ESCOLA DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO

FERNANDO INGLEZ DE SOUZA MACHADO

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO: *profiling* e risco de discriminação

Porto Alegre
2018

FERNANDO INGLEZ DE SOUZA MACHADO

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO:

profiling e risco de discriminação

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul como requisito parcial para obtenção do título de Mestre em Direito.

Orientadora: Profª Drª Regina Linden Ruaro

Porto Alegre

2018

FERNANDO INGLEZ DE SOUZA MACHADO

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO:

***profiling* e risco de discriminação**

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direito da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul como requisito parcial para obtenção do título de Mestre em Direito.

Aprovada em: ____ de _____ de 2018.

Banca Examinadora:

_____

Professora Doutora Regina Linden Ruaro – Orientadora

_____

Professor Doutor Carlos Alberto Molinaro – PPGD/PUCRS

_____

Professora Doutora Gabrielle Bezerra Sales Sarlet

_____

Professora Doutora Márcia Santana Fernandes - HCPA

AGRADECIMENTOS

Expressar nossa gratidão sempre é uma tarefa árdua. Isso não significa que não somos gratos; pelo contrário, demonstra o quanto damos importância àqueles que nos cercam, nos apoiam, nos encorajam e até mesmo nos desafiam a crescer. É exatamente com essa mentalidade que me proponho a agradecer àqueles que amo.

Primeiramente, gostaria de agradecer à minha família. Meus pais, João e Ruth, a eles sou eternamente grato pela minha vida, pelo suporte, carinho, afeto, dedicação e amor incondicional, certamente sem eles não seria possível estar vivenciando mais essa conquista.

À minha outra mãe, Mara, a quem sou grato pela energia inesgotável, pelo imenso amor, mimos, carinhos e lições de vida, uma pessoa que certamente protagonizou a formação do meu caráter.

Aos meus irmãos, Patrícia e Rodrigo, pelas conversas francas e, outras vezes, devaneios sobre a vida. Muito obrigado por momentos de risada e de reflexão.

Ao meu cunhado, Gabriel, agradeço pelo carinho, parceria, camaradagem e conselhos.

Ao meu afilhado, Francisco, por arrancar sorrisos em dias tristes, por encher de vida e alegria cada lugar que adentra. Obrigado por fazer a vida dessa família mais alegre e ainda mais linda.

Gostaria de agradecer, também, à minha namorada, Nathalia, pela cumplicidade, compreensão e companheirismo nessa fase árdua que é um Mestrado. Agradeço imensamente pelo teu sorriso e tolerância nos não raros momentos de ansiedade e de frustração que marcaram essa caminhada.

Aos meus amigos, alegro-me de pensar que são tantos que não é possível nomeá-los. A vocês gostaria de agradecer a camaradagem, a verdadeira parceria que se constrói no dia a dia e, por vezes, subsiste a um distanciamento pelas

fatídicas “coisas da vida”. Agradeço a vocês por serem a família que escolhi. Não poderia deixar de mencionar, contudo, meus colegas de mestrado Ana Carolina Bonotto, Andrei De Araújo Lima, Eduardo Kronbauer, Leiliane Vidaletti e Paola Sartori pelo coleguismo nesses dois anos.

Agradeço à Pontifícia Unicersidade Católica do Rio Grande do Sul – PUCRS - e ao CNPq pelo apoio e pela infraestrutura disponibilizados durante a pesquisa. Certamente o suporte deles contribui significativamente para o curso de meu mestrado, especialmente desta disssertação.

Por fim, mas não menos importante, gostaria de agradecer à minha orientadora, Dra. Regina Ruaro. Nessa caminhada de mestrado, agradeço não só pela atenção, orientação e profissionalismo, mas, principalmente, pela parceria, amizade e carinho. Mais que uma orientadora, foi um exemplo, uma amiga e uma fonte de imenso conhecimento, por tudo isso quero deixar meu muito obrigado.

RESUMO

O presente trabalho busca enfrentar a temática do direito à proteção de dados pessoais no âmbito do ordenamento jurídico brasileiro, enfocando a figura do *profiling*. O trabalho inicia na construção do direito à privacidade e nas suas mutações em razão dos incrementos tecnológicos, notadamente no que toca às tecnologias da informação e da comunicação. Com isso, ele enfrenta desde as primeiras formulações do direito à privacidade, enquanto um direito a ser deixado só, até suas formulações mais recentes, enquanto um direito de cada indivíduo controlar suas próprias informações privadas. Depois, ele analisa o sistema norte-americano de proteção de dados pessoais, albergado pela figura do *right to privacy,* bem como o sistema europeu de proteção de dados pessoais a partir das normativas em nível de União Europeia. Tal análise serve para que ambos os sistemas sirvam de amparo para o estudo do tema no ordenamento jurídico brasileiro, observadas as devidas adequações para este sistema jurídico. Por fim, o presente trabalho enfrenta a temática da proteção de dados pessoais no ordenamento jurídico brasileiro sob o prisma do *profiling*, o qual consiste em uma ferramenta de tratamento de dados pessoais que figura entre as que ostentam o maior potencial lesivo. Reconhecendo o caráter fundamental do direito à proteção de dados pessoais, inclusive no sistema jurídico brasileiro, o trabalho evidencia a importância da observância dos princípios da proteção de dados pessoais – como o da transparência, o da finalidade e o do consentimento – na utilização de mecanismos de *profiling*. Somente assim é possível conciliar o tratamento de dados pessoais com o respeito aos direitos do titular dos dados.

Palavras-chave: *Profiling*. Dados pessoais. Direito à privacidade. Proteção de dados.

ABSTRACT

The present paper seeks to face the thematic of the right to personal data protection on the scope of the Brazilian legal system, emphasizing on the profiling figure. The paper starts on the construction of the right to privacy and its mutations in face of technological advances, especially on the information and communication technologies. With that it faces from the firsts formulations of the right to privacy, as a right to be let alone, until it's most recent formulations, as a right of each individual to control its own private information. After that, it analyses the north-american personal data protection system, housed on the figure of right to privacy, as well as the European personal data protection system, based on laws of European Union level. This analysis suits so that both systems can be used as reference for the study of the thematic on the Brazilian legal system, observed the due alterations to fit this legal system. In the end, the present paper faces the thematic of personal data protection on the Brazilian legal system, focusing on the profiling, with consists in a personal data treatment tool that figures between the ones that offers the hirer risk. Recognizing the fundamental character of the right to personal data protection, including in the Brazilian juridical system, the paper demonstrates the importance of the observation of personal data protection principles – as the transparency, the purpose and the consent – on the utilization of profiling mechanisms. Only this way it's possible to conform the treatment of personal data with the rights of the data subject.

Keywords: Profiling. Personal data. Right to privacy. Data protection.

SUMÁRIO

INTRODUÇÃO

O debate entre o que é de natureza pública ou privada nunca esteve tão em roga como agora. Os incrementos tecnológicos e a própria dinâmica da sociedade aproximam de tal maneira o público do privado que aspectos outrora tidos como particulares hoje são expostos para todos verem. Redes sociais são verdadeiras vitrines da vida particular do indivíduo e a internet permite que uma mensagem seja veiculada para o mundo inteiro em questão de segundos, independentemente do caráter de seu conteúdo.

Mais do que isso, a própria informação do individuo passou a ser objeto de grande preocupação nessa realidade pós-moderna. Os dados pessoais ganham novo significado a partir do incremento das tecnologias da informação e comunicação (TICs), as quais permitem que as informações sejam coletadas, cruzadas e compiladas para revelar novos aspectos da vida da pessoa. Outrossim, a manipulação de dados pessoais permite a criação de perfis individuais ou de grupos de indivíduos, que podem ser utilizados para os mais diversos fins. É notória a relevância desses dados para o mercado, empresas e até mesmo Estados reconhecem que as informações pessoais consistem em uma espécie de “matéria-prima” imprescindível para o desenvolvimento de suas atividades, servindo desde a prospecção de clientes até a gestão eficiente de recursos.

Consciente do valor inerente a essas informações, o mercado passou a tratá-las como verdadeiras mercadorias, inclusive, com forte participação do Estados nesse nicho de mercado. Nada obstante, o impacto que a utilização desses dados gera sobre seu titular, notadamente no que toca ao respeito ao seu direito à privacidade, à sua autonomia e ao seu livre desenvolvimento da personalidade, é frequentemente explorado por esses agentes do mercado. Nesse sentido, surge o chamado direito à proteção de dados pessoais o qual, mais do que resguardar a vida privada do titular dos dados, busca assegurar o respeito a sua autonomia e ao seu direito de autodeterminação no seio da sociedade da informação.

Importante apontar, contudo, que enfrentar toda a sistemática de proteção de dados pessoais no escopo deste trabalho não permitiria um real aprofundamento da

temática, vez que tal pretensão extrapolaria o fôlego de uma dissertação de mestrado. Nesse sentido, optou-se pelo enfoque na temática do *profiling*, justamente pelo modo que reverbera na vida do titular dos dados pessoais.

Enfatizando na figura do *profiling,* é possível identificar de forma mais evidente os reflexos negativos de uma utilização abusiva dos dados pessoais, bem como o potencial lesivo que o tratamento de dados pessoais apresenta. A criação de perfis possibilita a categorização do indivíduo ou de grupos de indivíduos e isso reflete no modo como eles interagem na sociedade. Obtenção de vistos e empregos, acesso a crédito, a bens e a serviços são apenas alguns dos aspectos da vida em sociedade que são afetados diretamente por esse mecanismo de gestão de dados de natureza pessoal.

Não raras vezes, os perfis criados por meios automatizados de tratamento de informações pessoais, quase sempre com amparo em algoritmos e em dados estatísticos, são a única representação do indivíduo perante inúmeros agentes sociais. A esse fenômeno, soma-se, ainda, o fortalecimento da prática de gestão de riscos (leia-se redução ou eliminação de riscos). Tal conjuntura implica um cenário em que os perfis de usuários são reduzidos a indicativos de risco, a fim de averiguar se determinada pessoa extrapola ou não os padrões “toleráveis” de risco quando do fornecimento de um bem ou serviço, ou, pior, se a pessoa é enquadrável, ou não, em uma categoria de risco ao se falar em segurança pública. Em tal cenário, a utilização de dados pessoais transforma-se em uma verdadeira ferramenta de marginalização e de discriminação. O tratamento de dados, nesse contexto, acaba não só fomentando a coisificação de pessoas, mas explorando economicamente e politicamente tal situação.

Entrementes, não se pode encarar o tratamento de dados pessoais como algo que, *per si*, atenta contra a pessoa humana. Tal postura é, no mínimo, retrógrada, a utilização de dados é imprescindível no desenvolvimento de inúmeras atividades, em especial as de cunho político e econômico. As diversas vantagens que sua utilização enseja vão desde a redução de custos, incremento de eficiência, à atenuação de riscos no desenvolvimento da atividade, fazendo dessa uma prática atividade cada vez mais presente na iniciativa privada e na pública. Também não é possível enxergar o tratamento de dados como algo inofensivo. O já mencionado potencial

lesivo do tratamento de dados sequer é passível de mensuração, sendo quase tão grande quanto às aplicações que o tratamento de dados pessoais proporciona. Nesse aspecto, enfatiza-se que a utilização desses para fins discriminatórios e a consequente marginalização de indivíduos de sua participação plena na sociedade figuram dentre as piores consequências da má gestão de informações pessoais.

Daí decorre a necessidade do estudo da temática da proteção de dados pessoais, notadamente no que toca à figura do *profiling*, o que consiste na proposta do presente estudo. O direito à igualdade e o direito a não discriminação são inerentes a um Estado Democrático de Direito e demandam uma proteção efetiva, em especial quando a prática discriminatória parte do próprio Estado. No mesmo sentido, a própria Constituição da República Federativa do Brasil de 1988 prevê, em seu art. 3º, inciso III, que a Nação tem como objetivo erradicar a pobreza e reduzir as desigualdades sociais. Outrossim, garante como direito fundamental a igualdade (art. 5º, *caput*), prevendo punição contra qualquer forma de discriminação (art. 5º, inciso XLI).

Dessa feita, dividiu-se o presente trabalho em três capítulos, a fim de se verificar em que medida a crescente utilização de dados pessoais para fins de estatísticas e de criação de perfis e de réplicas virtuais repercute negativamente no Estado brasileiro, especialmente ao se falar em discriminação e em marginalização de indivíduos no seio de um Estado carente de regulação específica a propósito do direito à proteção de dados pessoais.

Para tanto, no primeiro capítulo enfrenta-se a questão do direito à privacidade e suas mutações diante do desenvolvimento das tecnologias da informação e comunicação. Partindo das primeiras formulações do direito à privacidade enquanto um *right to be let alone*, esse capítulo verifica as alterações sofridas por esse direito em razão dos incrementos tecnológicos, perpassando pelas formulações do direito à privacidade como um direito da personalidade e como um direito fundamental. Ademais, o capítulo introduz noções como autodeterminação informativa, privacidade informacional e até mesmo proteção de dados pessoais.

No segundo capítulo, busca-se traçar um panorama dos modelos norte-americano e europeu de proteção de dados pessoais. Iniciando com o estudo do modelo norte-americano, calcado na figura do *right to privacy,* a qual engloba um

direito à proteção de dados pessoais, analisa-se a proteção atribuída pela sistemática estadunidense, seja em perspectiva constitucional, seja em perspectiva infraconstitucional. Posteriormente, enfrenta-se a sistemática europeia de proteção de dados pessoais, enfocando-se especificamente nas normativas em nível de União Europeia, notadamente no que toca ao novo regulamento de proteção de dados pessoais e à diretiva 95/46/CE. Essa parte do trabalho, inclusive, é desenvolvida a partir de uma pesquisa realizada junto à Universidad de San Pablo (CEU) de Madrid, com os professores Dr. Alejandro Corral Sastre e Dr. José Luis Piñar Mañas.

Por fim, no terceiro e último capítulo, propõe-se o enfrentamento da temática no âmbito do sistema jurídico brasileiro a partir do prisma da figura do *profiling.* Inicialmente, trabalha-se a ferramenta do *profiling* e alguns dos seus distintos mecanismos de operacionalização. Superada tal questão, busca-se traçar uma análise de um direito à proteção de dados no Brasil, com base nas normativas brasileiras que enfrentam a temática e em alguns julgados nacionais – com enfoque no Superior Tribunal de Justiça e no Tribunal de Justiça do Estado do Rio Grande do Sul – que têm a matéria do *profiling* e da proteção de dados pessoais como objeto da lide.

A partir desses três capítulos, propõe-se o enfrentamento da temática do *profiling* dentro do ordenamento jurídico brasileiro, com base no reconhecimento de um direito fundamental à proteção de dados pessoais. Em que pese não se tenha a pretensão de esgotar a temática, busca-se contribuir para o tão necessário debate acerca da proteção de dados pessoais, principalmente em uma nação que carece de regulação específica, como é o caso do Brasil.

1 O DIREITO À PRIVACIDADE E SUAS MUTAÇÕES DIANTE DO DESENVOLVIMENTO DAS TECNOLOGIAS DE INFORMAÇÃO E DE COMUNICAÇÃO (TICS)

A construção de um direito à privacidade sempre foi marcada pelas possiblidades e implicações decorrentes do desenvolvimento de novas tecnologias. Desde suas primeiras formulações, nos Estados Unidos, como um *right to be let alone*[1]*,* até suas formulações mais atuais como um direito de controlar o fluxo das próprias informações pessoais na saída da esfera pessoal e na entrada (direito de não saber)[2], verifica-se, no direito à privacidade, uma tentativa de tutela da esfera privada do indivíduo e de sua própria personalidade frente a ameaças que os avanços tecnológicos ensejam.

Do desenvolvimento desse direito no âmbito doutrinário e jurisprudencial, depreende-se uma constante expansão de sua esfera de abrangência, frequentemente relacionando-o com outros direitos, a exemplo do acesso à informação, do livre desenvolvimento da personalidade e da liberdade. Ademais, tal expansão resta evidente ao se verificar que o desenvolvimento do direito à privacidade é berço do chamado direito à proteção de dados pessoais[3].

Dada a sua singular importância, o direito à privacidade foi reconhecido como um direito fundamental. No âmbito internacional, a Declaração Universal dos Direitos Humanos (DUDH), de 1948, expressa, em seu art. 12, que:

> Ninguém será sujeito a interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.[4]

---

[1] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, dec. 1890. Disponível em: <http://www.jstor.org/stable/1321160>. Acesso em: 06 abr. 2017.

[2] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

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

[4] ONU. **Declaração Universal dos Direitos Humanos**. Adotada e proclamada pela resolução 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Disponível em: <http://unesdoc.unesco.org/images/0013/001394/139423por.pdf>. Acesso em: 9 mar. 2017.

Já no âmbito nacional, a Constituição da República Federativa do Brasil de 1988 dispõe, em seu art. 5º, inciso X, que "[...] são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação"[5].

Em se tratando de direito fundamental, não se pode ignorar o contexto social, político e econômico em que ele é inserido. A inobservância da realidade fática de determinada organização social importa não só o esvaziamento do conteúdo desse direito, mas a impossibilidade de concretização do mesmo. Por conseguinte, pensar no direito à privacidade, hoje, nos mesmos moldes em que esse era pensado no século XIX, implicaria ignorar inúmeras de suas facetas e furtar-se ao enfrentamento de diversas problemáticas que o envolvem, resultando, invariavelmente, em uma tutela insuficiente do mesmo[6].

Nesse sentido, o exemplo dos direitos da personalidade é emblemático. A construção jusnaturalista como resposta aos excessos perpetrados após as revoluções liberais é prova cabal da constante necessidade de atualização do direito. Em um contexto de opressão de minorias com base no poder econômico e de concentração dos meios de produção, a própria noção de autonomia foi objeto de releitura e mitigação, consagrando-se direitos que se sobrepunham à própria liberalidade do indivíduo, os chamados direitos da personalidade[7]. Tal contexto, também, justificou a superação de uma teoria liberal clássica que restringia o alcance dos direitos fundamentais às relações públicas, passando esses a afetar,

---

[5] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 05 mar. 2017.

[6] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

[7] A Revolução Industrial fora marcada pela constante exploração do proletariado por parte daqueles que detinham o poder econômico – burguesia – evidenciando que não mais bastava coibir as ingerências do Estado frente ao particular para garantir a tão aclamada liberdade que motivara a derrubada dos regimes absolutistas. O monopólio dos meios de produção fazia com que as classes menos favorecidas se submetessem a condições de trabalho degradantes, bem como a jornadas de trabalho desumanas, a fim de garantir sua subsistência. Rompeu-se, então, com essa falsa noção de autonomia, a partir do reconhecimento de direitos que se sobrepunham à própria liberdade do indivíduo, vez que se tratavam de direitos inatos, inerentes à própria pessoa e, portanto, inalienáveis, intransmissíveis e irrenunciáveis. SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014.

também, as relações entre particulares[8]. No mesmo sentido, as mutações constitucionais[9] ganham cada vez mais espaço no ordenamento jurídico nacional como meio de readequação do direito posto à realidade jurídico-social.

Destarte, é fundamental ter presente as características e as peculiaridades do contexto social em que se pretende inserir o direito à privacidade. Porém, em uma pós-modernidade marcada por constantes e rápidas transformações, tal tarefa não é simples. A própria explosão de conceitos criados para representar uma sociedade marcada pelos grandes avanços das tecnologias da informação e da comunicação (TICs)[10] evidencia essa dificuldade de se definir e conceituar uma realidade caracterizada por uma constante mutabilidade.

Forçoso notar que diversos são os efeitos da assimilação das TICs na sociedade: globalização, eliminação de barreiras na comunicação, aumento do fluxo de informações, dentre outros[11]. Invariavelmente, os avanços tecnológicos influenciam nosso modo de organização social, por vezes com tamanha intensidade que provocam rupturas no tecido social[12]. Tal conjuntura implica a necessidade de readequação da própria sociedade, a fim de solucionar os inúmeros problemas decorrentes dessas rupturas sociais que, frequentemente, denunciam uma nova

---

[8] SARMENTO, Daniel; GOMES, Fábio Rodrigues. A eficácia dos direitos fundamentais nas relações entre particulares: o caso das relações de trabalho. **Rev. TST**, Brasília, v. 77, n. 4, p. 60-101, out./dez. 2011.

[9] Para fins deste trabalho, entende-se mutações constitucionais como um fenômeno de alteração do sentido ou do alcance da Constituição, sem que haja, contudo, uma aleteração em seu texto normativo. Ou seja, trata-se de um ressignificação do texto Constitucional, a fim de readequar a Constituição à realidade social. A esse respeio ver: SBROGIO GALIA, Susana. **Mutações constitucionais interpretativas e proteção do núcleo essencial dos direitos fundamentais**. 2006. 191 f. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2006.

[10] Bauman refere-se a uma "Modernidade Líquida"; Castells, por sua vez, utiliza a denominações como "Sociedade em Rede" ou "Era da Informação"; Beck utiliza o termo "Sociedade de Risco"; Rodotà traz a figura da "Sociedade de Vigilância". BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013; CASTELLS, Manuel. **A galáxia internet**. Reflexões sobre internet, negócios e sociedade. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004; BECK, Ulrich. World risk society. In: OLSEN, J. K. B.; PEDERSEN, S. A.; HENDRICKS, V. F. (Ed.). **A companion to the philosophy of technology**. Oxford: Blackwell Publishing Ltd, 2009. p. 495-499; RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

[11] CASTELLS, op. cit.

[12] O fenômeno da internet, por exemplo, rompeu com noções de tempo e distância ao tornar a comunicação praticamente instantânea em todo o globo a um custo relativamente baixo, e com isso, também pôs em xeque a soberania dos Estados, por se tratar de ferramenta de difícil regulação. Nesse sentido ver: CASTELLS. Ibid.

forma de distribuição de poder[13]. No caso específico do direito à privacidade, as inovações tecnológicas geram novos meios de ingerência na esfera privada do indivíduo, os quais demandam novas respostas da sociedade, notadamente a partir da reformulação desse direito.

O frequente discurso de que "[...] para se aproveitar os benefícios da sociedade moderna, temos que, necessariamente, abrir mão de certo grau de privacidade", para Garfinkel[14], trata-se de um *trade off* não só desnecessário, mas equivocado. Segundo o autor, situação semelhante verificou-se na crise ambiental das décadas de 1950 e 1960, na qual se sustentava que o desenvolvimento econômico só era possível à custa da degradação ambiental, o que foi amplamente fragilizado a partir da construção da noção de sustentabilidade[15]. Ou seja, o direito à privacidade não está fadado à morte, o que se infere é a necessidade de uma releitura do mesmo na sociedade contemporânea.

Reconhece-se que a formulação inicial desse direito – o direito a ser deixado só – não mais é reivindicado com a mesma força, ou se quer é objeto de reivindicação pela parcela majoritária da população contemporânea[16]. Partindo das ideias de Pérez Luño, Rodotà e Castells, Limberger perpassa pelas possíveis consequências dos avanços tecnológicos em relação à privacidade. O primeiro aventa a mutação da intimidade de um direito da personalidade a um direito

---

[13] Rodotà defende que as novas formas de tratamento de dados pessoais e a crescente necessidade desses dados por instituições públicas e privadas implicam transformações na distribuição e uso do poder. "Somente assim será possível desfazer o nó das relações entre a tutela das liberdades individuais e a eficiência administrativa e empresarial. Identificando as raízes do poder fundado na disponibilidade de informações e seus reais detentores, será possível não somente projetar formas de contra-poder e de controle, como também aproveitar as possiblidades oferecidas pela tecnologia da computação para tentar produzir formas diversas de gestão do poder [...]."RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 24.

[14] "*Many people today say that in order to enjoy the benefits of modern Society, we must necessarily relinquish some degree of privacy. If we want the convenience of paying for a meal by credit card, or paying for a toll with an electronic tag mounted on our rear view mirror, then we must accept the routine collection of our purchases and driving habits in a large database over wich we have no control. Its's a simple bargain, albeit a Faustain one. I think this tradeoff is both unnecessary and wrong* […]." [Tradução livre]. GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010. p. 5.

[15] Ibid.

[16] LIMBERGER, Têmis. Mutações da privacidade e a proteção dos dados pessoais. In: RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (Org.). **Privacidade e proteção de dados pessoais na sociedade digital**. Porto Alegre: Fi, 2017. p. 145-168.

patrimonial[17]. O segundo pensa uma reinvenção da privacidade a partir da "constitucionalização da pessoa humana" e da ressignificância da liberdade de expressão, especialmente pelo prisma da transparência e do exercício da cidadania como mecanismos de redistribuição do poder[18]. Por fim, Castells trabalha o panóptico eletrônico e os riscos inerentes às formas de controle e a grande exposição existente na rede, afinal, "[...] uma proporção significativa da vida cotidiana, inclusive o trabalho, o lazer, a interação pessoal, tem lugar na Internet"[19].

Portanto, a construção proposta no presente capítulo perpassa pelo enfrentamento de algumas tendências tecnológicas no âmbito das TICs e das tecnologias de vigilância, bem como das implicações dessas tendências na construção de um direito à privacidade. A partir de tal enfrentamento, busca-se traçar um delineamento de um direito à privacidade dentro do paradigma sociopolítico-econômico atual, ainda que sem a pretensão de esgotar a matéria.

1.1 O *RIGHT* TO *PRIVACY*[20] ENQUANTO UM *RIGHT TO BE LET ALONE*

Trabalhar com a primeira formulação jurídica[21] do direito à privacidade representa não só uma construção histórica desse direito, mas o enfrentamento de uma de suas inúmeras faces. A existência de mutações na sua formulação,

---

[17] Em síntese, o direito à intimidade manter-se-ia como direito da personalidade – dotado dos atributos de inviolabilidade, irrenunciabilidade e inalienabilidade – somente em relação às crianças e aos adolescentes. Para os maiores, ele se deslocaria para a órbita patrimonial, podendo "[...] ser objeto de transações consentidas, de renúncias e cessões, em troca das correspondentes prestações econômicas". PÉREZ LUÑO, Antonio Enrique. **Los derechos humanos en la sociedad tecnológica**. Madrid: Universitas, 2012, apud LIMBERGER, op. cit., p. 154.

[18] RODOTÀ, Stefano. **El derecho a tener derechos**. Madrid: Trotta, 2014, apud LIMBERGER, op. cit., p. 155.

[19] CASTELLS, Manuel. **A galáxia internet**. Reflexões sobre internet, negócios e sociedade. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

[20] O termo em inglês *right to privacy* é utilizado frequentemente sem tradução no presente trabalho, vez que o *right to privacy* americano não corresponde exatamente ao direito à privacidade no ordenamento jurídico brasileiro. Tal direito corresponde quase a um direito geral de personalidade abordando, não raras vezes, questões que transcendem a noção de direito à privacidade. Destarte, adota-se, em diversas oportunidades, o termo na língua original, a fim de se evitar possíveis inadequações.

[21] Ressalta-se que, enquanto construção cultural, pode-se identificar uma formulação de *privacy* na própria noção de liberdade trabalhada por filósofos como Aristóteles, Cícero e Thomas de Aquino, ou então em contratualistas como John Mill, Locke e Hobbes, bem como em raízes anglo-saxônicas com a máxima *man's house is his castle*. Ou seja, a noção de privacidade já existia, o que tardou para ocorrer foi a recepção desta figura no ordenamento jurídico. MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008.

enquanto mecanismos de atualização desse direito frente a novos problemas na sociedade, não implica a superação das formulações anteriores – ainda que a primeira delas remonte ao século XIX[22]. O que se observa, na realidade, é um fenômeno de expansão do direito à privacidade que, paulatinamente, passa a agregar diversas faces (ou dimensões) que podem se manifestar tanto individualmente como concomitantemente, a depender do caso concreto.

Posto isso, importante traçar uma breve contextualização do cenário que foi berço para a formulação do artigo *Right to Privacy*, de Warren e Brandeis[23] para a *Harvard Law Review*, publicado em 15 de dezembro de 1890. Tal artigo é considerado um marco "inicial" na construção doutrinária de um direito à privacidade, em que pese não seja, de fato, o primeiro a abordar o assunto. Ademais, até hoje, ele é o artigo mais influente e o mais citado na área do direito à privacidade.

O final do século XIX é considerado o apogeu do liberalismo jurídico clássico e a "idade de ouro da privacidade". Nesse sentido, não é de se estranhar que ela surge como um direito "tipicamente burguês", de conotação elitista e individualista[24], amplamente apoiado em uma visão patrimonialista típica da época[25]. Warren e Brandeis[26] buscaram dar respostas às circunstâncias e problemas de seu tempo, motivados, basicamente, pelas implicações do surgimento das câmeras fotográficas e de seu uso de modo intrusivo na privacidade [27], do próprio artigo, depreende-se,

---

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

[23] Do próprio artigo de Warren and Brendeis se depreende que a noção de um *the right to be let alone* já era empregada pelo juiz *Cooley* na obra Cooley on Torts. Ademais, eles mencionam que, na França, já se reconhecia um *right to privacy.* WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, dec. 1890. Disponível em: <http://www.jstor.org/stable/1321160>. Acesso em: 06 abr. 2017.

