UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE DIREITO PROFESSOR JACY DE ASSIS
GRADUAÇÃO EM DIREITO

THIAGO PINHEIRO VIEIRA DE SOUZA

A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL E A [IN]CIVILIDADE DO USO DE *COOKIES*

UBERLÂNDIA/MG
NOVEMBRO DE 2018

THIAGO PINHEIRO VIEIRA DE SOUZA

A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL E A [IN]CIVILIDADE DO USO DE *COOKIES*

Monografia apresentada à Faculdade de Direito Professor Jacy de Assis, da Universidade Federal de Uberlândia/MG, como pré-requisito para a obtenção do Título de Bacharel em Direito.
Orientador: Prof. Dr. Fernando Rodrigues Martins

UBERLÂNDIA/MG
NOVEMBRO DE 2018

THIAGO PINHEIRO VIEIRA DE SOUZA

A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL E A [IN]CIVILIDADE DO USO DE *COOKIES*

Esta monografia foi julgada e aprovada para obtenção do título de bacharel, no Curso de Graduação em Direito, da Faculdade de Direito Professor Jacy de Assis, da Universidade Federal de Uberlândia/MG.

Uberlândia, _____ de _____ de _____.

BANCA EXAMINADORA

_____

Prof. Fernando Rodrigues Martins

Orientador

_____

Prof. João Victor Rozzati Longhi

Membro

_____

Yuri Gonçalves dos Santos Rodrigues

Membro

Uberlândia, _____ de _____ de _____.

"Technology is nothing. What's important is that you have a faith in people, that they're basically good and smart, and if you give them tools, they'll do wonderful things with them."

Steve Jobs

RESUMO

O presente trabalho tem como primeira finalidade a apresentação do direito à proteção de dados pessoais como sendo um direito autônomo e fundamental à pessoa humana. Para isso, são expostos os princípios que regem o tema, a classificação das informações pessoais e a própria evolução de tal direito a partir do antigo conceito de privacidade, passando pela autodeterminação informativa e posteriormente segregando-se em um direito autônomo. O foco do trabalho desloca-se, depois, para o uso de *cookies* na *Internet*, que se propagou, nos últimos anos para todas as áreas do mercado atual, de forma que a segurança *online* dos usuários esteja cada vez mais comprometida em razão das múltiplas operações de coleta e tratamento as quais seus dados são submetidos. Por fim, será feita uma análise de algumas legislações que tratam do tema, quais sejam o Regulamento Geral de Proteção de Dados, da Europa, que vem sendo utilizado como modelo de edição de todas as demais legislações nacionais e regionais no mundo, tão como da recente Lei Geral de Proteção de Dados brasileira, que cuida do assunto de maneira pormenorizada, suplementando o Marco Civil da Internet.

Palavras-chave: Proteção de dados pessoais. Direito autônomo. Direito fundamental. Autodeterminação informativa. Uso de cookies. Publicidade comportamental. Lei Geral de Proteção de Dados. Regulamento Geral de Proteção de dados.

ABSTRACT

This work aims, at first, to expose the right to personal data protection as an autonomous and fundamental right. To do so, the main principles that rules the subject will be presented, and so will the sorting of personal information and the very evolution of that right from the ancient concept of privacy, through informational self-determination and the later segregation into an autonomous right. The focus will be shifted, then, to the use of cookies on the Internet, which has spread in recent years to all areas of the modern market, so that the online safety of users is increasingly compromised due to the multiple collection and treatment operations to which their data are submitted. At last, there will be made an analysis of a couple of legislations witch deal with this subject, namely the General Regulation on Data Protection in Europe, which has been used as a role model for the edition of almost all other national and regional legislation in the world, as well as the recent Brazilian Data Protection Act, which takes care of the subject in detail, supplementing the Civil Rights Framework for the Internet.

Palavras-chave: *Data protection. Autonomous right. Fundamental right. Right to self-determination. Use of cookies. Behavioral Advertising. Data Protection Act. General Data Protection Regulation.*

SUMÁRIO

INTRODUÇÃO

Há muitos séculos instituições sociais, como a Igreja e o Estado, estiveram associadas ao controle do poder na sociedade e, consequentemente, ao controle da informação. Isso mudou a partir de meados do século XX, quando o desenvolvimento tecnológico acarretou a intensificação dos fluxos de informação de uma forma nunca antes vista, o que levou à denominação da sociedade atual como *sociedade da informação* ou *era da informação*[1].

Uma das consequências mais claras da informatização de muitos aspectos da vida cotidiana atual é justamente a possibilidade de registro de praticamente todos atos realizados através de meios informatizados. Muitos desses atos, que antes seriam efêmeros e gerariam consequências apenas imediatas e previsíveis dentro de determinados padrões, passam a ser informações armazenadas, o que abre a possibilidade de serem utilizadas em contextos diferente daqueles nos quais foram inicialmente praticados, e com finalidades também diversas, fugindo, muitas vezes, do poder de previsão e controle de quem inicialmente os praticou. Não apenas atos são armazenados, mas também – e principalmente – os dados de identificação dos sujeitos que os praticam, e que são fornecidos frente a uma empresa, podendo ser coletados e utilizados para diversas finalidades. O perfil de uma pessoa, do que ela gosta, o que compra, quais suas

---

[1] Sobre as expressões, ver: Lyon, D. **The Information Society: Issues and Illusions**, 1988.

necessidades, hábitos e, em alguns casos, até mesmo sua localização e seu perfil genético valem tanto para o mercado que o consumidor, nesse contexto, não é mais visto como somente um destinatário de informações, mas como a própria fonte delas, determinando, inclusive, a forma como ele poderá ser abordado e tratado futuramente.

Ao mesmo tempo que a informação pessoal é utilizada como capital e moeda do mercado, a cessão de informações pessoais é feita em troca de quaisquer tipos de serviços digitais, sem qualquer preocupação com a forma pela qual será feito seu tratamento, onde esses dados são armazenados, quem tem acesso a eles, ou quais as regras para a transferência dos mesmos. O valor desses dados nunca foi tão subestimado pela sociedade. Poucos parecem se preocupar com o fato de que a maior parte das informações cedidas a empresas virtuais são vendidas e compartilhadas com outras, de forma que é possível identificar e rastrear os usuários consumidores em quase todas atividades realizadas.

Diante do fato de que as informações pessoais são comercializadas livremente em grande escala no mercado, a indiferença do direito perante o desenvolvimento tecnológico deixa de ser possível, devendo este estar preparado para enfrentar as novas situações decorrentes das tecnologias informacionais inovadoras. Assim, desenvolveu-se na doutrina um debate acerca da possibilidade de se garantir um direito de propriedade sobre os dados pessoais, seguindo o pretexto de que o direito tem de se adequar à realidade e ao fato social. Sob essa ótica, e para possibilitar a resposta adequada aos desafios sociais advindos da revolução tecnológica, é fundamental que a teoria do direito se reconstrua a ponto de compreender e solucionar os novos problemas enfrentados pelo homem na era da informação. Desse modo, o presente trabalho busca analisar quais são as consequências da conexão entre sociedade de informação e sociedade de consumo, bem como as formas pelas quais o direito pode contribuir para proteger a privacidade do consumidor.

Simson Garfinkel[2] aproxima tal questão com a devastação do meio ambiente pela tecnologia moderna, que foi tratada nas décadas de 1950 e 1960 como um problema inevitável: sob tal ótica, seria necessário conviver com a destruição das reservas naturais do planeta como condição para o desenvolvimento econômico e o aumento do nível de vida da população. Ocorre, no entanto, que tal visão foi superada a partir da concepção do desenvolvimento sustentável, que propugna conciliar o desenvolvimento econômico com a preservação ambiental. Assim, ao se analisar o tema da proteção de dados pessoais na sociedade da

---

[2] GARFINKEL, Simson. **Database Nation: The Death of Privacy in the 21th Century.** California: O'Reilly Media, 2000, p. 5.

informação, é fundamental compreender que o cerne do problema não está situado na tecnologia. Afinal, a tecnologia não se encontra em um vácuo, devendo ser compreendida a partir do meio social, econômico e político em que está inserida. Nesse sentido, é fundamental que o debate sobre a proteção de dados pessoais tenha como foco as opções jurídicas e econômicas relativas às funções que a tecnologia deve assumir na sociedade, rejeitando-se a ideia de que ela é a responsável pela perda de privacidade pessoal da sociedade contemporânea.

Dessa forma, a construção da esfera privada deve ser compreendida, nas sociedades contemporâneas, como a possibilidade de o indivíduo controlar o acesso e o uso dos dados que constituem a sua identidade pessoal e permitem o livre desenvolvimento de sua personalidade[3]. Não se trata mais de assegurar o segredo, mas sim de assegurar o controle sobre os fluxos de informação, devendo a privacidade ser pensada como um direito também atinente à esfera de liberdade pessoal e política, com repercussões coletivas[4].

Normas relativas à proteção de dados são, assim, uma maneira indireta de atingir um objetivo último, que é a proteção da própria pessoa humana. Os dados pessoais, por definição, representam algum atributo de uma pessoa identificada ou identificável e, portanto, mantém uma ligação concreta e viva com a pessoa titular destes dados, podendo ser considerados uma extensão de sua personalidade, o que merece adequado tratamento. O presente trabalho vem, então, expor algumas noções acerca das teorias para o tratamento de dados pessoais e defender, conforme apresentado, sua intitulação como um direito fundamental constitucional da pessoa humana.

Para isso, falar-se-á de sua evolução a partir do direito à privacidade, que ensejou maiores estudos acerca do tema, e levou a doutrina à criação de um direito autônomo – e constitucional – à proteção de dados. Mostra-se necessária a exposição do imperativo de vigilância do consumidor nesse contexto, bem como as formas de coleta e as técnicas de processamento de dados pessoais. Será feita, também, uma explicação dos fundamentos e princípios norteadores e da aplicação concreta do referido direito, o que será enriquecido com uma análise da principal norma de proteção de dados em vigência no mundo, norteadora dos demais sistemas nacionais que tratam do tema: o Regulamento Geral sobre a Proteção de Dados (RGPD)[5], da União Europeia.

---

3 RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p. 24.

4 *Idem*, *Ibidem*, p. 27.

5 **REGULAMENTO (UE) 2016/679,** do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Considerações iniciais nº (38).

Em um segundo momento, o estudo será focalizado no uso de *cookies* de rastreamento pelos provedores e navegadores *online*. Serão apresentadas as tecnologias que permitem a prática, tão como os sujeitos responsáveis e suas responsabilidades para com os usuários cedentes. Atualmente, os *cookies* são o principal meio pelo qual é feita a coleta de informações pessoais, anúncios *online*, formação de perfis de consumidores e publicidades individualizadas, de modo que seu estudo aprofundado e entendimento pode contribuir cada vez mais com o desenvolvimento de sistemas jurídicos e de medidas protetivas que sejam efetivamente úteis no cotidiano virtual.

A partir de pesquisas desenvolvidas sob a perspectiva do método de abordagem dedutivo, com base em bibliografias e estudos existentes sobre o tema, tão como na – relativamente – recente jurisprudência nacional e internacional, o objetivo do presente trabalho é, assim, procurar e evidenciar soluções que possam ser implementadas pelos sistemas jurídicos atuais quando se fala em proteção da pessoa no ambiente *online*. Mas não apenas, visa, também, a exposição dos fatores que levaram à atual situação de lacuna legislativa, recém suprida pela edição de regulamentos gerais (brasileiro e europeu) apontando métodos para sua aplicação prática efetiva.

1. PROTEÇÃO DE DADOS PESSOAIS

1.1. Dados pessoais e categorias especiais de informação

A importância da tutela jurídica dos dados pessoais reside no fato de que esses dados, assim como as demais informações contraídas a partir deles, constituem uma representação virtual da pessoa perante a sociedade, constituindo uma verdadeira parcela de sua personalidade. Em razão disso, embora nem sempre de utilidade prática visível, o esclarecimento acerca da distinção das expressões *dados pessoais* e *informações pessoais* pode ser útil quando se estuda o tema a fundo. Por outro lado, em um campo de estudo muito mais funcional, os *dados sensíveis* são tidos pela doutrina como uma parcela compreendida dentro do termo maior *dados pessoais*, como uma categoria especial de informação subsumida à primeira expressão.

Dados pessoais vs. informações pessoais

Quando se trata da utilização dos termos aludidos, é indiscutível que ambos se sobrepõem em várias circunstâncias, servindo para representar um fato, um determinado aspecto da realidade. Quanto às peculiaridades, os dados podem ser vistos como uma expressão mais primitiva e fragmentada, podendo ser entendidos como uma informação em estado

potencial[6], se transformando em informação apenas quando comunicado, recebido e compreendido. Seria algo semelhante à uma *pré-informação*, anterior à interpretação e ao processo de elaboração[7]. Representam, assim, o conjunto de fato, comunicações e ações concernentes à pessoa[8], com capacidade de revelar seus caracteres e conteúdos quanto à personalidade, relações afetivas e familiares, etnia, circunstâncias físicas, domicilio (físico e eletrônico), acervo patrimonial, registros telefônicos, preferências políticas ou religiosas e orientação sexual[9]. Em regra, os sujeitos deverão ser identificados, ou, ao menos, inidentificáveis, mas isso nem sempre ocorrerá, como nas hipóteses em que os dados se referem a pessoas indeterminadas por natureza, por exemplo. Nesses casos, os dados são considerados anônimos, e servirão para fins estatísticos, servindo como uma forma de proteção às pessoas que tiveram seus dados coletados e armazenados anteriormente[10]. Vale ressaltar que, uma vez que tais dados são transformados em anônimos e tratados de modo a impossibilitar qualquer identificação pessoal, eles não mais estão sujeitos à disciplina e tutela da proteção de dados pessoais[11], por não violar a essência protetiva do direito em questão: a privacidade e personalidade da pessoa.

A informação pessoal, por sua vez, remete a algo além do simples conteúdo do dado, pressupondo uma fase inicial de depuração de seu conteúdo. Pode ser transmitida por diversas formas – gráfica, fotográfica e acústica[12] – e em muitos contextos, carregando consigo diversas ordens de valores. Fica, assim, "quase como ato reflexo, ligada à privacidade por uma equação

---

6 Vale mencionar, também, a definição de Wacks: "*Personal information* consists of those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use, or circulation. (WACKS, Raymond. **Personal information**. Oxford: Clarendon Press, 1989, p. 25 e 26.)

7 DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental**, vol. 12, nº 2. Joaçaba: Espaço Jurídico, 2011, p 94.

8 Lei de Proteção de dados da Alemanha (Bundesdatenschutzgesetz – BDSG), 2017.

9 RODOTÀ, Stefano. *Op. Cit.*, p. 6. *Apud.* MARTINS, Fernando Rodrigues. **Sociedade de informação e proteção à pessoa.** Revista de direito do Consumidor, vol. 96. Uberlândia, 2014, p. 16.

10 Nesse sentido, vale mencionar a amplamente conhecida decisão da Corte Constitucional alemã de 15 de dezembro de 1983, ao julgar a "Lei do Recenseamento de População, Profissão, Moradia e Trabalho", em que se determinou que os dados pessoais coletados para o censo somente poderiam ser transferidos a outros órgãos da Administração Pública se fossem tornados anônimos ou após o seu processamento estatístico. (BVerfGe 65, 1, Volkszählung) – *Cf.* tópico 3.3, acerca do direito à autodeterminação informativa na referida decisão.

11 Assim dispôs o preâmbulo da antiga Diretiva Europeia 95/46/CE, segundo o qual não se aplica o regime de proteção de dados pessoais aos dados anônimos, já que não possibilitam a identificação da pessoa: "[...] os princípios da proteção não se aplicam a dados tornados anônimos de modo tal que a pessoa já não possa ser identificável".

12 MALTA, Tatiana. **O Direito à Privacidade na Sociedade da Informação: efetividade desse direito fundamental diante da tecnologia da informação.** Porto Alegre: Sergio Antônio Fabris Editor, 2007, p. 252.

simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa"[13]. Nas palavras de P. Catala, vale dizer que:

> *"Mesmo que a pessoa em questão não seja a 'autora' da informação, no sentido de sua concepção, ela é a titular legítima de seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade"*[14].

