf. também: MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor.* Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

Por se basear em um amplo conceito de dado pessoal, todo tratamento de dado pessoal a princípio está submetido à LGPD, seja ele realizado pelo setor público ou pelo privado (art. 3º). O seu âmbito de aplicação abrange também o tratamento de dados realizado na Internet, seja por sua concepção de lei geral, seja por disposição expressa de seu art. 1º. Estas são características fundamentais em uma lei geral, que permitem a segurança do cidadão quanto aos seus direitos independente da modalidade de tratamento de dados e quem o realize, bem como proporciona isonomia entre os diversos entes que tratam dados, o que facilita o seu fluxo e utilização legítimos. Destaca-se que apenas os dados referentes a pessoas naturais merecem proteção no âmbito da LGPD, conforme dispõem os seus arts. 1º e 5º, I.

As poucas exceções à aplicação da lei são localizadas e justificadas de forma particular, seja pela sua fundamentação em um direito fundamental (liberdade de informação, como no caso da exceção à atividade jornalística), seja pelo interesse público relevante (como nas exceções à segurança pública e defesa nacional), nos termos do art. 4º da LGPD. Tais exceções, no entanto, são moldadas de forma a não comprometer a integridade da lei, visto que para diversas delas refere-se à existência de legislação específica sobre proteção de dados que compreenda os princípios da LGPD.

Como visto, o ordenamento jurídico brasileiro já contava com algumas normas setoriais de proteção de dados, mas não havia ainda uma lei aplicável horizontalmente a todos os setores econômicos e também ao setor público, como é o caso da LGPD. Outra inovação, que também não estava presente ainda no nosso sistema jurídico, é a ideia de que todo o tratamento de dados deve se amparar em uma base legal. Essas bases são variadas e estão previstas no art. 7º da Lei, destacando-se, entre elas, o consentimento, a execução de um contrato, o dever legal do controlador, o tratamento pela administração pública, o legítimo interesse, entre outros.

3.2. Aplicação da LGPD: o modelo de três níveis

Para a aplicação da LGPD, formulamos um modelo em três níveis: em primeiro lugar, é preciso analisar quais são as condições de legitimidade para se realizar o tratamento de dados pessoais; em seguida, são estabelecidos os procedimentos para a garantia desse direito; e, por fim, se determinam quais as consequências administrativas e civis decorrentes da violação das fases anteriores. O modelo proposto pode ser sumariamente apresentado da seguinte forma:

a) qualquer tratamento de dados pessoais somente pode ser iniciado se atendidas as condições para a sua legitimidade (condições de legitimidade);

b) atendidas as condições de legitimidade, todo o tratamento de dados deve cumprir determinados procedimentos, que se encontram na Lei tanto na forma de direitos do titular como de obrigações dos agentes de tratamento (procedimentos para garantir a proteção de dados pessoais); e

c) em caso de violação a esse direito, são aplicáveis sanções administrativas e civis (sanções e reparação).

A seguir, examinaremos, com mais detalhes cada um desses níveis.

3.2.1. Condições de legitimidade para o tratamento de dados pessoais

Para que um tratamento de dados pessoais seja considerado legítimo, é preciso que sejam atendidas as seguintes condições:

i) o tratamento de dados deve se amparar em uma das bases legais previstas no art. 7º ou no art. 23 da LGPD; e

ii) o tratamento de dados deve levar em conta os princípios previstos no art. 6º da LGPD, entre eles, a boa-fé objetiva, a finalidade e a necessidade.

Pressuposto fundamental da lei é de que o tratamento de dados só poderá ser realizado se houver base legal que o autorize. Assim, os tratamentos de dados pessoais somente serão legítimos quando se enquadrem em ao menos uma das hipóteses previstas no art. 7º ou no art. 23 da LGPD, totalizando 11 hipóteses autorizativas para o tratamento de dados pessoais.

Quanto ao consentimento, para que esse seja considerado válido, deve ser livre, informado, inequívoco e com uma finalidade determinada, conforme explicitado na parte conceitual da Lei (art. 5º, XII).