[24] A própria motivação do artigo foi a constante exposição desarrazoada de aspectos pessoais da vida dos Warren pela imprensa (que focava suas atenções na elite ou *blue bloods*), mais especificamente a reportagem sobre o casamento de sua filha foi o divisor de águas para a elaboração do artigo intitulado *The Right to Privacy*. PROSSER, William L. Privacy. **California Law Review**, v. 48. i. 3, ago. 1960. Disponível em: <http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1>. Acesso em: 28 jun. 2017.

[25] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 8-10.

[26] "*The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle*." WARREN; BRANDEIS, op. cit., p. 196.

[27] MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008.

inclusive, uma preocupação especial com a exposição abusiva de indivíduos por parte da imprensa.

Tecidas essas considerações iniciais, cabe enfrentar o artigo em questão. Ele parte do pressuposto de que mudanças políticas, econômicas e sociais implicam o reconhecimento de novos direitos de forma a atender as demandas da sociedade. Nesse sentido, Warren e Brandeis identificam uma alteração qualitativa do direito à vida (*right to life*), que passou a significar não só um direito a "(sobre)viver", mas um direito a aproveitar a vida (*right to enjoy life*). Ou seja, reconheceram-se direitos para além dos bens materiais e do próprio corpo do indivíduo, tutelando-se questões como "a natureza espiritual do homem, seus sentimentos, e seu intelecto"[28].

É sobre essa premissa que os autores americanos trabalham um direito a ser deixado só (*right to be let alone*), enquanto um instrumento de resguardar o indivíduo frente às constantes invasões à vida privada e doméstica perpetradas pelos jornais e agravadas pelo aprimoramento da fotografia[29]. Ainda que arraigado em noções de *property-privacy*, ou seja, em uma construção de um *right to privacy* a partir de um direito de propriedade, o artigo lança bases a uma construção do *right to privacy* que transcende essa noção de propriedade, vinculando esse direito ao ser humano em si, reconhecendo o resguardo à privacidade e até o isolamento como essenciais ao ser humano[30].

Entendendo como superficial uma possível analogia entre a proteção contra uma difamação (*law of defamation*) e a proteção à *privacy*, os autores vêm buscar, na proteção aos direitos da propriedade intelectual e artística, bases para fundamentar um *geral right to privacy*. Eles defendem que "[...] o *common law*

---

[28] "*Later, there came a recognition of man's spiritual nature, of his feelings and his intellect*." [Tradução livre]. WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, dec. 1890. Disponível em: <http://www.jstor.org/stable/1321160>. Acesso em: 06 abr. 2017. p. 193.

[29] "*Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'. For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; 5 and the evil of the invasion of privacy by the newspapers* […]." Ibid., p. 195.

[30] "*The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury*." Ibid., p. 196.

garante a cada indivíduo o direito de determinar, ordinariamente, e em que extensão, seus pensamentos, sentimentos e emoções podem ser compartilhados com terceiros"[31].

Destarte, os autores sustentam que o sistema norte-americano assegura ao cidadão o direito de permitir, ou não, a revelação de tais aspectos de sua vida a terceiros, ou de ele mesmo os revelar – ressalvados casos de depoimentos e de testemunhos em que o indivíduo é obrigado a expor os fatos. Ademais, entendem que é assegurado ao cidadão o direito de definir os limites à publicidade que é dada às suas informações pessoais[32]. Em suma, eles trazem a figura do consentimento e as bases para a formulação de uma autodeterminação informativa.

Trabalhando com base em diversos julgados, partindo de uma análise, *a priori*, de direitos autorais, o artigo constrói uma diferenciação desses da proteção inerente ao direito à privacidade a partir de dois critérios: valor econômico e objeto de tutela. No caso dos direitos autorais, o que se tutela é a forma da produção e seu valor econômico, artístico ou intelectual, ao passo que a privacidade não leva em conta o valor, mas sim o conteúdo do que foi produzido. Por exemplo, sob o escopo do direito autoral, não seria possível proibir a descrição do conteúdo de uma carta, limitando-se a tutelar seu texto, a tutela do conteúdo, dessa feita, dar-se-ia por meio do *right to privacy*[33].

Nesse sentido, a proteção dada contra publicações não autorizadas em determinados casos seria a expressão de um direito a ser deixado só (*right to be let alone*). Ela se daria não com base no princípio da propriedade privada, mas em uma inviolabilidade da própria personalidade[34]. Calcados nesse raciocínio, Warren e Brandeis sustentam uma proteção contra ingerências da imprensa, de fotógrafos ou

---

[31] "[…] *for the legal doctrines relating to infractions of what is ordinarily termed the common-law right to intellectual and artistic property are, it is believed, but instances and applications of a general right to privacy* […]. *The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others*." [Tradução livre]. WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, dec. 1890. Disponível em: <http://www.jstor.org/stable/1321160>. Acesso em: 06 abr. 2017. p. p. 198.

[32] Ibid.

[33] Ibid.

[34] "*The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality*." Ibid., p. 205.

de qualquer outro sujeito detentor de aparelhos capazes de gravar e reproduzir imagens, vídeos ou áudios. Segundo os autores,

> [...] as decisões analisadas indicam um *general right to privacy*, para pensamentos, emoções e sensações, estes devem receber a mesma proteção, seja quando expressados por escrito, em condutas, em conversas, por atitudes ou em expressões faciais.[35]

Para além da ideia de propriedade, ainda que sem lançar mão dela, os autores conseguiram identificar nos julgados das cortes norte-americanas valores como confiança e confidência para a proteção de um *right to privacy.* A utilização de tais termos consiste no reconhecimento judicial de que a "[...] a moralidade pública, a justiça privada e o senso comum demandam o reconhecimento de tal direito"[36].

Com acurada sensibilidade, Warren e Brandeis[37] perceberam que tal construção não era suficiente para a tutela da privacidade, vez que negligenciava os casos em que a invasão à esfera privada é perpetrada por um terceiro estranho. Nesse sentido, os autores negam como fundamentos base para o direito à privacidade noções como confiança especial (*special trust*) ou um contrato, vez que, para eles, o próprio princípio que norteia tal direito não é a propriedade, ao menos não em seu sentido convencional.

Por fim, Warren e Brandeis[38] trazem alguns critérios para definição dos limites do *right to privacy*, dentre os quais se destacam o consentimento e o interesse público ou da coletividade. Isso posto, pode-se extrair do artigo *Right to Privacy* que as mudanças sociais implicam o reconhecimento de novos direitos, identificando-se no direito à privacidade um mecanismo de tutela contra ingerências na vida privada

---

[35] "*If, then, the decisions indicate a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression*." WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, dec. 1890. Disponível em: <http://www.jstor.org/stable/1321160>. Acesso em: 06 abr. 2017. p. 206.

[36] "*This process of implying a term in a contract, or of implying a trust (particularly where the contract is written, and where there is no established usage or custom), is nothing more nor less than a judicial declaration that public morality, private justice, and general convenience demand the recognition of such a rule, and that the publication under similar circumstances would be considered an intolerable abuse*." Ibid., p. 210.

[37] Ibid.

[38] Ibid.

do indivíduo. Constata-se, ademais, a forte influência que o desenvolvimento de novas tecnologias enseja sobre a construção do escopo de proteção desse direito.

1.2 O DIREITO À PRIVACIDADE COMO UM DIREITO DE PERSONALIDADE E UM DIREITO FUNDAMENTAL

Seguindo as bases lançadas por Warren e Brandeis, que consagraram o direito à privacidade enquanto um direito de defesa, a partir de um *right to be let alone*, a doutrina reconheceu e consagrou o direito à privacidade como um direito de personalidade e um direito fundamental. No ordenamento jurídico pátrio, os direitos à vida privada e à intimidade restam previstos no próprio capítulo do Código Civil de 2002 destinado aos direitos de personalidade (art. 21)[39] e na Constituição Federal de 1988, em seu art. 5º, inciso X[40].

Tal reconhecimento foi essencial para a superação daquela conotação elitista que esse direito ostentava em sua origem, o que ocorreu, em termos de Tribunais, na década de 1960. A mudança de um estado liberal para um *welfare state* e o fortalecimento de movimentos sociais que reivindicavam direitos deram forças a uma democratização do direito à privacidade, que veio a ostentar a natureza de um direito fundamental[41].

Somada a essa nova lógica de relação entre indivíduo e Estado, os avanços tecnológicos, em especial aqueles relacionados às TICs, também evidenciaram a íntima relação do direito à privacidade com o livre desenvolvimento da

---

[39] "Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma." BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, seção 1, Brasília, DF, a. 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/CCivil_03/leis/2002/L10406.htm>. Acesso em: 20 mar. 2017.

[40] "[...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...]." Id. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 05 mar. 2017.

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

personalidade, o direito à liberdade e a própria figura da autonomia[42]. Em 1948, a distopia de Orwell, em sua obra 1984, externava inúmeras possiblidades de vigilância que os incrementos tecnológicos proporcionavam ao Estado na figura do Grande Irmão que tudo vê e tudo sabe. Além disso, o autor articulava como tais mecanismos contribuíam na manutenção do poder desse regime totalitário, notadamente enquanto ferramentas de repressão[43], fazendo verdadeira alusão à sistemática do panóptico de Jeremy Bentham[44] tão bem trabalhado por Foucault em sua obra Vigiar e Punir[45].

Partindo de uma premissa da disciplina, Foucault[46] demonstra como o corpo pode ser objeto e alvo do poder. Ao enfrentar a figura do soldado no capítulo "Os corpos dóceis", percebe-se uma verdadeira redução do indivíduo à condição de um produto, uma máquina construída a atender suas finalidades a partir de um constante processo de manipulação, modelagem e treino do corpo.

A estrutura disciplinar nada mais é do que uma evolução da estrutura de exclusão; primeiro se trabalha com a lógica binária da exclusão, distinguindo aqueles que estão dentro do padrão daqueles que não estão. Passa-se, assim, à individualização do anormal, para que esse seja submetido a táticas disciplinares, dentre as quais destaca-se a vigilância constante[47].

É nesse contexto que Foucault[48] trabalha a figura do panóptico de Bentham. Sua estrutura, idealizada, *a priori*, para instituições prisionais[49] é uma verdadeira

---

[42] Nesse sentido ver: VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007.

[43] ORWELL, George. **1984**. Tradução Alexandre Hubner, Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

[44] FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 31. ed. Tradução Raquel Ramalhete. Petrópolis: Vozes, 2006.

[45] Outras obras consagradas também evidenciam essa íntima relação entre a informação (ou conhecimento) e o poder. Segundo a arte da guerra – Sun Tzu –, uma das premissas para vitória em uma batalha é não só conhecer o inimigo, mas a si mesmo. Maquiavel, em sua obra O Príncipe, defende que é preciso saber de que espécie é determinado principado para saber qual a melhor forma de conquista-lo ou de mantê-lo sob seu domínio. Ou seja, ainda que com algumas variações essas obras identificam o conhecimento sobre o outro como premissa de subjugá-lo a sua vontade. TZU, Sun. **A arte da guerra**. Tradução Sueli Barros Cassal. Porto Alegre: L&PM, 2006; MAQUIAVEL, Nicolau. **O príncipe**. 4. ed. São Paulo: Edipro, 2015.

[46] À própria docilidade mencionada no capítulo é dado um significado de um objeto analisável e manipulável. FOUCAULT, op. cit., p. 117-119.

[47] Ibid., p. 165.

[48] Ibid., p. 165-166.

[49] Posteriormente se verifica a possiblidade de implementação dessa estrutura em outros ambientes disciplinares como as fábricas, as escolas, os quarteis, os conventos etc.

alegoria da vigilância e é largamente conhecida: uma torre principal, ao centro da estrutura, circundada por uma segunda construção, em forma de anel, disposta com aberturas estratégicas, de forma que seu interior esteja completamente exposto a qualquer observador localizado na torre. Essa estrutura ainda seria dividida em celas (ou células) que comportariam apenas um indivíduo, impedindo sua comunicação com os demais. Por sua vez, a torre seria disposta de tal forma que ninguém que estivesse em qualquer uma das celas pudesse observar o interior da torre, onde seria colocado um vigia (na ideia original de Bentham, esse mecanismo se dava a partir de um jogo de iluminação, enquanto as celas eram atingidas pela luz a torre permanecia no escuro, fora da visão dos presos).

A visibilidade figura, aqui, como uma armadilha para o vigiado. Esse é reduzido apenas a um "objeto da informação, nunca sujeito numa comunicação". É a ameaça da vigilância constante, por fim, que asseguraria o funcionamento automático do poder, vez que o vigiado assume, simultaneamente, os papeis de vigia e de vigiado. Espontaneamente, ele passa a adotar o comportamento desejado[50].

Para além do âmbito literário, o incremento no fluxo de informações, o barateamento e o aprimoramento de mecanismos de coleta e tratamento das mesmas aumentaram sensivelmente a possiblidades de utilização e manipulação desses dados, fazendo com que as "pessoas de relevo social" não fossem as únicas a terem sua privacidade ameaçada. Não só o número de situações que ameaçam a vida privada e a intimidade dos indivíduos aumentaram drasticamente, mas a parcela da população afetada por tais situações[51]. Câmeras fotográficas, filmadoras, câmeras de segurança, maior coleta de informações pelo Estado, criações de *credit bureaus*[52], são apenas alguns exemplos de mecanismos que representavam ameaças à privacidade dos indivíduos e que ignoravam o seu "status social*".*

[50] FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 31. ed. Tradução Raquel Ramalhete. Petrópolis: Vozes, 2006. p. 166.
[51] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.
[52] Os *credit bureaus* são, basicamente, departamentos ou empresas que trabalham com arquivos de consumo para relações de crédito, amplamente utilizados pelo mercado norte-americano já em 1969. As figuras dos *credit bureaus* e dos arquivos de consumo serão enfrentadas com maior profundidade no capítulo 3 deste trabalho. GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010.

O panóptico do século XVIII é importado para os tempos digitais. O panóptico digital ou o panóptico do século XXI prescinde do enclausuramento essencial para o panóptico de Bentham e é tema recorrente para aqueles que enfrentam uma sociedade da vigilância[53]. Vive-se em um mundo no qual a distopia do Grande Irmão, imaginada por Orwell em 1984, é tecnicamente viável. Retoma-se, assim, a ideia de uma vigilância constante, articulada a partir do uso de ferramentas e de instrumentos de monitoramento de indivíduos e de tratamento de dados pessoais, os quais são cada vez mais implementados, tanto na iniciativa pública como na privada.

Diante de tal conjuntura, o reconhecimento de um direito fundamental à privacidade e a inserção desse direito no âmbito dos direitos da personalidade foram (e ainda são) essenciais para uma efetiva tutela do indivíduo. Com isso, tal direito não depende apenas da construção doutrinária e jurisprudencial para atestar sua importância, mas encontra no ordenamento jurídico toda uma sistemática própria de proteção com respaldo constitucional, consoante será analisado a seguir.

1.2.1 Direito fundamental à privacidade

Enfrentar todas as nuances que permeiam a categoria dos direitos fundamentais, ainda que aplicadas especificamente ao direito à privacidade, consiste em uma tarefa extremamente complexa, a qual extrapola o objeto da presente dissertação. Isso posto, adianta-se que não se tem a pretensão de esgotar a temática da eficácia e do conteúdo do direito fundamental à privacidade, cabendo,

---

[53] Nesse sentido ver: RUARO, Regina Linden. Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância? **Arquivo Jurídico**, Teresina, v. 2, n. 1, p. 41-60, jan./jul. 2015; RODRIGUEZ, Daniel Piñeiro. **O direito fundamental à proteção de dados pessoais**: as transformações da privacidade na sociedade de vigilância e a decorrente necessidade de regulação. Dissertação (Mestrado em Direito) – Faculdade de Direito, Programa de Pós-Graduação em Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2010; VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007; LEONARDI, Marcel. Vigilância tecnológica, bancos de dados, Internet e privacidade. **Revista Jus Navigandi**, Teresina, a. 9, n. 499, 18 nov. 2004. Disponível em: <https://jus.com.br/artigos/5899>. Acesso em: 3 abr. 2017. RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

apenas, enfrentar algumas questões pontuais no escopo dessa matéria que são imprescindíveis ao desenvolvimento do presente estudo.

Inicialmente, cabe afirmar que a privacidade, enquanto direito fundamental (de primeira dimensão), encontra-se em um constante processo de expansão e fortalecimento[54]. Tal constatação corrobora com a já mencionada tese de que o *trade off* entre privacidade e as comodidades da vida moderna não pode ser admitido como uma alternativa adequada[55], obviamente que sem legitimar, com isso, qualquer releitura de um discurso *luddite*[56].

No que concerne à oponibilidade desse direito fundamental, é possível identificar que o cidadão pode opor tal direito tanto frente ao Estado – eficácia vertical –, como frente a outros particulares – eficácia horizontal[57]. Ou seja, trata-se de direito oponível *erga omnes*[58].

Por sua vez, a fundamentalidade atribuída à privacidade, na perspectiva constitucional brasileira, investe-a no papel de verdadeiro parâmetro hermenêutico[59]

---

[54] É o que se extrai da crítica de Sarlet ao emprego do vocábulo "gerações" de direitos fundamentais, o qual "[...] conduz ao entendimento equivocado de que os direitos fundamentais se substituem ao longo do tempo, não se encontrando em permanente processo de expansão, cumulação e fortalecimento". SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado, 2015. p. 45.

[55] GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010.

[56] O Ludismo foi um movimento do Século XIX que era contra a automação ou mecanização do trabalho durante a Revolução Industrial, em razão da substituição da mão de obra humana pela máquina. Tal conceito é utilizado hoje para representar aqueles que se opõe à industrialização ou às inovações tecnológicas, também podendo ser chamado de neoludismo. JIN, Julia. Luddism during the Industrial Revolution. In: **WESTERN Civilization II guides**. 24 abr. 2012. Disponível em: <http://westerncivguides.umwblogs.org2012/04/24/luddism-during-the-industrial-revolution/>. Acesso em: 30 maio 2017..

[57] No que toca ao emprego da expressão *eficácia horizontal,* oportuno apontar a ressalva feita por Limberger no sentido de que, ainda que tal termo possa levar a uma falsa impressão de que se trabalha com sujeitos em situação de igualdade material, tal situação nem sempre é verdadeira, especialmente em se tratando de grandes empresas ou instituições financeiras e seus trabalhadores ou consumidores. Destarte, deve-se atentar que *eficácia horizontal* significa que se está tratando da aplicabilidade em termos de relações privadas e não necessariamente isonômicas. LIMBERGER, Têmis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

[58] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado, 2015.

[59] A propósito do valor hermenêutico do direito fundamental à privacidade, Sarlet, Marinoni e Mitidiero sustentam que "[...] da perspectiva objetiva decorre, além da assim chamada eficácia irradiante e interpretação da legislação civil (notadamente no campo dos direitos de personalidade), em sintonia com os parâmetros normativos dos direitos fundamentais, um dever de proteção estatal, no sentido tanto da proteção da privacidade na esfera das relações privadas, ou seja, contra intervenções de terceiros, quanto no que diz com a garantia das condições constitutivas da fruição da vida privada."

e de valor superior – ao lado dos demais direitos fundamentais – de toda a ordem constitucional e jurídica[60]. É essa fundamentalidade, também, que denuncia o conteúdo essencial desse direito: a dignidade da pessoa humana[61].

Nesse sentido, rompe-se com aquela noção elitista e patrimonialista do direito à privacidade, o qual passa a ser um meio de se concretizar a dignidade da pessoa humana. Não só os detentores de propriedades são tutelados por esse direito, mas qualquer indivíduo. No Brasil, em que pese a Constituição Federal atribuir apenas aos "brasileiros e aos estrangeiros residentes no País" a titularidade dos direitos e garantias fundamentais (art. 5º, *caput*), já se consolidou entendimento no sentido de observância do princípio da universalidade[62] quando da interpretação do direito positivo constitucional pátrio[63]. Desse modo, parece tranquila a noção de que todas as pessoas humanas são titulares de direitos fundamentais, inclusive do direito à privacidade.

Outrossim, digna de nota é a disposição no §1º do art. 5º da Constituição Federal de 1988, que confere aplicabilidade imediata às "normas definidoras de direitos e garantias fundamentais"[64]. A partir de tal disposição constitucional, ganha

---

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017. p. 449.

[60] SARLET, op. cit.

[61] É o que sustenta Virgílio Afonso da Silva no sentido de ser a dignidade conteúdo essencial de todos os direitos humanos e que seria um limite às restrições dos direitos fundamentais. SILVA, Virgílio Afonso da. **Direitos fundamentais**: conteúdo essencial, restrições e eficácia. 2. ed. São Paulo: Malheiros, 2011.

[62] "De acordo com o princípio da universalidade, todas as pessoas, pelo fato de serem pessoas são titulares de direitos e deveres fundamentais, [...]." SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado, 2015. p. 217.

[63] Ibid.

[64] "[...] § 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata." BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 05 mar. 2017.

força a tese de que essas normas constitucionais são dotadas de eficácia (jurídica)[65] plena, da qual decorre sua aplicabilidade imediata[66].

Quanto à previsão constitucional desse direito, dispõe o art. 5º, inciso X, que "[...] são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação"[67]. Opta, assim, o constituinte pelo termo vida privada em vez de privacidade, bem como por trabalhar a intimidade autonomamente.

No que toca ao vocábulo empregado, em que pese a identidade semântica, filia-se à doutrina mais atual que emprega a expressão privacidade[68]. Já no que concerne à diferenciação feita pelo legislador entre vida privada (privacidade) e intimidade, entende-se que ela não justifica o tratamento de ambos os direitos de forma individualizada, uma vez que esse consiste em uma esfera daquele[69].

---

[65] Eficácia, no presente estudo, é entendida como a capacidade de produção de efeitos jurídicos. Nos termos de Sarlet, a eficácia jurídica seria "[...] a possiblidade (no sentido de aptidão) de a norma vigente (juridicamente existente) ser aplicada aos casos concretos e de – na medida de sua aplicabilidade – gerar efeitos jurídicos, ao passo que a eficácia social (ou efetividade) pode ser considerada como englobando tanto a decisão pela efetiva aplicação da norma (juridicamente eficaz, quanto o resultado concreto decorrente – ou não – desta aplicação". SARLET, op. cit., p. 248.

[66] Nos dizeres de Sarlet: "Se, portanto, todas as normas constitucionais sempre são dotadas de um mínimo de eficácia, no caso dos direitos fundamentais, à luz do significado outorgado ao art. 5º, §1º, de nossa Lei Fundamental, pode afirmar-se que aos poderes públicos incumbem a tarefa e o dever de extrair das normas que os consagram (os direitos fundamentais) a maior eficácia possível, outorgando-lhes, neste sentido, efeitos reforçados relativamente às demais normas constitucionais, já que não há como desconsiderar a circunstância de que a presunção de aplicabilidade imediata e plena eficácia que milita em favor dos direitos fundamentais constitui, em verdade, um dos esteios de sua fundamentalidade formal no âmbito da Constituição". Ibid., p. 280.

[67] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 05 mar. 2017.

[68] É o termo utilizado por Stefano Rodotà, Regina Ruaro, Ingo Sarlet, Danilo Doneda, dentre outros. Especificamente sobre o tema, inclusive, Doneda, após tecer críticas à expressão vida privada, enfocando na questão da proteção de dados pessoais, sustenta que o termo privacidade "[...] é específico o suficiente para distinguir-se de outras locuções com as quais eventualmente deve medir-se, como a imagem, honra ou a identidade pessoal; e também e claro o bastante para especificar o seu conteúdo, um efeito da sua atualidade. Mas esta escolha não é a conseqüência somente da fragilidade das demais opções: ao contrário, ela revela-se por si só a mais adequada, justamente por unificar os valores expressos pelos termos intimidade e vida privada." DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 111-112.

[69] Nesse sentido, Sarlet, Marinoni e Mitidiero apontam que: "Na Constituição Federal, todavia, embora ambas as dimensões (privacidade e intimidade) tenham sido expressamente referidas, haverão de ser analisadas em conjunto, pois se cuida de esferas (níveis) do direito à vida privada [...] o fato de a esfera da vida íntima (intimidade) ser mais restrita que a da privacidade, cuidando-se de dimensões que não podem pura e simplesmente ser dissociadas, recomenda um tratamento

Tal construção remonta à teoria alemã dos círculos concêntricos, ou teoria das esferas[70]. Em que pese datar do ano de 1953, ela ainda segue atual e parte de uma primeira diferenciação – esfera individual (*Individualsphäre*) v. esfera privada (*Privatsphäre*). Tal distinção se presta a separar a proteção da personalidade na vida pública, do "eu social" – na qual se inseriria, por exemplo, o direito à honra e o direito à imagem – e a proteção em um âmbito de retiro, particular, do "eu privado" – na qual figuraria a proteção à vida privada e à intimidade[71].

Para além dessa divisão, a esfera privada é dividida em três círculos concêntricos ou esferas, sucessivamente menores e englobados pelo anterior. A primeira e mais ampla de todas é a esfera privada (*Privatsphäre*), que englobaria todos os comportamentos e informações pessoais que não se queira expor irrestritamente, ou seja, que não se tornem públicos. A esfera do meio, a qual seria englobada pela primeira, é a esfera da intimidade (*Vertrauenssphäre; Vertraulichkeitssphäre ou Intimsphäre*), que está atrelada a uma noção de confiança, familiaridade e, obviamente, intimidade. Assim, não só questões públicas estão fora de sua abrangência, mas aquelas questões que o indivíduo só compartilha com pessoas mais próximas, com quem tenha um convívio mais intenso. Por fim, a esfera mais restrita de todas – e abrangida pelas demais – é a esfera do sigilo (*Geheimsphäre*), a qual abrangeria apenas as questões que o indivíduo não compartilha com ninguém mais, ou apenas com aqueles melhores amigos e familiares mais próximos[72].

Cabe ressaltar, ainda, que tais esferas não são rígidas e variam consoante aspectos subjetivos do titular, como a cultura, a realidade social em que ele está

---

conjunto de ambas as situações." SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017. p. 445-446.

[70] "No Brasil, os direitos à intimidade e à privacidade estão referidos no artigo 5º, X, da Constituição Federal – CF, reconhecendo a distinção proveniente da doutrina e jurisprudência alemãs, da teoria das esferas ou dos círculos concêntricos. As esferas da vida privada comportam o grau de interferência que o indivíduo suporta com relação a terceiros. Para tal, leva-se em consideração o grau de reserva do menor para o maior. Assim, no círculo exterior está a privacidade; no intermediário, a intimidade; e, no interior desta, o sigilo. Deste modo, a proteção legal torna-se mais intensa, à medida que se adentra no interior da última esfera." LIMBERGER, Têmis. Mutações da privacidade e a proteção dos dados pessoais. In: RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (Org.). **Privacidade e proteção de dados pessoais na sociedade digital**. Porto Alegre: Fi, 2017. p. 145-168. p. 150.

[71] COSTA JR., Paulo José Da. **O direito de estar só**: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1970.

[72] HENKEL. **Der Strafschutz des Privatlebens gegen Indiskretion, in Verhandlugen des 42.** Deutschen Juristentages (Düsseldorf, 1957), Band II, Teil D, Erste Abteilung, Tübingen, 1958, apud COSTA JR., op. cit.

inserido e a atividade desempenhada pelo mesmo[73]. Outrossim, é importante referir que tal teoria não está isenta de críticas. Costa Jr.[74] assinala que a divisão em três esferas é "excessiva" e que a distinção em apenas duas seria suficiente, inclusive tal posicionamento estaria mais alinhado ao ordenamento jurídico pátrio que só prevê a proteção à vida privada e à intimidade – *vide* art. 5º, inciso X da Constituição Federal de 1988. Em sentido semelhante, Sarlet, Marinoni e Mitidiero transportam a teoria das esferas com apenas três distinções:

> [...] uma esfera íntima (que constitui o núcleo essencial e intangível do direito à intimidade e privacidade), uma esfera privada (que diz com aspectos não sigilosos ou restritos da vida familiar, profissional e comercial do indivíduo, sendo passível de uma ponderação em relação a outros bens jurídicos) e uma esfera social (em que se situam os direitos à imagem e à palavra, mas não mais à intimidade e à privacidade) [...].[75]

Por sua vez, Doneda, em que pese realizar a distinção entre vida privada, intimidade e privacidade, entende que a teoria dos círculos concêntricos já está superada desde a decisão do Tribunal Constitucional Alemão no caso da lei do censo de 1983. Segundo o autor, trabalhar com essas diferenciações daria mais margem a confusões do que a uma construção coerente em si – situação constatável, inclusive, em muitos textos jurídicos que não conseguem trabalhar adequadamente a diferenciação entre esses dois direitos. Nesse sentido, Doneda adota o vocábulo privacidade, por entender que ele é específico o suficiente para distinguir sua esfera de proteção de outros direitos da personalidade, como a imagem e a honra e "[...] claro o bastante para especificar seu conteúdo, um efeito da sua atualidade [...], justamente por unificar os valores expressos pelos termos intimidade e vida privada"[76].