De maneira mais concreta, utilizando-se da Convenção de Strasbourg[15], uma possível definição do termo em questão seria "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação". Assim, a informação pessoal se difere das demais em razão de seu vínculo objetivo, estabelecido entre o sujeito e a informação, que menciona aspectos que lhe dizem respeito. Indo além, é o vínculo subjetivo aqui estabelecido que "afasta outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais"[16]. Em razão disso, é fundamental esclarecer que, na realidade, a tutela de dados (ou informações) visa à proteção da pessoa e de sua personalidade, e não dos dados *per se*[17].

Categorias especiais de informação

O estudo desta categoria de dados se desenvolveu a partir da percepção de que o tratamento de certos dados pode constituir uma maior e mais grave ameaça à personalidade e liberdade individual do que o de outros, podendo acarretar um novo problema de igualdade sempre que sua utilização inadequada puder causar ações potencialmente discriminatórias[18]. De forma mais concreta, a expressão *dados sensíveis* pode ser compreendida, nas palavras de José de Oliveira Ascensão, como sendo as "convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada, origem racial ou étnica, saúde e vida sexual,

---

13 RODOTÀ, Stefano. *Op. Cit.*, p. 6. *Apud.* MARTINS, Fernando Rodrigues. *Op. Cit.*, p. 16.

14 CATALA, Pierre. **Ebauche d'une théorie juridique de l'information"**. Informatica e Diritto, ano IX, jan-apr. 1983, p. 20. *Apud.:* DONEDA, Danilo. *Op. Cit.,* 2011, p 93.

15 Convenção nº 108 do Conselho da Europa– Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais, art. 2º.

16 DONEDA, Danilo. *Op. Cit.*, 2011, p 93.

17 ARGENTINA. **Protección de Datos Personales**. Secretaria de Investigaión de Derecho Comparado, Corte Suprema de Justicia de La Nación, República Argentina. *Apud* MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Departamento de Pós-Graduação Unb. Brasília, 2008, p. 71.

18 MENDES, Laura Schertel. *Op. Cit.*, p. 62.

incluindo os dados genéticos"[19]. Ou seja, o próprio conceito já demonstra uma necessidade de delimitar uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior, e na qual a atuação de diversos sujeitos será consequentemente diminuída.

A questão é tratada de diferentes maneiras pelos ordenamentos nacionais ao redor do mundo[20], sendo, em regra, acompanhada de disposições normativas mais severas e de maior rigor, visando a melhor proteção do cidadão e da sociedade.

É fundamental, ademais, proteger as categorias restantes de dados que, embora aparentemente insignificantes, possam vir a se tornar sensíveis a depender do tipo de tratamento a que são submetidos. Conforme Laura Schertel Mendes, "trata-se [...] de um tratamento sensível dos dados, que é capaz de transformar dados inofensivos em informações potencialmente discriminatórias"[21]. Nessa linha, afirmou o Tribunal Constitucional alemão, no referido julgamento sobre a lei do recenseamento, que a partir das possibilidades de ligação e processamento da tecnologia da informação, "um dado em si insignificante pode adquirir um novo valor. Desse modo, não existem mais dados insignificantes no contexto do processamento eletrônico de dados"[22].

Partindo de uma definição de *dados* como um material que serve a um propósito de análise, e de *informação* como o que resulta dessa análise interpretativa de dados, e, tendo em vista que os dados tem uma certa potencialidade de fornecer uma grande e diversa quantidade de informações, primordialmente, não são os dados em si que devem ser protegidos, mas os sujeitos a quem tais dados se referem. Na verdade, a absoluta proibição de acesso e a vedação de utilização não deve ser preponderante no processamento de dados pessoais, visto que tal prática impediria a segurança exigida para a consecução dos negócios jurídicos, esbarrando na autonomia negocial[23]. Não só nesses casos, mas também quando o uso é legítimo e necessário, a exemplo de pesquisas de caráter científico ou mesmo a atividades médicas, uma plena negação do tratamento de dados pessoais não se mostra interessante.

---

19 ASCENSÃO, José de Oliveira. **Direito civil: teoria geral**. São Paulo: Saraiva, 2010. Vol. 1, p. 105.

20 Na Europa, países como a Suíça e a Alemanha restringem o processamento de dados sensíveis, sem determinar, no entanto, a sua proibição total, enquanto nas legislações da Noruega, Finlândia, Dinamarca, França e Grã-Bretanha observa-se a proibição total do tratamento desses dados.

21 MENDES, Laura Schertel. *Op. Cit.*, p. 62.

22 MARTINS, Leonardo. **Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão**. Montevidéu: Fundação Konrad Adenauer, 2005, p. 244 e 245.

23 MARTINS, Fernando Rodrigues. *Op. Cit.*, p. 16.

O artigo 6º da *GDPR* (*General Data Protection Regulation*)[24], regula o tema na União Europeia, de modo que não se impede o total uso desses dados, apenas em uma certa parcela dos casos. Nesse contexto, só seria legítima a coleta de dados provida de consentimento explícito, anterior e específico por parte do sujeito que os cede[25].

1.2. Direito à privacidade *ou* proteção de dados pessoais?

Ainda no início do século XIX, em decorrência da utilização de novas formas e instrumentos tecnológicos, o início dos debates acerca do direito à privacidade se deu como consequência do crescente acesso e divulgação de fatos relativos à esfera privada dos indivíduos. Warren e Brandeis[26] foram pioneiros no assunto, traduzindo o cotidiano da época e denunciando como os jornais, a fotografia e outras novas tecnologias invadiram o setor da vida privada e doméstica de uma forma nunca antes vista nas sociedades. Ressalta-se a associação feita entre o objeto "vida privada" e um direito – até então – desconhecido. Ao fundamentarem o direito à privacidade, os autores relacionam a sua proteção à inviolabilidade da personalidade, rompendo com uma tradição anterior que associava a proteção da vida privada à propriedade. Nas suas palavras, "o princípio que protege escritos pessoais e outras produções pessoais, não contra o furto ou a apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas da inviolabilidade da personalidade"[27].

---

[24] Artigo 6º, GDPR: **Licitude do tratamento**. 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrônica.

[25] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 2/2010 on online behavioral advertising.** 2010, p 20.

[26] WARREN e BRANDEIS. **The Right to Privacy**. In Harvard Law Review, Vol. IV, 1890. Os autores estudaram juntos no curso de direito da Harvard Law School, e, posteriormente, Brandeis se tornou ministro da Suprema Corte dos EUA. O referido artigo é considerado um dos mais citados e relevantes da história norte-americana. (SHAPIRO, Fred. "The Most-Cited Law Review Articles Revisited", in: 71 Chicago-Kent Law Review 751 [1996]). *Apud.:* DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006, p. 137.

[27] MENDES, Laura Schertel. *Op. Cit.*, p. 14.

No decorrer do século XX, a transformação da função do Estado, aliado à contínua revolução tecnológica, contribuiu para modificar o sentido e o alcance do direito à privacidade. Hoje, a necessidade do reconhecimento desse direito se dá no próprio estilo de vida pós-moderno, com relações cada vez mais complexas, que tornaram as pessoas mais sensíveis e expostas à publicidade, tornando a solidão e a privacidade algo essencial. A doutrina coloca, então, o direito à privacidade relacionado com a aversão a qualquer intromissão não consentida na vida privada (definida como o espaço da vida doméstica e das relações sexuais).[28]

Dessa forma, fica fácil perceber que a proteção de dados pessoais, apesar de ter como fundamento o direito à privacidade, ultrapassa o seu âmbito[29], podendo ser compreendida como um fenômeno coletivo, na medida em que os danos causados pelo tratamento impróprio desse material são, em razão de sua própria natureza, difusos, exigindo uma tutela jurídica coletiva específica. Naturalmente, tanto o direito à privacidade como a proteção de dados pessoais fundamentam-se, em última medida, na proteção da personalidade e da dignidade do indivíduo. Entretanto, a proteção de dados pessoais modifica os elementos da privacidade, aprofundando seus postulados e tocando em certos pontos centrais dos interesses em questão[30]. Ora, "nem todos os problemas advindos do processamento de dados pessoais são passíveis de serem plenamente examinados sob a ótica da privacidade. Isso acontece vez que esse conceito não é capaz de abordar os problemas individuais e coletivos oriundos dos atuais sistemas de classificação e risco, como por exemplo, a utilização de dados genéticos dos pacientes por planos de saúde ou a discriminação por supermercados em razão do código postal"[31].

Na medida que novas tecnologias surgem, o armazenamento e processamento rápido e eficiente de dados pessoais permite a associação entre a proteção à privacidade e informações pessoais. Percebe-se não apenas uma alteração na substância do direito à privacidade, mas em sua própria nomenclatura, surgindo termos como *privacidade informacional*, *proteção de dados pessoais*, *autodeterminação informativa*, etc. A tutela do objeto – inclusive através de dispositivos constitucionais[32] – vai além, não se limitando apenas à privacidade, pois entende-se, agora, que tais dados e informações constituem uma projeção da própria personalidade dos indivíduos.

---

28 DONEDA, Danilo. *Op. Cit.*, 2006, p. 139.

29 *Idem, Ibidem*, p. 205.

30 *Idem, Ibidem*, p. 205.

31 MENDES, Laura Schertel. *Op. Cit.*, 2008, p. 11.

32 *Cf.* capítulo 1.4, acerca da fundamentalização da proteção de dados pessoais.

Vale mencionar, aqui, a teoria das esferas de Heinrich Hubmann, que embasou essa distinção terminológica pelo constituinte brasileiro. Segundo o autor, o sentimento de privacidade do indivíduo pode ser compreendido a partir de um esquema de círculos concêntricos, que representam diferentes graus de manifestação da privacidade. No núcleo estaria a esfera da intimidade – ou do segredo – (*Geheimsphäre*); em torno dela, a esfera privada (*Privatsphäre*); e em torno de ambas, em um círculo de maior amplitude, a esfera pessoal (*Öffentlichkentsbereich*), abrangendo a vida pública do indivíduo[33].

Assim, não se fala mais em um direito à privacidade quando se trata das questões de informações pessoais, mas sim à um direito autônomo à proteção desses dados, ou, ainda, numa possível transformação e adaptação daquele direito às novas situações cotidianas decorrentes das inovações tecnológicas, que nos remetem, muitas vezes, ao ambiente virtual.

1.3. Princípios da proteção de dados pessoais

Visando a limitação do tratamento de dados pessoais, para que os indivíduos possam exercer plenamente seu poder de autodeterminação informativa, a doutrina desenvolveu ao longo dos anos uma série de princípios norteadores da prática. Não obstante a clara evolução do tema durante tal período, é possível agrupar materialmente alguns objetivos e linhas de atuação principais, presentes em diversos ordenamentos, em diversos graus. Através disso, percebe-se uma forte convergência do tratamento da matéria nos diferentes ordenamentos rumo à consolidação de alguns princípios básicos e à vinculação cada vez mais estreita com os direitos fundamentais e a proteção da pessoa[34]. Esses princípios têm suas origens nas leis de primeira e segunda geração, podendo remeter até mesmo aos princípios norteadores do *National Data Center*, ainda na década de 60[35].

---

33 A teoria das esferas foi utilizada pelo Tribunal Constitucional alemão em 1969, quando foi declarado que a mais restrita delas, a esfera do segredo (*Geheimsphäre*), não poderia ser limitada sequer por lei, por se constituir em um âmbito inviolável da vida do indivíduo. Apesar disso, pode-se dizer que tal teoria foi alvo de inúmeras criticas, tendo sido superada pela própria doutrina alemã. Sob essa perspectiva, é importante mencionar a inutilidade prática da distinção conceitual efetuada pela Constituição Federal brasileira entre *vida privada* e *intimidade*. Muito embora haja menção de ambos os termos, tal distinção não deve operar efeitos jurídicos na tutela da privacidade pelo direito pátrio, porque, tanto o seu âmbito de proteção como as suas limitações, assim como os efeitos de sua violação, independem da distinção entre *vida privada* e *intimidade*. Isso porque a gravidade da violação ao direito à privacidade não estará relacionada necessariamente ao grau de intimidade ou de segredo de determinada informação armazenada, mas sim ao seu potencial discriminatório, como ocorre nos casos de dados sensíveis. (MENDES, Laura Schertel. *Op. Cit.*, p. 19.)

34 DONEDA, Danilo. *Op. Cit.*, 2011, p 98.

35 O *National Data Center* foi projetado para reunir as informações sobre os cidadãos estadunidenses disponíveis em diversos órgãos da administração federal em um único banco de dados, a partir de um projeto original, que pretendia unificar

De forma concisa, são eles:

a) *Princípio da publicidade (ou transparência)*: a existência de bancos de dados deve ser de conhecimento público, o que se dará por meio de autorização estatal prévia para seu funcionamento, de uma notificação às autoridades acerca de sua existência, ou ainda por meio de relatórios periódicos de livre acesso ao público;
b) *Princípio da exatidão*: necessário à manutenção da qualidade dos dados, trata-se da exigência de que os dados de um banco reflitam a realidade, o que é traduzido pela necessidade de coleta e tratamento com cuidado e correção, além de atualizações periódicas conforme a necessidade;
c) *Princípio da finalidade*: a utilização dos dados pessoais deve, obrigatoriamente, obedecer às finalidades anunciadas antes da coleta ao sujeito cedente. Isso é de extrema relevância prática, pois restringe a transferência de dados pessoais a terceiros, podendo, inclusive, estruturar um critério de valoração da razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade);
d) *Princípio do livre acesso*: assegura a plena disponibilidade dos dados armazenados aos sujeitos à que se referem, garantindo a obtenção de cópia dos registros e, em consonância com o princípio da exatidão, a retificação de informações incorretas ou obsoletas, podendo haver supressão ou acréscimo de informações;
e) *Princípio da segurança (lógica e física)*: assegura a proteção dos dados contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado por aqueles à que se referem, tanto no meio físico quanto virtual.

Tais princípios passaram a ser encontradas em diversas normativas sobre a proteção de dados, e passaram a ser chamados de *Fair Information Principles*. Esse núcleo comum se consolidou como tal principalmente a partir da Convenção de Strasbourg, e das *guidelines* da OCDE[36], no início da década de 80[37].

---

os cadastros do Censo, dos registros trabalhistas, do fisco e da previdência social. Após acirradas discussões sobre a ameaça potencial que representaria às liberdades individuais, o governo desistiu do projeto. (DONEDA, Danilo. *Op. Cit.*, 2011, p 98)

[36] **Guidelines on the Protection of Privacy and Transzborder Flows of Personal Data**, disponível em: <www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>. Os princípios elencados são: (1) collection limitation; (2) data limitation; (3) purpose specification; (4) use limitation; (5) security safeguard; (6) openness; (7) individual participation. Acesso em 12 de setembro de 2018.

[37] DONEDA, Danilo. *Op. Cit.*, 2011, p 100.

No Brasil, a recente lei de proteção de dados pessoais[38] trata do assunto de forma bastante clara, elencando, no artigo 6º, princípios que devem ser observados no tratamento de dados pessoais, além da própria boa-fé. São eles:

> *I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;*
> *II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;*
> *III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;*
> *IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;*
> *V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;*
> *VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;*
> *VII - segurança: 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;*
> *VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;*
> *IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;*
> *X - responsabilização e prestação de contas: 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.*

Dessa forma, o tema é tratado de forma bastante direta e explícita, em uma clara tentativa de não deixar margens de atuação desfavoráveis ao sujeito a que se referem os dados.

---

38 Lei nº 13.709, de 14 de agosto de 2018. *Cf.* capítulo 3.2, que trata minuciosamente e de forma específica da lei.

1.4. A fundamentalização da proteção de dados pessoais

Antes de trabalhar com a proteção de dados pessoais como um Direito Fundamental, faz-se necessário determinar a amplitude do termo, bem como o processo de formação e características dos mesmos.