Apesar da sua relevância como meio de expressão da vontade do titular dos dados, há outras hipóteses de tratamento de dados que igualmente legitimam o seu tratamento, tais como o cumprimento de obrigação prevista em lei ou regulamento (art. 7º, II) , a execução de contrato do qual o titular é parte (art. 7º, V), para a realização de interesses legítimos do controlador ou de terceiro (art. 7º, IX), para a execução de políticas públicas (art. 7º, III) e no exercício geral das competências ou cumprimento das atribuições legais da Administração Pública (art. 23).

Para avaliar as condições de legitimidade de tratamento de dados, deve-se ter em conta também os princípios previstos no art. 6º da LGPD.

Uma parte dos princípios enunciados na Lei são comuns à maioria das legislações de proteção de dados e decorrem de instrumentos internacionais, como a Convenção 108 do Conselho da Europa. Esse quadro comum de princípios é conhecido por *Fair Information Principles* e teve a sua origem na década de 70 de forma quase simultânea nos EUA, Inglaterra e Alemanha[30].

Em 1972, no âmbito do Departamento de Saúde, Educação e Bem-Estar (*Department of Health, Education, and Welfare*), deu-se a primeira ação do Poder Executivo americano em relação ao tratamento dos dados pessoais[31]. Neste ano, foi designado pelo então Secretário desse departamento, um comitê consultivo de sistemas automatizados de dados pessoais (*Advisory Committee on Automated Personal Data Systems*), para o estudo da questão. Em 1973, o comitê emitiu um relatório sobre "Registros, Computadores e Direitos do Cidadão", que propunha a redefinição do conceito de privacidade, além de cinco princípios fundamentais que todo o processamento de dados deveria seguir:

> "1. Não deve existir nenhum banco de dados pessoais, cuja existência seja secreta;
>
> 2. Deve haver um meio para o indivíduo conhecer quais informações a seu respeito estão armazenadas e de que forma elas são usadas;
>
> 3. Deve existir um meio pelo qual o indivíduo possa impedir que uma informação obtida para uma finalidade seja utilizada para outros fins, sem o seu consentimento;
>
> 4. Deve existir um meio pelo qual o indivíduo possa corrigir ou emendar uma informação pessoal armazenada a seu respeito;
>
> 5. Qualquer organização que crie, mantenha, use ou dissemine dados de pessoas identificadas deve assegurar que a informação somente será usada da forma pretendida e deverá tomar as precauções razoáveis para prevenir o abuso do dado."[32]

No mesmo período, já estava em andamento na Grã-Bretanha a análise pelo Comitê de Privacidade, coordenado por Kenneth Younger, a respeito dos riscos do

30. BENNETT, Colin. *Regulating Privacy*: data protection and public policy in Europe and the United States, cit., p. 96 a 99.

31. Ibidem, p. 70 e 71.

32. EUA, HEW. *Records, Computers, and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. Julho, 1973, tradução livre. O relatório pode ser acessado na seguinte página: []. Acesso em: 24.02.2012.

tratamento automatizado de dados realizado por organizações privadas. O comitê emitiu um relatório que sugeria dez princípios para a proteção da privacidade[33].

Os princípios tradicionais da proteção de dados estão previstos na LGPD entre os incisos I e VII, do art. 6º, da Lei, quais sejam: finalidade, adequação, necessidade, livre acesso, qualidade, transparência e segurança. Entre eles, destaca-se o princípio da finalidade, que vincula o tratamento de dados pessoais à finalidade que motivou e justificou a sua coleta. A aplicação deste poderoso princípio tem como objetivo garantir a privacidade contextual, evitando que os dados pessoais sejam utilizados posteriormente para finalidades incompatíveis com aquela para a qual ele foi coletado.

Ademais, a Lei inova ao prever outros princípios, que buscam endereçar os novos riscos e possibilidades da tecnologia da informação, como o princípio da não discriminação pelo tratamento de dados, abordando o potencial discriminatório do uso de dados de algoritmos e de decisões automatizadas, bem como o princípio da prevenção e da responsabilização e prestação de contas, também conhecido pelo anglicismo *accountability*.