De fato, a teoria das esferas da privacidade não se presta à especificação do conteúdo da privacidade, vez que as demais esferas – intimidade e segredo – são englobadas pela maior – privacidade. Nada obstante, entende-se que a distinção

---

[73] COSTA JR., op. cit.
[74] Ibid., p. 33.
[75] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017. p. 446-447.
[76] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 108-112.

proposta serve como um dos critérios para a fixação do *quantum debeatur* de eventual indenização quando da violação da privacidade[77]. Ademais, ela também se presta para definir um nível de proteção, *a priori,* mais rígido no que toca à tutela da esfera da intimidade e menos rígida no que concerne à esfera da privacidade em si[78].

A esse respeito, de suma importância a lição de Sarlet, Marinoni e Mitidiero, no sentido de que o principal critério para a determinação do âmbito de proteção do direito à privacidade deve ser de cunho "material e não formal"[79]. Ademais, em termos de sua dimensão subjetiva, ganha relevância o fato de que ele opera, em um primeiro momento, como um direito de defesa e, em um segundo momento, como verdadeiro direito de autodeterminação, enquanto expressão da liberdade pessoal[80].

Trabalhando o direito à intimidade (que é abrangido pelo direito à privacidade) Limberger ressalta não só sua dimensão negativa – enquanto direito a não ser molestado –, mas sua dimensão positiva, desdobradas em prestações concretas pelo Estado. Segundo ela, resultam desta "[...] a objetividade dos dados, o direito ao esquecimento, a necessidade de prazo para armazenamento de informações

---

[77] A fixação da indenização por danos extrapatrimoniais é um dos aspectos mais controvertidos da responsabilidade civil exatamente por seu caráter não monetário e pela falta de critérios bem definidos para seu arbitramento. Sob essa lógica, percebe-se, no âmbito doutrinário, uma crescente tipificação dos danos extrapatrimoniais, superando aquela noção de que o dano extrapatrimonial limitar-se-ia ao dano moral, situação que também serviria como parâmetro para sua fixação. Nesse sentido ver: SOARES, Flaviana Rampazzo. **Responsabilidade civil por dano existencial**. Porto Alegre: Livraria do Advogado, 2009.

[78] Em sentido semelhante Sarlet, Marinoni e Mitidiero apontam que é insuficiente "[...] qualquer tipo de categorização fechada [para a distinção entre vida privada e intimidade] é possível, contudo, distinguir um âmbito que, ao menos em princípio, é – já pela sua conexão com a dignidade da pessoa humana – absolutamente protegido, insuscetível, portanto, de intervenção estatal, e uma esfera mais aberta, em que a pessoa se encontra entre pessoas e com elas interage, que, por sua vez, é passível de intervenção, desde que mediante estrita observância dos critérios da proporcionalidade e para salvaguardar outros direitos fundamentais ou bens e interesses constitucionalmente assegurados". SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017. p. 448.

[79] Ibid., p. 449.

[80] "Dada a sua dupla dimensão objetiva e subjetiva, o direito à privacidade opera, na condição de direito subjetivo, em primeira linha como direito de defesa, portanto, como direito à não intervenção por parte do Estado e de terceiros no respectivo âmbito de proteção do direito e, como expressão também da liberdade pessoal, como direito a não ser impedido de levar sua vida privada conforme seu projeto existencial pessoal e de dispor livremente das informações sobre os aspectos que dizem respeito ao domínio da vida pessoal e que não interferem em direitos de terceiros. Assim, o direito à privacidade é também direito de autodeterminação do indivíduo." Ibid., p. 449.

negativas e a comunicação de repasse dados, a fim de favorecer o direito de acesso e retificação de informação"[81].

Por fim, no que diz respeito à limitação desse direito fundamental, aponta-se que não só inexiste expressa reserva legal, mas foi assegurada a inviolabilidade desse direito. Em que pese tal situação não importar em um direito absoluto, sua estrutura normativa constitucional demanda que eventuais restrições à sua aplicação se limitem aos casos em que forem necessárias a conformação da privacidade com outros direitos fundamentais ou valores constitucionalmente assegurados, o que só pode ser verificado, invariavelmente, diante do caso concreto[82].

1.2.2 Privacidade e personalidade

Enquanto direito de personalidade[83], o direito à privacidade é dotado de todos os atributos próprios dessa categoria de direitos. Os direitos da personalidade consistem em direitos inatos, personalíssimos, extrapatrimoniais e imprescindíveis. Posto isso, tratam-se de direitos intransmissíveis, imprescritíveis, impenhoráveis, vitalícios e oponíveis *erga omnes*[84]. Inclusive, o próprio Código Civil de 2002, em seu art. 11, dispõe expressamente que, "[...] com exceção dos casos previstos em

---

[81] LIMBERGER, Têmis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007. p. 40.

[82] "[...] o direito à privacidade não se revela ilimitado e imune a intervenções restritivas. Todavia, ao não prever, para a privacidade e intimidade, uma expressa reserva legal, além de afirmar que se cuida de direitos invioláveis, há que reconhecer que a Constituição Federal atribuiu a tais direitos um elevado grau de proteção, de tal sorte que uma restrição apenas se justifica quando necessária a assegurar a proteção de outros direitos fundamentais ou bens constitucionais relevantes (no caso, portanto, de uma restrição implicitamente autorizada pela Constituição Federal), de modo que é em geral na esfera dos conflitos com outros direitos que se pode, em cada caso, avaliar a legitimidade constitucional da restrição." SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017. p. 449.

[83] Com a devida adequação ao caráter mais amplo da privacidade, pode-se inferir que a afirmação de Limberger, no sentido de que "[...] o direito fundamental à intimidade pessoal e familiar deriva-se da dignidade humana e está vinculado à própria personalidade, sendo seu núcleo central. Como direito que é da expressão da própria pessoa, desfruta da mais alta proteção constitucional." LIMBERGER, Têmis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007. p. 116.

[84] Nesse sentido: CUPIS, Adriano de. **Os direitos da personalidade**. Tradução Afonso Celso Furtado. Campinas: Romana, 2004; BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed. São Paulo: Saraiva, 2015; BELTRÃO, Silvio Romero. **Direitos da personalidade**: de acordo com o novo Código Civil. São Paulo: Atlas, 2005; SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014.

lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária"[85].

A intransmissibilidade está atrelada à noção de infungibilidade; transmitir é colocar uma pessoa no lugar de outra. Como os direitos da personalidade consistem em direitos personalíssimos, a transferência de um direito de personalidade para um terceiro seria incompatível com a natureza do mesmo. Cumpre asseverar, apenas, que a intransmissibilidade não atinge os efeitos patrimoniais decorrentes desses direitos, os quais são passíveis de transmissão[86].

A irrenunciabilidade, por sua vez, encontra fundamento na qualidade de direito intrínseco ao ser humano, característica inerente aos direitos da personalidade. Em que pese a existência de um combate doutrinário entre as correntes juspositivita e a corrente jusnaturalista, ambas são uníssonas na definição dos direitos de personalidade enquanto direitos essenciais e, portanto, inatos.

Segundo os juspositivistas, os direitos da personalidade não são impostos por uma ordem natural (ou sobrenatural) aos sistemas jurídicos[87]. Eles seriam, nos termos de Pontes de Miranda,

> [...] efeitos de fatos jurídicos, que se produziram nos sistemas jurídicos, quando, a certo grau de evolução, a pressão política fez os sistemas jurídicos darem entrada a suportes fáticos que antes ficavam de fora, na dimensão moral ou na dimensão religiosa.[88]

---

[85] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, seção 1, Brasília, DF, a. 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/CCivil_03/leis/2002/L10406.htm>. Acesso em: 20 mar. 2017.

[86] PONTES DE MIRANDA. **Tratado de direito privado**. Atualizado por Rosa Maria Barreto Borriello de Andrade Nery. São Paulo: Revista dos Tribunais, 2012. t. VII.

[87] Ainda que trabalhando sob uma perspectiva dos direitos fundamentais, e não dos direitos da personalidade em si, Sarlet se afasta, ao menos em parte, de uma concepção Jusnaturalista dos direitos fundamentais ao reconhece-los como fruto de processos históricos e reivindicações sociais, sendo antes produtos culturais do que de uma ordem (sobre)natural. SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado, 2015.

[88] PONTES DE MIRANDA. **Tratado de direito privado**. Atualizado por Rosa Maria Barreto Borriello de Andrade Nery. São Paulo: Revista dos Tribunais, 2012. t. VII. p. 58-59.

Cupis[89], por sua vez, entende que, somente a partir da atribuição desses direitos subjetivos à pessoa pela ordem jurídico-positiva, é possível afirmar que determinados direitos subjetivos podem ser, de fato, inatos. Outrossim, assevera-se que os direitos da personalidade são direitos inatos em face de sua essencialidade, e, como tais, não se enquadram na categoria de direitos derivados ou adquiridos[90]. É o que também expõe Bittar[91] acerca do Juspositivismo, em que pese não compartilhar o entendimento de tal corrente doutrinária.

Em contrapartida, a Corrente Jusnaturalista é fortemente influenciada por correntes filosóficas existencialistas. Segundo a linha de pensamento dessa corrente, não há, por parte do Estado, uma criação de direitos da personalidade. Tratam-se de direitos inatos e, portanto, pré-existentes à própria noção de Estado. A esse, por conseguinte, caberia, apenas, o reconhecimento e a tutela desses direitos que lhe são anteriores. Inclusive, poder-se-ia dizer, seguindo essa corrente, que é a própria tutela dos direitos da personalidade que dá legitimidade ao Estado, e não o contrário[92].

Independentemente da corrente doutrinária adotada, é preciso reconhecer que a aceitação e consolidação dos direitos da personalidade perpassam por uma mudança paradigmática no ordenamento jurídico, em especial no âmbito do direito civil. A superação de um direito em que a propriedade era parâmetro para tudo a um ordenamento estruturado a partir da (dignidade da) pessoa humana permitiu o reconhecimento de que existem direitos que compõem uma base essencial para o livre desenvolvimento da personalidade de forma autônoma e digna[93].

Por fim, no que toca à vedação de limitação voluntária, é preciso diferenciar essa do exercício regular de um direito da personalidade. Seguindo a linha do

---

[89] CUPIS, Adriano de. **Os direitos da personalidade**. Tradução Afonso Celso Furtado. Campinas: Romana, 2004. p. 24-25.

[90] Os direitos derivados ou adquiridos pressupõem o preenchimento de certos requisitos, além da própria personalidade. Por outro lado, os direitos inatos seriam aqueles em que bastaria a personalidade para sua atribuição. BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed. São Paulo: Saraiva, 2015.

[91] Ibid.

[92] SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014.

[93] DONEDA, Danilo. Os direitos da personalidade no Código Civil. **Revista da Faculdade de Direito de Campos**, Rio de Janeiro, a. VI, n. 6, p. 71-99, jun. 2005. Disponível em: <http://www.uniflu.edu.br/arquivos/Revistas/Revista06/Docente/03.pdf >. Acesso em: 10 abr. 2017.

Enunciado nº 4[94] da I Jornada de Direito Civil de 2002 que dispõe que "[...] o exercício dos direitos da personalidade pode sofrer limitação voluntária, desde que não seja permanente nem geral", Schreiber sustenta que, quando há uma limitação voluntária pontual, por exemplo: furar a orelha para colocar um brinco ou um *piercing;* a participação em um *reality show;* ou a prática de uma luta, essa limitação voluntária é lícita[95]. O autor, inclusive, estabelece critérios para a verificação da legitimidade dessa limitação, quais sejam: "[...] (i) o alcance, (ii) a duração, (iii) a intensidade e (iv) a finalidade da autolimitação"[96].

Em sentido semelhante, Delgado[97] aponta que o art. 11 do Código Civil não veda a "fruição econômica" dos direitos da personalidade. Daí ser possível, por exemplo, a comercialização da própria imagem para fins comerciais ou até mesmo para pornografia, sendo vedada apenas a cessão duradora – no que toca ao aspecto temporal – e indeterminada – no que concerne ao objeto.

Não obstante as opções terminológicas supracitadas, prefere-se a noção de disponibilidade dos direitos trabalhada por Bittar[98], tendo em vista que tal definição não vai de encontro ao disposto no art. 11 do Código Civil de 2002, que veda, expressamente, a limitação voluntária. Ademais, entende-se que, dependendo das características e da natureza do direito em análise, determinadas situações que, *a priori,* aparentariam uma renúncia ou limitação voluntária, consistem, na verdade, no regular exercício do direito. Segundo Bittar:

> [...] diante das necessidades decorrentes de sua própria condição, da posição do titular, do interesse negocial e da expansão tecnológica, certos direitos da personalidade acabaram ingressando na circulação jurídica, admitindo-se ora a sua disponibilidade, exatamente para permitir a melhor

---

[94] AGUIAR JÚNIOR, Ruy Rosado de (Coord. Científico). **Jornadas de direito civil I, III, IV e V**: enunciados aprovados. Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2012.

[95] Também nessa esteira, Vieira defende que, "[...] no caso do direito à privacidade, o art. 20 do CC expressamente prevê a possibilidade de *limitação temporária de exercício,* desde que exista prévia autorização do titular ou quando for necessária tal limitação, em atendimento à administração da Justiça ou à ordem pública". [Grifo no original]. VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007. p. 127.

[96] SCHREIBER, op. cit., p. 29.

[97] DELGADO, Mário Luiz. Big Brother Brasil: reality shows e os direitos da personalidade. **Revista Jurídica Consulex**, Brasília, a. VIII, n. 169, p. 24-26, jan. 2004. Disponível em: <https://marioluizdelgado.files.wordpress.com/2014/04/mario-luiz-delgado-3.pdf>. Acesso em: 13 jun. 2017.

[98] BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed. São Paulo: Saraiva, 2015.

> fruição por parte de seu titular, sem, no entanto, afetar-se os seus caracteres intrínsecos.[99]

Ou seja, tornar um fato público não configuraria uma limitação (voluntária) à privacidade por parte do próprio titular do direito. Ao se entender o direito à privacidade como um direito não só de constranger terceiros – Estado ou particular – contra ingerências na sua esfera privada, mas de controlar as informações de caráter pessoal[100], a exposição de um fato, *a priori*, privado não pode implicar a limitação desse direito, vez que inerente ao seu próprio exercício: controle de informações.

Nesse sentido, os critérios trazidos por Schreiber[101] para verificar a legitimidade de uma limitação voluntária pontual são de grande valia. Trabalhando o exemplo dos direitos autorais trazido por Bittar[102], identifica-se, de forma clara, o interesse do próprio titular na ampliação da circulação de sua obra, inclusive mediante remuneração, sendo tal disponibilidade essencial para a melhor fruição desse direito.

No âmbito específico do direito à privacidade, o caso dos *reality shows* também encontra solução a partir dos critérios trazidos por Schreiber, especialmente no que toca ao critério (ii) da duração[103]. Em se tratando de uma exposição temporária, reconhece-se a possibilidade de o indivíduo participar de programas como o "Big Brother", uma vez que tal situação não viola, *a priori,* seu direito à privacidade[104].

---

[99] Ibid., p. 44

[100] Nesse sentido: VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007; DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006; RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

[101] SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014.

[102] BITTAR, op. cit.

[103] SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014.

[104] Nesse sentido ver: CANOTILHO, José Joaquim Gomes. **"Reality shows" e liberdade de programação**. Portugal: Coimbra, 2003.

Dessa feita, a disponibilidade defendida não é absoluta (ou irrestrita), tendo em vista que deve obedecer a determinados critérios, a fim de não esbarrar na proibição prevista no art. 11 do Código Civil de 2002[105].

Outro ponto controvertido na construção da privacidade enquanto um direito da personalidade é a extensão dos direitos da personalidade às pessoas jurídicas. Uma vez que se trata de direitos intrínsecos do ser humano e imprescindíveis ao livre desenvolvimento de sua personalidade, tais direitos seriam incompatíveis com as pessoas não humanas[106]. Por outro lado, alguns defendem que o art. 52 do Código Civil de 2002[107], ao dispor que "[...] aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade", estendeu tais direitos às pessoas jurídicas[108].

Em se tratando de questão que foge ao objeto do presente trabalho, julga-se pertinente referir, apenas, que o Superior Tribunal de Justiça editou Súmula a respeito do tema, reconhecendo a possiblidade de uma pessoa jurídica sofrer dano moral – Súmula 227[109].

Superada tais questões, cabe delinear um direito à privacidade na conjuntura jurídico-social atual.

1.3 NOVOS CONTORNOS DO DIREITO À PRIVACIDADE

---

[105] SCHREIBER, op. cit.

[106] Segundo essa linha de pensamento, o que o art. 22 do Código Civil de 2002 estende às pessoas jurídicas é a "proteção" dos direitos da personalidade e não o direito em si. Ademais o legislador faz a ressalva de que a proteção é só "no que couber", ou seja, apenas nos casos em que ela for compatível com a figura das pessoas jurídicas. Ibid., p. 22.

[107] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, seção 1, Brasília, DF, a. 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/CCivil_03/leis/2002/L10406.htm>. Acesso em: 20 mar. 2017.

[108] Segundo Fábio de Andrade, a tutela das pessoas jurídicas por meio dos direitos da personalidade, perpassa por uma "concepção funcionalizante" desses direitos como meio de garantir interesses e valores básicos de uma pessoa jurídica a partir de uma "visão jurídica finalista". ANDRADE, Fábio Siebeneichler de. O desenvolvimento da tutela dos direitos da personalidade nos dez anos de vigência do Código Civil de 2002. In: LOTUFO, Renan; NANNI, Giovanni Ettore; MARTINS, Fernando Rodrigues (Coord.). **Temas relevantes do direito civil contemporâneo**: reflexões sobre os 10 anos do Código Civil. São Paulo: Atlas, 2012. p. 51-85. p. 68.

[109] BRASIL. Superior Tribunal de Justiça. Súmula n° 227. A pessoa jurídica pode sofrer dano moral. **Diário de Justiça**, seção 2, Brasília, DF, p. 126, 08 out. 1999.

Trabalhar numa perspectiva mais atual do direito à privacidade, reitera-se, não exclui suas formulações anteriores. Tal perspectiva, consoante aponta Mills, importa no reconhecimento das influências que "[...] família, religião, riqueza, estrutura política, história, clima, hábitos de trabalho, geografia, ideologia, urbanização, normas culturais e tecnologia"[110] geram sobre a definição social e jurídica desse direito.

Nesse sentido, importante destacar que se vive na chamada sociedade da informação ou era da informação. Tal sociedade, dita mais aberta, solidária e democrática[111], é marcada pelo fenômeno da globalização e tem na rede de computadores – internet – a sua principal figura[112].

A definição de "sociedade da informação" parte da ideia de uma sociedade estruturada a partir da informação, sendo essa matéria-prima imprescindível ao desenvolvimento de qualquer atividade. Entrementes, resta incontroverso o fato de que a comunicação e a coleta de dados consistem e sempre consistiram nos pilares de toda e qualquer interação social[113], portanto, tal situação, *per si,* não justificaria a nomenclatura dada a essa sociedade[114].

O que diferencia essa sociedade das demais – e justifica sua nomenclatura – é a forma como a informação é tratada e aplicada no cotidiano social. As transformações vivenciadas a partir do século XX, em especial no que concerne às tecnologias da informática, revolucionaram a capacidade de organização, armazenamento e transmissão de dados de uma forma sem precedentes. Tal

---

[110] MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008. p. 18.

[111] LEMOS, André; LÉVY, Pierre. **O futuro da internet**: em direção a uma ciberdemocracia planetária. São Paulo: Paulus, 2010.

[112] Segundo Castells, "[...] se a tecnologia da informação é hoje o que a eletricidade foi na Era Industrial, em nossa época a Internet poderia ser equiparada tanto a uma rede elétrica quando ao motor elétrico, em razão de sua capacidade de distribuir a força da informação por todo o domínio da atividade humana". CASTELLS, Manuel. **A galáxia internet**. Reflexões sobre internet, negócios e sociedade. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004. p. 25.

[113] O reconhecimento do valor do conhecimento e da informação remonta para bem antes dos primeiros escritos acerca da sociedade da informação datados do início da década de 1960 nos Estados Unidos, porém, até então, ela era considerada apenas como mais um recurso e não como o principal recurso. Nesse sentido ver: MAY, Christopher. **The information society**: a sceptical view. Cambridge: Polity, 2002.

[114] Doneda aponta que não só a coleta, mas o tratamento de dados consiste em uma prática milenar. Há registros de coletas sistematizadas de informações populacionais, ou seja, censos que datam à mais de 2.000 a.C., como é o caso do censo solicitado pelo imperador chinês Yao em 2238 a.C. DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2. p. 91-108, jul./dez. 2011.

incremento no fluxo de comunicações foi tamanho que acarretou significativas mudanças na estrutura socioeconômica global, atingindo todos os âmbitos de interação social[115].

O início da era da informação é marcado exatamente pelos meios de comunicação em massa – rádio, tv, jornais impressos etc. Torna-se gritante o poder da imprensa e dos meios de comunicação – o chamado quinto poder –, surgindo inúmeros trabalhos acadêmicos, cuja preocupação recai na manutenção da lógica do pensamento único que tais meios proporcionam[116]. A internet, nesse contexto, surge como promessa de quebrar com esse monopólio, apresentando-se como ferramenta capaz de democratizar a informação, tanto no polo do receptor como no do comunicador, desde que articulada corretamente.

Desde suas origens, na rede de computadores da ARPA – *Advanced Research Projects Agency* – na década de 1960, a interatividade era um dos objetivos da internet, ainda que sua construção inicialmente atendesse a fins militares. Posteriormente, com a intercessão de uma cultura libertária no desenvolvimento da rede, a ferramenta *www* (*world wide web*), projetada em 1990, possibilitou que a internet ostentasse um alcance global[117], o que, somado ao seu caráter descentralizado, abriu margem para uma maior participação social a nível global.

Assim, a internet – especialmente em sua faceta de *web* participativa ou *web* 2.0[118] – desempenha papel essencial no exercício da democracia, a ponto de se

---

[115] DELSON, Ferreira. **Manual de sociologia**: dos clássicos à sociedade da informação. São Paulo: Atlas, 2003.

[116] MAY, op. cit.

[117] CASTELLS, Manuel. **A galáxia internet**. Reflexões sobre internet, negócios e sociedade. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

[118] A definição de *web* 2.0 decorre de uma classificação criada para diferenciar as diferentes fases do desenvolvimento da rede mundial de computadores: a internet. A *web* 1.0, seria a internet em sua versão inicial, consistente em *sites* de conteúdo estático com pouca ou nenhuma interatividade. A *web* 2.0, por sua vez, é marcada pelo surgimento dos *blogs*, *chats*, redes sociais e outras formas de mídia colaborativa, nas quais o conteúdo dos *sites* na internet é gerado pelos próprios usuários, por isso também e chamada de *web* participativa. A *web* 3.0, por fim, seria a inserção de mecanismos inteligentes na internet, não só a partir de mecanismos como *smartphones*, mas com o desenvolvimento de *softwares* capazes de filtrar o conteúdo da internet, gerlamente com base na utilização do usuário. EX2. **Web 1.0, Web 2.0 e Web 3.0...** Enfim o que é Isso? 2013. Disponível em: <http://www.ex2.com.br/blog/web-1-0-web-2-0-e-web-3-0-enfim-o-que-e-isso/>. Acesso em: 28 mar. 2017.

falar, até, em uma ciberdemocracia[119]. Além de possibilitar a utilização de inúmeros mecanismos de participação direta, ela também rompe com o monopólio detido pelas mídias clássicas na veiculação de informações[120].

Ainda no âmbito das TICs, a Comissão Europeia de 2010 – *European 2020 Strategy* – fez da *Digital Agenda* um de seus aspectos mais importantes, dando especial destaque ao *Big Data*[121]. O próprio "EU Commissioner Kroes afirmou que o 'Big Data é o novo petróleo' que pode ser gerenciado, manipulado e utilizado como nunca antes, graças a ferramentas eletrônicas de alta performance". Em momento posterior, ainda, ele afirmou que o *Big Data* seria um verdadeiro "combustível da inovação", enaltecendo sua utilidade na seara econômica[122].

Tamanha euforia não é por acaso. Espera-se que, em 2020, o universo digital conterá 44 *zettabytes*, ou seja, 44 trilhões de *Gigabytes*, sendo que em 2013 eram apenas 4.4 *zettabytes* (um aumento de 1.6 *zettabytes* em relação a 2012)[123]. Desses 44 *zettabytes*, espera-se que ao menos 16 *zettabytes* serão de dados utilizáveis[124]. Com essa crescente disponibilidade de dados e a apropriação dos mesmos a partir

---

[119] A partir de uma análise dos presentes processos sociais marcados por um conjunto de tecnologias (especialmente de informação e os meios de sociabilidade que essas criam), aos quais se atribui a denominação "Cibercultura", Levy e Lemos identificam princípios como a da liberação do pensamento e da palavra e o da conexão e conversação mundial (também chamada de "inteligência coletiva"). Tais princípios seriam a base de uma sociedade mais cooperativa, mais aberta e mais politicamente consciente e inteligente. Assim, "[...] o que se espera são mudanças globais da esfera política em direção a uma ciberdemocracia. [...] Pensar a ciberdemocracia do futuro deve partir do reconhecimento dos rumos da democracia não apenas em uma sociedade de *fluxo massivo industrial informacional*, mas em uma sociedade planetária em que ao fluxo massivo juntam-se *funções pós-massivas pós-industriais conversacionais*". [Grifo no original]. LEMOS, André; LÉVY, Pierre. **O futuro da internet**: em direção a uma ciberdemocracia planetária. São Paulo: Paulus, 2010.p. 28.

[120] Nesse sentido: LEMOS; LÉVY, op. cit.; CASTELLS, op. cit.

[121] *Big Data* é o nome dado a um grande volume de dados armazenados de forma ordenada, a fim de que a interpretação destes permita a previsão de tendências e auxilie nas tomadas de decisão de uma empresa, do Estado ou até mesmo de um indivíduo. SAS Institute. **Big data**: o que é e por que é importante? Disponível em: <https://www.sas.com/pt_br/insights/big-data/what-is-big-data.html#>. Acesso em: 16 ago. 2017.

[122] "*EU Commissioner Kroes stated, 'Big Data is the new Oil' that can be managed, manipulated, and used like never before thanks to high-performance digital tools, making big data the fuel for innovation*", em razão da importância da utilização do *Big Data* no âmbito econômico. [Tradução livre]. CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang. The big data value opportunity. In: _____ (Org.). **New horizons for a data-driven economy**: a roadmap for usage and exploitation of big data in Europe. Cham (Suiça): Springer Open, 2016. p. 3-11. p. 5.

[123] Dados disponíveis em SAS Institute. **Big data**: o que é e por que é importante? Disponível em: <https://www.sas.com/pt_br/insights/big-data/what-is-big-data.html#>. Acesso em: 16 ago. 2017.

[124] TURNER, V., GANTZ, J. F., REINSEL, D. & MINTON, S. **The digital universe of opportunities**: rich data and the increasing value of the internet of things. Rep. from IDC EMC. 2014. Disponível em: <https://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf>. Acesso em: 5 abr. 2017.

de mecanismos de tratamento de *Big Data* em todos os setores da economia, abre-se a possiblidade de um aumento na eficiência da gestão e aplicação de recursos, implicando uma significativa economia dos mesmos.

No setor público, mais especificamente na seara administrativa, a redução de custos gestão em termos de Continente Europeu é estimada em 15% a 20%, o que equivaleria a aproximadamente 300 bilhões de euros. No âmbito da saúde, estima-se uma economia de 90 milhões de euros com o uso de sistemas informatizados que recepcionam a *Big Data*[125]. Nos EUA, a economia é avaliada em mais de 300 bilhões de dólares até 2020[126]. Por sua vez, a utilização de *Big Data* nos setores de energia e transporte possibilita uma maior eficiência no que toca aos sistemas de logística, principalmente quando realizada a partir da coleta de dados de programas de navegação com GPS – por exemplo, o *Waze* ou *Google Maps*. Em uma perspectiva global, a utilização desses dados pode gerar uma economia – em termos de tempo e combustível – de 500 bilhões de dólares, além de reduzir 380 *megatonnes* da emissão de CO^2 [127].