Conforme doutrina Bobbio[39], a caracterização de um Direito Fundamental é feita a partir do fato de serem universais, ou seja, de valerem para todo homem, independente de nacionalidade, raça, etc. Intitular um direito de fundamental é demonstrar que o mesmo é imprescindível à condição humana e ao convívio social, integrando o núcleo substancial da ordem normativa[40], que visa, acima de tudo, a proteção dos direitos à liberdade, à igualdade, à propriedade e à dignidade de todos os seres humanos. Assim, surgem a partir de um processo de positivação dos próprios Direitos Humanos, quando ocorre seu reconhecimento nas legislações positivas de cada ordenamento nacional. Além da mencionada universalidade, os Direitos Fundamentais podem ser caracterizados principalmente pela (1) relatividade, haja vista que não podem ser considerados absolutos, podendo ser sopesados quando aplicados conjuntamente; (2) imprescritibilidade, pois não são perdidos pela falta de uso; (3) indisponibilidade, dada a impossibilidade de venda, doação, empréstimo, etc.; (4), e indivisibilidade, devido à sua interpretação conjunta, não permitindo uma análise individual ou parcial dos mesmos.

Os Direitos Fundamentais são uma construção histórica, variando de época para época, e de lugar para lugar. Na antiga França em período de revolução, por exemplo, os Direitos Fundamentais eram, basicamente, a liberdade, a igualdade e a fraternidade, e nem se cogitaria pensar na possibilidade de um Direito Fundamental a um meio ambiente ecologicamente equilibrado ou à igualdade entre os sexos. Ou seja, por mais fundamentais que pareçam ser, são direitos históricos, nascidos em certas circunstâncias e caracterizadas por lutas em defesa de novas liberdades, sendo desenvolvidos de modo gradual, e o que parece fundamental numa época e numa determinada civilização não é, necessariamente, fundamental em outras épocas e culturas[41].

---

39 BOBBIO, Norberto. **A era dos direitos**. 7ª edição. Rio de Janeiro: Elsevier, 2004, p. 79.

40 SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na constituição federal de 1988**. 5ª ed. Porto Alegre: Livraria do Advogado, 2005, p. 70.

41 BOBBIO, Norberto. *Op. Cit.*, p. 9.

Em meio às infinitas ameaças e perigos à vida, à liberdade e à segurança, provenientes do aumento do progresso tecnológico, nascem esses direitos da nova geração. A partir disso, considerado o contexto que a sociedade humana em geral passa atualmente, o direito à proteção de dados pessoais, principalmente nos ambientes virtuais, é de suma importância, relacionando-se com o pleno desenvolvimento dos demais direitos e garantias. Citando Pinãr Manãs:

> *"En general se dice que el derecho a la protección de datos personales es un derecho nuevo, [...] que C. E. Delpiazzo*[42] *lo llama "novel derecho", razón por la cual, se le ha considerado un derecho de la tercera generación y un derecho autónomo, [...] instrumental"*[43]

Ou seja, em decorrência de seu recente surgimento e temática, o direito à proteção de dados pessoais é tido, por alguns autores, como um direito de terceira dimensão – conforme teoria do checo-francês Karel Vasak acerca das gerações de direitos fundamentais – e, sendo considerado um direito autônomo, num contexto de modernização da sociedade e desenvolvimento de novas tecnologias, tal proteção torna-se imprescindível para a eficácia dos demais direitos.

O tratamento autônomo dessa proteção de dados, tão como sua especial proteção, vem sendo uma tendência fortemente enraizada nos ordenamentos jurídicos, sendo um caso emblemático de uma tendência que, a princípio, "parecia apenas destinada a mudar de terminado patamar tecnológico e a solicitar previsões pontuais no ordenamento, mas que, em seus desdobramentos, veio a formar as bases para o que vem sendo tratado, hoje, como um direito fundamental à proteção de dados"[44].

A partir das mudanças de tratamento sofridas nos últimos anos, gozando de tutela autônoma, e, algumas vezes, de proteção constitucional[45], o direito à proteção de dados pessoais cada vez mais se estabelece como um direito fundamental, não apenas nos ordenamentos nacionais, mas também em textos internacionais. Exemplo disso é a antiga *Diretiva 95/46/ CE* sobre proteção de dados pessoais na União Europeia, que coloca como um dos objetivos

---

42 DELPIAZZO, Carlos. **A la búsqueda del equilibrio entre privacidad y acceso.** Instituto de Derecho Informático, Facultad de Derecho, Universidad de la República. Montevideo, 2009, p. 9.

43 PIÑAR MAÑAS, José Luis. **Guía del Derecho Fundamental a la protección de datos de caracter personal**, Agencia Española de Protección de Datos, 2004, p 36.

44 *Idem, Ibidem*, p. 36.

45 É o caso das constituições de Portugal (1976) e Espanha (1978), com dispositivos destinados a enfrentar os problemas da utilização da informática e, no caso da Constituição portuguesa, com referência explícita à proteção de dados pessoais.

principais o tratamento de dados pessoais, utilizando, inclusive, a expressão *Direitos Fundamentais* para tal, e, posteriormente, a própria Carta de Direitos Fundamentais da União Europeia[46], de 2000, que tem em seu corpo uma seção exclusiva para a proteção de dados pessoais. Como exemplo atual, é possível perceber a fundamentalização de tal direito pela leitura do novo Regulamento Geral sobre a Proteção de Dados (RGPD) pessoais na Europa, que reforça ainda mais a característica de tal direito.

Além da legislação internacional europeia, sem nem adentrar nas legislações nacionais do continente, uma breve busca nos ordenamentos vizinhos leva à uma sólida comprovação do exposto. No Uruguai, por exemplo, o artigo 1° da Lei 18.331 dispõe expressamente que o direito à proteção de dados pessoais é inerente à pessoa humana[47]. E, ainda mais além, conforme estudo publicado por D. Banisar[48], existem, atualmente, mais de 100 países com uma lei de proteção de dados em vigência, e outros mais de 40 com algum projeto ou iniciativa pendente, sendo a maioria deles composta por projetos fortemente embasados nas mencionadas legislações, o que traça um caminho rumo à efetiva fundamentalização do direito.

Fato é, que uma considerável parcela dessas menções – talvez em razão de sua antiga elaboração – dizem respeito aos dados pessoais transmitidos por meios físicos, pois falam em *correspondências*, na sua maioria. Interessa aqui, entretanto, examinar o conteúdo formal de tal direito, que, há quase vinte anos atrás, já era tido como fundamental para o desenvolvimento social. A leitura atual de tais dispositivos – que ainda não tiveram devida adequação terminológica às novas tecnologias – deve ser feita de forma ajustada, abrangendo quaisquer informações que possam identificar uma pessoa, tanto no ambiente físico quanto virtual.

Dessa forma, a titulação do direito à proteção de dados pessoais – na *Internet* – como um Direito Fundamental faz-se necessária não só em razão de sua classificação como um direito autônomo, mas como um meio difusor de informação, na medida que quanto maior for o nível

---

[46] Art. 8°: 1- Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2- Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

[47] Artigo 1° da Lei n° 18.331, de 2008: "el derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República".

[48] O pesquisador Daniel Banisar faz parte de um projeto que analisa as leis nacionais de proteção de dados pessoais e privacidade, publicando um mapa-múndi com todos os países classificados como (1) lei já promulgada/em vigor, (2) iniciativa pendente e (3) sem iniciativa/sem informações. A partir disso, sua mais recente publicação, em janeiro de 2018, conta com mais de 100 países no primeiro grupo e mais de 40 no segundo, traduzindo o enorme crescimento e preocupação dada ao tema. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

de conhecimento e consciência da sociedade, menor será o nível de abusos realizados pelos diferentes sujeitos ativos. É, assim, um passo necessário à integração da personalidade humana, em sua acepção mais completa, nas diversas questões que cercam a Sociedade da Informação.

2. USO DE INFORMAÇÕES DE NAVEGAÇÃO – COOKIES

2.1. Aspectos técnicos que permeiam o tema

O foco do trabalho desloca-se, agora, dos dados pessoais como um termo genérico e imerge de maneira específica em uma de suas manifestações: os *cookies* de navegação na *Internet*. Diferentemente dos temas já estudados, em razão de sua forte característica técnica, faz-se imprescindível uma prévia análise de alguns termos mais importantes, cruciais para o bom entendimento do que segue.

Em primeiro lugar, os *bancos de dados* são os conjuntos estruturados de dados pessoais, podendo ser estabelecidos em uma ou mais localidades, em meio físico (na forma de dossiês ou fichários) ou virtual. A grande questão gira em tordo dessa segunda hipótese, sendo razão para o Tribunal Constitucional Alemão relacioná-la com a própria necessidade de uma proteção de dados pessoais, visto que

> *"em processos decisórios não se precisa mais lançar mão, como antigamente, de fichas e pastas compostos manualmente. Hoje, com a ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (...) podem ser, do ponto de vista técnico, ilimitadamente armazenados e*

> *consultados a qualquer momento, a qualquer distancia e em segundos" (BVerfGe 65, 1, Volkszählung).*

Assim, o tratamento de tais dados constitui basicamente toda operação técnica com eles realizada[49], de modo informatizado ou não, com a finalidade de se refinar a informação, tornando-a mais valiosa ou útil. É feito pelos *operadores*, em nome dos *controladores*, a quem compete as decisões referentes. Tanto estes como aqueles podem ser pessoas físicas ou jurídicas, de direito público ou privado, sendo considerados *agentes de tratamento*. Aqui, os sujeitos detentores dos dados (a quem eles se referem) são chamados de *usuários*, vez que são os frequentadores de *websites,* os quais tem como *editores* aqueles que disponibilizam o conteúdo num espaço para que possa ser visualizado. Ainda nessa relação subjetiva, os *provedores* são as empresas que fornecem serviços de acesso e utilização de *Internet* pelos usuários.

Os *cookies,* por sua vez, compõem a principal tecnologia de rastreamento e monitoramento de usuários na *Internet*. Permitem a análise de navegação do usuário por um período certo de tempo[50], funcionando da seguinte forma: em regra, a empresa coloca um *cookie* de rastreamento (*tracking cookie)* em um instrumento denominado DTE (*data terminal equipment*), que ordinariamente converte informações do usuário em sinais quando se acessa algum *website* que contém tais tecnologias. Essencialmente, os *cookies* são arquivos de texto simples, armazenados pelo navegador frequentado, contendo informações básicas acerca das preferências dos usuários.

Num contexto de publicidade comportamental (*Online Behavioral Advertising - OBA*), tais *cookies* irão permitir que as empresas publicitárias – e suas parceiras – reconheçam um usuário que retorna posteriormente ao *website*, o que permitirá, ao longo do tempo, a formação de um perfil consumidor. Levando-se em conta, ainda, as inúmeras possibilidades de processamento dos dados pessoais pelos meios automatizados, tão como a quase ilimitada capacidade de armazenamento, combinação e cruzamento de informações, é possível a

---

[49] Conforme o artigo 5º, X, da Lei de Proteção de dados (L. 13.709/18), "tratamento é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração". De modo semelhante, a *GDPR*, considera como sendo tratamento de dados toda operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

[50] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Op. Cit.*, p 6.

formação de quadros de personalidade quase completos, aumentando exponencialmente as hipóteses de consulta e influência nos comportamentos dos indivíduos. Isso expõe ainda mais os usuários na *Internet*, reforçando a necessidade de estudo e regulamentação legislativa do tema.

2.2. Tutela da informação pessoal

A informação pessoal pode, num certo sentido, ser desvinculada da pessoa, submetendo-se a tratamentos, sendo comunicada, etc., mas até o ponto em que ela continua sendo uma informação *pessoal,* ou seja, se referindo à uma pessoa e a identificando, tal informação mantém seu vínculo com ela, devendo ser valorada de acordo com essa carga. Logo, em razão dessa valoração intrínseca que carrega, deve ser entendida como uma efetiva extensão da personalidade do sujeito a quem se refere[51].

Partindo desse pressuposto, é importante destacar que muitas modalidades de coleta e tratamento de dados provocam, de uma maneira ou de outra, um distanciamento entre a informação conscientemente fornecida pelo sujeito, e a utilidade na qual ela é transformada. É possível identificar uma *informação base* e uma *informação resultado*, conforme explica Pierre Catala, em razão da aplicação de métodos de tratamento, de forma a gerar uma utilidade a quem os realiza. E é justamente essa diferença entre uma informação e outra que diminui o controle das pessoas sobre o que se sabe delas, limitando sua própria liberdade[52]. De um ponto de vista técnico, o que ocorre é que a informação fica cada vez mais manipulável, se tornando um objeto exclusivamente de potencialidades econômicas.

2.2.1. Papéis e responsabilidades de diferentes sujeitos

Como já mencionado, o processo de tratamento de dados como um todo envolve uma diversidade de sujeitos, como editores, empresas de publicidade e seus provedores. É de extrema importância, assim, estabelecer quais os papéis e responsabilidades de cada um, de uma forma adequada à legislação a que se submetem, facilitando, assim, a própria execução dessas normas.

---

51 DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia.** Escola Nacional de Defesa do Consumidor. Brasília, 2010, p. 29.

52 *Idem, Ibidem*, p. 36.

No que diz respeito às empresas de publicidade e seus provedores – que, na sua essência, são aquelas que colocam os *cookies* nos navegadores dos usuários, e deles retiram informação previamente coletada – é irrelevante se são meros processadores de dados ou efetivamente quem os controla: em um contexto de publicidade direcionada, é exigido a obtenção de consentimento informado anterior à coleta dos dados, além do dever de informação ao usuário.

A formação e coleta de dados se faz com base no tipo de anúncio que levou o usuário a um *site* diferente. Ou seja, a partir do momento em que a publicidade atrai o usuário, fazendo com que ele redirecione o foco de sua pesquisa, e a empresa coleta e rotula esses dados como sendo de interesse do mesmo, a responsabilidade dessa empresa publicitária é integral, devendo empregar um correto tratamento das informações obtidas.

Os editores, posto que detém controle de frequência de usuários, tão como um relevante alcance midiático, atuam nesse sistema alugando espaço *online*, nos *websites*, para que as empresas de publicidade possam realizar seus anúncios. A questão acerca de sua responsabilidade surge quando se observa a existência de instrumentos que redirecionam o usuário de seu próprio *site* à pagina anunciada. Por óbvio, sua responsabilidade quanto ao tratamento dos dados coletados é nula, dado o caráter de mediação de sua participação; mas essa responsabilidade é apenas reduzida quando se trata do dever de informação ao usuário acerca da coleta de tais dados, que deve ser promovido por todos os envolvidos. Ou seja, como medida de prevenção, os editores devem ter ciência de que um contrato firmado com uma empresa de publicidade pode vir a ser motivo gerador de responsabilidade perante os usuários, sendo aconselhado, quando possível, acordo prévio de delimitação de responsabilidade.

De forma semelhante, quando se trata da responsabilização dos bancos de dados, deve-se analisar o fato unicamente sob a ótica de uma eventual culpa na deterioração dos dados sob sua custódia. Isso acontece pois, aqui, não há qualquer tratamento de dados, ou seja, não se analisa, transforma ou realiza qualquer procedimento, limitando a atuação na simples tutela das informações. Assim, a responsabilidade deverá ser apurada de modo proporcional à eventual culpa em sua perda ou deterioração.

2.2.1.1. Quais informações e por quem deverão ser providas?

Não só no contexto de publicidade direcionada, tema a ser abordado adiante, mas também nos vários campos em que os dados são coletados, os usuários ordinariamente não sabem ou não entendem as tecnologias utilizadas para tal. É de suma importância, então, assegurar que será providenciada informação clara e suficiente aos usuários, que, só após, serão capazes de exercer seu direito de escolha.

Valendo-se, mais uma vez, de normativas europeias, o *Article 29 Working Party,* em recomendação acerca da antiga Diretiva 95/46/EC, estabelece que as informações dadas deverão ser *as user friendly as possible*[53], e o principal meio para alcançar isso seria através de uma informação curta, interativa, facilmente identificada e entendida. E essas informações deverão conter ao menos a identidade de quem está coletando dados e o propósito de tal coleta, além de outras informações acerca do modo e abrangência da mesma. Dizer, por exemplo, que determinado *website* "usa *cookies* e poderá compartilhar tais dados com terceiros em parceria" é visivelmente uma afronta ao direito de informação do usuário. É essencial que essas informações não se deem através de termos e condições genéricas, e uma maneira de concretizar tal proposta é pela utilização de ícones nas páginas dos editores (*websites*) com *links* para informações adicionais.