Importante ressaltar o papel central que a Lei atribui ao princípio da boa-fé objetiva, previsto no *caput* do art. 6º, de modo a lembrar que todo o tratamento de dados pessoais deve se pautar pela ética e por padrões objetivos de lealdade aferidos em cada contexto concreto.

33. Os princípios previstos no relatório eram os seguintes: "1. A informação deve ser armazenada para uma finalidade específica e não deve ser utilizada para outras finalidades, sem a devida autorização. 2. O acesso à informação deve ser conferido àqueles que têm a autorização de mantê-la com os fins pelos quais elas foram coletadas. 3. A quantidade de informações coletadas e armazenadas deve ser o mínimo necessário para se atingir um objetivo específico. 4. Em sistemas computadorizados que processam dados pessoais com fins estatísticos, medidas adequadas devem ser tomadas em seu *design* e programas para separar a identidade do restante dos dados. 5. Deve haver mecanismos pelos quais o sujeito possa ser comunicado sobre a informação armazenada a seu respeito. 6. O nível de segurança a ser atingido por um sistema deve ser especificado previamente pelo usuário e deve incluir precauções contra abusos deliberados ou mau uso da informação. 7. Um sistema de monitoramento deve ser provido para facilitar a detecção de qualquer violação da segurança do sistema. 8. No *design* de sistemas de informação, devem ser especificados períodos para além dos quais a informação não pode mais ser armazenada. 9. Os dados armazenados devem ser corretos. Deve haver instrumentos para a retificação de incorreções e para a atualização da informação. 10. Deve ser tomado cuidado na codificação de julgamentos válidos. (tradução livre)." (BENNETT, Colin. *Regulating Privacy*: data protection and public policy in Europe and the United States, cit., p. 98 e 99.)

3.2.2. Procedimentos para garantir a proteção de dados pessoais

Atendidas as condições de legitimidade, passa-se então ao segundo nível do modelo: os agentes de tratamento devem assegurar que o tratamento de dados seja realizado em atenção aos direitos dos titulares e às obrigações impostas pela Lei. De forma geral, esses procedimentos buscam assegurar que o tratamento de dados se dará de forma leal, transparente, segura e de modo a possibilitar tanto o controle do indivíduo como o controle por parte das autoridades públicas.

Os direitos mais básicos atribuídos ao titular dos dados pelas diversas legislações nacionais e tratados internacionais para o controle do fluxo de seus dados são conhecidos pela sigla "ARCO", que é uma abreviação dos direitos de acesso, retificação, cancelamento e oposição. Afinal, à luz do paradigma do controle, entende-se que o titular deve ter livre acesso aos seus dados (direito de acesso), deve poder corrigir dados equivocados e desatualizados (direito de retificação) e deve poder cancelar dados que foram indevidamente armazenados ou cujo consentimento tenha sido revogado por ele (direito de cancelamento).

Os direitos do titular estão estabelecidos, principalmente, no art. 18 da LGPD:

> "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> I – confirmação da existência de tratamento;
>
> II – acesso aos dados;
>
> III – correção de dados incompletos, inexatos ou desatualizados;
>
> IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nessa Lei;
>
> V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; *(Redação dada pela Lei n. 13.853, de 2019.)*
>
> VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
>
> VII – informação das entidade públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
>
> VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
>
> IX – revogação do consentimento, nos termos do § 5º do art. 8º desta Lei."

Outros direitos relevantes são aqueles atribuídos ao titular sujeito a decisões exclusivamente automatizadas, conforme o que prevê o art. 20 da LGPD:

> "Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
>
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
>
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.
>
> § 3º A revisão de que trata o *caput* deste artigo deverá ser realizada por pessoa natural, conforme previsto em regulamentação da autoridade nacional, que levará em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados."

Do referido artigo, extraem-se pelo menos três direitos do titular: direito à intervenção humana em processos decisórios automatizados (*caput* e § 3º), direito à explicação (§ 1º), e direito à auditoria pela autoridade, nas hipóteses em que a decisão possa trazer riscos de discriminação para o titular.