Entrementes, é necessário cuidado para não ser vítimas do viés do otimismo excessivo[128] em relação à internet e sua promessa de liberdade inesgotável. “A internet é de fato uma tecnologia da liberdade – mas pode libertar os poderosos para oprimir os desinformados, pode levar à exclusão dos desvalorizados pelos conquistadores do valor”[129].

A internet tornou-se não só uma ferramenta indispensável, mas praticamente um instrumento onipresente em nossas vidas, projetando-se no ambiente familiar, profissional e até mesmo se tornando uma extensão de nossos corpos através dos *smartphones*. Com isso, cresce significativamente o interesse de grandes polos

---

[125] CAVANILLAS; CURRY; WAHLSTER, op. cit., p. 3-11.

[126] OECD. **Exploring data-driven innovation as a new source of growth** – mapping the policy issues raised by “Big Data.” Rep. from OECD, 2013. Disponível em: <http://dx.doi.org/10.1787/5k47zw3fcp43-en>. Acesso em: 20 abr. 2017.

[127] Ibid.

[128] O viés do otimismo excessivo consiste, basicamente, na confiança extremada, guardando conexão “[...] com previsões exageradamente seguras (e negligentes), ligadas a erros nem sempre inocentes”. Como solução, Juarez Freitas propõe um a dose moderada de otimismo, balizando eventual excesso a partir dos princípios da prevenção e da precaução. FREITAS, Juarez. A hermenêutica jurídica e a ciência do cérebro: como lidar com os automatismos mentais. **Revista da AJURIS**, Porto Alegre, v. 40, n. 130, p. 223-244, jun. 2013.

[129] CASTELLS, Manuel. **A galáxia internet**. Reflexões sobre internet, negócios e sociedade. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

econômicos e entes políticos sob sua infraestrutura e conteúdo[130]. Sob esse aspecto, a utilização da internet é complementar a ferramenta do *Big Data*, vez que serve de meio para a captação de dados, inclusive de natureza pessoal e que gera novas problemáticas no campo da privacidade.

É em face de tais questões que o aspecto informacional se tornou, hoje, a principal preocupação daqueles que trabalham com o direito à privacidade. O fato de o indivíduo estar sempre sujeito a coletas de seus dados pessoais – quando realiza uma compra via cartão de crédito ou navega pela internet – faz com que ele perca o controle sobre suas próprias informações, bem como tenha ameaçada a sua esfera privada.

Tal preocupação é evidente nos conceitos mais modernos de privacidade. Partindo de Rodotà, esse define privacidade como "[...] o direito de manter o controle sobre as próprias informações e de *determinar as modalidades de construção da própria esfera privada"*[131]. [Grifo no original].

Doneda, por sua vez, aponta que a privacidade não se limita a uma questão de isolamento e não publicização, muitas vezes está atrelada a questões como liberdade, autonomia, não discriminação, igualdade e, também, à própria personalidade, reconhecendo uma íntima relação entre privacidade e livre arbítrio ou autonomia. Segundo ele, a privacidade não é, por si só, um valor, assumindo "[...] um caráter relacional, que deve determinar o nível de relação da própria personalidade com as outras pessoas e com o mundo exterior – pela qual a pessoa determina sua inserção e de exposição"[132]. Ainda, Vieira conceitua o direito à privacidade como

> [...] um direito subjetivo de toda pessoa – brasileira ou estrangeira, residente ou transeunte, física ou jurídica – não apenas de constranger os outros a respeitaram sua esfera privada, mas também de controlar suas informações

[130] Ibid.
[131] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 109.
[132] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 146.

> de caráter pessoal – sejam estas sensíveis ou não – resistindo às intromissões indevidas provenientes de terceiros.[133]

Em todos os autores percebe-se que a construção da privacidade perpassa pelo controle das próprias informações, estando fortemente presente a figura da autonomia. Mills[134], por sua vez, parte de uma abordagem um pouco distinta. Em que pese reconhecer a privacidade como um conceito subjetivo, no âmbito legal o autor prefere trabalhar com base em uma *resonable expectation of privacy*, cuja variação é lastreada na sociedade e não no indivíduo em si.

Nesse aspecto, filia-se à ideia de que o indivíduo possa definir, ainda que não de forma absoluta[135], a sua esfera privada, vez que capaz de decidir o que expor e o que manter protegido. Situação fática que corrobora com essa tese é o próprio *design* dos *sites* de relacionamento, os quais, de tão utilizados, são considerados como indispensáveis pela população em geral. Tomando o *Facebook* como exemplo, verifica-se que o usuário define quais informações pretende inserir na sua página pessoal, inclusive delimitando quem terá acesso a essas informações e em que medida será esse acesso (se ao todo ou apenas parte delas).

Ademais, dessa noção de autonomia reitera-se que o direito à privacidade é um direito fundamental, caracterizado como um direito da personalidade e oponível *erga omnes,* servido como proteção, tanto frente ao Estado como frente a particulares. Para um delineamento do mesmo, ainda que em linhas gerais, adota-se

---

[133] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007. p. 30.

[134] "*Despite multiple general definitions, privacy is a subjective and highly personal concept. […] In legal terms, however, the individual does not get to define his or her own boundaries in modern society. The legal system cannot respond to and redress harm according to an individual's view of his or her privacy rights. Legal recognition of privacy is based on a reasonable expectation of privacy rather than a personal subjective perception.*" MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008. p. 20-21.

[135] Não se está, aqui, negando a validade de critérios objetivos para a definição da esfera privada, os quais serão, inclusive, enfrentados no decorrer deste trabalho. O que se sustenta é que a percepção subjetiva influencia sim na construção da privacidade individual (e até coletiva) devendo ser levada em consideração caso a caso.

as “categorias” de privacidade propostas por Vieira[136], a fim de trazer a ideia dos diferentes direitos que compõem um direito “geral” à privacidade.

A autora trabalha com “categorias” de privacidade a partir de seu âmbito de proteção[137]. Partindo da ideia de Sarlet[138] de que um direito é dotado de diversas dimensões a partir da posição subjetiva de seu titular (ou titulares), as categorias trabalhadas pela autora são bastante ilustrativas para mostrar as diferentes formulações e posições que o direito à privacidade assume no caso em concreto e que são englobadas por uma dimensão objetiva do direito à privacidade.

A *privacidade física* corresponderia à proteção contra procedimentos invasivos não autorizados, como testes de drogas e exames genéticos. A *privacidade do domicílio* seria aquela expressa no art. 5º, inciso XI da Constituição Federal de 1988, que dispõe que “[...] a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial”. A *privacidade das comunicações* também respaldada no texto constitucional – art. 5º, inciso XII – garantindo a inviolabilidade de correspondências, comunicações telegráficas, de dados e telefônicas. A *privacidade decisional* corresponderia ao direito à autodeterminação, consistente no poder de decisão do indivíduo, ou seja, sua liberdade de escolha. Por fim, a *privacidade informacional*, cujo âmbito de proteção recai nas informações pessoais e íntimas dos indivíduos[139].

Dessa feita, percebe-se que trabalhar com uma definição permanente de privacidade seria incorrer em um equívoco[140]. O direito à privacidade ainda encampa a ideia de um *right to be let alone* – tutelando a pessoa contra a ingerência de terceiros na sua esfera privada –, bem como tutela a pessoa contra a coleta e a transmissão de informações privadas sem a autorização do próprio titular. No futuro,

---

[136] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007.

[137] Ibid.

[138] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado, 2015.

[139] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007.

[140] MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008.

tal direito certamente sofrerá a influência de inovações tecnológicas e das consequentes ameaças que essas implicarão sobre a esfera privada do indivíduo.

Outra aproximação de suma importância é a do direito à privacidade em relação ao livre desenvolvimento da personalidade e à própria identidade dos indivíduos. Como bem aponta Garfinkel, a privacidade não se reduz a esconder coisas, ela está atrelada a uma noção de "[...] auto-posse, autonomia, e integridade [...] é o direito da pessoa controlar quais detalhes de sua vida permanecem dentro de sua própria casa e quais são expostos para fora"[141]. A bem da verdade, a privacidade é um direito que se presta a proteger o indivíduo contra outros estigmas e problemas sociais ainda não solucionados, decorrendo daí sua imprescindibilidade[142].

O direito de as pessoas controlarem e definirem suas esferas privadas, escolhendo quais detalhes de sua vida permanecem resguardados e quais são expostos, permite que cada um desenvolva a sua individualidade, furtando-se ao julgamento e à opinião alheia. A privacidade, assim, consubstancia-se em uma verdadeira proteção contra estigmas e preconceitos sociais ao permitir que o indivíduo desenvolva sua personalidade e suas convicções sem se submeter a uma pressão social geralmente imposta por uma lógica imposição de valores dominantes.

Nesse diapasão, o simples exercício da liberdade pressupõe a existência de privacidade, pois somente essa proporciona um momento de reflexão – a relação entre o ser e seu íntimo –, sem a influência externa da sociedade para interferir nas escolhas individuais, ou seja, é a privacidade que garante a autodeterminação do indivíduo. Da mesma forma, a liberdade é pressuposto imprescindível para a efetivação do direito à privacidade[143]. Não demanda muito esforço a percepção de que, em Estados autoritários, um dos principais mecanismos de manutenção do

---

[141] "*Privacy isn't just about hiding things. It's about self-possession, autonomy, and integrity* [...] *It's the right of people to control what details about their lives stay inside their own houses and what leaks to the outside.*" GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010. p. 4.

[142] Nas palavras de Garfinkel: "*One of the purposes of privacy in society is to protect us from other social problems that we have not yet eradicated.*" Ibid., p. 133.

[143] É o que se extrai de Vieira ao afirmar que: "privacidade e liberdade se amalgamam como duas faces de uma mesma moeda, uma vez que tão-somente o manto de proteção da privacidade proporciona a um indivíduo o direito ao exercício da liberdade [...] [Ou seja], não se assegura privacidade sem liberdade, e não se exercita liberdade sem privacidade". VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação:** efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007. p. 27-29.

poder é a supressão da privacidade dos indivíduos, a qual possibilita um controle "total" do cidadão[144].

1.4 DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS[145]

Com base no exposto, aufere-se que o direito à privacidade é um direito em um constante processo de construção. Nota-se que o conteúdo desse direito é amplamente influenciado pelos avanços tecnológicos e pelas implicações desses na esfera privada do indivíduo, de modo a readequá-lo ao contexto socioeconômico em que se insere.

A dimensão negativa desse direito, consubstanciada especialmente no *right to be let alone,* ainda que de grande pertinência para a defesa do indivíduo, é insuficiente para dar respostas aos novos meios de tratamento de informações pessoais. O direito à privacidade, ao se deparar com novas tecnologias, tem que dar respostas a problemas mais complexos na sociedade. As ingerências físicas não são mais as maiores ameaças à esfera privada. Hoje, é o corpo informacional do indivíduo que fica mais exposto a violações através da coleta sistemática de dados.

Mecanismos de *Big Data*, em especial aqueles capazes de depurar uma grande quantidade de informações, a fim de identificar aquelas potencialmente interessantes (por exemplo, *data mining*)[146], somam-se a um cenário em que o armazenamento de informações é cada vez mais facilitado. Migrou-se do disquete para o CD, *pendrive* até o armazenamento na nuvem (*cloud computing*), com

---

[144] Tal constatação é identificada até no âmbito literário com o Grande Irmão da obra de Orwell 1984. O mesmo é possível, também, a partir de uma breve análise dos regimes Nazifascistas e Comunista. ORWELL, George. **1984**. Tradução Alexandre Hubner, Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

[145] Título em alusão à obra de Danilo Doneda de mesma denominação: Da Privacidade à Proteção de Dados Pessoais.

[146] O *Data Mining* consiste em uma técnica de identificação de informações de "potencial interesse" a partir de uma busca, em grandes volumes de informação, de "correlações, recorrências, formas, tendências e padrões significativos" sempre com base em instrumentos estatísticos e algoritmos matemáticos. BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Elaboração Danilo Doneda. Brasília: SDE/DPDC, 2010. Disponível em: <http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf>. Acesso em: 23 jul. 2017. p. 34.

capacidades de armazenamento cada vez maiores, por preços cada vez menores[147]. Assim, informações que antes provavelmente estariam fadadas ao esquecimento, hoje são armazenadas trazendo a mudança do paradigma do esquecimento ao paradigma da memória[148], no qual tudo é lembrado e tomado em consideração nos mais diversos aspectos da vida da pessoa.

Um exemplo emblemático do estigma que o passado do indivíduo pode causar é o caso conhecido como *Google Spain,* em que um cidadão espanhol ingressou com uma reclamação junto à AEPD (Agência Espanhola de Proteção de Dados) contra o *Google*, para que esse retirasse de seus mecanismos de busca informações referentes a uma penhora de um imóvel de propriedade desse cidadão, motivada por dívidas que o mesmo possuía junto à seguridade social espanhola. Tal reclamação foi objeto de apreciação judicial (Processo C-131/12) e é considerado um caso paradigmático na temática do direito ao esquecimento ou do direito à desindexação[149].

É diante de tais situações que a mutação do direito à privacidade se mostra tão importante. O reconhecimento da doutrina dessa nova problemática foi fundamental para o delineamento de um direito à privacidade que tutela o indivíduo não só contra ingerências físicas externas, mas no que toca ao controle de suas próprias informações pessoais[150]. Nesse sentido, identifica-se no desenvolvimento do direito à privacidade as raízes da formulação de um novo direito: o direito à proteção de dados pessoais.

A partir deste, busca-se dar resposta aos problemas relacionados à coleta e ao tratamento de dados pessoais, em especial aqueles realizados por meios informatizados. Aqui, não só a exposição indesejada da pessoa está em roga, mas a própria proteção contra a discriminação e a manutenção da autonomia do indivíduo.

---

147 Ibid.

148 MAYER-SCHÖNBERGER, Viktor. **Delete**. The Virtue of Forgetting in the Digital Age. Pinceton: Princeton University Press, 2009, apud BRASIL, op. cit.

149 Nesse sentido, ver: RUARO, Regina Linden; MACHADO, Fernando Inglez de Souza. Ensaio a propósito do direito ao esquecimento: limites, origem e pertinência no ordenamento jurídico brasileiro. **Revista do Direito Público**, Londrina, v. 12, n. 1, p.204-233, abr. 2017.

150 "[...] *o direito à privacidade traduz-se na faculdade que tem cada pessoa de obstar a intromissão de estranhos na sua intimidade e vida privada, assim como na prerrogativa de controlar as suas informações pessoais, evitando acesso e divulgação não autorizados.*" [Grifo no original]. VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007. p. 30.

O debate em torno do direito à proteção de dados pessoais foge da dicotomia do público ou privado, buscando dar respostas a problemas distintos daqueles enfrentados pelo direito à privacidade. Dados pessoais considerados “públicos” ou de acesso público podem ser utilizados de forma lesiva, ainda que não impliquem nenhuma violação da esfera privada do indivíduo. A elaboração de perfis de consumo ou de comportamento também não afeta, *a priori*, a privacidade do titular dos dados, mas certamente tem implicações significativas na sua vida. É a questões dessa natureza que a tutela do direito à privacidade se mostra insuficiente, sendo a proteção de dados pessoais a alternativa mais apta a dar respostas satisfatórias a esses novos desafios de um mundo informatizado, consoante se verá a seguir.

2 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE DOS MODELOS EUROPEU E NORTE-AMERICANO DE PROTEÇÃO DE DADOS DE CARÁTER PESSOAL

Trabalhar com noções como o direito à privacidade e o direito à proteção de dados pessoais é sempre algo complexo. A velocidade dos avanços tecnológicos e os novos meios de ingerência sobre indivíduos que esses proporcionam fragilizam qualquer construção que se paute por tecnologias específicas. Tal contexto, assim, demanda uma abordagem mais elaborada desses direitos, os quais devem ser maleáveis o suficiente para se adaptar a novos problemas que as TICs ensejam, sem que, com isso, se esvazie seus conteúdos.

A primeira dificuldade no enfrentamento do tema consiste na opção de se trabalhar o direito à proteção de dados pessoais enquanto uma das faces do direito à privacidade, ou enquanto um direito autônomo. Para responder tal questão, nada obstante, é preciso enfrentar a construção do direito à proteção de dados pessoais em si, vez que diferentes ordenamentos jurídicos dão diferentes respostas ao problema. Cabe, portanto, primeiro, definir qual o modelo de proteção de dados que se está trabalhando e se o contexto político-econômico-social em que se busca alinhar tal modelo é, de fato, compatível com as respostas que ele propõe.

Dessa feita, o presente capítulo aventa um panorama dos modelos norte-americano e europeu de proteção de dados pessoais para, então, enfrentar o tema no ordenamento jurídico pátrio[151]. Com isso pretende-se lançar as bases para a construção de uma proteção de dados pessoais brasileira, verificando qual dos modelos estudados é mais compatível com a normativa pátria. Importante frisar que, ainda que esse cotejamento sirva para a tomada de um dos modelos como norte para uma construção brasileira, ele não implica o afastamento de todos os elementos do outro, os quais podem ser importados, uma vez que verificada sua compatibilidade e sua pertinência em relação ao ordenamento jurídico nacional. Tais desdobramentos, assim, são essenciais quando da articulação do direito à proteção de dados pessoais no âmbito do sistema jurídico brasileiro que, por carecer de uma

[151] A proteção de dados pessoais no Brasil será enfrentada no capítulo 3 desta dissertação.

regulação específica sobre o tema, é marcado por inúmeras lacunas e por uma grande insegurança jurídica.

Primeiramente, trabalhar-se-á o modelo norte-americano de proteção de dados, enfocando basicamente no âmbito federal e constitucional. Não será objeto de estudo, portanto, as legislações e constituições estaduais, sem qualquer pretensão de questionar a importância de tais proposições normativas para o debate[152].

Posteriormente, enfrentar-se-á o modelo europeu de proteção de dados, concentrando maior atenção nas Diretivas da União Europeia e no Novo Regulamento de Proteção de Dados que entrará em vigor em 2018. Destarte, não se enfocará legislações específicas dos países que compõem o bloco, tendo-se como objeto primordial as normativas em nível de União Europeia.

2.1 PANORAMA DO MODELO NORTE-AMERICANO DE PROTEÇÃO DE DADOS PESSOAIS

A fim de se trabalhar com um modelo norte-americano, impõe-se a elucidação prévia de algumas questões inerentes ao sistema legal estadunidense, vez que esse difere significativamente do sistema brasileiro. Primeiro, aponta-se que o país adota o sistema de *common law* em que a figura dos precedentes desempenha papel de fonte do direito[153]. Segundo, na sistemática norte-americana, país marcadamente influenciado por uma corrente liberal, os direitos fundamentais previstos na Constituição, *a priori*, não atingem as relações entre particulares[154], sendo oponíveis

[152] Nesse sentido Doneda destaca o estado da Califórnia, o qual menciona a *privacy* no primeiro artigo de sua Constituição, bem como foi o primeiro estado do país a possuir uma agência de proteção de dados pessoais, ainda que a atuação desta seja bem mais restrita em comparação às agências europeias. DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[153] A esse respeito, digna de nota a observação de Doneda no sentido de: "[...] a expressão *common law* pode apresentar significados diversos, conforme o contexto no qual se encontra. Em seu sentido mais amplo, refere-se a um inteiro sistema jurídico. [...] um segundo significado, no qual *common law* representa o direito judiciário, o patrimônio das regras criadas pela corte que se contrapõe à lei como fonte de direito – frequentemente referidas como *unwritten law."* Ibid., p. 263-264.

[154] O desenvolvimento da teoria da *State Action* passou a flexibilizar essa inoponibilidade frente a particulares, admitindo exceções pontuais com base na *public function exception* e na

apenas frente ao Estado – eficácia vertical –, ao passo que no ordenamento jurídico pátrio esses direitos são oponíveis *erga omnes*. Trata-se da teoria denominada *State Action*, que é fundamentalmente calcada nas noções de autonomia privada e de federalismo, vez que caberia, fundamentalmente*,* aos estados e não à União regular o direito privado[155].

Ou seja, nesse modelo, a proteção de dados pessoais é distinta no que toca à proteção frente ao Estado e frente a outros particulares. Ademais, em razão de um federalismo forte e da significativa influência do *lobby*, a sistemática de proteção desse modelo é extremamente fragmentada, sendo possível identificar diferentes níveis de proteção com base não só no Estado norte-americano que se analisa, mas no tipo de dado que se pretende proteger[156].

Traçando um panorama do modelo norte-americano de proteção de dados pessoais, percebe-se que esse se encontra albergado na figura do *right to privacy*. Consoante já fora exposto anteriormente, o *right to privacy* americano não corresponde ao direito à privacidade brasileiro, dado que seu conteúdo extrapola as questões relativas à privacidade em si. Tal direito engloba diversas facetas relativas ao próprio desenvolvimento da personalidade[157]. Inclusive, a jurisprudência

---

entanglement exception. SARMENTO, Daniel; GOMES, Fábio Rodrigues. A eficácia dos direitos fundamentais nas relações entre particulares: o caso das relações de trabalho. **Rev. TST**, Brasília, v. 77, n. 4, p. 60-101, out./dez. 2011.

155 Ibid.

156 "O fato da proteção de dados pessoais no direito norte-americano ser um sistema basicamente empírico, cujo desenvolvimento foi marcado pelo embate de forças no qual elementos como o *lobby* têm importância fundamental, pode ser inferido do regime de proteção diferenciado reservado a determinados setores e espécies de dados pessoais." DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 297.

157 Nesse sentido, Mills aponta que "[…] *the words we normally associate with privacy are independence, freedom, autonomy, liberty, individuality, dignity, seclusion, and the absence of intrusion. All of these are treasured concepts.* […] *There is a continuing struggle to define privacy. Some suggest that it is not worth the struggle, because privacy cannot be understood as a unified concept. Privacy is hardy a one-dimensional concept and is probably more akin to the 'bundle of rights' we talk about when legally conceptualizing property rights*." MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008. p. 4.

americana já enfrentou temas como o aborto[158] e a utilização de anticoncepcionais[159], fundamentando sua decisão no *right to privacy*[160].

O fenômeno de expansão do campo de abrangência do *right to privacy* transcendeu aquele experienciado pelo direito à privacidade, acabando por englobar, também, o direito à proteção de dados pessoais. Essa, inclusive, é uma das principais diferenças entre o modelo norte-americano e o modelo europeu, o qual trabalha a proteção de dados pessoais enquanto um direito fundamental e autônomo.

Atualmente, a proteção legal da *privacy* nos EUA se dá a partir da combinação de "*constitutional law, tort law, property law, and satutory law*"[161], as quais oferecem diferentes níveis de proteção para diferentes problemas concernentes à *privacy*[162]. No caso específico da *tort law*, cuja proteção maior seria contra intrusões e revelações não autorizadas de informações, percebe-se grande descompasso entre as formulações legais e o contexto tecnológico atual, fragilizando a proteção dos dados pessoais dos indivíduos estadunidenses[163].

A doutrina norte-americana costumeiramente propõe uma divisão entre *informational* e *decisional privacy*[164], porém se valerá daquela proposta por Mills[165], cuja divisão se dá em quatro esferas, as quais podem se sobrepor umas às outras

---

[158] Nesse sentido ver: Caso Roe v. Wade de 1973, na construção do *judge* Blackmun. Importante apontar, contudo, que a tutela do aborto por meio da *privacy* não é pacífica nos Estados Unidos, havendo aqueles que defendem se tratar de questão envolvendo uma liberdade de escolha – caso Bowers v. Hardwick, 478 U.S. 186 (1986). DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[159] Trata-se de questão envolvendo a *fundamental decision privacy* da qual, no caso *Griswold v. Connecticut,* o juiz Douglas trabalhou um *marital privacy.* Ibid., p. 286.

[160] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007.

[161] MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008. p. 6.

[162] "*The law has several avenues to analyze and protect individual privacy. For example, constitutional principles (including those of the First Amendment), tort protection, federal and state statutory protection, and even a recognition of informational privacy as a property interest all work to create the legal framework for both analyzing and protecting privacy*." Ibid., p. 107.

[163] "[...] *the reasonable expectation of privacy recognized by the law does not keep pace with the varying types of information disclosure afforded by rapidly advancing Technologies, such as the Internet, digitally recorded closed-circuit television, and mobile communication devices. As a result, data that was once within the reasonable expectation of personal and private information has become readily available and easily disseminated*". Ibid., p. 7.

[164] "[…] em uma tentativa de sistematização, a doutrina procurou indvidiuar (*sic*) dentro do *right to privacy (sic)* algumas grandes vertentes, como a já mencionada *fundamental-decision privacy,* e (*sic*) no que toca os dados pessoais, estabeleceu a existência de uma *informational privacy*. DONEDA, op. cit., p. 301.

[165] MILLS, op. cit.

em determinados momentos. Tal divisão, pensa-se, possibilita uma melhor compreensão do cenário da *privacy* americana, uma vez que permite uma diferenciação mais completa das distintas posições que a *privacy* apresenta em diferentes situações.

A primeira delas é a chamada *The Autonomy Sphere,* que estaria basicamente atrelada às noções de liberdade e de identidade. Mills[166] identifica dentro esta esfera uma "penumbra", que englobaria questões como o direito de determinar a própria aparência – roupas, cabelo, tatuagens etc. –; o direito à liberdade religiosa; liberdade de associação; e até mesmo a liberdade de expressão.

A segunda é a chamada *The Personal Property Sphere,* que ainda atrela a privacidade à noção de propriedade privada. Tal esfera denuncia que o impacto do artigo de Warren e Brandeis, ao menos no que toca à vinculação da *privacy* com a personalidade, repercutiu mais no âmbito europeu do que no próprio país de origem dos autores. Essa se trata da esfera mais antiga da *privacy* e, também, a mais protegida, usualmente, por meio de *tort law – tort of trespass* –, que consagra indenizações contra danos à propriedade. Inserem-se aqui, além dos direitos de propriedade sobre bens materiais, os de propriedade sobre bens imateriais (*copyrights, patents, trademarks* etc.)[167].

A terceira esfera é a denominada *The Control-of-Physical-Space Sphere.* Tal esfera difere significativamente da anterior, vez que está atrelada a uma noção de personalidade, protegida por princípios extraídos da *tort law* e da *criminal law*. Segundo Mills[168], essa esfera corresponde à tutela do espaço físico que se ocupa e o direito de controlá-lo, o que é protegido até em sociedades em que não se reconhece um direito à propriedade privada – por exemplo, a Coréia do Norte. Seria tal esfera que tutelaria o indivíduo contra *paparazzi* que tiram fotos das celebridades no interior de suas casas.

Por fim, a quarta e última esfera é a *The Personal-Information Sphere*, cujo objeto de tutela são as informações pessoais. Protegida por meio de *constitutional,*

---

[166] "*Privacy is a constitutionally created 'penumbra' – a combination of freedom of speech, freedom of religion, and freedom of association and the Ninth Amendment's reservation of 'other' rights to people.*" MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008. p. 16.

[167] Ibid.

[168] Ibid.

satutory, e *tort law*, trata-se da esfera menos desenvolvida e que mais carece de proteção legal[169]. Para além da proteção contra a revelação de informações privadas, é essa esfera que abrange a proteção de dados pessoais, sendo, a partir dela, que se fará a análise do sistema norte-americano de proteção de dados pessoais.

Posto isso, cabe a análise da proteção constitucional e infraconstitucional atribuída à proteção de dados pessoais dentro do modelo norte-americano.

2.1.1 Proteção constitucional norte-americana dos dados pessoais

O *right to privacy* encontra guarida na 4ª Emenda (*IV Amendment*) da Constituição dos Estados Unidos da América, reconhecendo-se, no caso *Kats v. United States* (1967)*,* que tal proteção abrangeria não apenas a privacidade de lugares físicos, mas das informações privadas dos indivíduos[170]. Até então, a interpretação da 4ª Emenda restringia sua aplicação a objetos tangíveis, dependendo de um *tresspassing* ou de uma apropriação indevida de propriedade privada. O caso supracitado, assim, redimensionou uma construção constitucional da *privacy*[171], a partir de um parâmetro de expectativa razoável de *privacy*[172],

---

[169] MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008.

[170] O caso envolvia uma escuta telefônica que, em razão da desnecessidade de intromissão no espaço físico ocupado pela parte, não estaria abrigada pela proteção do *trespassing*, porém extrai-se do julgamento que a 4ª Emenda protege pessoas e não lugares, portanto, seu alcance não pode ser condicionado à existência ou não de invasão de um espaço físico. "*Because the Fourth Amendment protects people, rather than places, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure*". USA. Supreme Court. **Katz v. United States, 389 U.S. 347, 360 (1967)**. Washington, DC, 18 dez. 1967. Disponível em: <https://supreme.justia.com/cases/federal/us/389/347/case.html>. Acesso em: 21 abr. 2017.