Mas isso não deve ser feito apenas uma única vez: é essencial que as coletoras de dados informem os usuários periodicamente acerca da coleta e monitoramento realizados: ou seja, a menos que os sujeitos sejam constantemente lembrados de forma clara e de fácil entendimento, é bastante provável que após um certo período de tempo eles se esquecerão de sua anuência, e quiçá da própria existência de tal monitoramento. Uma outra solução proposta[54] é a criação de um símbolo ou mensagem que terá como principal função a identificação fácil de que certa página monitora a navegação e cede dados à certas empresas, não só informando, mas controlando se o usuário quer ou não continuar.

Fica clara, assim, a necessidade de uma cooperação entre provedores, editores e publicitários, buscando encontrar quem será o responsável por disponibilizar tal informação, bem como a forma que isso será feito. Isso é ressaltado ainda mais quando se verifica que, para os usuários, os provedores publicitários são sujeitos invisíveis, sendo perceptível apenas os editores de *websites* e os anúncios.

---

53 ARTICLE 29 DATA PROTECTION WORKING PARTY. *Op. Cit.*, p 17.

54 *Idem, Ibidem,* p 18 e 19.

2.2.1.2. Dever de obtenção de consentimento informado anterior

O consentimento informado é o meio pelo qual o direito faz valer a autonomia privada do cidadão, quando sob a ótica dos dados pessoais. A nova *GDPR*, em seu artigo 4º, 11, define consentimento como "qualquer manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento". Nesse sentido, o consentimento pode ser compreendido como um ato unilateral, que visa autorizar o tratamento dos dados pessoais, sem que isso implique uma estrutura contratual, sendo fundamental a distinção do consentimento em relação ao processamento de dados pessoais em dois momentos: (I) o consentimento para a autorização da coleta e processamento dos dados, isto é, para o acesso à esfera privada do indivíduo; e (II) o consentimento para a autorização da transferência dos dados[55].

Assim, para que uma coleta de dados seja válida, é necessária a obtenção de um consentimento que diga respeito à concordância do usuário na cessão de seus dados às empresas para que deem uma certa e específica destinação. Ocorre que, para que isso seja por si só válido, independentemente da circunstância em que seja coletado, a anuência do usuário deve ser obtida de forma livre e específica, numa real demonstração da vontade do mesmo. Além disso, deverá ser obtido antes da coleta dos dados, como uma medida prévia necessária para que os sujeitos possam entender plenamente com o que estão consentindo, tão como as consequências de não consentir, se for o caso[56]. Deve, por fim, ser revogável, tanto com relação à autorização para o tratamento, quanto para a própria circulação dos dados colhidos.

Em regra, os usuários normalmente não têm a correta noção de que estão sendo monitorados, dos propósitos de tal monitoramento, não sabem como programar seus navegadores para que bloqueiem os *cookies*, ou mesmo que existe tal opção. Logo, é um engano supor que a falta de uma atitude positiva dos usuários, em utilizar a opção de bloqueio de *cookies* no navegador, por exemplo, configura uma demonstração clara de suas vontades. Uma pesquisa feita em 2010 mostrou que três dos quatro maiores navegadores existentes tem como opção padrão, desde sua instalação, a livre utilização de *cookies* por terceiros publicitários. Nesses casos observa-se a existência de monitoramento e coleta de dados, mesmo não havendo

---

55 DONEDA, Danilo. *Op. Cit.*, 2006, p. 376 a 379.

56 Conforme a Lei de proteção de dados alemã (*BDSG*), em sua seção 4ª, (1): os pressupostos de um consentimento válido, no âmbito da proteção de dados pessoais, são os seguintes: (I) que o titular dos dados que emita o consentimento o faça por sua livre vontade; (II) que o consentimento seja voltado a uma finalidade específica; (III) que o titular seja informado acerca do objetivo da coleta, do processamento e do uso dos dados, assim como das consequências de não consentir com o tratamento.

anuência do usuário e, como se não fosse suficiente, foi identificado que essa coleta de dados continua sendo realizada mesmo após eventual alteração de tal opção[57].

" Opt out options"

Cada vez mais as empresas publicitárias disponibilizam uma seção na qual os usuários podem exercer o direito de auto exclusão, que pode ser alcançada, em regra, por meio de um redirecionamento a partir da página principal do anunciante. Tal mecanismo funciona a partir de uma conduta positiva do usuário, que deve procurar o *website* da empresa publicitária por trás do anúncio e demonstrar sua vontade de exclusão do processo de monitoramento e coleta de dados. Isso demonstra uma certa tendência à correção do desequilíbrio causado pelos problemas acima descritos, relacionados com o consentimento nos navegadores.

Entretanto, mesmo após reconhecer que esse instrumento tende a reequilibrar a situação, não seria o mecanismo ideal a ser utilizado quando se trata do problema do consentimento informado prévio. Primeiramente, em razão da própria noção dos usuários acerca da tecnologia utilizada, pois na maioria das vezes não se sabe da existência de uma opção em que é possível a retirada do procedimento de coleta de dados. Ou seja, na prática, apenas uma mínima parcela dos usuários exerce tal direito, justamente por não compreender que ao não realizar essa tarefa de auto exclusão, eles estão, de fato, concordando com as condições impostas. Em segundo lugar, pelo fato de que uma *opt out option* se dá em decorrência de uma não ação prévia do sujeito, uma omissão deste em relação ao procedimento de coleta e monitoramento. Mesmo que haja participação, ela será posterior e derivada de uma conduta passiva anterior[58].

Assim, para que seja devidamente respeitado o consentimento informado anterior, conforme a nova norma europeia, o usuário deve ser informado previamente acerca do uso de *cookies*. Essa informação deve ser feita de forma clara e indicar quais dados serão colhidos, suas finalidades e o período de duração – que deverá ser razoável, de forma que as pessoas não se esqueçam de sua escolha, devendo ser revalidado após o decurso do prazo. Somente após deve ser dado uma opção de escolha, sendo necessária uma ação positiva do mesmo para consentir[59].

Consentimento informado por crianças

---

57 ARTICLE 29 DATA PROTECTION WORKING PARTY. *Op. Cit.*, p 14.

58 *Idem, Ibidem,* p 16.

59 *Idem, Ibidem*, p 16.

Na medida em que as normativas acerca da proteção de dados pessoais se tornam cada vez mais presentes nos ordenamentos nacionais e internacionais, por óbvio, as questões relacionadas às crianças ficam cada vez mais pormenorizadas. Exemplos de normas que exigem autorização do responsável para a coleta de dados de menores de 16/18 anos incluem o *Children's Online Privacy Protection Act* (*COPPA*) nos Estados Unidos, o Regulamento Geral sobre a Proteção de Dados *(General Data Protection Regulation - GDPR*) na União Europeia e a Lei de Proteção de Dados Pessoais (*PIPA*) na Coreia do Sul.

Assim, conforme a *GDPR*, dada a situação de maior vulnerabilidade das crianças, ressaltada no meio virtual – em razão de estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais – faz-se necessária uma atenção especial quanto à sua proteção. Como regra geral,

> *"Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças quando da utilização de serviços disponibilizados diretamente à elas.*

Tal proteção específica é feita, principalmente, por meio da linguagem pela qual as crianças são dirigidas, devendo qualquer informação e comunicação estar redigida numa linguagem clara, simples e de fácil compreensão.

Ocorre que em alguns casos o consentimento não poderá ser dado pela própria criança, a depender da idade da mesma, ou ainda do tipo de informação a ser colhida. Nesses casos, o consentimento deverá ser dado pelos pais ou representantes legais, que será feito por meio de uma notificação informando acerca das especificidades de tal tratamento, de forma que nenhuma ação será realizada até que tenha sido obtido o consentimento. Aqui o *COPPA* toma forma, atuando por meio de um instrumento de cobertura aplicado à determinados *sites* e serviços *online*, obtendo o consentimento dos pais ou responsáveis de forma anterior à utilização dos filhos.

Por fim, vale mencionar que, conforme a *GDPR*, caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança[60].

---

[60] **REGULAMENTO (UE) 2016/679,** do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Artigo 8º.

2.2.2. Publicidade comportamental – Online Behavioral Advertising (OBA)

Adentrando efetivamente no campo do direito do consumidor, *publicidade interativa* é o nome dado ao sistema de métodos que visam a criação de anúncios mais relevantes para os usuários da *Internet,* podendo ser classificada em diferentes categorias, tais como *publicidade contextual*[61], *segmentada*[62] e *comportamental*. Esta última, foco do presente capítulo, pode ser considerada a de maior potencial publicitário, vez que consegue fornecer às empresas publicitárias um cenário bastante detalhado acerca da vida virtual das pessoas, sinalizando, por exemplo, páginas específicas que foram acessadas, a duração das visitas, os itens e ordem de visualização.

Pode-se conceituar a publicidade comportamental como sendo aquela baseada na observação do comportamento de indivíduos ao longo do tempo, e que busca estudar as características de tal comportamento através de suas ações (visitas reiteradas à *websites*, interações, palavras-chave, produção de conteúdo *online*, etc.), visando desenvolver um perfil específico e assim apresentar aos usuários anúncios individualizados cujas chances de se enquadrar dentro de seus interesses é presumivelmente maior[63]. Representa, assim, a fronteira na qual se desenvolvem as novas tecnologias de abordagem do consumidor, a partir da utilização intensiva de informações pessoais a seu respeito.

Nessa nova economia altamente customizada[64], a obtenção de informações sobre os consumidores é pressuposto para a adaptação e diversificação dos produtos e serviços para diferentes segmentos de clientes. Assim, para a obtenção de vantagens no mercado, é necessário que que a comunicação da empresa se individualize, criando e fidelizando nichos de consumo, sendo cada vez mais observada a oferta de volumes menores de produtos especializados, altamente qualificados e segmentados, o que permite a manutenção de um alto grau de lucratividade e estabilidade comercial[65]. Nesse sentido, a interação direta com o consumidor e

---

61 *Publicidade contextua*l se refere à publicidade direcionada ao usuário que é baseada no conteúdo momentaneamente visualizado por ele, seja por meio de palavras-chave utilizadas, histórico de buscas ou até mesmo a localização fornecida pelo IP da máquina utilizada.

62 *Publicidade segmentada* diz respeito aos anúncios realizados com base em informações conhecidas (idade, sexo, localização, etc.), disponibilizadas previamente no registro ou processo similar.

63 "Advertising that is based on the observation of the behavior of individuals over time. Behavioral advertising seeks to study the characteristics of this behavior through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests". (ARTICLE 29 DATA PROTECTION WORKING PARTY. *Op. Cit.*, 2010, p 4.)

64 MENDES, Laura Schertel. *Op. Cit.*, p. 81.

65 MENDES, Laura Schertel. *Op. Cit.*, p. 81.

a segmentação do marketing passam a ser ainda mais valorizadas, concretizando a concepção do marketing *one to one*[66].

Hoje, uma das fontes mais visadas para a obtenção de dados que permitam estabelecer o perfil de um consumidor a partir do seu comportamento é justamente o conjunto de hábitos de sua navegação na *Internet*, conforme observa a própria *Federal Trade Comission* estadunidense, em documento no qual caracteriza especificamente a publicidade comportamental *online*:

> *"A publicidade comportamental é o monitoramento das atividades de um consumidor quando conectado à Internet - incluindo as pesquisas que ele fez, as páginas que ele visitou e o conteúdo consultado - com a finalidade de fornecer-lhe publicidade dirigida aos interesses individuais deste consumidor"*[67]

É fato que as informações comportamentais não são, em sua maioria, fruto de manifestações de sua expressão livremente articulada, mas sim informações agregadas a partir de seu comportamento cotidiano; não são ponderadas e refletidas, mas sim disponibilizadas de modo ostensivo e sem o devido controle. Deste modo, cumpre verificar a natureza das informações que são provenientes dos consumidores, como medida de legitimidade da prática.

Pode-se dizer que o tratamento de dados pessoais pelas empresas privadas objetiva atingir, principalmente, as seguintes finalidades no mercado: (I) previsibilidade e diminuição de riscos; (II) interação com o consumidor; (III) diferenciação de produtos; e (IV) diferenciação de serviços[68]. A partir disso, não fica difícil fazer uma previsão dos possíveis riscos que possam permear a prática, devendo seus efeitos ser cuidadosamente assimilados pela prática consumerista. Um possível efeito colateral dessa utilização de informações sobre o comportamento de uma pessoa é o risco concreto de ampliar a assimetria informacional na relação de consumo, somando-se uma boa parcela de outros riscos inerentes à utilização de dados pessoais, refletindo na potencial discriminação entre consumidores, na relativização da

---

66 Esse conceito foi desenvolvido pelos americanos Pepper e Roger, que propagaram a necessidade de utilização de bancos de dados de consumidores e de meios interativos para oferecer ao consumidor o máximo de produtos e serviços possíveis, em substituição à antiga máxima de oferecer o mesmo produto à maior quantidade de clientes possíveis. (SCHWENKE, Matthias. **Individualisierung und Datenschutz.** Deutscher Universitäts-Verlag 2006, p. 42) *Apud.:* MENDES, Laura Schertel. *Op. Cit.*, p. 81.

67 Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles. FTC Staff Report. Disponível em: http://www. ftc.gov/os/2007/12/P859900stmt.pdf. Acesso em 29 de setembro de 2018.

68 SCHWENKE, Matthias. **Individualierung und Datenschutz**. Deutscher Universitäts-Verlag, 2006, p. 58.

ideia de escolha livre[69]. Isso se torna plausível em razão de uma mudança de paradigma, que Mayer-Schönberger[70] chama de paradigma da memória, no qual cada vez mais os nossos atos passaram a deixar rastros e de serem capazes de se transformar em informação definitiva, se antepondo ao antigo paradigma do esquecimento, no qual os atos cotidianos eram evanescentes e seus traços quase sempre restavam apenas em nossa memória e nas daqueles com quem compartilhávamos momentos.

Muito embora apresente grande potencial para se tornar maligno, caso o consumidor não tenha consciência efetiva do que ocorre, tal estabelecimento de perfis de consumidores não é, por si só, um mal em si. Mas quando se veicula apenas a publicidade que se ajusta ao seu pretenso perfil comportamental, ocorre uma limitação do rol de escolhas futuras daquela pessoa, a partir de uma dedução de um comportamento passado. Tal fenômeno já foi chamado de *boxing*[71], numa analogia ao encaixotamento das possibilidades de compras oferecidas à uma pessoa, que tem suas escolhas guiadas, a partir de presunções realizadas por ferramentas de análise comportamental com base em escolhas passadas.

Apesar de não ser diretamente ligado à formação de perfis de marketing comportamental, o desvio de finalidade na coleta de dados é um grave problema que permeia essa nova prática: a partir de dados coletados para a elaboração destes mencionados perfis, alimentam-se outras atividades, sem o conhecimento ou autorização do consumidor[72].

Uma outra prática decorrente do mau uso dos dados coletados é o chamado *adaptative pricing*, que consiste em uma variação do preço cobrado por determinados produtos unicamente em razão do perfil do consumidor. Desta forma, é possível a discriminação uma partir de critérios individuais, o que viola o princípio da igualdade dos consumidores perante o mercado, configurando prática claramente discriminatória[73]. Indo além, isso pode levar a uma discriminação de determinados consumidores em sentido estrito, hipóteses nas quais determinados perfis podem ter acesso negado a determinados bens e/ou serviços[74].

---

69 DONEDA, Danilo. *Op. Cit.*, 2010, p. 62.

70 MAYER-SCHÖENBERGER, Viktor. **Delete: The Virtue of Forgetting in the Digital Age**. Princeton: Princeton University Press, 2009. *Apud.:* DONEDA, Danilo. *Op. Cit.*, 2010, p. 68.

71 ABRAMS, Martin. **Boxing and concepts of harm**, in: Privacy and Data Security Law Journal, 2009, p. 673-676.

72 DONEDA, Danilo. *Op. Cit.*, 2010, p. 68.

73 DONEDA, Danilo. *Op. Cit.*, 2010, p. 69.

74 Por exemplo, no caso de uma negativa quanto à compra de um determinado bem unicamente em razão de constar no perfil do consumidor a consulta anterior a sites que tratam de proteção ao crédito, sugerindo ao fornecedor - sem dados concretos - que tratar-se-ia de um potencial inadimplente. Ou ainda, de maneira ainda mais prática, nos casos de vendas de seguros de automóveis ou planos de saúde.