Nessa segunda fase do modelo de aplicação da lei, devem os agentes de tratamento observar, além dos direitos previstos na Lei, também as obrigações estabelecidas para todos aqueles que realizam o tratamento de dados.

Entre as principais obrigações, está a do controlador de instituir um encarregado pelo tratamento de dados, nos termos do art. 41 da LGPD. Note-se que se trata de uma obrigação a ser cumprida pelo controlador e não pelo operador. O encarregado terá como funções receber reclamações dos titulares, comunicar-se com a autoridade nacional e orientar os funcionários para a que a organização cumpra com as normas de proteção de dados. A própria Lei estabelece a possibilidade de dispensa dessa obrigação, que dependerá, contudo, de norma a ser editada pela Autoridade Nacional de Proteção de Dados (art. 41, § 3º).

Importante obrigação, anteriormente inexistente no nosso ordenamento de forma tão abrangente, diz respeito à manutenção do registro pelos agentes de tratamento, conforme estabelece o art. 37 da LGPD: "*O controlador e o operador*

devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse."

A LGPD estabelece também uma obrigação central aos agentes de tratamento de adoção das medidas de segurança, técnicas e administrativas adequadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. É o que determina o seu art. 46, que inaugura o capítulo de segurança da informação da LGPD, aplicável tanto aos controladores quanto ao operadores.

O capítulo de segurança da informação é um pilar fundamental da Lei e exige a adoção por todos que tratam dados de medidas que garantam a integridade, a confidencialidade e a disponibilidade dos dados sob tratamento. Ademais, em caso de incidente de segurança, como o vazamento de dados, surge a obrigação para o controlador de comunicar à autoridade de proteção de dados, que pode determinar, conforme o caso, a adoção de medidas para mitigar os efeitos do incidente ou a ampla divulgação para a sociedade (art. 48). Fundamental também, nesse contexto, é o conceito de de *privacy by design*, segundo o qual é preciso se implementar medidas de proteção à privacidade desde a concepção dos produtos ou serviços, conforme se extrai do art. 46, § 2º, da LGPD.

Outra obrigação relevante é a do controlador realizar um relatório de impacto à privacidade, que é uma descrição de uma operação de tratamento de dados pessoais que execute juntamente com as medidas que tenha adotado para aumentar a segurança e mitigar o risco presente no tratamento. Este relatório será solicitado pela Autoridade Nacional de Proteção de Dados, nos termos do art. 38 da LGPD.

3.2.3. Fiscalização, aplicação de sanções e reparação

O terceiro nível do modelo de proteção de dados consiste na responsabilidade dos agentes na hipótese de ocorrência de danos decorrentes do tratamento de dados, estabelecida na lei tanto na forma de responsabilidade administrativa (art. 52, LGPD) quanto na forma de responsabilidade civil (arts. 42 a 45, LGPD).

Esse nível do modelo dialoga diretamente com os dois primeiros, isto é, em caso de descumprimento das condições de legitimidade de tratamento ou dos procedimentos para a proteção dos dados pessoais, sujeitam-se os agentes de tratamento às sanções administrativas e ao pagamento de indenização

ao titular. Objetivo dessa etapa é conferir efetividade às normas previstas na LGPD, seja por meio da reparação de eventuais danos morais e materiais realizados a partir do descumprimento da lei, seja por meio da aplicação de sanções administrativas que buscam inibir o comportamento vedado pela legislação.

Nota da editora: Importante ressaltar que foram derrubados pelo Congresso Nacional os vetos sobre os dispositivos que tratavam de sanções administrativas aplicáveis aos agentes de tratamento de dados que infringirem normas estabelecidas na LGPD. Referidas sanções estabelecem:

– suspensão parcial do funcionamento do banco de dados por até seis meses;

– suspensão do exercício da atividade de tratamento dos dados pessoais pelo mesmo período

– proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

4. Conclusão

Como vimos anteriormente, a tutela jurídica para a proteção da personalidade em face do tratamento de dados pessoais envolve o estabelecimento de uma série de procedimentos, princípios e direitos, que limitam o processamento de dados pessoais ao mesmo tempo que empoderam o cidadão para controlar o fluxo de seus dados. Apesar dos diferentes sistemas jurídicos, é possível concluir pela existência de um regime jurídico razoavelmente homogêneo de proteção de dados pessoais, com princípios e instrumentos semelhantes. Essa similaridade incide, especialmente, em torno do "paradigma do controle"[34], que prevê princípios gerais e mecanismos legais para que seja atribuído aos indivíduos maior liberdade de controle sobre a informação coletada, armazenada, processada e disseminada[35]. Assim, as normas dos mais diversos países compartilham de uma concepção procedimental, segundo a qual a regulamentação estatal somente deve estabelecer princípios e procedimentos para

34. "*Privacy-control*" (SCHWARTZ, Paul. Internet Privacy and the State. In: *Connecticut Law Review*, v. 32: 815, 1999-2000).

35. Bennet e Raab descrevem um paradigma da privacidade dominante, baseado na ideia de controle do indivíduo: "The overall policy goal in every country was to give individuals greater control of the information that is collected, stored, processed, and disseminated about them by public and, in some cases, private organizations." (BENNET, Colin; RAAB, Charles. *The Governance of Privacy*, cit., p. 8.)

o tratamento dos dados pessoais, devendo o conteúdo desse direito ser estabelecido pelo titular dos dados pessoais[36].

Ocorre, no entanto, que, com a evolução tecnológica, a criação de novos produtos e serviços e a crescente dependência dos indivíduos em relação à tecnologia da informação, iniciou-se um processo de questionamento acerca da real adequação e efetividade desse conceito de proteção de dados. Há um reconhecimento generalizado de que o enorme desenvolvimento das tecnologias da informação nos últimos anos alterou os comportamentos e os hábitos dos indivíduos, ampliando especialmente a relação de dependência entre o homem e a tecnologia. Conforme afirma Yves Poullet, "as tecnologias de informação e comunicação são *ubíquas* e estão funcionando cada vez mais como sistemas autônomos, capazes de aprender com os dados que coletam e recuperá-los de formas insuspeitas"[37]. A palavra-chave que tem sido usada para caracterizar esse processo é ubiquidade. Trata-se do processamento onipresente de dados, que designa o fenômeno segundo o qual a tecnologia da informação e o processamento de dados perpassam todas as áreas da vida de um indivíduo[38].

Os exemplos de ubiquidade são inúmeros: redes sociais (ex.: *Facebook*, *Myspace*, *Google+*), *sites* de produção do conhecimento com estrutura colaborativa (ex.: Wikipedia), *cloud computing*, publicidade comportamental, *chips* de identificação por radiofrequência (Etiqueta de RFID) e a crescente utilização de objetos cotidianos e domésticos associados à internet[39]. As etiquetas de RFID podem ser colocadas em objetos ou pessoas e viabilizam a comunicação de dados entre elas e uma base transmissora. Já os objetos de uso cotidiano associados à internet abrangem desde os aparelhos celulares "inteligentes" (*smartphones*), a aparelhos domésticos e sistemas de energia em rede (*e-energy*[40]).

36. BENNET, Colin; RAAB, Charles. *The Governance of Privacy*, cit., p. 8 e 9.

37. POULLET, Yves. *About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In:* POULLET, Yves et al. (Org.). *Data Protection in a Profiled World*. Dordrecht: Springer, 2010. p. 5.

38. HOFFMANN-RIEM, Wolfgang. Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme. In: *JuristenZeitung* 21, p. 1010, 2008.

39. HOFFMANN-RIEM, Wolfgang. *Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation*, cit., p. 520-523.

40. Ibidem, p. 522.

O principal efeito do fenômeno da ubiquidade da tecnologia da informação é o desequilíbrio de poderes entre o indivíduo e os organismos que processam os dados pessoais e a consequente perda de controle individual sobre o fluxo de seus dados[41]. Percebe-se, assim, que essas novas condições tecnológicas alteram o pressuposto central no qual se baseia o conceito clássico de dados pessoais: a possibilidade do indivíduo de efetivamente controlar o fluxo dos dados pessoais na sociedade.