[171] Em que pese ser uma construção paradigmática, não se pode considerar tal decisão como um marco "evolutivo" da *privacy* americana. Tal situação é perceptível no caso *Smith v. Maryland*, de 1979, em que a Corte entendeu não haver razoável expectativa de privacidade no que concerne à utilização de um aparelho por parte dos agentes governamentais para o registro dos números discados por determinada linha telefônica, vez que a própria companhia de telefonia poderia fornecer espontaneamente tais dados a polícia. DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[172] "'*The Fourth Amendment', the Court declared, 'protects people, not places'.71 After Katz, so long as a person exhibits a subjective expectation of privacy in an object, activity, or statement, and that privacy expectation is one that society finds to be objectively reasonable, the Fourth Amendment protects it from warrantless search*." MCNEIL, Sonia. Privacy and the modern grid. **Harvard Journal of Law & Technology**, v. 25, fall 2011. Disponível em: <https://ssrn.com/abstract=1928254>. Acesso em: 21 abr. 2017. p. 9.

(reasonable expectation of privacy)[173], reconhecendo a tese de Brandeis no seu *dissent* do caso *Olmstead*[174].

Posteriormente, a Suprema Corte entendeu, no caso *Wahlen v. Roe*[175], que a *constitutional privacy* engloba "[...] um interesse individual em evitar a revelação de questões pessoais". Inclusive, no próprio julgado, já se percebe uma grande preocupação com a acumulação de grandes volumes de informações de cunho pessoal, sobretudo quando realizado em bancos de dados computadorizados[176].

A esse respeito, parte da doutrina norte-americana, ao trabalhar informações sigilosas no âmbito da segurança da informação por parte do Estado, consagra a premissa fundamental do *need to kown.* Segundo ela, só podem acessar informações sigilosas – por exemplo, dados pessoais de natureza médica – sujeitos

---

[173] A partir da *current opinion* (concordância com a decisão com motivação diferente) do juiz Harlan que previa uma espécie de teste que fora, posteriormente, aceito e padronizado pela suprema corte norte-americana, "[...] somente se reconheceria esta violação da privacidade quando julgasse que uma pessoa não poderia razoavelmente esperar ter sua privacidade garantida em uma determinada situação [...] que porém deserta várias críticas, não apenas quanto à falta de critérios concretos, mas também por desobrigar o magistrado da expressão de sua própria avaliação, em critérios normativos, sobre os reais contornos do que seria uma esfera privada." DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 282-283.

[174] O caso *Olmstead v. United States* de 1928 é considerado como o primeiro julgado em que a Suprema Corte dos Estados Unidos manifestou-se a propósito do *right to privacy*, oportunidade em que se discutia a licitude da utilização de escutas telefônicas sem a obtenção de um *warrant* (mandado judicial) de contrabandistas de bebidas alcoólicas (na época proibidas pela lei seca estadunidense). No caso, a Suprema Corte manteve, por maioria, o entendimento de que a 4ª Emenda só era aplicável no caso de *trespass* (quando há uma invasão não autorizada na propriedade) e como o "grampo" fora realizado sem que os agentes governamentais adentrassem na propriedade não restou configurada qualquer violação da constituição. Do julgado, extrai-se ainda o posicionamento vencido de Brandeis – autor do artigo *Right to Privacy* – no sentido de que a interpretação constitucional em contextos distintos do original demanda maior flexibilidade para atender aos valores originalmente tutelados pela mesma, trata-se do *translaction* que se poderia aproximar das mutações constitucionais. Ibid.

[175] O caso *Whalen vs. Roe* foi julgado pela Suprema Corte Norte-Americana envolvendo uma lei do estado de *New York* que determinava que informações relativas a drogas prescritas fossem armazenadas e enviadas ao *New York Department of State.* Dentre as informações a serem enviadas, constavam: o nome do médico que prescreveu a droga; a framácia que fornece a droga; a droga prescrita e a sua dosagem; e o nome, o endereço e a idade de paciente. MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008.

[176] "*We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files [...] a concomitant statutory or regulatory duty to avoid unwarranted disclosures* […] *some circumstances, that duty arguably has its roots in the Constitution* […]." MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008. p. 17.

que tenham a "[...] *necessidade de conhecer* tais informações para o exercício do cargo, função, emprego ou atividade"[177]. [Grifo no original]

Mills, por sua vez, identifica o chamado *rational-basis scrutiny*, padrão segundo o qual se conforma a *privacy* com outros valores constitucionalmente protegidos. A partir dele, exige-se um "legítimo interesse governamental na intrusão sobre a *informational privacy",* que, contudo, seria menos rigoroso que aquele necessário para a intromissão na autonomia do indivíduo[178].

Dessa garantia, inclusive, pode-se identificar a articulação de diversos princípios da proteção de dados pessoais, como: os princípios da proibição de excesso e da necessidade, o princípio da finalidade e o princípio da segurança no tratamento, destacando-se, ainda, o princípio da proporcionalidade[179]. Trata-se do principal critério em termos de conformação da *informational privacy* com outros interesses, comumente operacionalizada por meio de um *balancing test*[180].

Para além da 4ª Emenda, sem ignorar a ausência de menção expressa ao *right to privacy* no texto constitucional, a Suprema Corte Norte-Americana reconhece-o de forma implícita na Constituição, mais especificamente nas 1ª, 5ª e 14ª Emendas[181]. Não obstante, é na 4ª Emenda que se encontra maior amparo a proteção de dados pessoais[182], ainda que também tenha respaldo em outras Emendas[183].

---

[177] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007. p. 232.

[178] "[...] *personal information is protected by a lower standard than that for personal autonomy. Termed 'rational-basis scrutiny,' the standard for personal information requires a legitimate governmental interest in the intrusion upon informational privacy, whereas the government must show a 'compelling governmental interest' to intrude on autonomy interests*". [Tradução livre]. MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008. p. 17.

[179] Esses serão enfrentados mais detalhadamente quando se analisar o modelo europeu de proteção de dados pessoais.

[180] Nesse sentido ver: *Whalen v. Roe; Doe v. City of New York;* e *United States v. Westinghouse Electric Corp.* MILLS, op. cit., p. 125.

[181] No que toca à *privacy* nas 1º e 14ª Emendas ver: DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 285. Quanto à *privacy* na *fifth amendment*, ver: STUNTZ, William J. Privacy's problem and the law of criminal procedure. **Michigan Law Review**, n. 93, p. 1016-1078, 5 mar. 1995. Disponível em: <go.galegroup.com/ps/i.do?p=AONE&sw=w&u=capes&v=2.1&id=GALE%7CA17353728&it=r&asid=1e4616fcc39ef94467d7cab05b3a9c80>. Acesso em: 27 jun. 2017.

[182] "O *right to privacy* fundamentado na quarta emenda é certamente o que mais se identifica com a proteção de dados pessoais [...]. Nela, uma noção de segredo e isolamento que parecia proteger os domínios da pessoa representados pelas suas propriedades foi transmutada em uma proteção

A esse respeito, cumpre destacar que as liberdades da primeira Emenda não são mutuamente exclusivas no que concerne ao *right to informational privacy*, pelo contrário, ambas recaem sobre o mesmo direito de liberdade de expressão[184]. O direito de a pessoa controlar suas próprias ideias, pensamentos e informações, em especial enquanto mecanismo de subterfúgio da censura do público em geral (ou do senso comum), insere-se facilmente no prisma da liberdade de expressão, vez que consiste exatamente no modo como a pessoa vai se expressar perante a sociedade[185]. Em outros termos, a liberdade de falar também deve ser interpretada como a liberdade de não falar[186]. Mais do que um limite à primeira Emenda, o *right to privacy* funciona como verdadeiro norteador de como se interpretar as garantias e liberdades previstas na primeira Emenda, bem como os valores a ela inerentes[187].

Para Doneda, em que pese a valiosa contribuição da Suprema Corte Americana na construção constitucional do *right to privacy*, "[...] a posição da Corte

---

de natureza *pessoal*, o que favorece a superposição de uma estrutura que compreende os dados pessoais." DONEDA, op. cit.

183 Nesse sentido, Stuntz reconhece que a proteção à *informational privacy* constante da *fifth amendment* é mais branda do que a prevista na *fourth*, porém ele aponta para a grande pertinência da mesma. Segundo o autor: "*The strength of the informational privacy interest in Fifth Amendment law is less obvious and less strong. It is hard to explain the basic structure of self-incrimination doctrine in informational privacy terms: the privilege does not apply to physical evidence, which can be at least as 'Private' as testimony, and it does not protect immunized testimony, no matter how 'private' in the ordinary sense of that word. Yet the privilege is still bedeviled by the effort to articulate just what the relevant interest is. Why it is that a defendant need not answer possibly incriminating questions? A large portion of the literature says that the answer is something akin to informational privacy. Peter Arenella, for example, argues that forcing someone to tell of his own wrongdoing violates the privacy of his mind and thoughts; Robert Gerstein suggests that it transgresses the privacy of one's self-judgment. These are basically interests in nondisclosure – in keeping a category of information secret*". STUNTZ, William J. Privacy's problem and the law of criminal procedure. **Michigan Law Review**, n. 93, p. 1016-1078, 5 mar. 1995. Disponível em: <go.galegroup.com/ps/i.do?p=AONE&sw=w&u=capes&v=2.1&id=GALE%7CA17353728&it=r&asid=1e4616fcc39ef94467d7cab05b3a9c80>. Acesso em: 27 jun. 2017.

184 "*A free press also ensures that the government will not oppress the people from whom it derives its power. However, sacrificing individual liberties of the governed to ensure that the government will protect those same individual liberties is illogical and inconsistent with the First Amendment.*" MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008. p. 113.

185 "*The right ot privacy and First Amendment freedoms are not mutually exclusive, but instead rest on the same principle: freedom of expression. An individual's right to privacy is inherent in the spirit of the First Amendment's protection of the expression of ideas. The right to privacy protects an individual's personal and private ideas and thoughts by allowing the individual to have autonomy and control over his or her own expression. It also ensures that the individual will have the freedom to make independent choices about the direction of his or her own life. Undoubtedly, the freedom to express oneself without fear of public censure fosters self-expression and the freedom to withhold self-expression form public view.*" Ibid., p. 108.

186 Essa associação de Mills entre liberdade e *privacy* se aproxima daquela realizada por Vieira, já enfrentada acima neste trabalho. A esse respeito, ver: VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007. p. 27.

187 MILLS, op. cit.

em casos que envolvam a expectativa de privacidade e a divulgação de dados pessoais permite concluir que ela ainda não estabeleceu um direito à privacidade para os dados pessoais". Entrementes, é possível identificar nos julgados da Corte certa tutela desses dados sob o prisma da "razoável expectativa de privacidade", ainda que sem uma preocupação específica no que concerne à questão da proteção de dados pessoais[188].

A esse respeito, é de grande valia a ainda atual crítica de Stuntz acerca da relativização da *privacy* calcada nas 4ª e 5ª Emendas, com base nas diferentes correntes jurisprudenciais norte-americanas:

> Casos de "investigações regulatórias" permitem investigações governamentais sobre negócios com base em pouca ou nenhuma suspeita de conduta indevida, dando ao governo muito mais margem de atuação quando da aplicação de regulações banais do que quando da aplicação de leis contra estupro ou assassinato. Casos de "Registros requeridos" permitem ao governo compelir revelações condescendentemente incriminatórias via estatutos regulatórios de natureza civil; uma vez mais, essa doutrina concede ao governo maior poder para aplicação de regulações triviais do que quando investigando crimes sérios. Finalmente, a doutrina "razoável expectativa de privacidade" permite a policiais revelarem detalhes bancários ou de conversas telefônicas de um suspeito, apesar da mesma doutrina reafirmar e proteger constitucionalmente a privacidade de sacolas de almoço, maços de cigarro, e da parte inferior de caixas de som. Nenhum balanceamento plausível de interesses governamentais com a privacidade individual consegue explicar esses resultados.[189]

Parece, assim, que a perspectiva constitucional da *privacy* serve, aprioristicamente, para a tutela do indivíduo contra *criminal procedures*

---

[188] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 290.

[189] "*'Regulatory search' cases allow government searches of businesses with little or no suspicion of misconduct, giving the government much more leeway when enforcing fairly trivial regulations than it has when enforcing laws against rape or murder. 'Required records' cases allow the government to compel concededly incriminating disclosures via civil regulatory statutes; once again this doctrine gives the government greater power when enforcing run-of-the-mill regulations than when investigating serious crime. Finally, the 'reasonable expectation of privacy' doctrine permits police officers to uncover the details of a suspect's finances or phone calls, even though the same doctrine reaffirms and constitutionally protects the privacy of lunch bags, cigarette packets, and the underside of stereos. No plausible balancing of government need against individual privacy interests can explain these results.*" [Tradução livre]. STUNTZ, William J. Privacy's problem and the law of criminal procedure. **Michigan Law Review**, n. 93, p. 1016-1078, 5 mar. 1995. Disponível em: <go.galegroup.com/ps/i.do?p=AONE&sw=w&u=capes&v=2.1&id=GALE%7CA17353728&it=r&asid=1e4616fcc39ef94467d7cab05b3a9c80>. Acesso em: 27 jun. 2017.

(investigações criminais), vez que a maioria dos casos paradigmáticos acerca da temática versam sobre escutas telefônicas, ou outro meio de vigilância estatal. Obviamente, tal proteção não afasta as demais (relativas a procedimentos cíveis e administrativos)[190], mas corrobora com o entendimento de que a *privacy* abrigada pela 4ª (1ª, 5ª e 14ª) Emenda é, basicamente, um instrumento que se presta a obstaculizar a ingerência do Estado em determinadas situações em que tal intervenção se mostra desarrazoada ou abusiva[191].

Destarte, restam constitucionalmente protegidas, basicamente, duas espécies de *privacy*: a *decisional privacy* – ao se tutelar interesses como o de escolhas pessoais e íntimas, ou de realização de atividades alheias à observação e à ingerência de terceiros – e a *informational privacy* – ao se tutelar interesses como a proteção de dados pessoais contra a má utilização de dados sensíveis ou confidenciais. Contudo, tal diferenciação não é sempre tão simples. Na prática, não são raras as ocasiões em que a *decisional* e a *informational privacy* se justapõem[192].

2.1.2 Quadro da proteção infraconstitucional de dados pessoais nos Estados Unidos da América

Para além da proteção constitucional, a proteção de dados pessoais é prevista em *statutory law* e *tort law,* consoante já referido anteriormente. Essa última baseia-se especialmente nos princípios da *false light, defamation, public disclousure of private facts* e *intrusion upon seclusion,* todos articulados a partir de uma *reasonable expectation of privacy*[193].

O fato desses remédios legais – *trespass, defamation, false light,* dentre outros – serem anteriores a um conceito distinto de *privacy* denuncia a inadequação

[190] Inclusive, uma pessoa privada pode ser considerada, para fins constitucionais, como um ente governamental, nos casos em que ela desempenhe função que atenda a finalidades de soberania do Estado ou está tão atrelada ao governo que suas ações podem ser atribuídas a este. MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008. p. 124.

[191] STUNTZ, William J. Privacy's problem and the law of criminal procedure. **Michigan Law Review**, n. 93, p. 1016-1078, 5 mar. 1995. Disponível em: <go.galegroup.com/ps/i.do?p=AONE&sw=w&u=capes&v=2.1&id=GALE%7CA17353728&it=r&asid=1e4616fcc39ef94467d7cab05b3a9c80>. Acesso em: 27 jun. 2017.

[192] MILLS, op. cit.

[193] Ibid., p. 17.

dos mesmos ao se falar em ameaças decorrentes de novas tecnologias. Muito embora a grande maioria das Constituições modernas preveem expressamente o *right to privacy*, a lacuna da Constituição americana demanda um processo contínuo de interpretação, no qual esse direito encontra espaço na chamada *penumbra of rights*[194].

Trabalhando-se sob um prisma mais prático da questão, o *leading case* consiste no caso *Pavesich v. New England Life Insurance Co* (1905)*,* que figura como contraponto ao caso *Roberson v. Rochester Folding Box Co* (1902)[195], o qual havia interrompido um constante processo de evolução da *privacy* nos Tribunais norte-americanos[196].

Naquele julgado da Suprema Corte do Estado da Geórgia, a Corte seguiu a linha do Estado de New York[197], recepcionando diversos argumentos expostos por Warren e Brandeis. Ademais, a Corte rejeitou o precedente criado no caso *Roberson,* em que pese semelhante a questão de fundo: a utilização por terceiros da imagem (e do nome no caso Pavesich) de uma pessoa para fins publicitários sem seu consentimento[198].

No âmbito da *tort law*, é possível tomar como noção inicial a classificação trazida por Prosser, em seu artigo *Privacy*, responsável pela consolidação da temática no âmbito da *tort law*[199]. O autor propôs uma espécie de sistematização da

---

[194] MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008. p. 106.

[195] A questão de fundo do caso Roberson consistia na utilização não autorizada da foto de uma cidadã americana, para fins de publicidade, por parte de uma empresa que manufaturava e comercializava farinha. "[…] *in a four-to-three decision, over a most vigorous dissent, it rejected Warren and Brandeis and declared that the right of privacy did not exist, and that the plaintiff was entitled to no protection whatever against such conduct. The reasons offered were the lack of precedent, the purely mental character of the injury, the 'vast amount of litigation' that might be expected to ensue, the difficulty of drawing any line between public and private figures, and the fear of undue restriction of the freedom of the press*". STUNTZ, William J. Privacy's problem and the law of criminal procedure. **Michigan Law Review**, n. 93, p. 1016-1078, 5 mar. 1995. Disponível em: <go.galegroup.com/ps/i.do?p=AONE&sw=w&u=capes&v=2.1&id=GALE%7CA17353728&it=r&asid=1e4616fcc39ef94467d7cab05b3a9c80>. Acesso em: 27 jun. 2017.

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

[197] "*In consequence [to case Roberson] the next New York Legislature enacted a statute making it both a misdemeanor and a tort to make use of the name, portrait or picture of any person for 'advertising purposes or for the purposes of trade' without his written consent. This act remains the law of New York, where there have been upwards of a hundred decisions dealing with it.*" STUNTZ, op. cit.

[198] DONEDA, op. cit.

[199] Ibid.

privacy na *tort law*, partindo dos mais de trezentos casos que envolviam a matéria até então[200].

Percebendo que não estava diante de apenas uma, mas de quatro *torts* que, em que pese compartilharem o mesmo nome – *privacy* – e tutelarem um direito a ser deixado só, pouco tinham em comum. Seriam elas:

> 1. Intrusão na solidão ou isolamento do autor, ou em suas questões privadas. *[intrusion upon seclusion]*
>
> 2. Exposição pública de fatos privados embaraçosos a respeito do autor. *[disclosure of private facts]*
>
> 3. Publicidade que dá ao autor uma imagem errônea perante o público em geral. *[false light]*
>
> 4. Apropriação, para vantagem do réu, do nome ou equivalente do autor. *[misappropiation].*[201]

Para Doneda, a ideia traçada por Prosser propõe a estruturação de um esqueleto da *privacy,* porém destituído de um núcleo ou de uma ideia central do que essa seria. Tal proposição, além de implicar o afastamento da teoria da realidade social, na prática representava um verdadeiro esvaziamento do que se entende por *privacy*[202].

---

[200] "*Today, with something over three hundred cases in the books, the holes in the jigsaw puzzle have been largely filled in, and some rather definite conclusions are possible.*" STUNTZ, William J. Privacy's problem and the law of criminal procedure. **Michigan Law Review**, n. 93, p. 1016-1078, 5 mar. 1995. Disponível em: <go.galegroup.com/ps/i.do?p=AONE&sw=w&u=capes&v=2.1&id=GALE%7CA17353728&it=r&asid=1e4616fcc39ef94467d7cab05b3a9c80>. Acesso em: 27 jun. 2017.

[201] "[…] *1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.*
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness". [Tradução livre]. Ibid.

[202] "O caminho de Prosser era claro e passava pela desconsideração completa de um eventual núcleo, ou elemento central, de um direito à privacidade unificado. O problema mais óbvio de sua teoria era o completo afastamento que ela realizava da realidade social e mesmo lingüística que envolvia o problema da privacidade e sua aplicação prática nas cortes; se teoricamente isto podia ser contornável, na prática representava um esvaziamento da própria idéia de *privacy*, fraturada em quatro ações que pouco tinham em comum [...]." DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 292.

Nesse sentido, pontual a ressalva – e crítica – feita por Doneda[203], assim como por Bloustein[204], de que é possível identificar um "denominador comum" entre todas as formulações do *right to privacy*, não só na *tort law*, mas na *constitutional privacy*, vez que todos são desdobramentos do mesmo aspecto da dignidade da pessoa humana, ainda que cada um vincule um sujeito diferente – a *tort law* tem como destinatário os particulares, ao passo que a Constituição tem como destinatário o Estado.

De grande relevância, também, a constatação de Doneda[205] no sentido de que o *Restatement* (*Second*) *of Torts* não reconhece a *liability* nos casos de publicação de dados pessoais constantes de registros públicos. Tal entendimento, somado ao fato de que o *Freedom of Information Act*, que é posterior ao *Restatement*, estabelece que as informações armazenadas junto à agência federal são consideradas públicas, gerando grande preocupação no que diz respeito ao uso de dados pessoais.

Em termos de *statutory law*, já em 1903 tem-se a primeira lei sobre *privacy*, do Estado de New York, editada justamente para se desvincular da decisão prolatada no já mencionado caso *Roberson* (1902). Porém, é a partir dos anos 1970 que se identificam leis infraconstitucionais de maior expressão[206], especialmente após a elaboração do *Fair Information Practices Principles*[207]. A partir daí foram-se editando leis de políticas de privacidade sobre os mais variados tópicos, dentre eles, "[...] *Social Security numbers, library records, credit-card information, banking records, medical information, vídeo voyeurismo, autopsy photos, vídeo-rental records*", entre outros[208].

Em 1970, o *Fair Credit Reporting Act* (FCRA) foi aprovado pelo congresso americano, e tal lei, inclusive, veio a influenciar fortemente o ordenamento jurídico

---

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

[204] BLOUSTEIN, Edward J. Privacy as an aspect of human dignity: an answer to Dean Prosser. **New York University Law Review**, v. 75, n. 6. p.1535-1537, dec. 2000, apud GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010.

[205] DONEDA, op. cit.

[206] Segundo Garfinkel, "[…] *the biggest privacy failure of American government has been its failure to carry through with the impressive privacy groundwork that was laid in the Nixon, Ford, and Carter administration*". GARFINKEL, op. cit., p. 6.

[207] O *Code of Fair Information Practices* será analisando no decorrer deste capítulo.

[208] MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008. p. 131.

brasileiro no que toca ao CDC e aos cadastros de consumo. Posteriormente, a lei foi alterada pelo *Consumer Credit Roperting Reform Act* (CCRRPA), em 1996, e tem como objeto a regulação dos chamados *credit bureaus* e *credit reports*, estabelecendo que esses só poderiam revelar informações sobre os consumidores:

> [...] (i) para cumprimento de ordem judicial, (ii) mediante consentimento do interessado, (iii) quando existam razões para crer que pretende-se utilizar esta informação para verificações concernentes a qualquer requisição do interessado de crédito, emprego, seguro, benefícios governamentais ou similares (incluindo-se uma cláusula bastante ampla como a de *legitimate busines needs*).[209]

A essa lei sucederam-se o *Accurate Credit Transactions Act*, de 2003, e o *Gramm-Leach-Bliley Act*, de 1999, que protege informações pessoais "não públicas" constantes em bancos de dados de instituições financeiras, vedando sua transmissão para terceiros. Dentre suas definições, a lei prevê que, para a divulgação de uma informação, a instituição financeira deve notificar o titular da informação, bem como oportunizar que ele obste a divulgação por meio de um sistema de *opt-out*[210].

Em 1972, Elliot Richardson (Secretário de Saúde, Educação e Bem-Estar do Governo Nixon) criou uma comissão, a fim de verificar o impacto de computadores na privacidade. O relatório, oriundo de anos de testemunhos junto ao Congresso americano, tornou-se referência na matéria de proteção de dados pessoais, sendo considerado, inclusive, "[...] a mais significante contribuição americana no tópico dos computadores e da privacidade até hoje"[211].

O relatório criou uma espécie de "*bill of rights for the computer age*", sob o nome de *Code of Fair Information Practices*. Esse elencou cinco princípios básicos para o resguardo da *privacy* na utilização de meios informatizados:

---

[209] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 295.

[210] MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008.

[211] "*That Code remains the most significant American thinking on the topic of computers and privacy to this day.*" [Tradução livre]. GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010. p. 7.

- Não pode haver qualquer sistema de armazenamento de dados pessoais, cuja existência é secreta.
- Deve haver um meio para a pessoa descobrir qual informação ao seu respeito foi coletada e como ela é utilizada.
- Deve haver um meio para a pessoa obstar que informações obtidas ao seu respeito para determinado fim sejam utilizadas para outras finalidades sem seu consentimento.
- Deve haver um meio para a pessoa corrigir ou emendar uma informação identificável a seu respeito.
- Qualquer organização criando, mantendo, usando, ou compartilhando dados de pessoas identificáveis deve assegurar a confiabilidade dos dados pessoais para o fim pretendido e tomar precauções, a fim de prevenir o uso indevido desses dados.[212]

Tal documento, entrementes, foi ter sua maior repercussão não nos EUA, mas na Europa, continente no qual praticamente todos os países vieram a aprovar leis com base nesses princípios. Inclusive, os países criaram agências e comissões de proteção de dados com a finalidade de fiscalização e aplicação dessas leis[213].

Foi em 1974, porém, que restou editada a primeira lei norte-americana reconhecendo a existência de um "*general right to privacy*". Não obstante, o *Privacy Act* de 1974 é dotado de uma aplicabilidade muito restrita, tendo em vista ter como destinatários apenas as agências federais, tão somente no que concerne ao armazenamento e tratamento de dados (*records*) a respeito de cidadãos americanos[214]. Uma das determinações mais importantes da lei é a de que os dados só podem ser utilizados para atender a finalidade específica para a qual foram

---

[212] "1. *There must be no personal data record-keeping systems whose very existence is secret. 2. There must be a way for a person to find out what information about the person is in a record and how it is used. 3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent. 4. There must be a way for a person to correct or amend a record of identifiable information about the person. 5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.*" [Tradução livre]. GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010.

[213] Ibid.

[214] USA. Department of Justice. **The Privacy Act of 1974 5 U.S.C. § 552a (2012)**. Establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. Washington, DC, 01 maio 1974. Disponível em: <https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition>. Acesso em: 04 jul. 2017.

coletados. Entrementes, as Emendas decorrentes do *Computer Matching and Privacy Protection Act* de 1988 abriram margem para que as informações coletadas por uma agência fossem compartilhadas com outra, sendo que essa última poderia utilizá-las para finalidade diversa da que originalmente deu origem à coleta[215].

Para além disso, é possível identificar, na figura do consentimento, um dos elementos centrais da lei[216]. O *act* também prevê algumas garantias, como o direito de acesso e o de retificação de dados pessoais constantes de bancos de dados governamentais[217], indo de encontro à lei de acesso à informação americana – *Freedom of Information Act* (FOIA) –, promulgada em 1967[218]. Essa garante o direito de acesso a informações pessoais constantes de agências federais e, inclusive, o direito de obtenção de cópias das mesmas[219]. Ademais, a lei prevê exceções à liberdade de (acesso à) informação que visam justamente ao resguardo da *privacy*[220].

Existem, ainda, leis cujo alcance é significativamente restrito, atingindo apenas setores específicos da sociedade. Nesse cenário, a figura do *lobby* desponta

---

[215] MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008.

[216] "No *Privacy Act,* a regra do consentimento é um elemento central em torno do qual a lei se estrutura, ao negar a divulgação de informações pessoais pela agência sem o consentimento do interessado e também estabelecer a pertinência de sanções civis e criminais para a sua violação. [...] Além disso, e não menos importante, é o fato de que cabe a vítima demonstrar que o agente do Estado revelou seus dados violando culposamente *(willfully*) a lei e também que este fato causou danos a si; [...]." DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 295-296.

[217] USA. Department of Justice. **The Privacy Act of 1974 5 U.S.C. § 552a (2012)**. Establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. Washington, DC, 01 maio 1974. Disponível em: <https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition>. Acesso em: 04 jul. 2017.

[218] A respeito da FOIA, ver: USA. Department of Justice. **DOJ Guide to the Freedom of Information Act**. Washington, DC, 23 Jul. 2014. Disponível em: <https://www.justice.gov/oip/doj-guide-freedom-information-act>. Acesso em: 05 jul. 2017.