Tendo em vista esses e outros possíveis problemas que podem surgir, devem ser conferidos ao consumidor, em igual proporção, condições para perceber e identificar claramente quando uma mensagem publicitária comportamental lhe é dirigida, de forma a distingui-la das demais em situações onde tal dúvida possa ocorrer[75]. Essa seria a única forma pela qual os consumidores seriam capazes de julgar efetivamente a conveniência do recebimento dessa publicidade, buscando, também, solucionar eventuais abusos. Isso possibilitaria não só esse julgamento acerca de eventuais abusos, mas legitimaria, ao mesmo tempo, o consentimento que se pretende para tal tipo de publicidade. Assim, o dever de informar o consumidor seria suprido na mesma medida em que este é informado sobre a forma e modalidade da coleta de dados, quem os recolhe, quem os utilizará e quais dados estarão sendo coletados.

Conforme explica Doneda[76], "uma outra proposta que, muito embora ainda não seja mais do que uma especulação, tem um potencial concreto para tornar-se uma ferramenta importante para fornecer aos consumidores uma importante retomada de controle sobre seus dados através de uma técnica ligada ao consentimento é a *Do Not Track List*[77], uma lista de pessoas inscritas que desejam não se submeter ao monitoramento de sua navegação na *Internet* mantida por uma organização governamental que, reporta-se, está em estudos pela *FTC* (*Federal Trade Commission*).

2.2.2.1. Sistemas e tecnologias de rastreamento

Tendo analisado as minúcias da publicidade comportamental em si, passa-se, agora, à análise dos métodos e tecnologias que permitem o processamento dos dados coletados, transformando-os em informação útil aos anunciantes, processo que é chamado de *refinamento de informação*. Para isso, são utilizadas sofisticadas tecnologias de análise de dados, que permitem às empresas a formulação de uma complexa estratégia de relacionamento com os seus clientes, a partir de informações "cruas" armazenadas em banco de dados. As empresas podem, assim, classificar e segmentar seus clientes em diversos grupos, diferenciando os consumidores de maior ou menor valor para a companhia, visando a obtenção de maior previsibilidade de

---

75 DONEDA, Danilo. *Op. Cit.*, p. 70.

76 *Idem, Ibidem,* p. 72.

77 Esta lista inspira-se francamente em uma outra lista mantida pela *Federal Trade Comission*: a *Do Not Call List*, que se destina ao bloqueio de marketing telefônico, que teve sua viabilidade e eficácia comprovadas ao longo dos últimos anos.

variações no mercado, de modo a reduzir seus riscos, bem como conhecer novas áreas para qual seja interessante direcionar publicidade[78].

Tais tecnologias são, em sua grande maioria, baseadas no uso de *cookies* de rastreamento nos navegadores dos usuários, dada sua capacidade de monitoramento ao longo do tempo e em diferentes ações. Quanto às técnicas, podem ser citadas, dentre outras, a construção de perfis (*Profiling*), o sistema de avaliação (*Scoring/rating system*) e a mineração de dados (*Data mining*).

Profiling

Para a realização de uma efetiva publicidade comportamental, a coleta e agregação de informações sobre consumidores e o seu enquadramento em um certo perfil são condições preliminares. Esse perfil pode ser considerado como sendo um registro sobre uma pessoa, expressando uma completa e abrangente imagem sobre a sua personalidade. Para isso, a construção de perfis depende de uma reunião de inúmeros dados sobre uma pessoa, com a finalidade de se obter uma imagem detalhada e confiável, objetivando a previsibilidade de padrões de comportamento, de gostos, hábitos de consumo e preferências[79]. A partir deste perfil, o consumidor é exposto a uma mensagem publicitária sob medida, cujas chances de se enquadrar dentro de seus interesses é presumivelmente maior, de acordo com os critérios do mecanismo utilizado.

Mas, nas palavras de Matthias Schwenke,

> *"A criação de perfis dos consumidores é problemática em diversos aspectos: perfis apresentam riscos à esfera privada e íntima, uma vez que possibilitam a manipulação relativa à sua vontade, bem como ensejam o mau uso dos dados no perfil. Problemático é também que o perfil seja criado sem o conhecimento e o consentimento do consumidor, sem que sejam asseguradas adequada proteção do sujeito submetido a essa técnica"*[80].

No *profiling,* estão em jogo não somente aspectos da privacidade do consumidor, porém da sua própria autonomia decisional e liberdade de escolha, a medida que uma publicidade estritamente baseada no perfil obtido limita incondicionalmente a liberdade de escolhas futuras

---

78 MENDES, Laura Schertel. *Op. Cit.*, p. 101.

79 *Idem, Ibidem*, p. 105.

80 SCHWENKE, Matthias. **Individualierung und Datenschutz**. Deutscher Universitäts-Verlag, 2006, p. 127 e 128. *Apud.:* MENDES, Laura Schertel. *Op. Cit.*, p. 105.

das pessoas. Apesar disso, conforme exposto, o estabelecimento de um perfil para um determinado consumidor não é, taxativamente, um mal em si, uma ameaça à personalidade, pois o que determinará a sua legitimidade é o uso que dele se fará, bem como o consentimento e o conhecimento do consumidor a respeito da criação de perfis relativos à sua pessoa[81].

Scoring system (rating system)

O Sistema de avaliação de consumidores funciona exclusivamente em razão de políticas de publicidade direcionada, objetivando identificar os consumidores que têm maior valor para a empresa, para que esses sejam os alvos de promoções e estratégias de fidelização de clientes. Ou seja, analisa-se um grande grupo de pessoas que poderão ser alvo de publicidade, mas escolhe-se apenas aqueles que têm comportamento *online* mais harmonizado com os produtos ou serviços oferecidos pelas empresas, que buscam construir uma relação mais duradoura, garantindo vantagens competitivas e um aumento dos níveis de lucratividade.

De uma maneira quase inevitável, ao passo que se seleciona um grupo e os classifica como *melhores consumidores* se faz o mesmo do outro lado, rotulando outros como os *piores consumidores*. No Brasil, são exemplos de empresas que oferecem tal serviço a SERASA e a Experian Brazil. Aqui, mais do que nunca, um erro na utilização dos dados, seja em razão da qualidade do objeto ou de seu tratamento, pode gerar graves danos aos consumidores, violando sua dignidade e personalidade.

E é justamente em razão desse maior potencial lesivo dessa prática que se aplica a proibição de que as pessoas fiquem sujeitas a decisões automatizadas que influenciem significativamente sua esfera jurídica[82]. A utilização desse sistema só é valida, então, nos casos em que se verifica seu uso como instrumento de auxílio na tomada de decisão, desde que os seus critérios sejam claros e transparentes.

Data mining

Essa prática consiste, basicamente, na utilização de certas técnicas de informática de combinação de dados e estatística para a identificação de informação relevante para uma determinada atividade, a partir de informação em estado bruto. Isso permite a transformação de

---

81 MENDES, Laura Schertel. *Op. Cit.*, p. 105.

82 Artigo 22, da *GDPR*: Decisões individuais automatizadas, incluindo definição de perfis. 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

grandes volumes de dados primitivos e de difícil compreensão em informações relevantes e de fácil aplicação prática, a partir de um processo de identificação e ordenação de padrões.

Essa informação em estado bruto é o que se denomina *Big Data.* O conceito de *Big Data* não se refere à técnica de processamento de informações em si, porém às gigantescas massas de dados que as modernas técnicas de comunicação tornaram possível armazenar e processar, mas cuja análise é severamente dificultada em razão de seu tamanho[83].

Em regra, a mineração de dados tem como finalidade a criação de regras para a classificação de pessoas e/ou comportamentos, inferindo-se um risco inerente de análises discriminatórias, que nega o direito constitucional à igualdade de todos os cidadãos[84]. Aqui, novamente, pode ser observado que "não é tal técnica em si que propicia a discriminação, mas sim o seu modo de utilização e as decisões que serão tomadas com base nas informações extraídas"[85]. Mas isso não isenta o sistema de responsabilidade, de modo que deve ser sempre considerado não só seu uso ideal, mas possíveis degenerações e hipóteses nas quais seu uso não será legítimo: de antemão, sempre que seu uso puder causar discriminação, será considerado ilegal em razão da violação de direitos fundamentais.

Uma outra questão que permeia o tema é o fato de que o tratamento de grandes quantidades de dados potencializa a dissociação entre os fatos representados pela informação armazenada e o contexto no qual estes se encontram e dentro do qual assumem seu significado próprio. Tal dependência não é fato desconhecido pela comunidade acadêmica, mas o problema se engrandece, aqui, em decorrência justamente em razão da dificuldade em se estabelecer o contexto de grandes volumes de informação, o que demanda soluções que não são somente de ordem técnica.

Assim, o processamento de dados por meio da mineração só será legítimo se a relação entre o consumidor e a empresa for transparente a ponto de ele ser informado sobre todas as finalidades da coleta e do processamento de seus dados, fazendo uso legal das informações colhidas, afastando-se do potencial discriminatório e seguindo à risca as diretrizes apontadas antes da coleta e do tratamento.

2.2.2.2. Direitos e obrigações

---

83 DONEDA, Danilo. *Op. Cit.*, 2010, p. 67.

84 MENDES, Laura Schertel. *Op. Cit.*, p. 103.

85 *Idem, Ibidem*, p. 103.

Em um contexto de publicidade comportamental, os problemas enfrentados pelos usuários frente às empresas publicitárias e navegadores de *Internet* são um pouco mais complexos e profundos do que aqueles trabalhados anteriormente, quando se tratava de modo mais abrangente do uso de *cookies*.

Os mesmos princípios e direitos dos usuários são válidos, quais sejam a necessidade de obtenção de um consentimento informado – juntamente com todos seus requisitos de validade inerentes – e a necessidade de uma prestação de informações aos usuários, de forma que sejam alertados das finalidades da coleta de dados, tão como os possíveis usos futuros, das parcerias com empresas terceiras, da abrangência dos *cookies* utilizados, etc. Acima de tudo, deve ser lembrado que o acesso dos usuários aos dados coletados é direito absoluto, e inclui, ainda, eventual modificação, retificação ou exclusão dos mesmos.

Em contrapartida, no outro lado da relação jurídica, é dever das empresas publicitárias, tão como daquelas que coletam e tratam os dados, a aplicação de medidas organizacionais e técnicas para que possa existir uma proteção efetiva das informações contra acidentes e furtos, por exemplo. Ou seja, é necessária aplicação de tecnologia de ponta para a garantia as segurança e confidencialidade das informações existentes[86].

Indo além, em razão do tratamento de dados na publicidade comportamental funcionar através da transformação de dados irrelevantes em informação relevante, o tratamento posterior desses dados deve ser semelhante àquele referente aos dados sensíveis. Em razão disso, para haver o processamento adequado desse tipo de informação, as empresas publicitárias devem obter um consentimento explícito e específico para tal prática, de forma separada daquele necessário para o processamento de dados em geral – que já deve ser dado de forma livre, específica e anterior à coleta dos mesmos, para constituir efetiva manifestação de vontade dos sujeitos[87].

Apesar de ainda não existir uma solução legislativa, deverão ser feitas, assim, duas coletas distintas. Por essa razão, estuda-se que seria mais intuitivo, do ponto de vista dos usuários, o recebimento de uma notificação no *website* visitado (que fará a coleta dos dados), ou ainda, na própria publicidade apresentada ao usuário consumidor (já no campo do dever de informação acerca da publicidade direcionada).

---

86 Artigo 5º, 1, da *GDPR*: Os dados pessoais são: *f)* Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas (integridade e confidencialidade).

87 ARTICLE 29 DATA PROTECTION WORKING PARTY. *Op. Cit.*, p 19.

2.3. Alcançando a civilidade no uso dos *cookies*

Ainda em 1994, ao se deparar com um problema na programação de *websites* relacionado ao *e-commerce*, Lou Montulli buscou uma solução que, à época, era impensável para o campo da *Internet*. Não existia qualquer conceito de memória e armazenamento de informações quando se pensava na *World Wide Web*, não sendo possível qualquer tipo de interação com os materiais disponibilizados. Tudo mudou quando Montulli desenvolveu uma pequena tecnologia capaz de armazenar algumas informações nos próprios navegadores utilizados, com a finalidade de que os usuários consumidores pudessem adicionar itens em seus carrinhos virtuais sem que os mesmos desaparecessem no segundo seguinte, quando saíssem das respectivas páginas. Isso revolucionou o comércio *online*, possibilitando cada vez mais uma interação entre usuário e páginas. Esses *cookies* visavam facilitar um processo que tinha uma atuação deveras limitada, permitindo, então, que as páginas pudessem absorver o modo pelo qual estavam sendo utilizadas, tornando muito mais conveniente para os usurários, vez que não seria necessária uma seleção reiterada dos mesmos itens e preferencias, além de uma nova identificação completa toda vez que se adentrasse em um *website*.

Esse propósito original dos *cookies* acabou por ser subvertido por alguns agentes que descobriram métodos para processar essas informações de modo a rastrear e monitorar o comportamento dos usuários na *Internet*. Isso é feito, conforme já explicado, com a implementação dos *cookies* nos navegadores para que sejam colhidas certas informações, possibilitando a criação de perfis de interesse de consumo. Essas informações vieram a se mostrar extremamente valiosas para a economia atual, expandindo o uso dos *cookies* por empresas imediatas para empresas terceiras, que identificam, agora, que podem utilizá-los para monitorar o comportamento dos indivíduos online e fazê-los de alvo para de publicidade direcionada. Nesse contexto, quando um usuário visita dois websites diferentes, mas que têm a mesma parceria com anunciantes já conhecidos, serão oferecidos os mesmos anúncios específicos para o seu comportamento, de modo que quanto maior a empresa e seu número de parceiros, maior o alcance e potencial de rastreamento, funcionando de uma forma global e unificada.

Atualmente, entretanto, o uso dos *cookies* vai muito além da publicidade direcionada, podendo ser colocado como um dos fatores que contribuíram para o enorme sucesso e popularidade da própria *Internet* nos dias atuais. A *Internet* sem os *cookies* estaria restrita

basicamente a informações gráficas de Teletexto[88], sem qualquer possibilidade de realização de compras *online*, uso de redes sociais, fóruns virtuais, etc. Ou seja, os *cookies* não são uma tecnologia ruim por si só; o que ocorre é que algumas vezes são utilizados de maneira abusiva. Exemplo disso é o caso das grandes empresas internacionais que atuam no âmbito virtual, como *Google* e *Facebook*, que detém informações pessoais e hábitos de navegação que podem de forma extraordinária caracterizar e identificar uma pessoa, muitas vezes relacionando isso ao seu verdadeiro nome. Nesses casos, o simples uso dos *cookies* não é ruim, pois permite que essas empresas se moldem aos seus consumidores, possibilitando uma experiência de navegação infinitamente melhor, em razão da simplicidade e praticidade aplicada, quando comparada àqueles que têm um bloqueio completo da tecnologia como configuração padrão.

Tendo em vista a grave situação de desvantagem informacional do consumidor quando posto ao lado dessas grandes empresas que controlam e utilizam *cookies*, fica gritante a necessidade de uma proteção especial que vise nivelar essa relação. Uma comparação com o Código de Defesa do Consumidor se faz muito bem vida, ao passo que existe uma proteção especial a uma das partes da relação de consumo – o consumidor – que se encontra em uma situação exagerada de desigualdade. Assim, fica claro que quando a informação é trocada entre experts e particulares, tal dever será qualificado, havendo que se pressupor que a outra parte é leiga. Existirá, então, o dever de esclarecimento, aconselhamento e explicação de procedimentos e técnicas que seriam banais e pressupostos entre duas empresas de publicidade, mas não entre um profissional e um imperito, por exemplo[89].

Dessa forma, uma das maneiras de reverter essa situação estabelecida nos últimos anos, qual seja a crescente expansão da técnica de coleta e tratamento de dados para todos os setores do mercado, principalmente no que tange ao uso de *cookies* e dados na publicidade direcionada, poderia ser semelhante àquela solução dada à própria coleta de dados pessoais. Assim, esbarra-se novamente na questão da necessidade de obtenção do consentimento informado anterior, mas vai-se além: não seria suficiente a mera disponibilização de informações em algum lugar do *website* visitado, devendo ser providenciado uma mensagem direta e clara antes do processamento.