Dessa forma, pode-se dizer que tal processo foi o catalizador de uma reflexão acerca da necessidade de maior regulação estatal para o controle do tratamento de dados pessoais. Nesse contexto, se inserem as propostas de reformas normativas em curso em diversos países, no sentido de modernizar, atualizar e reforçar a proteção de dados. É o caso, por exemplo, da Europa que aprovou em 2016 o Regulamento Geral de Proteção de Dados em substituição à Diretiva Europeia 95/46/CE. Também, na Alemanha, fala-se há muito tempo sobre a necessidade de uma modernização do regime jurídico de proteção de dados pessoais[42]. O debate alemão a respeito de uma reforma ganhou ainda mais relevo no ano de 2008, com uma decisão da Corte Constitucional do país, que "criou" um direito fundamental referente à garantia da confidencialidade e integridade dos sistemas eletrônicos (*Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme*)[43].

41. HOFFMANN-RIEM, Wolfgang. Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, cit., p. 1010. No mesmo sentido, POULLET, Yves. *About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?* cit., p. 7.

42. Em 2001, a pedido do Ministério do Interior alemão, foi elaborado um relatório sobre a modernização do direito à proteção de dados pessoais. Cf. ROßNAGEL, Alexander et. al. Modernisierung des Datenschutzrechts, Gutachten. In: *Auftrag des Bundesministeriums des Inneren*. Berlin, 2001.

43. No caso, que envolvia o monitoramento da navegação na internet do usuário, no âmbito de uma investigação policial, a Corte Constitucional alemã reconheceu a existência de um "direito fundamental à garantia da confidencialidade e da integridade dos sistemas informáticos". Segundo a Corte, este direito exige que qualquer monitoramento policial da navegação da internet do usuário somente possa ser realizado se houver uma base legal específica, uma autorização judicial e a identificação de um perigo concreto a um bem jurídico fundamental, como a vida e a liberdade individuais ou a segurança da coletividade. Em todo caso, mesmo quando atendidos esses requisitos, em nenhuma hipótese pode o monitoramento policial violar o núcleo da intimidade e das formas de vida privada do indivíduo. (BVerfGE 120, 274, *"Online Durchsuchung"*)

Em todos esses casos, percebe-se uma preocupação com a efetividade das normas atuais de proteção de dados pessoais, diante das mudanças sociais e da ubiquidade da tecnologia da informação. Busca-se, em regra, um aprimoramento da regulação da proteção de dados pessoais, de modo a possibilitar uma maior adequação das normas aos desafios da atualidade. Não se trata aqui da substituição ou da anulação do conceito de proteção de dados como controle do indivíduo sobre os seus dados pessoais. Trata-se, na realidade, de uma reflexão legítima sobre os limites e as perspectivas desse conceito, que poderá apontar no futuro para um conceito atualizado, mais completo e apto a enfrentar os novos desafios da proteção de dados.

Esse processo de evolução é natural e esperado. Afinal, como visto na análise da evolução geracional das leis de proteção de dados, um componente essencial dessa disciplina é a busca permanente pela evolução, de modo a não ficar obsoleta diante dos novos desenvolvimentos tecnológicos e das novas práticas sociais e econômicas propiciadas pela tecnologia.

REFERÊNCIAS

BENNET, Colin; RAAB, Charles. *The governance of privacy*, cit., p. 125.

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

HASSEMER, Winfried. Datenschutz: die Aufgaben der nächsten Jahre. In: BÄUMLER, Helmut; MUTIUS, Albert von (Orgs.). *Datenschutzgesetze der dritten Generation*. Neuwied, Kriftel: Luchterland, 1999.

HOFFMANN-RIEM, Wolfgang. Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme. In: *Juristen Zeitung* 21, 2008.

MAYER-SCHÖNBERGER, Viktor. *Generational Development of Data Protection in Europe*.

POULLET, Yves. About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In: POULLET, Yves et al. (Org.). *Data Protection in a Profiled World*. Dordrecht: Springer, 2010.

SIMITIS, Spiros. *Revisiting Sensitive Data*. Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 24-26 November 1999.

WESTIN, Alan. *Privacy and Freedom*. Nova York: Atheneum, 1970.