[219] De grande valia apontar, também, que o FOIA foi objeto de significativas emendas, dentre elas destacam-se a *Freedom of Information Reform* Act (1986) para tratar do uso de informações para fins de segurança pública e o *Freedom of Information Amendments* (1996), que passou a contemplar a questão das tecnologias da comunicação em rede. DONEDA, op. cit.

[220] Dentre as exceções, constam segredos comerciais e informações comerciais e financeiras consideradas confidenciais, registros médicos e outros similares, cuja exposição geraria uma violação da privacidade, dentre outros aspectos. Nesse sentido ver: USA. Department of Justice. **The Freedom of Information Act. 5 U.S.C. § 552 (2000)**. Vol. XVII, n. 4, 1996. Disponível em: <https://www.justice.gov/oip/blog/foia-update-freedom-information-act-5-usc-sect-552-amended-public-law-no-104-231-110-stat>. Acesso em: 10 jul. 2017.

como elemento capaz de gerar incongruências no ordenamento norte-americano, em especial no âmbito da proteção de dados pessoais, cuja salvaguarda decorre, basicamente, do desenvolvimento de um sistema empírico[221].

Dentre essas leis, destacam-se: o *Dirver's Privacy Protection Act* (1994)[222], que teve origem no assassinato de uma atriz americana por um fã que obteve acesso a informações da vítima – no caso, o endereço – por meio dos registros de habilitação de motoristas[223]; o *Video Privacy Protection Act* (1988)[224], que teve origem na divulgação não autorizada dos filmes que Robert Bork, então candidato a Juiz da Suprema Corte, teria supostamente alugado, tal informação, ainda, fora apontada como causa da frustração de sua candidatura[225]; o *Eletronic Communications Privacy Act* (1986)[226]; o *Right to Financial Privacy Act* (1978)[227]; e o *Family Educational Rights and Privacy Act* (1974)[228].

---

[221] É o que aponta Doneda ao constatar que "[...] uma pessoa pode cultivar maior expectativa de privacidade em relação à lista de filmes alugados em uma vídeo-locadora do que a respeito de seu histórico clínico". DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 297-298.

[222] "*In General – A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity:*
(1) personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section; or
(2) highly restricted personal information, as defined in 18 U.S.C. 2725(4), about any individual obtained by the department in connection with a motor vehicle record, without the express consent of the person to whom such information applies, except uses permitted in subsections (b)(1), (b)(4), (b)(6), and (b)(9): Provided, That subsection (a)(2) shall not in any way affect the use of organ donation information on an individual's driver's license or affect the administration of organ donation initiatives in the States." **LEGAL Information Institute**. Disponível em: <https://www.law.cornell.edu/uscode/text/18/2721>. Acesso em: 05 jul. 2017.

[223] DONEDA, op. cit.

[224] Essa lei se presta, basicamente, à proibição da divulgação por parte das locadoras de vídeos dos filmes alugados pelos seus clientes sem o devido consentimento. Em 2012 a lei recebeu uma emenda – *H.R. 6671 (112th): Video Privacy Protection Act Amendments Act* – que veio a contemplar a questão do *ongoing consent* e da possibilidade de consentimento via internet. EPIC. **Video protection privacy act**. Disponível em: <https://epic.org/privacy/vppa/>. Acesso em: 05 jul. 2017.

[225] DONEDA, op. cit.

[226] Regula basicamente a questão da interceptação de comunicações eletrônicas, protegendo o indivíduo não só contra escutas de agências estatais, mas de outros particulares quando para fins de vigilância. EPIC. **Electronic Communications Privacy Act** (ECPA). Disponível em: <https://epic.org/privacy/ecpa/>. Acesso em: 06 jul. 2017.

[227] 12 U.S. Code Chapter 35 - RIGHT TO FINANCIAL PRIVACY estabelece as regras para a divulgação, por parte das instituições financeiras, das informações financeiras relativas a seus clientes. USA. **Right to Finantial Privacy Act. Sec. 1108, Right to Financial Privacy Act of 1978, 92 Stat. 3697 et seq., 12 U.S.C. 3401 et seq.; (5 U.S.C. 301)**. To authorize Departmental units to request financial records from a financial institution pursuant to the formal written request procedure authorized by section 1108 of the Act, and to set forth the conditions under which such requests may be made. Washington, DC, 20 mar. 1979. Disponível em:

Para além dessas leis, cabe falar, em separado, ainda, do *Cable Communications Policy Act* (1984), que, ao estabelecer, em linhas gerais, uma política das TVs a cabo, traz, a partir do 47 U.S. Code § 551, um rol de determinações no intuito de resguardar os dados pessoais dos assinantes. Dentre essas determinações, pode-se destacar a obrigatoriedade de um relatório periódico (intervalo não superior a um ano) contendo:

> (A) *the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information*;
>
> (B) *the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made*;
>
> (C) *the period during which such information will be maintained by the cable operator*;
>
> (D) *the times and place at which the subscriber may have access to such information in accordance with subsection (d); and*
>
> (E) *the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under subsections (f) and (h) to enforce such limitations*.[229]

Já no âmbito da saúde, o *Health Insurance Portability and Accountability Act*, de 1996, consiste na lei americana mais expressiva. Ela propicia que os dados

---

<https://www.gpo.gov/fdsys/pkg/CFR-2011-title31-vol1/pdf/CFR-2011-title31-vol1-part14.pdf>. Acesso em: 06 jul. 2017.

228 20 U.S.C. § 1232g; 34 CFR Part 99 ou *Family Educational Rights and Privacy Act* regula a questão da comunicação de informações entre o estabelecimento educacional e os pais dos alunos, a fim de proteger a *privacy* dos dados educacionais dos estudantes. USA. **Family Educational Rights and Privacy Act. 20 U.S.C. 1221e–3(a)(1), 1232h**. To set out requirements for the protection of privacy of parents and students under section 444 of the General Education Provisions Act, as amended. Washington DC, 11 abr. 1988. Disponível em: <https://www.gpo.gov/fdsys/pkg/CFR-2010-title34-vol1/pdf/CFR-2010-title34-vol1-part99.pdf>. Acesso em: 07 jul. 2017.

229 Id. **Cable Communications Policy Act. 47 U.S.C. ch. 5, subch. V–A To**. "(1) establish a national policy cable television. (2) establish franchise procedures and standards which encourage the growth and development of cable systems and which assure that cable systems are responsive to the needs and interests of the local community; (3) establish guidelines for the exercise of Federal, State, and local authority with respect to the regulation of cable systems; (4) assure that cable communications provide and are encouraged to provide the widest possible diversity of information sources and services to the public; (5) establish an orderly process for franchise renewal which protects cable operators against unfair denials of renewal where the operator's past performance and proposal for future performance meet the standards established by this title; and (6) promote competition in cable communications and minimize unnecessary regulation that would impose an undue economic burden on cable systems. Washington, DC, 30 out. 1984. Disponível em: <https://transition.fcc.gov/Bureaus/OSEC/library/legislative_histories/1286.pdf>. Acesso em: 08 jul. 2017.

médicos figurem entre os mais bem protegidos tipos de informações pessoais[230]. Além disso, a lei proíbe a divulgação de dados de pessoas identificáveis (ou identificadas) sem o devido consentimento expresso do titular, prevendo algumas exceções à necessidade prévia de consentimento – por exemplo, quando as informações forem imprescindíveis ao desenvolvimento da atividade comercial, ou quando requerido por autoridade judicial. Por fim, ela prevê a destruição das informações pessoais dos registros da empresa quando elas não forem mais necessárias à finalidade para a qual foram coletadas[231].

O grande número de *statutory federal laws* – são mais de quarenta – e de *regulations* demonstra o esforço dos governos federal e estaduais para preencher as lacunas existentes nos "*common-law, tort, and constitutional remedies",* para a proteção da *privacy*[232]. Geralmente, o processo legislativo de proteção da *privacy* tem origem em reações e pressões políticas exercidas diante de casos específicos, valendo-se da analogia feita por Mills: "[...] se constroem semáforos em interseções somente após ocorrerem acidentes fatais no local, mas não antes"[233].

Por fim, é digno de nota que diversas proteções estatutárias sofreram grande esvaziamento em face das políticas de segurança previstas no *Patriot Act* e no *Foreing Intelligence Surveillance Ac*t de 1978 que, quando balizadas em juízo com o *right to privacy*, acabam prevalecendo sobre esse[234].

Dito isso, cabe analisar a sistemática europeia de proteção de dados pessoais.

---

[230] Apesar de prever algumas exceções concernentes a saúde pública e segurança nacional, a HIPAA protege todos os dados referentes a condições físicas e psicológicas passadas, presentes e futuras que possam ser associadas a um indivíduo em específico. MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008.

[231] USA. **Health Insurance Portability and Accountability Act. H.R. 3103. 42 USC 201**. To improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes. Washington, DC, 21 ago. 1996. Disponível em: <https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>. Acesso em: 10 jul. 2017.

[232] MILLS, op. cit., p. 130.

[233] "*Protections are enacted when new intrusions occur or new ways to intrude are invented. The legislative process reacts to crisis and political pressure. The analogy is that we build stoplights at the intersection after fatal accidents occur – but not before.*" Ibid., p. 131.

[234] Ibid.

2.2 PANORAMA DO MODELO EUROPEU DE PROTEÇÃO DE DADOS PESSOAIS

A abordagem europeia do problema da proteção de dados pessoais, em que pese partir de construções distintas do modelo americano, notadamente no que toca à inserção do direito à proteção de dados pessoais e a delimitação do conteúdo do direito à privacidade (ou *privacy)*, acaba não se distanciando tanto da abordagem norte-americana. Tal situação decorre da tendência de convergência dessas abordagens, não sob um prisma de unificação dos modelos, mas de uma comunicação dialética entre ambos[235].

Trata-se, na verdade, de uma resposta lógica ao problema da circulação de dados pessoais, para o qual a adoção de soluções pontuais dentro de um contexto nacional está fadada a ser uma resposta insuficiente e inadequada[236]. Ademais, não se pode ignorar a grande influência que o *Code of Fair Information Practices* de 1972 teve na formulação do direito à proteção de dados pessoais na Europa, consoante já referido anteriormente neste trabalho[237].

A fim de se trabalhar o modelo europeu de proteção de dados pessoais, ter-se-á como base as regulações elaboradas em nível de direito comunitário[238], ou seja, da União Europeia. Dessa feita, ainda que pontualmente venha-se referir legislações nacionais, o enfoque deste trabalho será em nível comunitário, notadamente sobre a Diretiva 95/46/CE, a Diretiva 2002/58/CE e o Novo Regulamento de Proteção de Dados Pessoais nº 2016/679, que entrará em vigor em 2018, revogando a Diretiva 95/46.

---

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

[236] Ibid.

[237] GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010.

[238] Como fruto dos novos meios eletrônicos de comunicação, verifica-se um processo de integração (distinto do fenômeno de globalização). A tal processo deu-se o nome de Direito Comunitário, o qual é viabilizado pela "[...] aproximação cultural, comercial e institucional dos Estados num processo em marcha irreversível".
A partir dessa integração, o estado delega parte de seus poderes à comunidade de Estados. Destarte, as normas comunitárias atuam diretamente sobre o território nacional prescindindo de um processo de ratificação como é típico do Direito Internacional Tradicional. Essa integração e a tendência ao surgimento de diplomas normativos supranacionais, os quais pressupõem uma ordem jurídica comum entre os Estados, são uma tentativa de readequação dos países à uma nova sociedade globalizada e integrada (a escala global) pela rede. PAESANI, Liliana Minardi. **Direito e internet**: liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2000. p. 29.

Para além dessas normativas, um dos principais marcos para a formulação de um direito fundamental à proteção de dados pessoais, no cenário europeu, consiste no caso da Lei do Censo, julgado em 1983 pelo Tribunal Constitucional Alemão, episódio em que se reconheceu, pela primeira vez, um direito à autodeterminação informativa enquanto um direito fundamental[239].

A Lei do Censo alemã (*Volkszählungsgesetz – BGBl. I, p. 369*), de 25 de março de 1982, determinava que, no início de 1983, fosse realizado o recenseamento da população germânica, a fim de se reunir dados a propósito do crescimento populacional, da distribuição da população no território nacional e de outras questões de ordem social e econômica. Para tanto, dados como profissão, moradia e local de trabalho seriam coletados, sendo que, em seu §9º, a lei previa a possiblidade de cruzamento, transmissão e comparação desses dados com os de outros registros públicos, inclusive provenientes de outras repartições públicas, desde que anonimizados[240].

Cumpre ressaltar, ainda, que, em determinados casos, o fornecimento dessas informações era de caráter obrigatório, havendo previsão legal de multa para aqueles indivíduos que não preenchessem o formulário de fins estatísticos, o qual era composto de cerca de 160 perguntas, algumas delas de natureza extremamente intrusiva[241].

Diante dos excessos da lei, diversas Reclamações Constitucionais foram ajuizadas contrárias à mesma, centradas, em sua grande maioria, no argumento de que a lei do censo alemã violava direitos fundamentais dos cidadãos germânicos, prejudicando o livre desenvolvimento da personalidade dos mesmos – art. 2 I GG. Analisando a questão de mérito, o Tribunal Constitucional Federal Alemão julgou parcialmente procedentes as reclamações, reconhecendo a constitucionalidade da

---

[239] RUARO, Regina Linden. Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância? **Arquivo Jurídico**, Teresina, v. 2, n. 1, p. 41-60, jan./jul. 2015.

[240] SCHWABE, Jürgen; MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Berlim: Konrad-Adenauer-Stifung E.V., 2005. Disponível em: <http://www.kas.de/wf/doc/kas_7738-544-4-30.pdf>. Acesso em: 12 jul. 2017.

[241] As perguntas incluíam desde aspirações profissionais dos cidadãos até questões concernentes às "suas práticas religiosas e políticas". RODRIGUEZ, Daniel Piñeiro. **O direito fundamental à proteção de dados pessoais**: as transformações da privacidade na sociedade de vigilância e a decorrente necessidade de regulação. Dissertação (Mestrado em Direito) – Faculdade de Direito, Programa de Pós-Graduação em Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2010. p. 58.

lei. Não obstante, declarou nulos trechos da normativa, em especial "[...] os dispositivos sobre a comparação e trocas de dados e sobre a competência de transmissão de dados para fins de execução administrativa"[242].

Segundo o Tribunal Constitucional Federal Alemão, tais disposições violariam o direito fundamental a autodeterminação informativa[243], cuja restrição só seria cabível em casos de interesse predominante da coletividade amparados em dispositivo constitucionais. Ademais, destacou-se a necessidade de observância do princípio da proporcionalidade, especialmente no que toca à adoção de medidas menos restritivas de direitos, bem como à diferenciação entre dados pessoais e dados anonimizados[244].

Seguindo o posicionamento jurisprudencial de não circunscrever de forma taxativa o conteúdo do direito da personalidade, o Tribunal entendeu que esse abrange "[...] também o poder do indivíduo, decorrente da idéia de autodeterminação, de decidir em princípio por si próprio, quando e dentro de que limites fatos pessoais serão revelados"[245]. Percebe-se, na própria fundamentação, uma preocupação com bancos de dados automatizados e com o processamento eletrônico de informações, sentimento que se intensificou no século XXI.

O julgado consolidou, portanto, um novo direito da personalidade, uma vez que pressuposto ao livre desenvolvimento dessa em um cenário marcado por novos meios de tratamento de dados pessoais. Trata-se, ainda, de direito fundamental, em que pese não absoluto, vez que a proteção contra a coleta, uso e transmissão de dados de cunho pessoal também deve se compatibilizar com outros interesses[246].

---

[242] SCHWABE, Jürgen; MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Berlim: Konrad-Adenauer-Stifung E.V., 2005. Disponível em: <http://www.kas.de/wf/doc/kas_7738-544-4-30.pdf>. Acesso em: 12 jul. 2017. p. 234.

[243] "A regulamentação sobre comunicação prevista no § 9 I a III da Lei do Recenseamento de 1983 (entre outro, atualização do registro de moradores) infringe o direito geral da personalidade." Ibid., p. 235.

[244] Ibid.

[245] Decisão (Urteil) do Primeiro Senado de 15 de dezembro de 1983 após audiência de 18 e 19 de outubro de 1983 – **1 BvR 209, 269, 362, 420, 440, 484/83** –. Ibid.

[246] "O livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. Esta proteção, portanto, é abrangida pelo direito fundamental do Art. 2 I c. c. Art. 1 I GG. O direito fundamental garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais.
b) Esse direito à 'autodeterminação sobre a informação' não é garantido ilimitadamente. O indivíduo não tem um direito no sentido de um domínio absoluto, ilimitado, sobre 'seus' dados; ele

É o que também defende Doneda, ao sustentar que o direito à autodeterminação informativa garante ao titular a possiblidade de controlar suas próprias informações, tratando-se de direito da personalidade e dotado de um "status de direito fundamental"[247]. No mesmo sentido, Ruaro define tal direito como a liberdade que a pessoa tem de dispor de suas informações pessoais, "consoante seu próprio interesse"[248]. Tal definição evidencia o caráter instrumental de tal direito que, segundo sustentam Rouvroy e Pullet[249], tem como foco principal o ser humano em si, e não o controle das informações.

É do desenvolvimento do direito à autodeterminação informativa que irrompe o direito à proteção de dados pessoais, enquanto direito autônomo e fundamental. Da própria articulação da autodeterminação informativa são formulados diversos princípios que vêm a integrar a proteção de dados pessoais, dos quais se destacam o princípio da finalidade, da necessidade, da adequação[250] e do consentimento[251].

é muito mais uma personalidade em desenvolvimento, dependente da comunicação, dentro da comunidade social." SCHWABE, Jürgen; MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Berlim: Konrad-Adenauer-Stifung E.V., 2005. Disponível em: <http://www.kas.de/wf/doc/kas_7738-544-4-30.pdf>. Acesso em: 12 jul. 2017. p. 238.

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

248 RUARO, Regina Linden. Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância? **Arquivo Jurídico**, Teresina, v. 2, n. 1, p. 41-60, jan./jul. 2015.

249 "Informações e dados não são os 'elementos' ou os 'blocos construtores' pré-existentes de uma personalidade individual ou 'própria'. [...] O que a expressão 'autodeterminação informacional' significa, mais que o controle do indivíduo sobre as informações e dados produzidos sobre si, uma (necessária mas insignificante) pré-condição para que ele viva uma existência que pode ser dita como 'autodeterminada'." ROUVROY, Antoinette e POULLET, Yves. The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. In: GUTWIRTH, Serge et al. **Reinventing data protection?** Rotterdam, Netherlands: Sispringer, 2009. p. 45-76. p. 51.

250 Analisando a obrigatoriedade de fornecimento de informações pessoais no caso da lei do censo, o TCF entendeu que "[...] a obrigação de fornecer dados pessoais pressupõe que o legislador defina a finalidade de uso por área e de forma precisa, e que os dados sejam adequados e necessários para essa finalidade. [...] Todas as autoridades que reúnem dados pessoais para cumprir suas tarefas devem se restringir ao mínimo indispensável para alcançar seu objetivo definido. O uso dos dados está restrito à finalidade prevista em lei. Já tendo em vista os perigos do processamento eletrônico de dados, é necessária uma proteção – que não pode ser enfraquecida pela cooperação administrativa (*Amtshilfefest*)". SCHWABE; MARTINS, op. cit., p. 240.

251 Segundo Ruaro, é do direito à autodeterminação informativa que "[...] decorre a necessidade de prévio consentimento à coleta e ao tratamento de dados pessoais", sendo que esse só será valido quando "[...] forem prestados os devidos esclarecimentos sobre quais serão os dados objeto da coleta, de que forma se dará o tratamento desses dados, com quem eles serão compartilhados e para que fim estão sendo coletados". RUARO, op. cit., p. 46.

Em que pese não se ignorar aqueles que trabalham a autodeterminação informativa enquanto um aspecto do direito à privacidade, mais especificamente a privacidade informacional[252], parece que tal construção se aproxima mais do modelo norte-americano do que do modelo europeu[253]. Em se trabalhando com esse último, as formulações a propósito do conteúdo do direito à privacidade não romperam (ao menos não em todo) com a dicotomia entre o público e o privado[254].

Nesse sentido, a constante evolução do direito à autodeterminação informativa ensejou o desenvolvimento de um direito à proteção de dados pessoais enquanto um direito autônomo, cujo reconhecimento se deu no ano 2000, pela Carta de Direitos Fundamentais na União Europeia (CDFUE) em seu art. 8º[255]. Tal construção fica evidente ao se verificar que o direito ao respeito à vida privada e familiar resta positivado na CDFUE, no art. 7º, ou seja, em artigo distinto daquele destinado à proteção de dados pessoais[256].

Discorridas tais ponderações, passa-se ao enfrentamento das normativas da União Europeia que abordam a matéria.

---

[252] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007.

[253] "A temática da privacidade passa a se estruturar em torno da informação e, especificamente, em torno dos dados pessoais. Esta guinada [...] pode ser verificada com clareza nas construções legislativas e jurisprudenciais que afrontaram o tema nos últimos 40 anos, das quais algumas referências mais significativas são a concepção de uma *informational privacy* nos Estados Unidos, cujo 'núcleo duro' é composto pelo direito de acesso a dados armazenados por órgãos públicos e também pela disciplina das instituições de proteção de crédito; assim como a autodeterminação informativa estabelecida pelo Tribunal Constitucional alemão e a Diretiva 95/46/CE da União Européia [...]." DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 203.

[254] As formulações a propósito do direito à privacidade já foram trabalhadas no primeiro capítulo deste trabalho.

[255] "Artigo 8º **Proteção de dados pessoais**

1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.

2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente." UNIÃO Europeia. Parlamento Europeu, o Conselho e a Comissão. Carta dos Direitos Fundamentais da União Europeia. **Jornal Oficial das Comunidades Europeias**, 2000/C 364/01. Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 30 jul. 2017.

[256] Nesse sentido ver PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia un nuevo modelo europeo de privacidade. Madrid: Reus, 2016. p. 53.

2.2.1 Diretiva 95/46/CE do Parlamento Europeu e do Conselho

Antes de se trabalhar o teor da Diretiva, é de suma importância apontar que ela, salvo em casos excepcionais, não é dotada de vinculação direta, tratando-se de fonte normativa secundária[257]. Ou seja, ela serve como uma estrutura normativa provida de uma disciplina ampla e detalhada, porém, cabe aos Estados membros da União Europeia transportar tais disposições para dentro de sua legislação interna, compatibilizando-a da melhor forma às peculiaridades do sistema normativo de cada país[258].

Por essa razão, não há uniformidade de fato nesse sistema, pelo menos não até a entrada em vigor do Regulamento nº 679/2016, em 2018, que, além de revogar a Diretiva 95/46/CE, é aquinhoado de uma aplicação imediata[259]. Diante disso, justifica-se a escolha de se abordar apenas os aspectos da Diretiva que são recepcionados pelo Regulamento, sem se adentrar em modelos nacionais de proteção de dados.

Bebendo da influência de inúmeros trabalhos na área de proteção de dados – *Fair Information Principles* do *HEW*, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* da OCDE (1980), *Convention for the Protection of Individuals wiht regar to Automatic Processing of Personal Data* (n. 108/1981) –, a Diretiva surge como uma tentativa do Parlamento Europeu de padronizar a matéria.

---

[257] "[...] no cenário europeu atual, podem ser destacadas duas fontes principais de direito: as primárias, que se identificam com os atos jurídicos criadores de regras, previamente pactuadas pelos Estados-membros, e as derivadas, que são os regulamentos, diretivas, decisões, recomendações e ditames. Interessam ao presente estudo as diretivas comunitárias, que se caracterizam por seu poder vinculante aos Estados integrantes da União Européia quanto ao resultado, sendo permitido, no entanto, que cada nação escolha a melhor forma de alcançá-lo." RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais: uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro. **Direitos Fundamentais e Justiça**, Porto Alegre, n. 11, p. 163-180, abr./jun. 2010. p.168.

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

[259] O Regulamento Europeu de Proteção de Dados Pessoais será objeto de análise no decorrer deste capítulo.

Dentre outras determinações, os legisladores restam obrigados a "[...] emanar normas de acordo com o conteúdo normativo da Diretiva"[260].

Dando continuidade ao processo europeu de codificação da proteção de dados em nível internacional, a Diretiva é marcada por dois antecedentes legislativos: o Convênio Europeu de Direitos Humanos (CEDH), de 1950, e o Convenio 108/1981. O CEDH, em seu art. 8º, garante o direito à proteção de dados pessoais no espectro do direito ao respeito à vida privada, à vida familiar, do domicílio e à correspondência (posteriormente, a proteção de dados pessoais foi inserida no art. 8º da Carta de Direitos Fundamentais da União Europeia como direito fundamental autônomo, conforme já aludido). Por sua vez, o Convenio 108 foi o primeiro instrumento de caráter vinculativo na matéria de proteção contra o tratamento automatizado de dados pessoais, tendo seus princípios, ao menos em essência, vigentes até hoje[261].

No que concerne à Diretiva 95/46, seu texto normativo traça parâmetros ao tratamento de dados relativos a pessoas singulares e promove a livre circulação desses, sendo composto por setenta e dois Considerandos e trinta e quatro Artigos. Ou seja, as pessoas fictícias ficam excluídas de seu âmbito de proteção[262]. Do próprio objeto – "[...] relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" –, é possível verificar que compõem os objetivos centrais dessa diretiva tanto a proteção do indivíduo, no que concerne ao uso de seus dados pessoais, como a legitimação do tratamento e transmissão desses dados. Esse propósito ficará muito mais evidente quando se falar no Novo Regulamento de Proteção de Dados Pessoais, que vem exatamente para facilitar essa circulação.

Ou seja, a finalidade da Diretiva 95/46/CE é exatamente legitimar o tratamento de dados pessoais a partir da proteção de seus titulares. Alicerçada em

---

[260] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 234.

[261] CONTE, Julen Fernández; BURGOS, Diego León. Antecedentes y processo de reforma sobre protección de datos en la Unión Europea. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 35-50.

[262] UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 95/46/CE, de 24 de outubro de 1995. **Jornal Oficial das Comunidades Europeias**, L 281/31. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 13 jul. 2017.

tal objetivo, a Diretiva busca fomentar a circulação dessas informações, tanto no âmbito da administração dos Estados membros, quanto no setor privado[263]. Ela estabelece, assim, um padrão mínimo de proteção aos dados, como forma de se garantir o respeito ao indivíduo objeto de coleta e de transmissão de dados[264].

Em seu art. 1º, a Diretiva traz os já mencionados objetos (ou objetivos) da normativa. Já no art. 2º, ela estabelece definições conceituais básicas do que se entende por dados pessoais, tratamento de dados pessoais, consentimento da pessoa em causa, responsável pelo tratamento, subcontratante, dentre outros. A propósito desse artigo, furta-se o legislador à definição da categoria dos dados sensíveis. Extrai-se da Diretiva, apenas, que há uma proibição, *a priori,* de tratamento dos dados sensíveis, a qual admite exceções basicamente vinculadas a questões de saúde pública, de segurança social e da saúde do próprio titular dos dados (Considerando 34)[265]. Ademais, depreende-se do art. 8º que é vedado o tratamento de dados pessoais que digam respeito à "[...] origem racial ou étnica, às

---

[263] Nesse sentido dispõem os Considerandos 3 e 5 da Diretiva: "(3) Considerando que o estabelecimento e o funcionamento do mercado interno no qual, nos termos do artigo 7º A do Tratado, é assegurada a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais, exigem não só que os dados pessoais possam circular livremente de um Estado-membro para outro, mas igualmente, que sejam protegidos os direitos fundamentais das pessoas; [...] (5) Considerando que a integração económica e social resultante do estabelecimento e funcionamento do mercado interno nos termos do artigo 7º A do Tratado irá necessariamente provocar um aumento sensível dos fluxos transfronteiriço de dados pessoais entre todos os intervenientes, privados ou públicos, na vida económica e social dos Estados-membros; que o intercâmbio de dados pessoais entre empresas estabelecidas em diferentes Estados-membros tende a intensificar-se; que as administrações dos Estados-membros são chamadas, por força do direito comunitário, a colaborar e a trocar entre si dados pessoais a fim de poderem desempenhar as suas atribuições ou executar tarefas por conta de uma administração de outro Estado-membro, no âmbito do espaço sem fronteiras internas que o mercado interno constitui; [...]". UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 95/46/CE, de 24 de outubro de 1995. **Jornal Oficial das Comunidades Europeias**, L 281/31. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 13 jul. 2017.

[264] É o que o considerando 7 explicita, ao dispor que "[...] as diferenças entre os Estados-membros quanto ao nível de proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada, no domínio do tratamento de dados pessoais, podem impedir a transmissão desses dados do território de um Estado-membro para o de outro Estado-membro", figurando como verdadeiros obstáculos ao desempenho de atividades econômicas. Ibid.