---

88 *Teletexto* é um sistema de transmissão de informações textuais e gráficas desenvolvido no Reino Unido, na década de 70, marcado pela simplicidade, em razão da sua carência de detalhes visuais e da não interação com o destinatário.

89 MARQUES, Claudia Lima. **Superação das antinomias pelo diálogo das fontes: o modelo brasileiro de coexistência entre o código de defesa do consumidor e o código civil de 2002.** Revista de Direito do Consumidor, vol.51, 2004, p. 11.

Uma possível solução seria uma alteração no modelo padrão dos navegadores, de modo que a rejeição de *cookies* de terceiros publicitários se torne a regra, vez que não é razoável a suposição de que a vasta maioria dos usuários que têm seus navegadores programados para aceitar os *cookies* exerceu tal escolha de maneira livre e consciente. Desse modo, seria necessária uma ação positiva do usuário para que tal situação se modifique. Uma outra forma de complementar tal dever de informação seria por meio de tutoriais, realizados pelo usuário ao instalar ou atualizar os navegadores, para que possa efetivamente entender e compreender a repercussão do que será realizado[90]. Ressalta-se, novamente, a necessidade de uma cooperação entre os agentes envolvidos, buscando uma forma de disponibilizar informações claras, visíveis e facilmente compreensíveis, não sendo satisfatórios meros avisos genéricos sem referencias explícitas ao conteúdo.

Ainda, de acordo com as diretivas propostas pela *EASA/IAB*[91], é possível que a utilização de um ícone amplifique a atuação das medidas já existentes. Visando a comunicação da situação que ocorre, é apresentado ao usuário um ícone que simboliza e identifica a publicidade comportamental direcionada, que estará ligado à uma página informacional[92] na qual será possível demonstrar interesse em fazer parte, ou não, da rede de dados de certas empresas, que estarão catalogadas como publicitárias[93]. O ícone funcionará como uma informação adicional quando o usuário se deparar pela primeira vez com a publicidade, e como um lembrete que servirá como uma revalidação da vontade colhida quando retornar ao *website* no futuro. Apesar disso, não poderá ser utilizado única e exclusivamente como meio de coleta de consentimento informado quando for anterior à coleta, pois não cumpre, sozinho, os requisitos necessários para a validação da mesma.

Não só no âmbito individual, mas também quando se pensa na sociedade como um todo, a utilização de dados pessoais tem inúmeras finalidades humanitárias, o que abrange análises

---

90 ARTICLE 29 DATA PROTECTION WORKING PARTY. *Op. Cit.*, p 15.

91 A Aliança Europeia de Normativas Publicitárias (*European Advertising Standards Alliance – EASA*) é a voz de autoridade europeia quando o assunto é publicidade e os problemas de auto-regulação dela decorrentes. *IAB* é o Escritório de Publicidade Interativa (*Interactive Advertising Bureau*), que atua na promoção de um ecossistema virtual mais harmônico, através de práticas de regulamentação e mercado na Europa.

92 A página *www.youronlinechoices.eu* trabalha como uma espécie de guia, listando ao usuário europeu todas as empresas publicitárias que fazem parte de seu cadastro, e informando a ele quais delas usam seus dados e de qual forma. É possível optar por excluir-se por completo do banco de dados dessas empresas, sendo todo o processo auxiliado pelo próprio *website*.

93 ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioral Advertising**. 2011, p. 4.

de diagnósticos, mapeamento e levantamento da quantidade e qualidade das moléstias que atingem a população, dentre outros. Isso permite, ao final, uma identificação das necessidades da sociedade, de modo que sejam feitas mais campanhas de prevenção e cuidado em certas áreas mais afetadas, de acordo com a necessidade específica de cada uma. E quando se agrega a tal feito a possibilidade de cruzamento de dados da saúde com dados sociais e econômicos fica cada vez mais possível uma efetiva proteção e desenvolvimento, sendo possível a elaboração de relações de causa e efeito e, consequentemente, maior controle e conhecimento sobre as situações que se verificam. De todo modo, diversos são também os benefícios que o correto tratamento de dados pode trazer para a área médica, como a inovação e o aprimoramento de processos a partir do levantamento de padrões e tendências de saúde pública. Vale destacar, ainda, que os dados pessoas são utilizados amplamente na área da saúde, o que torna esse campo objeto de interesse de estudo. Afinal, desde simples exames aos mais complexos diagnósticos são coletadas informações sobre os pacientes, o que permite a identificação de moléstias e tratamentos adequados.

3. A TUTELA JURÍDICA BRASILEIRA E O DIREITO COMPARADO

3.1. A proteção de dados no ordenamento nacional

Em 2014, o Marco Civil da Internet (MCI – Lei 12.965/14) entrou em vigor no Brasil, estabelecendo princípios, garantias, direitos e deveres para o uso da *Internet* no país. Foi uma forma de reconhecer e regulamentar as novas relações jurídico-virtuais, em razão da existência de inúmeros usuários e provedores, bem como de empresas que trabalham *online*, dado que grande parte não estava adaptada à nova realidade digital. O MCI trata dos delitos praticados *online* (crimes cibernéticos) e da neutralidade da rede, estabelecendo direitos e garantias para liberdade de expressão, e, apesar de cuidar da privacidade, acabou restando uma lacuna sobre o tratamento de dados pessoais, pois não foi dada a devida atenção ao seu uso, destino, comercialização, *etc*.

Com uma clara influência da entrada em vigor do novo Regulamento Geral sobre a Proteção de Dados (RGPD), da União Europeia, e, talvez, dos recentes escândalos de

vazamento de dados[94], foi sancionado o texto que trata do uso de informações pessoais de modo específico no ordenamento nacional, visando desenvolver a proteção da privacidade no meio eletrônico. Com o período de *vacatio legis* de 18 meses, a nova Lei Geral de Proteção de Dados (LGPD) passa a ter eficácia plena em todo território nacional em fevereiro de 2020, consagrando princípios e garantias semelhantes àqueles do Regulamento europeu e reforçando, ainda, o controle do titular sobre seus dados pessoais pela exigência do consentimento, o direito ao acesso e à informação, o direito de retificação e apagamento. Dispõe sobre o modo pelo qual informações pessoais podem ser coletadas e tratadas, seja a partir de cadastros, no fechamento de compras ou até mesmo em imagens publicadas, estabelecendo requisitos para que esses dados possam ser tratados, repassados, publicados e até comercializados.

Vale destacar que, apesar de versar sobre temas similares, o MCI se mantém integralmente vigente, tendo sido alterado apenas naqueles artigos que dizem respeito expressa e especificamente aos dados pessoais, quais sejam os artigos 7, X e 16, II[95].

O direito à privacidade sempre foi uma matriz constitucional na era dos dados físicos e agora recebe a devida estatura legal no ambiente eletrônico, fazendo com que o Brasil passe, então, a integrar o seleto time de países que reconhecem positivamente a relevância dos dados digitais e a necessidade de protegê-los.

Em tempos de *cloud* a transferência internacional de dados é uma realidade – ou melhor, uma virtualidade real[96] – que os localiza em qualquer parte do planeta. Em razão disso, fica explícita uma tendência das legislações dos países de se aproximarem para fomentar uma troca ainda mais intensa e segura de informações, principalmente quando o assunto são os próprios dados pessoais trocados. A LGPD vem, assim, como um primeiro e importante passo para o ingresso definitivo do Brasil no estabelecimento de garantias e na preservação dos direitos fundamentais do novo cidadão que surgiu com o meio digital.

---

94 O mais famoso com o fornecimento de informações de milhares de usuários para a empresa britânica de big data e marketing político Cambridge Analytica.

95 Artigo 7, X, MCI: O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

Artigo 16, II, MCI: Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

96 CAVALCANTI, Eduardo de Hollanda. **Proteção de dados, a vez do Brasil.** Disponível em: *https://www.migalhas.com.br/dePeso/16,MI286295,71043-Protecao+de+dados+a+vez+do+Brasil*. Acesso em 08 de novembro de 2018.

De modo geral, os princípios da *GDPR* são mais específicos e diretos ao assunto do que aqueles da lei brasileira, que tem se mostrado bastante subjetiva. Ficam excluídos de seu alcance, em qualquer das circunstâncias, todos os processos de tratamento de dados para fins jornalísticos, artísticos, acadêmicos, de segurança publica, defesa nacional, segurança do Estado ou de atividades de investigação e repressão de infrações penais.

De plano, é possível afirmar que o consentimento é a palavra chave para o tema em ambas as legislações, de forma que sem consentimento do titular dos dados ou informações pessoais, o controlador[97] dos dados não poderá manipulá-los. Deverá, desse modo, ser obtido nos mesmos moldes da *GDPR*, com o adicional do interesse legítimo, que funciona como uma motivação para a coleta dos dados (algo que se assemelha ao princípio da finalidade). Quando se fala em consentimento de crianças, assim como na norma europeia, o tratamento deve ser feito com o consentimento de ao menos um dos pais ou responsável legal, de modo prévio. Importante dizer que em determinados casos o uso da anonimização é obrigatória, conforme a lei nacional.

Na *GDPR*, não há menção alguma de comercialização das informações pessoais protegidas, se mostrando um tema que – talvez – devesse ser estudado de forma mais profunda antes de uma positivação de tal cunho. Apesar disso, existe previsão na LGPD que permite eventual comercialização de dados sensíveis na forma como são coletados, tendo como única limitação a finalidade obtenção de vantagem econômica e a autorização da agência ou estatal supervisora.

Um dos pontos mais importantes para a eficácia da nova lei, embora vetado do projeto originalmente aprovado[98], é a criação de uma autoridade supervisora fiscalizadora, a Agência Nacional de Proteção de Dados (ANPD). A autarquia (órgão público com personalidade jurídica de direito público indireta) deve ser ligada ao Ministério da Justiça, que deverá fiscalizar e garantir a aplicação da lei. De outro ponto de vista, a *GDPR* se mostrou mais flexível, permitindo um ou mais órgãos de fiscalização para cada estado-membro do bloco

---

97 Tal termo [controlador] é usado, no Brasil, de forma generalizada para tipificar a responsabilidade pelo tratamento dos dados em quaisquer órgãos ou instituições públicas ou privadas. A *GDPR*, contudo, criou o cargo *Data Protection Officer (DPO)* para ser essa função, que nada mais é do que um encarregado, dentro de cada empresa ou entidade que responde juridicamente por coleta de dados, por receber as reclamações dos titulares, prestar esclarecimentos, adotar providências, dialogar com autoridade nacional, orientar funcionários, *etc.*

98 O motivo foi de caráter técnico: o governo entendeu que poderia existir vício de inconstitucionalidade na criação, já que esta foi recomendada pelo legislativo (por meio do Projeto de Lei), e não uma manifestação própria do executivo. A proposta é que a agência seja independente, com orçamento próprio e capaz de fiscalizar e impor multas, dialogar com empresários de diferentes setores e estabelecer diretrizes para aquelas partes da lei que desentendem de maior direcionamento e interpretação.

europeu, que deverão manter a comunicação dos seus atos com a Comissão Europeia, não concentrando todo o poder de fiscalização nas mãos de um só órgão.

Em caso de descumprimento da lei, poderá haver a aplicação de advertências e/ou multas, que pode variar de 2% do faturamento da empresa, conglomerado ou grupo no Brasil no seu último exercício, limitando-se em 50 milhões de reais por infração.

Percebe-se que as sanções administrativas impostas pela lei brasileira são quase uma reprodução exata da *GDPR*, preservando sua diferença entre na maneira como as sanções foram impostas. Na *GDPR* as faltas e penalidades são claras e devidamente multadas, enquanto na LGPD é nítida a falta de clareza nas penalidades impostas aos agentes infratores, existindo lacuna, inclusive, quando se trata de determinar a cumulatividade das penas quando examinadas as condutas. Ademais, mesmo após escândalos relacionados à criptografia do caso Whatsapp, a LGPD não fez qualquer menção ao tema, assunto que é disciplinado objetivamente nos artigos 6, 32 e 34 da *GDPR*. Isso, juntamente com alguns outros temas importantes, tais como a questão da transparência das regras e dos dados e de práticas de *geo-pricing* e *geo-blocking*, bastante utilizadas atualmente, aumenta ainda mais a lista de temas que não tiveram a devida atenção na nova legislação.

No que diz respeito à transferência internacional de dados, será possível para todos os países que apresentem legislação de proteção de dados adequada àquela prevista no ordenamento nacional, ou seja, igual ou mais rigorosa. E isso independe de onde o tratamento de dados é feito: a norma vale para todas as operações de tratamento de dados nas quais a coleta de dados tenha sido feita em território nacional. Sendo caso de transferência de dados para uma filial ou sede estrangeira, a condição é de que o país de destino também tenha leis abrangentes de proteção de dados ou possa garantir mecanismos de tratamento equivalentes aos que são exigidos no Brasil. Não sendo mais necessários – quando uma conta ou serviço tiver sido finalizado, por exemplo – a organização tem o dever apagá-los, a menos que haja alguma obrigação legal ou outra razão justificável para a sua preservação.

As transferências são realizadas com base em uma decisão de adequação[99] (em conformidade com o artigo 45 da *GDPR*), sendo o método mais simples de implementar uma

---

[99] A decisão de adequação é dada pela Comissão Europeia ao considerar que um país, território ou organização internacional fornece um nível de proteção de dados suficientemente adequado aos padrões estabelecidos, a partir de uma avaliação periódica que avalia, dentre outros critérios, o respeito pelos direitos humanos e liberdades fundamentais, a existência e o funcionamento efetivo de autoridades de controle da proteção de dados e o compromisso do Estado em relação à proteção de dados. Atualmente, os países incluídos na lista da Comissão são Andorra, Argentina, Canadá (em relação às organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça, Uruguai e Estados Unidos (limitado ao

exportação de dados, uma vez que não há necessidade de autorização específica da autoridade supervisora para tanto ou de apresentação de demais garantias toda vez que for necessária realizar uma transferência internacional de dados. Logo, a transferência para um país terceiro considerado adequado se assemelha a uma realizada entre países da União Europeia, justamente em razão dessa garantia de segurança dada.

Assim, a correta implementação da LGPD projetará o Brasil como país que se preocupa e regulamenta a proteção dos dados pessoais, seguindo a tendência internacional capitaneada pela *GDPR*. Embora a lei brasileira, por si só, não garanta de imediato a transferência transfronteiriça de dados pessoais da Europa para o Brasil, futuramente ela poderá ser levada em consideração pela Comissão Europeia para avaliar se existe garantia de um nível de proteção adequado. Assim, tanto o responsável pelo tratamento (*data controller*, ou controlador), quanto o subcontratante (*data processor*, ou processador) precisam estar adequados não só com a LGPD, mas também com a *GDPR*, caso haja interesse em exportar dados pessoais para fora da União Europeia. Ou seja, todas as empresas de pequeno, médio e grande porte que têm, por algum motivo, interesse no tratamento de dados pessoais, terão que investir em cibersegurança e implementar sistemas de *compliance* efetivos para prevenir, detectar e remediar violações de dados pessoais, notadamente em razão da previsão de que a adoção de política de boas práticas será considerada como critério atenuante das penas, em caso de eventual responsabilização.

3.2. Regulamentação no direito comparado – União Europeia

Como uma evolução legislativa, o Regulamento Geral da Proteção de Dados (*General Data Protection Regulation – GDPR*) – Regulamento 2016/679, entrou em vigor em maio de 2018, após 2 anos de *vacatio legis*, para substituir a antiga Diretiva 95/46/CE, visando a harmonização das leis de proteção de dados dos países da União Europeia, ratificando a importância fundamental da circulação de dados nas sociedades atuais para as empresas, associações e entes públicos. O Regulamento alerta para o aumento exponencial do tratamento de dados pessoais associado ao desenvolvimento das tecnologias de informação e à necessidade de adaptação de seus princípios a um mundo que cada vez mais depende da coleta e do tratamento de dados na *Internet* e fora dela. Mostra, ainda, a necessidade de harmonizar a

---

Privacy Shield). O Japão e a Coréia do Sul estão sob análise da Comissão e, a depender do resultado, poderão ser objeto de decisão de adequação no porvir.

crescente utilidade e conveniência de tratamento desses dados com as liberdades e direitos fundamentais, tendo por objetivo reforçar e unificar a proteção de dados pessoais na União Europeia (UE), especificando direitos e obrigações correspondentes. Exemplo disso é a própria definição de *dado pessoal*, que se mostra muito mais detalhada, tratando com tal aquele cuja informação seja relativa a uma pessoa singular identificada ou identificável – titular dos dados, sendo considerada identificável todos aqueles que possam ser identificados, direta ou indiretamente, em especial por referência a um identificador, que pode ser um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.

O regulamento objetiva, ainda, no artigo 99, uma proteção de dados pessoais mais homogênea na Europa, por isso a opção por uma norma com aplicação direta nos Estados-membro, e não apenas a definição de parâmetros para futuras leis internas. Suas normas, por tomarem a forma de um *Regulamento* ao invés de uma *Diretiva*, tem efeito vinculativo aplicável a todos os Estados-Membros, mas garante a estes, todavia, certa margem de autonomia para a elaboração de disposições específicas para adaptar e efetivar a aplicação interna das regras previstas, empoderando os órgãos nacionais de proteção de dados e impondo novas obrigações às instituições que tratam dados.

Dos princípios

O artigo 5º da *GDPR*, em consonância com o já era consagrado na diretiva anterior, estabelece o princípio da licitude, lealdade e transparência (*Lawfullness, Fairness & Transparency*) como sendo o orientador de um tratamento de dados pessoais precedido pelo consentimento do titular – ou por hipóteses expressamente previstas na normativa, sempre pautado pela lealdade e transparência. Prevê o princípio da exatidão (*Accuracy*), que determina a correção e atualização dos dados pessoais armazenados, e os princípios da finalidade, adequação e de limitação de conservação (*Purpose Limitation, Data Minimisation & Storage Limitation*), que vinculam o tratamento de dados a finalidades específicas, e exigem que seu tratamento e conservação sejam proporcionais, adequados e pertinentes às finalidades para as quais serão processados, visando a diminuição da quantidade de dados, coletando apenas aqueles que sejam essenciais para o produto ou serviço ofertado. Ainda, o princípio da segurança, integridade e confidencialidade (*Integrity and Confidentiality*), voltados à garantia jurídica e técnica de um tratamento e armazenamento seguros e com garantia de confidencialidade; e, por fim, princípio da prestação de contas ou responsabilização

(*Accountability),* que faz com que as organizações implementem medidas técnicas e organizacionais apropriadas, e sejam capazes de prestar contas e demonstrar sua eficácia, quando solicitadas. Esses princípios fundamentam o direito a receber informações claras e transparentes sobre a coleta, uso e circulação desses dados, o direito de acesso, de retificação e de apagamento dos dados pessoais, e direito de controle sobre os dados pessoais que vão além do direito de decidir sobre o acesso imediato e se estende aos usos futuros desses dados.

Dessa forma, fica clara, mais uma vez, a enorme influência da doutrina e jurisprudência alemã, tão como a espanhola e portuguesa, no que diz respeito à autodeterminação informativa[100], reconhecendo ao indivíduo o poder de decidir sobre a utilização de suas informações pessoais não somente como um direito de defesa, de vedar o acesso, mas também de controlar o fluxo desses dados. Toma, assim, a forma de uma liberdade de dispor de suas informações pessoais, ou ainda, de um poder de controle cujo exercício permitirá a cada um dos indivíduos que o exerce, preservar sua identidade informática[101].

Da territorialidade

Um dos principais aspectos da *GDPR* é a preocupação em proteger a privacidade das pessoas que se encontram no território da União Europeia. Assim, quanto ao titular dos direitos aqui tratados, em razão da própria natureza dos dados pessoais e de sua capacidade de difusão, o conceito de territorialidade é ampliado. A *GDPR* é, afinal, aplicável aos indivíduos que residem no território da UE bem como àqueles que lá se encontram apenas transitoriamente, sejam cidadãos europeus ou não. Quanto às empresas, será aplicada quando o tratamento dos dados ocorrer no contexto das atividades daquelas estabelecidas na UE, independentemente do local do tratamento e da nacionalidade dos titulares dos dados, ou quando o tratamento de desses dados for realizado por empresa externa, desde que ofereça bens e serviços, ainda que de forma gratuita, ou monitore o comportamento de pessoas naturais que lá se encontram.

Do consentimento

De modo geral, a *GDPR* apresenta regras mais abrangentes do que as anteriormente vigentes na UE, reforçando a proteção aos usuários de internet e assegurando aos titulares de dados maior controle sobre seus dados. Dentre tais mudanças destaca-se a maior especificidade

---

100 *Cf.* tópico 3.2, que trata da decisão da suprema corte alemã acerca do direito à autodeterminação informativa.

101 CASTRO, Catarina Sarmento. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005, p. 28.

em relação aos requisitos do consentimento na coleta e tratamento de dados pessoais. Os titulares de dados têm direitos oponíveis perante as empresas e devem consentir não apenas inequivocamente, mas expressamente sobre a transferência dos seus dados, por meio de uma declaração ou ação afirmativa, mantendo seu consentimento mesmo após ser devidamente informado sobre os riscos envolvidos em tais transferências. O artigo 6º da *GDPR* estabelece que o tratamento somente será lícito e legítimo se o titular dos dados tiver dado o seu consentimento específico para o tratamento dos seus dados pessoais. De forma complementar, assegura o direito de revogação do consentimento a qualquer momento, sendo garantida a mesma facilidade para retirada quanto para sua concessão.

O quadro geral dado pelo regulamento nos permite concluir que o consentimento do titular ocupa lugar central na proteção de dados pessoais, apesar de não esgotar a regulação jurídica da matéria. Há dados que não estão incluídos no âmbito de tutela do direito à proteção dos dados pessoais, tais como os anônimos, os relativos a investigação e persecução criminal, e os que digam respeito à segurança pública, nacional e comunitária. E mesmo em relação aos dados protegidos pelo regulamento, estão previstas hipóteses de dispensa do consentimento para tratamento de dados, quando voltados ao atendimento do interesse público relevante (por exemplo, para formulação de políticas públicas, gestão e fornecimento de serviços públicos, segurança), ou que seja justificado pelo interesse legítimo de quem realiza o tratamento (como é caso dos serviços de proteção ao crédito, cadastros de consumidores, dentre outros). Assim, a tutela da privacidade e dos dados pessoais não opera mais, unicamente, na lógica da informação sigilosa em contraposição à informação revelada pelo titular.

É necessário, ainda, que esse consentimento seja obtido por uma resposta afirmativa do titular indicando sua manifestação de vontade livre, específica, inequívoca e informada, no sentido de que concorda que seus dados pessoais sejam objeto de tratamento. Ou seja, a obtenção do consentimento deve ser feita de forma explícita, numa linguagem clara e simples, inclusive quando feita na forma eletrônica e por *check mark* e, nos casos em que o tratamento sirva para diversas finalidades, deverá ser dado um consentimento específico para cada uma delas, conforme previsão do artigo 7º. Portanto, como já demonstrado[102], a política de consentimento deve ser sempre a do *opt-in*, não sendo mais aceito o *opt-out*. Em casos

---

102 *Cf.* tópico 2.2.1.2., Dever de obtenção de consentimento informado anterior, que trata do assunto de forma específica.

específicos, como no tratamento de dados sensíveis[103], transferência internacional[104] e decisões automatizadas[105], o consentimento exigido pela *GDPR* se mostra ainda mais rigoroso. O silêncio, as opções pré-validadas ou a omissão não são mais considerados meios apropriados para a obtenção de consentimento. De modo geral, as novas regras condicionam o desempenho dessas atividades ao aceite livre e informado, feito de uma maneira inequívoca para que não haja dúvidas acerca da sua real intenção.

Dos dados sensíveis

Em princípio o tratamento dessas categorias especiais é vedado. Entretanto, o próprio Regulamento elenca dez diferentes hipóteses em que tal vedação é excluída, podendo os dados sensíveis ser objeto de tratamento, primeiro, nos casos em que haja consentimento explícito do seu titular, ou em que este tenha os tornado, previamente, públicos (artigo 9º, 2, *a* e *e*), ou em caso de interesse público ou social relevante (artigo 9º, 2, *b*, *f*, *g*, *h*, *i* e *j*), de interesse legítimo de entidades sem fins lucrativos, em relação a seus membros, ou antigos membros, ou pessoas que mantenham com elas contato regulares relativos a seus objetivos (artigo 9º, *d*), e de proteção de interesses vitais do próprio titular ou de outra pessoa, se o titular estiver impossibilitado física ou legalmente de manifestar sua vontade (artigo 9º, *c*).

Quanto à sua definição, são tidos como sensíveis aqueles dados que se enquadram em alguma das categorias a previstas, quais sejam: origem racial ou étnica; opiniões políticas; crenças religiosas ou filosóficas; filiação sindical; saúde ou vida sexual e orientação sexual; ou dados genéticos e dados biométricos para fins de identificação pessoal. Fica claro, então, que, em razão de serem capazes de revelar informações de cunho íntimo e que, quando combinados, são capazes de identificar individualmente seu titular, é necessária uma camada extra de proteção a esses dados, devendo o consentimento ser livre, explicito, inequívoco, informado e específico.

---

103 O art. 9, da *GDPR* coloca como regra geral é proibido o tratamento de dados pessoais especiais (sensíveis), abrindo exceções para os casos em que haja consentimento específico do titular, ou que seja necessário para alguma das finalidades ali elencadas.

104 O art. 49, da *GDPR* prevê que, em regra, só será possível a transferência internacional de dados quando houver consentimento explícito do titular, ou nos casos em que seja necessária, conforme hipóteses descritas no artigo.

105 O art. 22, da *GDPR* dá o direito ao titular dos dados de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar, excetuando tal situação apenas nos casos em que houver consentimento explícito e específico, para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento ou quando previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados.

Das decisões automatizadas

O Regulamento prevê o direito dos titulares dos dados de obterem uma explicação para qualquer decisão feita por algoritmo, tão como o direito de optar pela não-coleta de dados nesses casos. Portanto, o titular de dados terá, via de regra, o direito de não se sujeitar a decisões tomadas exclusivamente com base em tratamento automatizado, o que é previsto no artigo 22 do Regulamento. As exceções a esse direito restringem-se às hipóteses nas quais o titular de dados tiver dado consentimento explícito, o uso for autorizado por lei da União Europeia ou do Estado Membro a que o responsável pelo tratamento estiver sujeito ou, ainda, caso o processamento seja necessário para a celebração ou execução de contrato entre o titular dos dados e o responsável por seu tratamento. O objetivo é justamente explorar meios diversificados para fornecer um maior grau de transparência sobre como os algoritmos tomam decisões que impactam a vida do indivíduo.

Da transferência internacional

Em razão da mitigação das fronteiras físicas trazida pela tecnologia moderna, que criou um mundo digital ilimitado, a aplicabilidade das leis, principalmente no que se refere àquelas referentes à própria *Internet*, apresenta um desafio especial quando deve ser feita fora de uma jurisdição. É o que acontece com o Regulamento aqui tratado, que tem aplicação em território europeu, mas acaba por produzir efeitos sobre cidadãos e empresas sediadas em outros países, em razão de seu efeito viral e amplo alcance. Como consequência, uma exigência importante da *GDPR*, no que diz respeito à transferência internacional de dados, é a sujeição das empresas que detém os dados a um sistema de gestão e tutela, para que seja possível a transmissão dessa informação apenas a quem garanta medidas adequadas de proteção. Ou seja, os responsáveis pelo tratamento de dados deverão assegurar que terceiros contratados também operem de acordo com as regras estabelecidas. Com isso, países fora da UE e organizações internacionais podem ser destinatários de uma transferência de dados desde que seja assegurado um nível de proteção adequado, e isso é feito por meio de uma avaliação prévia realizada pela Comissão Europeia, levando em conta diversos elementos do ordenamento em questão. Em caso de eventual transferência para país não aprovado, é necessário que os responsáveis pelo tratamento realizem diversas *garantias de adequação* para que se mostrem adequados ao tratamento de dados.

A ideia central do Regulamento é garantir uma proteção ampla a todos os indivíduos que tiverem seus dados coletados de alguma forma por empresas ou instituições que realizam transferência de internacional dados, e isso acaba afetando a política de uso de muitas empresas

cujas bases encontram-se no território da UE (mesmo com sede no exterior), ou mesmo àquelas destinatárias de seus dados, e a não adaptação será mais um obstáculo ao seu desenvolvimento, bem como um enfraquecimento da competitividade e da inovação na economia local. É justamente em razão disso isso que se mostra cada vez mais necessário que seus parceiros comerciais e fornecedores de dados também cumpram as normas do Regulamente, sob pena de reduzir ou cessar o fluxo de negócios e dados com as mesmas. Mais do que isso, o ambiente de negócios internacional envolvendo dados tenderá a gravitar progressivamente em torno daquelas que cumprem a *GDPR*[106].

Dos riscos e responsabilidades

A partir do momento em que se inicia o tratamento de dados, as empresas devem levar em conta o tipo de dado que está sendo tratado para adotar as medidas técnicas e organizacionais compatíveis com o risco a que os titulares desses dados estão sujeitos. Quanto mais sensível for o dado pessoal tratado, maior deve ser a preocupação com os riscos à privacidade e direitos fundamentais do titular dos dados. O objetivo dessas previsões do Regulamento, mais especificamente os artigos 24 e seguintes, juntamente com os princípios supracitados, é garantir que os dados pessoais não sejam tratados para qualquer fim, sem o consentimento do usuário e por um número indefinido de pessoas. Ou seja, apenas os dados pessoais necessários para cumprir determinado serviço devem ser coletados.

O responsável pelo tratamento dos dados tem a obrigação e a responsabilidade não só de aplicar as medidas técnicas e organizacionais necessárias para a proteção dos dados tratados, mas também de demonstrar que todos os processos do tratamento de dados estão de acordo com o Regulamento. A *GDPR* exemplifica o que pode ser considerado evidência de *compliance*, como documentos e logs de controle. De forma ainda mais específica, caso a empresa tenha mais de 250 funcionários ou o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, o responsável pelo tratamento deve manter os registros de tratamento sob a sua responsabilidade e deve cooperar com a autoridade de proteção de dados, disponibilizando os registros, quando necessário, para fiscalização das operações de tratamento. Empresas que tenham como núcleo da atividade operações de tratamento que

---

106 De acordo com o estudo "*The end of the beginning - Unleashing the transformational power of GDPR*"[2] da IBM, realizado com 1,5 mil líderes de negócios em 34 países, antes de sua entrada em vigo, 60% das organizações está adotando a *GDPR* como uma oportunidade para melhorar a privacidade, a segurança e o gerenciamento de dados ou como um catalisador de novos modelos de negócios, em vez de simplesmente um problema ou impedimento de conformidade. 96% acreditam que a prova de conformidade com a *GDPR* será vista como um diferenciador positivo para o público. 76% disseram que a *GDPR* permitirá relacionamentos mais confiáveis com os titulares de dados, que criarão novas oportunidades de negócios.

exijam um controle regular e sistemático de dados em grande escala, ou tratem de dados sensíveis ou dados pessoais relacionados com condenações penais e infrações, é obrigatória a indicação de um encarregado pela proteção de dados pessoais (*Data Protection Officer*), que terá diversas atribuições, dentre elas exercer o controle sobre o cumprimento do Regulamento e responder requisições da autoridade de proteção de dados e de outros órgãos governamentais. Em caso eventual de vazamento de dados, as empresas têm a obrigação de avisar as autoridades competentes em até 72 horas após tomar conhecimento do fato, a não ser que o vazamento não demonstre risco aos direitos e privacidade dos titulares dos dados.

As autoridades de controle, além da competência para investigar os responsáveis pelo tratamento de dados pessoais, podendo requisitar informações, acessar as instalações da empresa, e determinar o cumprimento de medidas relativas ao cumprimento do regulamento, também têm a prerrogativa de impor sanções administrativas, que podem chegar até 20 milhões de euros ou 4% do faturamento anual da empresa em nível mundial.