[265] "(34) Considerando que, sempre que um motivo de interesse público importante o justifique, os Estados-membros devem também ser autorizados a estabelecer derrogações à proibição de tratamento de categorias de dados sensíveis em domínios como a saúde pública e a segurança social – em especial para garantir a qualidade e a rentabilidade no que toca aos métodos utilizados para regularizar os pedidos de prestações e de serviços no regime de seguro de doença – e como a investigação científica e as estatísticas públicas; que lhes incumbe, todavia, estabelecer garantias adequadas e específicas para a protecção dos direitos fundamentais e da vida privada das pessoas; [...]." Ibid.

opiniões políticas, às convicções religiosas ou filosóficas, à filiação sindical, [...] à saúde e à vida sexual"[266].

A fim de definir a categoria dos dados sensíveis, vale-se do conceito trazido por Doneda, que os define como:

> [...] determinados tipos de informação que, caso sejam conhecidas e processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva e que apresentaria maiores riscos potenciais que a média, para a pessoa e não raro para uma coletividade.[267]

Destarte, entende-se que o rol de "certas categorias específicas de dados", trabalhadas no art. 8º da Diretiva, não é taxativo. A categoria de dados pessoais sensíveis não é classificada a partir da natureza do dado em si, mas com base na potencialidade de seu uso para fins discriminatórios[268].

Nesse sentido, é, em grande parte, procedente a crítica de Sieghart a propósito da classificação de dados pessoais em sensíveis e não sensíveis, porque, de fato, um "[...] dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo". Assim, o autor sustenta que não haveria o porquê da proteção dessas informações serem distintas das demais, uma vez que o uso de dados não sensíveis pode ensejar um dano tão grande, ou até maior do que o uso de dados considerados sensíveis[269].

Não obstante as duas constatações serem verdadeiras (a de que o dado em si não é discriminatório, e a de que a utilização de dados não sensíveis, por vezes,

---

[266] UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 95/46/CE, de 24 de outubro de 1995. **Jornal Oficial das Comunidades Europeias**, L 281/31. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 13 jul. 2017.

[267] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 160-161

[268] Em sentido semelhante: DONEDA, op. cit.; RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008; MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online.

[269] Paul Sieghart, "Information privacy and the data protection Bill", in: **Data protection**: Perspectives on information privacy. Colin Bourn; John Benyon (eds.) Leicester: University of Leicester, 1984. p. 35, apud DONEDA, op. cit., p.162.

pode gerar prejuízos mais graves do que a de dados sensíveis), alguns tipos de dados pessoais específicos – como aqueles previstos no art. 8.1. da Diretiva[270] – são marcados por um histórico de discriminação e, inclusive, de perseguições de cunho político[271]. Como tais, há um maior risco na sua utilização e no seu tratamento, de forma que seria imprudente lançar mão de uma proteção mais rigorosa no que toca à categoria de dados pessoais sensíveis. Mais que isso, tal postura irá à contramão da noção de gerenciamento de risco para qual caminha toda a sistemática de proteção de dados pessoais[272].

Outrossim, o contexto político, social e econômico também se presta à verificação da sensibilidade ou não de um dado[273]. A partir da contraposição do cenário em que o tratamento está inserido e da finalidade desse, é possível funcionalizar as exceções à proibição geral de tratamento de dados sensíveis. Inclusive, como bem aponta Doneda[274], uma proibição geral é, antes de tudo, inviável, vez que o tratamento de tais dados é, por muitas vezes, legítimo e imprescindível – por exemplo, nas pesquisas científicas e na atuação médica. Destarte, é preciso ponderar quando o tratamento de informações sensíveis é legítimo e quando ele consiste em uma prática abusiva.

O texto da Diretiva 95/46/CE dispõe, em seu art. 3º, a respeito do âmbito de aplicação da diretiva – tratamento de dados pessoais por meio não automatizado, parcialmente automatizado ou totalmente automatizado –, bem como exceções à

---

[270] "Artigo 8º **Tratamento de certas categorias específicas de dados**
1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual." UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 95/46/CE, de 24 de outubro de 1995. **Jornal Oficial das Comunidades Europeias**, L 281/31. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 13 jul. 2017.

[271] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007.

[272] Essa temática será enfrentada pontualmente quando da análise do novo regulamento de proteção de dados pessoais europeu.

[273] Nesse sentido, Doneda aponta que a "[...] própria seleção de quais seriam estes dados considerados sensíveis provém da valoração de que a circulação de determinadas espécies de informação apresentaria um elevado potencial lesivo aos seus titulares, em uma determinada configuração social". DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 161.

[274] "Na verdade, deve-se ter em conta que a diferenciação conceitual dos dados sensíveis atende à (*sic*) uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior – sem se deixar de reconhecer que há situações onde tal conseqüência pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos." Ibid., p. 163.

sua aplicação – tratamentos para fins de segurança e defesa pública e do Estado, inclusive econômica, e quando o tratamento é feito no exercício de atividades pessoais ou domésticas[275].

A parte mais substancial da Diretiva, no entanto, encontra-se no seu Capítulo II, referente às "condições gerais de licitude do tratamento de dados pessoais". Dele se extraem os princípios da proteção de dados pessoais – arts. 6º, 7º, 16 e 17, as categorias de tratamento – art. 8º, os deveres do responsável pelo tratamento – arts. 10, 11 e 18, e os direitos dos titulares dos dados – arts. 12 e 14[276].

Em vez de optar pelo enfoque no reconhecimento expresso de direitos e seus respectivos limites e garantias, sob a lógica do apontamento de direitos subjetivos enquanto instrumento de proteção do indivíduo, a Diretiva 95/46/CE propõe princípios a serem observados no tratamento de dados[277]. Esses princípios, somados aos pontuais direitos garantidos de forma expressa[278], permitem que se extraiam diversos outros direitos e limitações no que concerne à coleta e ao uso de informações pessoais, abrindo-se espaço para a constante e necessária atualização do direito à proteção de dados diante dos avanços tecnológicos na área informacional[279].

O primeiro princípio abarcado pela Diretiva é chamado princípio da finalidade – art. 6º, 1, *b*.[280]. Segundo ele, a coleta e o tratamento de dados pessoais devem ser

---

[275] UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 95/46/CE, de 24 de outubro de 1995. **Jornal Oficial das Comunidades Europeias**, L 281/31. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 13 jul. 2017.

[276] A divisão ora proposta não tem o intuito de afastar outras formas de classificação, até porque se reconhece que de diversos princípios decorrem tanto direitos ao titular das informações como deveres ao responsável pelo tratamento.

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

[278] Em que pese não seja a opção estrutural central da Diretiva 95/46/CE, ela prevê pontualmente alguns direitos subjetivos de forma expressa, consoante será enfrentado no decorrer deste capítulo.

[279] A partir desses princípios é possível identificar quais são os interesses tutelados pela diretiva e, também a forma de proteção destes. RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais: uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro. **Direitos Fundamentais e Justiça**, Porto Alegre, n. 11, p. 163-180, abr./jun. 2010.

[280] "Artigo 6º 1. Os Estados-membros devem estabelecer que os dados pessoais serão: b) Recolhidos para finalidades determinadas, explícitas e legitimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-membros estabeleçam garantias adequadas; [...]." UNIÃO Europeia, op. cit.

vinculados a uma finalidade específica, previamente comunicada ao titular dos dados. Calcado em tal princípio, desdobra-se o princípio da adequação ou pertinência, o qual determina que os dados coletados devem ser "[...] adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente" – art. 6º, 1, *c*. Com base na finalidade do tratamento, assim, pode-se fazer um juízo de razoabilidade a propósito de quais dados serão utilizados[281], bem como por quanto tempo eles serão conservados[282].

Também nessa esteira, um juízo de proporcionalidade estrita opera a partir do princípio da finalidade. Como o juízo de razoabilidade, ele se presta a afastar o tratamento de informações não pertinentes ao fim almejado pela coleta e, inclusive, garantir o direito de oposição ao tratamento por parte do titular. A diferença, aqui, recai na abusividade (e não excessividade) das informações[283].

Por sua vez, o princípio da exatidão determina que os dados deverão ser "exatos e, se necessário, atualizados" – art. 6º, 1, *d*. Dele decorre o dever dos responsáveis pelo tratamento de tomarem medidas adequadas para assegurar que os dados inexatos ou incompletos sejam devidamente retificados, além do dever de atualização periódica dessas informações. Ademais, o princípio da exatidão dá margem para que o próprio titular dos dados zele pela sua correção e atualização,

---

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

[282] "Artigo 6º, 1. e) Conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário pari a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente. Os Estados-membros estabelecerão garantias apropriadas para os dados pessoais conservados durante períodos mais longos do que o referido, para fins históricos, estatísticos ou científicos." UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 95/46/CE, de 24 de outubro de 1995. **Jornal Oficial das Comunidades Europeias**, L 281/31. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 13 jul. 2017.

[283] A fim de ilustrar essa diferença vale-se de passagem de Pallazi. Segundo o autor, "[...] operacionalizando o princípio da proporcionalidade verifica-se que não se poderão armazenar informações relativas a obrigações de caráter econômico ou financeiro quando tais informações não se caracterizarem como essenciais aos objetivos proposto ou em caso de dívidas já quitadas. Os organismos públicos, da mesma forma, não poderão comunicar a terceiros – exceto ao Judiciário e desde que resguardado o sigilo – informações a respeito de infrações penais ou administrativas prescritas ou quando já houverem sido cumpridas as penas impostas". PALLAZZI, Pablo A. Op. cit. pp. 176-177, apud VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007. p. 286-287.

garantindo o direito ao acesso a esses dados constantes em bancos de dados públicos ou privados e, também, à retificação dos mesmos[284].

No que concerne ao princípio do consentimento, esse consiste em requisito prévio à própria coleta de dados, a qual só poderá ser realizada após "[...] a pessoa em causa tiver dado de forma inequívoca o seu consentimento" – art. 7º *a*, ou o tratamento se enquadrar em alguma exceção prevista na Diretiva. Trata-se, aqui, da figura do consentimento informado (ou esclarecido) de influência marcadamente kantiana enquanto um pressuposto para a garantir a autonomia e a autodeterminação do indivíduo[285].

Quanto ao princípio da segurança, esse visa à adoção de medidas técnicas e administrativas que protejam bancos de dados, com a finalidade de impedir que as informações pessoais neles contidas sejam objeto de acesso não autorizado (*sigilo*), de alteração (*integridade*), e de destruição (*disponibilidade*)[286]. Essas medidas de segurança são imprescindíveis à coleta e ao tratamento de dados pessoais, por se tratarem de atividades de risco. Assim, haverá a responsabilização do responsável pelo tratamento das informações, mesmo no caso de o titular das informações sofrer algum dano decorrente de um acesso ilícito a esse banco de dados – seja ele público ou privado[287].

Por fim, há o princípio da publicidade (ou transparência), segundo o qual todos os bancos de dados pessoais devem ser de conhecimento público. Correlacionando-se com o princípio do consentimento, ele determina que se obtenha

---

[284] Nas palavras de Vieira, o *princípio da veracidade* ou *princípio da exatidão e atualização dos dados* "[...] dispõe que os dados pessoais arquivados sejam verdadeiros; garantindo-se ao seu titular o direito de corrigir as informações incorretas ou obsoletas, bem como apagar dados impertinentes". VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007. p. 288.

[285] A figura do consentimento em Kant perpassa pela formulação do seu segundo imperativo categórico –"Age de tal maneira que uses a humanidade, tanto na tua pessoa como na pessoa de qualquer outro, sempre e simultaneamente, como fim e nunca simplesmente como meio" – de onde se pode extrair que, ao se usar uma pessoa como meio ela também esteja de acordo com tal situação e, para tanto, é preciso que a pessoa conheça todas as informações que lhe sejam necessárias para consentir. Nesse sentido, Paton aduz que: "[…] *the words 'at the same time' and 'simply' must not be overlooked: they are absolutely necessary to Kant's statement. Every time we post a letter, we use post-office officials as a means, but we do not use them simply as a means. What we expect of them we believe to be in accordance with their own will, an indeed to be in accordance with their duty*". PATON, H. J. **The categorical imperative**: a study in Kant's moral philosophy. Chicago: The University of Chicago, 1948. p. 165.

[286] VIEIRA, op. cit.

[287] Ibid.

a autorização para coleta e tratamento junto ao titular dos dados e, quando esse for desnecessário, o responsável pelo tratamento seja obrigado a proceder a notificação do titular dos dados. Ademais, desse princípio decorre o dever do responsável pela coleta de dados de informar ao titular questões atinentes ao tratamento das informações coletadas, como: sua identificação, a finalidade da coleta, o período de conservação dos dados, o caráter obrigatório ou facultativo do fornecimento dos dados e outras informações relevantes[288]. No texto da Diretiva, tal princípio é extraído dos arts. 10, 11 e 21, que versam sobre o dever de "Informação em caso de recolha de dados junto da pessoa em causa", o dever de "Informação em caso de dados não recolhidos junto da pessoa em causa", e o dever de "Publicidade dos tratamentos", respectivamente.

Ademais, em que pese não seja a principal opção da diretiva, cumpre apontar que ela reconheceu dois direitos subjetivos ao titular, quais sejam: o direito de acesso aos dados (art. 12) e o direito de oposição (arts. 14 e 15). O primeiro consiste em desdobramento dos princípios da publicidade (transparência) e da exatidão, englobando, inclusive, o direito de retificação ou de apagamento dos dados a depender do caso concreto. O segundo, por sua vez, garante ao titular o direito de se opor ao tratamento e à transferência de suas informações pessoais, bem como o direito de se opor a uma decisão que lhe afete de forma significativa, quando essa for baseada exclusivamente em um tratamento automatizado de dados.

Por fim, em que pese ser uma diretiva distinta, digna de nota a Diretiva 97/66/CE, que trata da utilização de dados pessoais no âmbito das telecomunicações. Tal diretiva segue a linha da Diretiva 95/46/CE, trazendo apenas algumas normas de segurança pontuais relativas a setores específicos das telecomunicações[289]. Em 2002, contudo, ela foi revogada pela Diretiva 2002/58/CE, que será estudada a seguir.

---

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

[289] RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais: uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro. **Direitos Fundamentais e Justiça**, Porto Alegre, n. 11, p. 163-180, abr./jun. 2010.

2.2.2 Diretivas 2002/58/CE, 2006/24/CE e 2016/680 do Parlamento Europeu e do Conselho

Em julho de 2002 foi aprovado o texto da Diretiva 2002/58/CE, que dispõe a propósito do tratamento de dados pessoais e da proteção à privacidade no setor das comunicações eletrônicas. Composta por 49 Considerandos e 21 Artigos, trata-se de diretiva complementar à Diretiva 95/46/CE (art. 1º, n. 2.), inclusive, prevendo a aplicação de algumas disposições dessa no âmbito das comunicações eletrônicas (art. 15).

A Diretiva trouxe noções como "dados de localização", "dados de tráfego" e "serviços de valor acrescentado"[290], buscando adequar-se a incrementos tecnológicos para os quais as respostas propostas na Diretiva 95/46/CE não eram suficientemente específicas.

Outrossim, a Diretiva 2002/58/CE, em seu Considerando 24, enfrenta expressamente a utilização de mecanismos de rastreamento de atividades do usuário e de armazenamento de informações ocultas, os chamados "«programas-espiões» («*spyware*»), «gráficos-espiões» («*web bugs*») e «identificadores ocultos» («*hidden identifiers*»)", limitando seu uso apenas a fins legítimos e ao conhecimento do usuário. Ademais, o Considerando 25 trabalha os "testemunhos de conexão («*cookies*»)" e mecanismos análogos, reconhecendo a legitimidade e utilidade de sua utilização desde que para fins legítimos. Incentiva-se, ainda, a possibilidade de recusa por parte do usuário na utilização de tais mecanismos, ainda que se admita o condicionamento do acesso à determinada página à aceitação do uso de *cookies*. Veiga e Rodrigues identificam nesses Considerandos, quando lidos conjuntamente

---

[290] "Art. 2 Definições [...]
b) «Dados de tráfego» são quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma; c) «Dados de localização» são quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações electrónicas publicamente disponível; [...]
g) «Serviço de valor acrescentado» é qualquer serviço que requeira o tratamento de dados de tráfego ou dados de localização que não sejam dados de tráfego, para além do necessário à transmissão de uma comunicação ou à facturação da mesma; [...]." UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 2002/58/CE, de 12 de julho de 2002. Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). **Jornal Oficial das Comunidades Europeias**, L 201/37. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT>. Acesso em: 25 jul. 2017.

com o disposto no art. 6º, n. 3[291], uma limitação ao uso de dados pessoais para fins estatísticos e para fins de criação de perfis de usuário (*profiling*), que seriam condicionados por sua finalidade (fim legítimo) e pelo consentimento do usuário titular dos dados[292].

Em março de 2006, o Conselho e o Parlamento Europeu aprovaram a Diretiva 2006/24/CE, que altera a Diretiva 2002/58/CE. Uma de suas principais inovações consiste na determinação de conservação de dados por parte do prestador de serviços de comunicações eletrônicas e de redes públicas de comunicação – art. 3º. Em seu art. 5º, a Diretiva especifica as categorias e os dados a serem conservados, a exemplo dos dados necessários à identificação da fonte da comunicação (como o número de telefone de origem e o nome do assinante ou utilizador registrado, os códigos de identificação do usuário de serviços de correio eletrônico e o endereço do protocolo de IP); dos dados necessários à identificação do destino da comunicação (número discado e os dados do registro daquele número e código de identificação do destinatário pretendido no caso de comunicações via internet); e dos dados necessários à identificação da hora, duração e local da comunicação (como a data e o horário de *log in* e de *log off* de determinado IP na internet).

A excessividade de dados armazenados, comumente, justificada no jargão "quem não deve, não tem nada a esconder", é contraposta a uma realidade não tão simplista. Milhares de reclamações anuais foram apresentadas às autoridades de

---

[291] "Artigo 6. Dados de tráfego
3. Para efeitos de comercialização dos serviços de comunicações electrónicas ou para o fornecimento de serviços de valor acrescentado, o prestador de um serviço de comunicações electrónicas publicamente disponível pode tratar os dados referidos no n.º 1 na medida do necessário e pelo tempo necessário para a prestação desses serviços ou dessa comercialização, se o assinante ou utilizador a quem os dados dizem respeito tiver dado o seu consentimento. Será dada a possibilidade aos utilizadores ou assinantes de retirarem a qualquer momento o seu consentimento para o tratamento dos dados de tráfego." UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 2002/58/CE, de 12 de julho de 2002. Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). **Jornal Oficial das Comunidades Europeias**, L 201/37. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT>. Acesso em: 25 jul. 2017.

[292] VEIGA, Armando; RODRIGUES, Benjamim Silva. A monitorização de dados pessoais de tráfego nas comunicações eletrônicas. **Raízes Jurídicas**, Curitiba, v. 2, n. 2, p. 59-110, jul./dez. 2007. Disponível em: <http://ojs.up.com.br/index.php/raizesjuridicas/article/viewFile/168/140>. Acesso em: 22 ago. 2017.

proteção de dados pessoais, diversas delas referindo-se à abusividade do tratamento de informações médicas sensíveis[293].

Para além dos tipos de dados armazenados, o tempo de conservação também gera grande controvérsia. Em que pese a proposta de conservação por um período de 6 meses apresentada pela Comissão em setembro de 2005, a pressão do Conselho fez com que o período fixado pela Diretiva fosse de no mínimo 6 meses e de no máximo 24 meses – art. 6º[294].

No entanto, estudos realizados pela Faculdade de Direito da *Erasmus Universitat Rotterdam*, com base em 65 casos concretos, sugerem que o período de um ano seria suficiente para a conservação dos dados até mesmo nos casos de crimes mais complexos, sendo que a maioria dos pedidos se dava dentro do período de três meses. Ademais, um estudo apresentado pela Presidência do Reino Unido à União Europeia, em setembro de 2005, apontou que 85% dos casos de solicitação de informações telefônicas se davam em período inferior a seis meses. Apenas em casos mais complexos, sobretudo casos de crimes graves, como homicídios, devido ao maior cuidado dos suspeitos em eliminar vestígios do próprio crime, ou evidências que os liguem ao crime, a solicitação das informações se dava em período maior, variando entre sete e doze meses[295].

Também desfavoráveis ao período de conservação pelo prazo de dois anos, o Grupo de Trabalho do Artigo 29 entendia desproporcional a conservação por período superior a seis meses. O mesmo ocorreu com o Comité Econômico e Social e com a Agência Europeia de Proteção de Dados. Ambos acabaram editando pareceres desfavoráveis à conservação dos dados por período superior a um ano[296].

---

[293] SCHAAR, Peter. **Das Ende der Privatsphäre:** der Weg in die Überwachungsegesellschaft. C. Bertelsmann (München), 2007, p. 22, apud RODRIGUEZ, Daniel Piñeiro. **O direito fundamental à proteção de dados pessoais**: as transformações da privacidade na sociedade de vigilância e a decorrente necessidade de regulação. Dissertação (Mestrado em Direito) – Faculdade de Direito, Programa de Pós-Graduação em Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2010.

[294] VEIGA, Armando; RODRIGUES, Benjamim Silva. A monitorização de dados pessoais de tráfego nas comunicações eletrônicas. **Raízes Jurídicas**, Curitiba, v. 2, n. 2, p. 59-110, jul./dez. 2007. Disponível em: <http://ojs.up.com.br/index.php/raizesjuridicas/article/viewFile/168/140>. Acesso em: 22 ago. 2017.

[295] Ibid.

[296] Ibid.

No contexto das comunicações eletrônicas, as medidas adotadas para fins de segurança são aparadas por discursos que clamam por transparência, que rotulam a proteção de dados pessoais como mecanismos de proteção de criminosos e terroristas. Não obstante, é preciso maior ceticismo com essa falsa impressão de segurança. A partir de uma análise singela, Rodriguez[297] põe em xeque essa correlação entre transparência e segurança, denunciando que países com maiores níveis de proteção de dados ostentam menores índices de criminalidade em comparação àqueles países caracterizados por suas políticas de vigilância. Ainda, o autor questiona, com muita propriedade, a proporcionalidade da adoção dessas medidas, bem como a falta de sopesamento entre o potencial lesivo de se permitir a consolidação de um Estado superinformado e a eficiência dessas medidas no combate à criminalidade[298].

As indagações acerca da legitimidade da normativa no cenário europeu também foram significativas. Em 8 de abril de 2014 as chamadas sentenças *Digital Rights Ireland Ltda.* (C 293/12 e C 594/12) do Tribunal de Justiça da União Europeia declararam inválida a Diretiva de Retenção de Dados[299]. Nas decisões, o Tribunal entendeu como abusiva a conservação generalizada dessas informações por tanto tempo, porém deu margem para uma conservação "seletiva" dessas informações a partir de critérios objetivos preestabelecidos[300]. Porém, isso abre margem para uma

---

[297] Tomando estudos de 2006 e 2007 Rodriguez aponta que Alemanha e Canadá, em que pese sua política de fortalecimento da proteção de dados pessoais, possuíam menores índices de criminalidade quando comparados à Inglaterra e aos Estados Unidos, cuja política de vigilância é marcadamente intrusiva. Nesse sentido, ver: RODRIGUEZ, Daniel Piñeiro. **O direito fundamental à proteção de dados pessoais**: as transformações da privacidade na sociedade de vigilância e a decorrente necessidade de regulação. Dissertação (Mestrado em Direito) – Faculdade de Direito, Programa de Pós-Graduação em Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2010.

[298] Ibid.

[299] CONTE, Julen Fernández; BURGOS, Diego León. Antecedentes y processo de reforma sobre protección de datos en la Unión Europea. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 35-50.

[300] Nesse sentido, ver: *Digital Rights Ireland Ltda.* (C 293/12 e C 594/12). UNIÃO Europeia. Tribunal de Justiça (Grande Secção). Comunicações eletrônicas. **Diretiva 2006/24/CE** – Serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações – Conservação de dados gerados ou tratados no contexto da oferta desses serviços – Validade – Artigos 7.°, 8.° e 11.° da Carta dos Direitos Fundamentais da União Europeia. Acórdão do Tribunal de Justiça, C-293/12 e C-594/12 (processos apensos). Digital Rights Ireland Ltd. contra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General, 08 de abr. 2014. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=671099>. Acesso em: 15 set. 2017.

discussão mais profunda sobre a legitimidade e a legalidade dos critérios a serem estabelecidos, especialmente em se falando de categorias de risco voltadas para indivíduos[301].

Por fim, digna de nota é a Diretiva 2016/680, que vem a ser aplicada concomitantemente com o novo regulamento geral de proteção de dados. Em que pese também ter como objeto o tratamento de dados pessoais, ela destina-se apenas àquele realizado por autoridades para fins de "[...] prevenção, investigação, detenção, ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública" (art. 1º, *caput*). Em se tratando de finalidade distinta, ainda que se trate de autoridade que atue costumeiramente na seara penal, deve-se aplicar o regulamento (Considerando 12)[302].

Composta por 107 Considerandos e 65 Artigos, essa diretiva já se encontra em vigor desde 27 de abril de 2016, tendo como destinatários todos os Estados membros da EU. Trabalhando noções como segurança pública (ou nacional), especialmente no que toca ao combate ao terrorismo, essa Diretiva busca balizar o respeito à proteção de dados pessoais, enquanto um direito fundamental (Considerando 1), independente da nacionalidade do titular dos dados

---

[301] É o que se extrai da fala de Alessandra Silveira no VII Encontro Internacional do CONPEDI em Braga/PT no painel Democracia e tecnologias da informação realizado em 07 set. 2017, das 14h30min às 17h, na Universidade do Minho (CEDU), Braga, Portugal. SILVEIRA, Alessandra. Democracia e tecnologias da informação. In: VII ENCONTRO INTERNACIONAL DO CONPEDI, Portugal, Braga, 7 set. 2017.

[302] "(12) As funções de polícia ou de outras autoridades de aplicação da lei centram-se principalmente na prevenção, investigação, deteção ou repressão de infrações penais, incluindo as atividades policiais sem conhecimento prévio de que um incidente constitui ou não uma infração penal. Estas funções podem incluir o exercício da autoridade através de medidas coercivas, tais como as atividades da polícia em manifestações, grandes eventos desportivos e distúrbios. Essas funções incluem também a manutenção da ordem pública enquanto atribuição da polícia ou de outras autoridades de aplicação da lei, quando necessárias para a salvaguarda e prevenção de ameaças à segurança pública e aos interesses fundamentais da sociedade protegidos por lei, e à prática de infrações penais. Os Estados-Membros podem atribuir às autoridades competentes outras funções que não sejam necessariamente executadas para efeitos de prevenção, investigação, deteção ou repressão de infrações penais, nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública, de modo que o tratamento dos dados pessoais para esses outros efeitos, na medida em que se insira na esfera do direito da União, seja abrangido pelo âmbito de aplicação do Regulamento (UE) 2016/679." UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 2016/680, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**, L 119/89. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT>. Acesso em: 1 ago. 2017.

(Considerando 2), e a prevenção, a investigação e a repressão de atividades criminais, inclusive facilitando mecanismos de cooperação judicial penal e policial (Considerando 5).

Percebe-se que há por parte dessa Diretiva uma recepção dos princípios positivados em matéria de proteção de dados na Diretiva 95/46 e no RGPD; porém, com algumas especificidades (principalmente em relação à questão do consentimento[303] e à do direito de acesso)[304]. Como exemplo dessa recepção, destaca-se o dever de informação que se articula juntamente com o princípio da

[303] A respeito do consentimento, Rodríguez aponta que "[...] *en determinadas ocasiones las autoridades competentes podrán exigir a las personas físicas que atendam su solicitude de datos de caráter personal como una obligación, de tal forma que su consentimento no será fundamento jurídico necesario para su tratamento* [...]. *Aun así, los Estados membros podrán estabelecer en su legislación que el interessado acepte o no el tratamiento de sus datos personales a los efectos de la Directiva* [...]". RODRÍGUEZ, Ofelia Tejerina. VII. Interrelación com la directiva sobre protección de datos por autoridades competentes. In: PIÑAR MAÑAS, José Luis. **Regulamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 103.