Do direito ao apagamento

Denominado pela *GDPR*, *Right to Erasure,* o melhor chamado Direito ao Apagamento, em português, foi contemplado de forma explícita pelo atual Regulamento. O artigo 17, o dispositivo elenca diversas hipóteses não exaustivas em que o *Right to Erasure* poderá ser requerido, por exemplo, nas hipóteses em que os dados deixam de ser necessários em relação à finalidade que motivou a sua coleta e quando o titular dos dados retira o consentimento sobre o qual é baseado o tratamento. A garantia fundamenta-se na premissa de que o titular de dados pessoais deve ter o direito de dispor dos dados sobre ele coletados, a fim de retificá-los, se assim desejar. Mas, a disposição vai além: o titular possui um "direito a ser esquecido", em casos nos quais a retenção de tais dados infrinja o Regulamento ou a legislação da União ou Estado Membro a que o controlador está sujeito. No entanto, nota-se uma ampliação desproporcional do instrumento. Isto porque o conceito "tradicional" de direito ao esquecimento pressupõe uma ponderação mais cuidadosa dos critérios específicos, a fim de não ferir a liberdade de expressão e o acesso à informação. Já o *Right to Erasure* não apresenta tais critérios e, uma vez que requerido e concedido, a análise será feita pelo próprio responsável pelo tratamento, naquilo que couber. Ou seja, a *GDPR* inclui hipóteses de remoção muito amplas, ao mesmo tempo que deixa aos particulares a decisão daquilo que irão "apagar", a depender do que for alegado pelo titular dos dados.

3.3. Direito à autodeterminação informativa na decisão da Corte Constitucional Alemã

A expressão *autodeterminação informativa* foi utilizada pela primeira vez pelo Tribunal Federal Constitucional Alemão (*Bundesverfassungsgericht – BVerfG*), ao julgar inconstitucional a "Lei do Recenseamento" (*Volkszählungsgesetz*), em 1983. Apesar de a Lei Fundamental (*Grundgesetz - GG*) alemã não conter expressa previsão do direito fundamental de o indivíduo opor-se ao uso não consentido da informática para o tratamento de seus dados – que dizem respeito às convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica – e à cessão destes dados a terceiros, conforme ocorria com as Constituições da Espanha[107] e Portugal[108], o Tribunal reconheceu a existência de um direito de origem constitucional (*Grundrecht*), próprio à salvaguarda desses interesses[109].

A referida *Volkszählungsgesetz* previa ampla coleta de dados dos cidadãos alemães, num total de cento e sessenta perguntas, objetivando a coleta de dados referentes à profissão, moradia e local de trabalho, com intuito de fornecer à administração pública informações acerca do crescimento populacional, da distribuição espacial da população pelo território e das atividades econômicas realizadas no país, impondo-lhes, inclusive, a obrigação de resposta sob pena de sanção pecuniária. Os dados aferidos seriam utilizados não apenas com o fim de estabelecer padrões estatísticos, mas também para o desenvolvimento de atividades administrativas. Eram feitas, ainda, cessões a terceiros que não estavam especificadas pela lei, como a transmissão anônima para órgãos da administração federal.

Dessa forma, foram ajuizadas diversas reclamações demostrando a violação dos artigos 1 e 2, da Lei Fundamental[110], o que culminou na declaração de nulidade, pelo Tribunal, dos

---

107 A Constituição da República Espanhola, de 1978, trata, em seu artigo 10, dos direitos fundamentais à dignidade da pessoa humana e ao livre desenvolvimento da personalidade, e em seu artigo 18 elenca os direitos fundamentais à intimidade, à inviolabilidade de domicílio e ao segredo das comunicações, inclusive no campo da internet. Este feixe de direitos, que permite ao indivíduo exercer controle sobre os seus próprios dados e sobre a atividade estatal a respeito, é também designado pela doutrina de *direito fundamental à autodeterminação informativa.*

108 A Constituição da República Portuguesa de 1976, nos artigos 26, nº1, 28 e 34, traz cláusulas de proteção à intimidade da vida privada, de informações relativas a pessoas e famílias e da vedação à utilização abusiva ou contrária à dignidade humana. No seu artigo 35 cuida do direito de o indivíduo manter o controle sobre os seus dados pessoais, por meio do exercício do direito de acesso, retificação, atualização e do direito ao conhecimento das finalidades para as quais foram captados esses dados.

109 NAVARRO, Ana Maria Neves de Paiva. **O direito fundamental à autodeterminação informativa**. Departamento de Pós-Graduação UFRJ, LETACI. Rio de Janeiro, 2011, p. 11.

110 Artigo 1 [Dignidade da pessoa humana – Direitos humanos – Vinculação jurídica dos direitos fundamentais]: (1) A dignidade da pessoa humana é intangível. Respeitá-la e protegê-la é obrigação de todo o poder público. (2) O povo alemão

dispositivos que determinavam a comparação dos dados coletados, bem como a sua transferência para outros órgãos da administração.

A Corte afirmou que o moderno processamento de dados pessoais configura uma grave ameaça à personalidade do indivíduo, na medida em que possibilita o armazenamento ilimitado de dados, bem como permite a sua combinação irrestrita, de modo a formar um retrato completo da pessoa sem a sua participação ou conhecimento. Nesse contexto, entendeu que o elenco de dados classificados como sensíveis não resguardaria adequadamente o indivíduo diante da nova realidade tecnológica, pelo fato de não existir dado pessoal sem importância, não sendo possível subtrair nenhuma categoria de dados à disciplina jurídica, visto que as modernas tecnologias informáticas tornam possível extrair de dados aparentemente insignificantes informações mais delicadas. Argumentou, ainda, que a Constituição alemã protege o indivíduo contra o tratamento indevido de dados pessoais por meio do direito fundamental ao livre desenvolvimento da personalidade, segundo o qual o indivíduo tem o poder para determinar o fluxo de suas informações na sociedade[111]. Dessa forma, atendendo ao direito neonato, estabeleceu-se que os indivíduos devem possuir o poder de controlar a legitimidade do recolhimento, da divulgação e da utilização dos seus dados pessoais.

A a partir dessa construção jurisprudencial do *BVerfG* alemão é possível observar uma convergência de legislações voltadas à proteção desses dados nos Estados-membros da então Comunidade Europeia, de forma que as sucessivas Diretivas da Comunidade Europeia e legislações nacionais criaram apropriados instrumentos de manejo em tema de proteção de dados pessoais, fazendo com que se passasse a chamar o *direito à autodeterminação informativa* de *direito à proteção de dados pessoais.*

O grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais se baseia em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado. Ou seja, a decisão do tribunal criou um precedente que limitou o poder legislativo, fazendo com que o mesmo passasse a estar vinculado à configuração de um direito à autodeterminação da informação e, acima de tudo, à própria Lei Fundamental. Por fim, pode-se dizer que a decisão logrou demonstrar a fragilidade dos sistemas de proteção de dados pessoais baseados apenas em normas infraconstitucionais,

---

reconhece, por isto, os direitos invioláveis e inalienáveis da pessoa humana como fundamento de toda comunidade humana, da paz e da justiça no mundo. [...]

Artigo 2 [Direitos de liberdade]: (1) Todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral. (2) Todos têm o direito à vida e à integridade física. A liberdade da pessoa é inviolável. [...]

[111] MENDES, Laura Schertel. *Op. Cit.*, p. 47.

evidenciando a importância do reconhecimento constitucional de um direito subjetivo fundamental do cidadão, cujos dados pessoais são objeto de tratamento[112].

112 MENDES, Laura Schertel. *Op. Cit.*, p. 49.

4. CONCLUSÃO E RECOMENDAÇÕES

Em razão das modificações sociais e da evolução tecnológica que vêm ocorrendo nos últimos anos, a discussão sobre os danos causados pelo processamento de dados pessoais não se restringe mais apenas à ameaça do abuso do poder pelo Estado, mas abrange, principalmente, o setor privado, que utiliza massivamente dos dados pessoais para atingir seus objetivos econômicos. A combinação de diversas técnicas automatizadas permite a obtenção de informações sensíveis sobre os cidadãos, o que passa a fundamentar a tomada de decisões econômicas, políticas e sociais nos mais diferentes contextos. Destaca-se a técnica de construção de perfis pessoais, a partir dos quais podem ser tomadas decisões a respeito dos cidadãos que afetam diretamente suas vidas e influenciam seu acesso a oportunidades sociais e mercadológicas. Crescem, portanto, os riscos à personalidade do cidadão, na medida em que esses perfis representam informações fragmentadas e descontextualizadas, que podem ser utilizadas de modo a prejudicar a liberdade e as chances do indivíduo na sociedade. Esses riscos, ampliados pela irrestrita utilização da tecnologia da informação, tornam imperativa uma regulamentação jurídica da matéria.

Atualmente, o tratamento de dados pessoais de forma autônoma nas legislações pode ser visto como uma tendência em diversos ordenamentos jurídicos, de forma que as leis gerais de proteção de dados pessoais vêm se firmando como umas das formas mais eficazes maneiras

de se proteger a privacidade nos países mais desenvolvidos, em razão de nelas se estabelecem os princípios gerais para o tratamento de dados, os direitos subjetivos dos titulares dos dados pessoais, as limitações e as obrigações dos responsáveis pelo tratamento de dados, bem como a criação de autoridades administrativas competentes para a implementação eficaz da legislação. Emerge, assim, uma realidade que não comporta apenas uma proteção genérica à intimidade e da vida privada, não bastando mais que sejam elaboradas legislações baseadas naquele conceito antigo de um direito geral e flexível sobre a proteção da privacidade, válido para todas as situações numa sociedade em mutação.

No contexto brasileiro, o Código de Defesa do Consumidor, juntamente com o Marco Civil da Internet e a própria Constituição Federal, eram as normas que ofereciam a tutela aos indivíduos que tinham suas informações armazenadas em bancos de dados e cadastros de consumo via *Internet*. No entanto, como consequência da iniciativa de diversos outros países europeus, se mostrou de extrema importância a edição de uma Lei Geral de Proteção de Dados (Lei 13.709/18) que protegesse de forma mais efetiva e generalizada os dados pessoais armazenados ou em circulação, aumentando a privacidade de dados pessoais e o poder das entidades reguladoras para fiscalizar organizações (não se limitando, assim, aos dados pessoais utilizados em ambiente virtual). O próximo passo seria a criação de uma efetiva cultura jurídica apta a compreender os dados não só como um direito autônomo, mas também de caráter fundamental. O caminho a ser seguido seria aquele trilhado por diversas outras legislações, implementando uma autoridade independente para tutelar os dados pessoais dos usuários, na forma de um organismo central de proteção de dados, dotado de legitimidade normativa, responsável pela tutela dos dados pessoais na sociedade – o que acabou não sendo possível na edição da referida lei, em razão do veto legislativo no que dizia respeito à criação de uma entidade administrativa reguladora. Mas não apenas, cumpre, estabelecer uma arquitetura regulatória capaz de fazer emergir o tema da proteção de dados pessoais como um verdadeiro setor de políticas públicas, composto também por instrumentos estatutários, sancionatórios, bem como por um órgão administrativo responsável pela implementação e aplicação da legislação. Isso exige, conforme exposto, instrumentos legais próprios, órgãos reguladores específicos, uma rede de especialistas e juristas, um robusto grupo de ativistas dispostos a demonstrar todo tipo de abuso e violações, uma crescente comunidade acadêmica especializada

no tema, bem como uma rede internacional, pela qual se realiza o intercâmbio de experiências e ideias[113].

Tais medidas podem ser utilizadas, ainda, com uma segunda finalidade: regular o uso de *cookies* nos navegadores de *Internet*. Esbarra-se novamente na questão da necessidade de obtenção do consentimento informado anterior, a exposição de motivos e finalidades, a utilização de uma linguagem clara e direta, etc. Os exemplos aqui tratados, quais sejam a legislação da União Europeia e a legislação brasileira, têm previsão expressa de como deve ser feita a coleta desses dados, mas nenhuma delas adentra nas minuciosidades da informática, no que diz respeito às técnicas de uso de *cookies*. Isso faz com que a aplicação e efetivação de uma norma de tal cunho seja dificultada, em razão da amplitude de termos e generalidade das medidas previstas, não existindo soluções concretas que possam ser de plano aplicadas e fiscalizadas.

Assim, novamente, a solução está na implementação de textos adicionais que tratem do tema de maneira ainda mais específica, pormenorizando termos e práticas já utilizadas, de modo a efetivamente regulamentar as práticas que são utilizadas corriqueiramente pelos provedores e navegadores *online*[114].

---

113 MENDES, Laura Schertel. *Op. Cit.*, p. 147.

114 *Cf.* tópico 2.3, que trata da civilidade no uso dos *cookies* e expõe possíveis medidas que tornariam seu uso mais aceitável.

REFERÊNCIAS BIBLIOGRÁFICAS

ABRAMS, Martin. **Boxing and concepts of harm**, *in*: Privacy and Data Security Law Journal, 2009.

ARTICLE 29 DATA PROTECTION WORKING PARTY**. Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioral Advertising**. 2011.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 2/2010 on online behavioral advertising.** 2010.

ASCENSÃO, José de Oliveira. **Direito civil: teoria geral.** São Paulo: Saraiva, 2010. Vol. 1**.**

BOBBIO, Norberto. **A era dos direitos**. 7ª edição. Rio de Janeiro: Elsevier, 2004.

CASTRO, Catarina Sarmento. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005.

CATALA, Pierre**. Ebauche d'une théorie juridique de l'information"**. Informatica e Diritto, ano IX, jan-apr. 1983.

CAVALCANTI, Eduardo de Hollanda. **Proteção de dados, a vez do Brasil.** Disponível em: *https://www.migalhas.com.br/dePeso/16,MI286295,71043-Protecao+de+dados+a+vez+do+Brasil*. Acesso em 08 de novembro de 2018.

DELPIAZZO, Carlos. **A la búsqueda del equilibrio entre privacidad y acceso.** Instituto de Derecho Informático, Facultad de Derecho, Universidad de la República. Montevideo, 2009.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental,** vol. 12, nº 2. Joaçaba: Espaço Jurídico, 2011.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia.** Escola Nacional de Defesa do Consumidor. Brasília, 2010.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.

GARFINKEL, Simson. Database Nation: The Death of Privacy in the 21th Century. California: O'Reilly Media, 2000.

Guidelines on the Protection of Privacy and Transzborder Flows of Personal Data, disponível em: www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

LYON, David. The Information Society: Issues and Illusions, 1988.

MALTA, Tatiana. **O Direito à Privacidade na Sociedade da Informação: efetividade desse direito fundamental diante da tecnologia da informação.** Porto Alegre: Sergio Antônio Fabris Editor, 2007.

MARQUES, Claudia Lima. **Superação das antinomias pelo diálogo das fontes: o modelo brasileiro de coexistência entre o código de defesa do consumidor e o código civil de 2002.** Revista de Direito do Consumidor, vol. 51, 2004.

MARTINS, Fernando Rodrigues. **Sociedade de informação e proteção à pessoa.** Revista de direito do Consumidor, vol. 96. Uberlândia, 2014.

MARTINS, Leonardo. **Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão.** Montevidéu: Fundação Konrad Adenauer, 2005.

MAYER-SCHÖENBERGER, Viktor. **Delete: The Virtue of Forgetting in the Digital Age**. Princeton: Princeton University Press, 2009.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Departamento de Pós-Graduação Unb. Brasília, 2008.

NAVARRO, Ana Maria Neves de Paiva. **O direito fundamental à autodeterminação informativa**. Departamento de Pós-Graduação UFRJ, LETACI. Rio de Janeiro, 2011.

PIÑAR MAÑAS, José Luis. **Guía del Derecho Fundamental a la protección de datos de caracter personal**, Agencia Española de Protección de Datos, 2004.

REGULAMENTO (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

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

SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na constituição federal de 1988**. 5ª ed. Porto Alegre: Livraria do Advogado, 2005.

SCHWENKE, Matthias. **Individualierung und Datenschutz**. Deutscher Universitäts-Verlag, 2006.

SECRETARIA DE INVESTIGAIÓN DE DERECHO COMPARADO, Corte Suprema de Justicia de La Nación. **Protección de Datos Personales**, República Argentina.

WARREN e BRANDEIS. **The Right to Privacy**. In Harvard Law Review, Vol. IV, 1890.