[304] "Artigo 15º Limitações do direito de acesso
1. Os Estados-Membros podem adotar medidas legislativas para limitar, total ou parcialmente, o direito de acesso do titular dos dados, se e enquanto tal limitação, total ou parcial, constituir uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de: a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais;
b) Evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais;
c) Proteger a segurança pública;
d) Proteger a segurança nacional;
e) Proteger os direitos e as liberdades de terceiros.
2. Os Estados-Membros podem adotar medidas legislativas a fim de determinar as categorias de tratamento suscetíveis de ser abrangidas, total ou parcialmente, por uma das categorias previstas no nº 1.
3. Nos casos a que se referem os nº 1 e 2, os Estados-Membros preveem que o responsável pelo tratamento informe por escrito o titular dos dados, sem demora injustificada, de todos os casos de recusa ou limitação de acesso, e dos motivos da recusa ou da limitação. Essa informação pode ser omitida caso a sua prestação possa prejudicar uma das finalidades enunciadas no nº 1. Os Estados-Membros preveem que o responsável pelo tratamento informe o titular dos dados do direito que lhe assiste de apresentar reclamação à autoridade de controlo ou de intentar uma ação judicial.
4. Os Estados-Membros preveem que o responsável pelo tratamento detalhe os motivos de facto ou de direito em que a sua decisão se baseou. Essa informação deve ser facultada às autoridades de controlo." UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 2016/680, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**, L 119/89. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT>. Acesso em: 1 ago. 2017.

finalidade (Considerando 33)[305], de forma a possibilitar um controle contra a abusividade no tratamento de dados[306].

Em termos de cooperação transnacional, os artigos 35 e seguintes estipulam os requisitos para a transferência de dados pessoais para outras autoridades de outros países. Inclusive, deles destaca-se que, em havendo uma decisão da Comissão reconhecendo um nível de proteção adequado no país destinatário, essa transferência de dados prescinde de autorização específica (art. 36, 1º). Ademais, é possível que essa transferência se dê mesmo sem a aludida decisão, especialmente nos casos de urgência – gerlamente, situações de risco em que se ameasse a segurança nacional de um país – (art. 38, 1º, *d*)[307].

Consoante já referido anteriormente, tal diretiva tem aplicação concomitante ao Regulamento, vez que se restringe a tratamentos de dados cujas finalidades são distintas daquelas reguladas pelo Regulamento. Ou seja, trata-se de normativa complementar ao regulamento, visando à regulamentação de aspectos específicos que justificam um tratamento diferenciado, notadamente a segurança pública e nacional.

---

[305] "(33) Sempre que a presente diretiva se refira ao direito de um Estado-Membro, a um fundamento jurídico ou a uma medida legislativa, não se trata necessariamente de um ato legislativo adotado por um parlamento, sem prejuízo dos requisitos que decorram da ordem constitucional do Estado-Membro em causa. No entanto, esse direito de um Estado-Membro, esse fundamento jurídico ou essa medida legislativa deverão ser claros e precisos, e a sua aplicação deverá ser previsível para os particulares, como exigido pela jurisprudência do Tribunal de Justiça e pelo Tribunal Europeu dos Direitos do Homem. O direito dos Estados-Membros que rege o tratamento de dados pessoais no âmbito da presente diretiva deverá especificar, pelo menos, os objetivos, os dados pessoais a tratar, as finalidades do tratamento e os procedimentos destinados a preservar a integridade e a confidencialidade dos dados pessoais, bem como os procedimentos para a destruição dos mesmos, proporcionando assim garantias suficientes contra o risco de abusos e de arbitrariedade." UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 2016/680, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**, L 119/89. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT>. Acesso em: 1 ago. 2017.

[306] RODRÍGUEZ, Ofelia Tejerina. Interrelación con la directiva sobre protección de datos por autoridades competentes. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 97-114.

[307] A esse respeito, ver: RODRÍGUEZ, op. cit., p. 104-105.

2.2.3 Novo regulamento europeu de proteção de dados pessoais: Regulamento (UE) 2016/679

Em 2010, uma mudança de enfoque da Comissão Europeia para uma perspectiva mais global da proteção de dados pessoais denunciou a defasagem da Diretiva 95/46. O aporte legislativo lá de 1995, em que pese ainda cumprir seus objetivos originários, não mais se adaptava às inovações tecnológicas e à consolidação do fenômeno da globalização. Frente a tal quadro, a Comissão Europeia reconheceu a necessidade de modernização do quadro legislativo, formulando a proposta de um Regulamento Geral de Proteção de Dados em 2012[308].

Piñar Mañas aponta como aspecto mais criticado da Diretiva 95/46 o seu fracasso em propor um sistema unitário de proteção no território da União Europeia. As lacunas deixadas no texto normativo fragilizaram uma construção homogênea de proteção de dados pessoais, dando margem a uma aplicação fragmentada e assimétrica da Diretiva dentro dos países membros. Tal situação não só gerou grande insegurança jurídica, que debilita a livre circulação de dados, mas contribuiu para a falta de percepção da opinião pública acerca dos riscos que o tratamento automatizado de informações pessoais enseja[309].

Nesse sentido, a elaboração do novo regulamento introduziu, direta ou indiretamente, um novo modelo de proteção de dados para a Europa[310]. Porém, como bem aponta Piñar, a afirmação de que o regulamento supõe um "giro copernicano" em relação à proteção já existente deve ter presente a ressalva de que a grande maioria, se não a totalidade, dos princípios e fundamentos presentes na Diretiva 95/46/CE seguem os mesmos que figuram na base da construção da proteção de dados pessoais na Europa, bem como o conteúdo do direito à proteção

---

[308] CONTE, Julen Fernández; BURGOS, Diego León. Antecedentes y processo de reforma sobre protección de datos en la Unión Europea. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 35-50.

[309] Vide PIÑAR MAÑAS, op. cit., p. 60.

[310] Em termos de Espanha, chama atenção que se trata da primeira vez que a regulação de um direito se deu por meio de um regulamento (e não por intermédio de uma lei orgânica, consoante dispõe o art. 81 da Constituição Espanhola). Especialmente, porque o regulamento não se limita a regular apenas um aspecto específico do direito à proteção de dados, mas a totalidade de sua disciplina, inclusive seu conteúdo essencial.

de dados pessoais previsto no art. 8º da Carta Europeia de Direitos Humanos segue inalterado[311].

A normativa marca uma guinada nesse novo modelo de proteção de dados "[...] que passa da gestão dos dados ao uso responsável da informação", trazendo princípios como *accountability* (responsabilidade proativa)*, privacy by design* e *privacy by default*. Percebe-se, assim, uma aproximação da tutela das informações pessoais a uma tutela elaborada com base em análises de riscos[312].

Ademais, é notória a abordagem dualista proposta no novo regulamento. Esse incentiva tanto a autorregulação, por meio de uma responsabilidade proativa ou *accountability*[313], como fortalece os mecanismos de controle institucional em nível nacional e em nível de União Europeia[314].

Sua implantação se presta, ademais, a desempenhar um papel de marco normativo mais sólido e coerente (Considerando 7), que coíba uma aplicação fragmentada e a inseguridade jurídica, não raras vezes, proveniente das diferenças de proteção entre os sistemas normativos dos diferentes Estados membros (Considerando 9)[315].

A esse respeito, importante anotar que os Regulamentos da União Europeia "[...] são obrigatórios em todos os seus elementos e diretamente aplicáveis em cada Estado membro"[316]. No caso do Regulamento Geral de Proteção de Dados (RGPD), em que pese não necessariamente revogue as leis nacionais sobre a matéria, ele, no mínimo, derroga todas as disposições que lhe forem contrárias[317].

---

311 PIÑAR MAÑAS, José Luis. Introducción: hacia un nuevo modelo europeo de protección de datos. In: _____ (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 15-22. p. 16.

312 "*Un nuevo modelo que podemos decir que passa de la gestión de los datos al uso responsable de la información*." Ibid., p. 16.

313 O próprio NRPDP já dispõe que o responsável pelo tratamento aplicará "[...] as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento" trazendo um princípio geral de responsabilidade que abriga a figura do *accountability* em que a responsabilidade e o próprio cumprimento das normas dispostas no regulamento demandam uma postura proativa do responsável". REIGADA, Antonio Troncoso. Autoridades de control independientes. In: PIÑAR MAÑAS, op. cit., p. 461-512.

314 PIÑAR MAÑAS, op. cit.

315 Ibid.

316 Ibid., p. 17.

317 Tomando a *Ley Orgánica de Protección de Datos de Caráter Personal* Espanhola, Piñar Mañas aponta que o regulamento não a revogou, em que pese tenha revogado grande parte de seu

Como objeto, o Regulamento segue a tônica da Diretiva 95/46, sendo dotado de um duplo objetivo: a proteção de direitos e liberdades fundamentais, notadamente no que concerne à proteção dos dados pessoais; e a garantia da liberdade de uma livre circulação de dados. No caso do regulamento, contudo, parece mais presente a ideia de prevalência, *a priori*, do direito fundamental à proteção de dados pessoais sobre o interesse econômico daqueles responsáveis pelo tratamento, no mesmo sentido em que já se manifestou o Tribunal de Justiça de União Europeia, em 2014, no caso envolvendo a Agência Espanhola de Proteção de Dados Pessoais, um cidadão espanhol e o *Google Spain* (C 131/12). Destarte, a sistemática europeia proposta pelo novo regulamento parte do pressuposto que a "[...] livre circulação em nenhum caso pode justificar a redução o nível de proteção" dos dados pessoais[318].

No que concerne ao seu âmbito de aplicação material, o regulamento mantém basicamente a estrutura estabelecida na Diretiva 95/46. O §1º do art. 2º dispõe que a normativa se aplica aos tratamentos total ou parcialmente automatizados, bem como ao tratamento não automatizado de dados pessoais constantes, ou que venham a constar em ficheiros ou bancos de dados. Por sua vez, o §2º do mesmo artigo traz algumas exceções a essa aplicação, dentre elas o tratamento realizado: nas atividades desenvolvidas fora do âmbito de aplicação do direito comunitário (por exemplo, segurança nacional)[319], nas atividades de política exterior e de segurança comum (PESC) dos Estados membros da União Europeia, nas atividades domésticas ou pessoais[320], e nas atividades de persecução penal, sejam elas

---

conteúdo, demandando sua modificação. PIÑAR MAÑAS, José Luis. Introducción: hacia un nuevo modelo europeo de protección de datos. In: _____ (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 15-22. p. 18.

318 PIÑAR MAÑAS, op. cit., p. 61.

319 Nesse sentido ver. LANDA, Iñaki Uriarte. Ámbito de aplicación material. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia un nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 63-76.

320 A esse respeito dispõe o Considerando 18 que: "[...] o presente regulamento não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma atividade profissional ou comercial. As atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrônico no âmbito dessas atividades. Todavia, o presente regulamento é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas". UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

preventivas, investigativas ou sancionatórias, uma vez que a legislação competente para regular o tratamento de dados para tais finalidades é a Diretiva 2016/680[321][322].

Em termos de aplicação territorial, por outro lado, há uma alteração substancial das regras de competência em relação à Diretiva 95/46. Enquanto legislação diretamente aplicável, o regulamento permitiu-se furtar da discussão sobre qual era o direito nacional aplicável em cada caso, questão altamente conturbada na Diretiva 95/46[323]. Em dezembro de 2010, o Grupo de Trabalho do Artigo 29 emitiu um "*Dictamen 8/2010*" acerca da temática da aplicação territorial da Diretiva 95/46, do qual se extraía que não se aplicaria o direito nacional de nenhum Estado membro quando o responsável pelo tratamento não possuísse nenhum estabelecimento em algum país membro e não recorresse a meios de tratamentos situados neles, salvo quando apenas para fins de trânsito[324].

Esse entendimento foi alterado com a sentença do TJUE de maio de 2014, no famoso caso do *Google Spain,* que envolvera a temática do direito ao esquecimento

---

e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[321] Diretiva já trabalhada no item 2.2.3 deste capítulo.

[322] "Artigo 2º. Âmbito de aplicação material 1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados. 2. O presente regulamento não se aplica ao tratamento de dados pessoais: a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União: b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detenção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. 3. O Regulamento (CE) nº 45/2001 aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) nº 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no artigo 98. 4. O presente regulamento não prejudica a aplicação da Diretiva 2000/31/CE, nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12º a 15º. UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[323] No caso da Diretiva 95/46 se considerava aplicável o direito do Estado membro em que o haja um estabelecimento do responsável pelo tratamento, sendo que cada estabelecimento deveria observar as leis nacionais de onde estava localizado (em se tratando de mais de um estabelecimento) – *vide* art. 4. A ambiguidade do artigo e as inúmeras interpretações deste, contundo, denunciaram sua fragilidade. CARULLA, Santiago Ripol. Aplicación territorial del reglamento. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 77-186.

[324] Ibid., p. 85.

ou direito à desindexação[325]. Para além da questão material, o procedimento tratava da aplicação da Diretiva 95/46 sobre os motores e ferramentas de busca da internet, tendo de um lado da lide o Google (*Google Spain* e *Google Inc*.) e de outro a AEPD e Mario Costeja Gonzáles (enquanto interessado)[326].

Na sentença, o TJUE considerou que a empresa responsável pelo tratamento de dados possuía sede em pais não pertencente à União Europeia, porém, possuía estabelecimento situado em país membro da EU. Nesse sentido, o Tribunal firmou entendimento que, ainda que o estabelecimento que se encontra dentro da EU não seja o responsável pelo tratamento de dados pessoais ou por qualquer atividade diretamente relacionada a esse (no caso sua atividade era tão somente de fins publicitários), não se pode dissociar as operações realizadas pela empresa fora e dentro da EU, vez que o financiamento do tratamento realizado pelos motores de busca se dá pelo desenvolvimento de atividades de publicidade realizadas dentro da EU. Portanto, sustentou-se que a LEPD e a Diretiva 95/46 eram aplicáveis ao tratamento realizado, ainda que fora da EU[327].

Trata-se de exercício interpretativo que busca readequar a Diretiva à realidade tecnológica que a deixara obsoleta. Seguindo a construção proposta no caso *Google Spain*, o Regulamento Geral de Proteção de Dados Pessoais acabou não só incorporando tal extensão da proteção em seu corpo normativo como a aumentou, sendo seu art. 3º dotado da seguinte redação:

> Artigo 3º. **Âmbito de aplicação territorial**
>
> 1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União. L 119/32 PT Jornal Oficial da União Europeia 4.5.2016

[325] Dependendo da linha doutrinária que se segue, o direito à desindexação pode ser trabalhado tanto dentro do escopo do direito ao esquecimento quanto como um novo direito distinto daquele. Nesse sentido ver: RUARO, Regina Linden; MACHADO, Fernando Inglez de Souza. Ensaio a propósito do direito ao esquecimento: limites, origem e pertinência no ordenamento jurídico brasileiro. **Revista do Direito Público**, Londrina, v. 12, n. 1, p.204-233, abr. 2017.

[326] CARULLA, Santiago Ripol. Aplicación territorial del reglamento. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 77-186.

[327] Ibid.

2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:

a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;

b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.

3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.[328]

[328] Importante referir, também, os Considerandos 22, 23 e 24 que dispõem, respectivamente: "(22) Qualquer tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado na União deverá ser feito em conformidade com o presente regulamento, independentemente de o tratamento em si ser realizado na União. O estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto.
(23) A fim de evitar que as pessoas singulares sejam privadas da proteção que lhes assiste por força do presente regulamento, o tratamento dos dados pessoais de titulares que se encontrem na União por um responsável pelo tratamento ou subcontratante não estabelecido na União deverá ser abrangido pelo presente regulamento se as atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares, independentemente de estarem associadas a um pagamento. A fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio web do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrônico ou outro tipo de contatos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União.
(24) O tratamento de dados pessoais de titulares de dados que se encontrem na União por um responsável ou subcontratante que não esteja estabelecido na União deverá ser também abrangido pelo presente regulamento quando esteja relacionado com o controlo do comportamento dos referidos titulares de dados, na medida em que o seu comportamento tenha lugar na União. A fim de determinar se uma atividade de tratamento pode ser considerada «controlo do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes." UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

Então, não só nas hipóteses de casos semelhantes ao *Google Spain,* ou de que o tratamento em si se dê dentro do território da EU, será aplicável o regulamento (§1º), mas sempre que o tratamento envolva um residente da União Europeia, para fins de oferta de bens, ou serviços ou controle de comportamento (§2º). Ou seja, busca-se afetar todas as entidades que atuem na (ou sobre a) EU, ainda que não tenham sede nessa[329].

Em que pese muito completo, o art. 3º do RGPD que vem a substituir o art. 4º da Diretiva 95/46 se mostra, na prática, muito complexo e de difícil aplicação. Parece um verdadeiro desafio a aplicação desse regulamento no que concerne aos estabelecimentos situados em países não membros da EU, vez que suscita o debate acerca de questões como o respeito à soberania de outros países e de uma governança da internet.

Em termos de definições, o Regulamento também traz algumas inovações em relação à Diretiva 95/46. Em seu art. 4º, para além das definições trazidas na Diretiva 95/46 (nesta, no art. 2º) – relativas a dados pessoais, tratamento, consentimento, ficheiro de dados pessoais, destinatário, terceiro, responsável pelo e encarregado pelo tratamento –, o regulamento traz noções como limitação do tratamento[330], definição de perfis[331], dados genéticos, dados biométricos, dados

---

[329] CARULLA, Santiago Ripol. Aplicación territorial del reglamento. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 77-186.

[330] "3) «Limitação do tratamento», a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro;[...]." A esse respeito, o Considerando 67 dispõe que: "(67) Para restringir o tratamento de dados pessoais pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio web dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados. Deverá indicar-se de forma bem clara no sistema que o tratamento dos dados pessoais se encontra sujeito a restrições." UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[331] "4) «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;[...]." Ibid.

relativos à saúde, pseudonimização[332], autoridade de controle, autoridade de controle interessada[333], objeção pertinente e motivada, e tratamento transfronteiriço[334].

No que concerne aos princípios do direito à proteção de dados pessoais, eles seguem sem nenhuma alteração significativa em relação à Diretiva 95/46, de forma que se entende não ser pertinente aprofundar novamente essa questão. Cabível, contudo, tecer algumas considerações a propósito da figura do consentimento, vez que se identificam algumas alterações não apenas em relação à Diretiva 95/46, mas entre as próprias versões do Regulamento em diferentes idiomas[335][336].

De início, é possível constatar que o próprio termo consentimento (*conset*, em inglês, e *consentimento*, em espanhol) é utilizado 68 vezes nas versões em português e em espanhol, ao passo que é mencionado 72 vezes em sua versão original em inglês. Da redação do regulamento[337] depreende-se que ele pressupõe

---

[332] "5) «Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável; [...]." UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[333] "22) «Autoridade de controlo interessada», uma autoridade de controlo afetada pelo tratamento de dados pessoais pelo facto de: a) O responsável pelo tratamento ou o subcontratante estar estabelecido no território do Estado-Membro dessa autoridade de controlo; b) Os titulares de dados que residem no Estado-Membro dessa autoridade de controlo serem substancialmente afetados, ou suscetíveis de o ser, pelo tratamento dos dados; ou c) Ter sido apresentada uma reclamação junto dessa autoridade de controlo; [...]." Ibid.

[334] POU, María Arias. Definiciones a efecto del reglamento general de protección de datos. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 115-134.

[335] Para fins de tal análise, tomar-se-á como base a versão original em inglês e as versões em português e espanhol.

[336] A esse respeito ver: VARELA, Borja Adsuara. El consentimiento. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 151-170.

[337] Do art. 4º do Regulamento depreende-se: "11) «Consentimento» do titular dos dados, uma 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; [...]." Por sua vez, o Considerando 32 elucida que: "O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus

uma ação, seja ela uma manifestação explícita ou uma ação afirmativa, ao passo que a Diretiva 95/46 requer, apenas, uma livre manifestação de vontade. Em outras palavras, a nova redação trazida pelo regulamento buscou afastar de forma inequívoca o consentimento tácito e o consentimento brando, vez que ele deve sempre ser para fins específicos e mediante uma ação afirmativa[338].

Entrementes, a figura da ação afirmativa pode, por vezes, ser confundida com um consentimento implícito. Do Considerando 32, extrai-se que:

> O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração **ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais** [...].[339] [Grifo nosso].

Na prática, é possível identificar diversos *sites* da internet que se valem dos testemunhos de conexão (os *cookies*)[340], os quais abrem uma notificação quando o usuário acessa a página, notificando-o do uso dessa ferramenta e possibilitando que ele também visualize a política de *cookies* da página. Não obstante, para acessar o conteúdo da mesma não é possível se opor à utilização. As opões do usuário limitam-se a clicar na opção “aceito” que abre na janela de notificação do uso de *coockies,* ou continuar a acessar o conteúdo da página, o que se considera, também, como aceitamento da política de *cookies* do *site*. Para fins desse Regulamento, nada obstante, seguir acessando o conteúdo de um *site* é considerado como uma ação afirmativa. Ademais, importante referir que os *cookies*

---

dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrônica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido.” UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[338] VARELA, Borja Adsuara. El consentimiento. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 151-170.

[339] UNIÃO Europeia, op. cit.

[340] A figura dos *cookies* será enfrentada posteriormente neste trabalho

são objeto de regulação por parte da Diretiva 2002/58 (posteriormente alterada pela Diretiva 2009/136) e, em termos de Espanha, pela *Ley 34/2002, de servicios de la sociedade de la información y de comercio electrónico* (art. 22.2.), sendo clara, em ambas as normativas, a necessidade de consentimento prévio.

Como diferenças, chama atenção que o art. 4.11., nas versões em português e em inglês, referem-se ao "titular dos dados" ("*data subjetct"*), enquanto a versão espanhola desse artigo refere-se ao "*interesado*". Consoante aponta Varela[341], tal variação, ainda que sutil, abre margem para a ampliação da gama de sujeitos englobados pelo Regulamento em sua versão espanhola.

Assim como na Diretiva que o precedeu, o Regulamento trabalha a figura do consentimento não como um requisito imprescindível ao tratamento de dados pessoais, mas como uma das hipóteses de legitimação desse tratamento – art. 7º. Segundo assinala Varela, tal construção não seria a mais adequada, vez que eleva hipóteses tidas com exceção – por exemplo, quando o tratamento é imprescindível ao objeto do contrato celebrado (art. 7º, *b*) – ao mesmo patamar da regra[342]. Contudo, a opção do legislador parece adequada ao reconhecer as limitações da figura do consentimento já denunciadas por Rodotà em 2008, em especial se for trabalhada a questão do consentimento enquanto condicionante de acesso a bens e serviços[343].

Outrossim, a construção do Regulamento parece mais coerente com a sua proposta de um novo modelo de proteção da dados baseado não mais na gestão

---

[341] "*La tradución de <<data subjetct>> por <<interessado>> (en los datos) creemos que amplía mucho el ámbito subjetivo de los derechos: no es lo mismo <<sujeto>> o <<titular>> de datos que <<afectado>> o <<interessado>> por unos datos personales.* [...] *Por último, <<personal data relating to him or her>> se traduce como los <<datos personales que le conciernen>> (al interesado) y aunque no se usa el mismo término, hay que destacar que tanto <<concernir>> como <<relacionar>> son dos términos amplios, que admiten la existência de diferentes tipos de relaciones jurídicas de distintos sujetos (de derechos) sobre unos mismos datos*." VARELA, Borja Adsuara. El consentimiento. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 151-170. p. 155-156.

[342] "*No estamos de acuerdo con este enfoque (aunque es el mismo que sigue el artículo 10 del Reglamento de desarrollo de la LOPD, referido a <<supuestos que legitiman el trataminento o cesión de los datos>>), pues se pone al mismo nivel la regla y las excepciones; y creemos que há de destacarse, por encima de todo, el principio de libertad y autodeterminación respecto de los propios datos*." Ibid., p. 158.

[343] Essa questão do consentimento será abordada de forma mais aprofundada no capítulo 3 deste trabalho. A esse respeito, também, ver: RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 101-102.

dos dados pessoais, mas no uso responsável da informação, consoante bem assevera Piñar[344].

Ainda em termos de consentimento, importante asseverar que a figura dos menores também foi considerada, sendo lícito a partir dos 16 anos completos, salvo disposição específica de algum Estado membro que pode reduzir tal idade até o limite mínimo de 13 anos. Em se tratando de menor com idade inferior legalmente exigida, o consentimento só é lícito se realizado pelo responsável do menor (art. 8º)[345].

Quanto aos dados sensíveis, basicamente segue-se a mesma estrutura da Diretiva 95/46. O art. 9º do Regulamento disciplina o "[...] tratamento de categorias especiais de dados pessoais" que correspondem aos dados sensíveis (Considerando 10). Do texto legal, depreende-se uma proibição geral de tratamento desses dados (art. 9.1)[346]; porém, a própria normativa já prevê hipóteses de derrogação dessa proibição (art. 9.2 e Considerandos 51 e 52).

No que toca aos direitos do titular dos dados (segundo a versão espanhola, do interessado), pouca ou nenhuma alteração substancial se identifica no direito de acesso, de retificação e de apagamento dos dados. Nesse último, contudo, aponta-se que houve a inclusão da expressão "direito a ser esquecido" (art. 17) e, na versão espanhola do Regulamento, a alteração da nomenclatura clássica de *derecho a la*

---

344 "[...] *el Reglamento introduce, a veces diretamente, a veces de forma algo soterrada, un nuevo modelo de protección de datos para Europa. Un nuevo modelo que podemos decir que passa de la gestión de los datos al uso responsable de la información*." PIÑAR MAÑAS, José Luis. Introducción: hacia un nuevo modelo europeo de protección de datos. In: _____ (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 15-22. p. 16.

345 Na Espanha, por exemplo, a idade para consentir é de 14 anos em razão das disposições da LOPDP espanhola.

346 "Artigo 9º. **Tratamento de categorias especiais de dados pessoais**
1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa." UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

cancelación para o termo *derecho a la supresión,* ambas as modificações feitas, ao que parece, para englobar, também, os motores de busca da internet[347].

O direito à limitação do tratamento, por sua vez, restringe a possiblidade de tratamento que não à conservação dos dados. Nesse caso, o tratamento só é lícito quando se obtém um novo consentimento do titular dos dados, para fins de declaração ou exercício de defesa em processo judicial, ou por poderosos motivos de interesse público (art. 18.2). É possível o exercício de tal direito nas seguintes hipóteses (art. 18.1):

> [...] a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão;
>
> b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;
>
> c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
>
> d) Se tiver oposto ao tratamento nos termos do artigo 21, n. 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.[348]

Por sua vez, o direito de oposição é aprimorado em relação à Diretiva 95/46, ainda que conserve a mesma estrutura. Ele se divide em direito à oposição ao tratamento (art. 21 do Regulamento e art. 14 da Diretiva) e em direito de oposição contra decisões individuais automatizadas (art. 22 do Regulamento e art. 15 da Diretiva)[349].

Começando pela oposição ao tratamento, trata-se de direito que pode ser exercido a qualquer tempo e sem qualquer custo contra os tratamentos realizados

---

[347] CARO, María Álvarez. El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas. In: PIÑAR MAÑAS, José Luis(Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 227-240.

[348] UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[349] CARO, op. cit.

para o “exercício de funções de interesse público” ou para “efeitos dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros”, inclusive quando para a elaboração de perfis[350]. Como explicita o Considerando 69, caberá ao responsável pelo tratamento demonstrar que seu interesse prevalece sobre o do titular dos dados, *in verbis:*

> (69) No caso de um tratamento de dados pessoais lícito realizado por ser necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento ou ainda por motivos de interesse legítimo do responsável pelo tratamento ou de terceiros, o titular não deverá deixar de ter o direito de se opor ao tratamento dos dados pessoais que digam respeito à sua situação específica. Deverá caber ao responsável pelo tratamento provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados.[351]

Por sua vez, o direito de opor-se a decisões individuais automatizadas pressupõe, primeiro, que o titular tenha o direito de saber quais dados são objeto de coleta, a finalidade da coleta e “[...] da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências” (Considerando 63). Tal direito consiste, basicamente, na faculdade de “[...] não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspectos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar”, incluindo-se, aqui, tratamentos que visem definições de perfis de comportamento de natureza econômica, social, profissional ou relativa à saúde do indivíduo (Considerando 71). Nesse sentido, o titular dos dados tem “[...] direito de obter a intervenção humana,

---

[350] A respeito da elaboração de perfis dispõe o Considerando 70 que: “Sempre que os dados pessoais forem objeto de tratamento para efeitos de comercialização direta, o titular deverá ter o direito de se opor, em qualquer momento e gratuitamente, a tal tratamento, incluindo a definição de perfis na medida em que esteja relacionada com a referida comercialização, quer se trate do tratamento inicial quer do tratamento posterior. Esse direito deverá ser explicitamente levado à atenção do titular e apresentado de modo claro e distinto de quaisquer outras informações”. UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[351] Ibid.

de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão" (Considerando 71)[352].

Inovação trazida pelo Regulamento, o direito à portabilidade dos dados pessoais surge como um direito novo e autônomo (em relação àqueles já previstos na Diretiva 95/46) e vem positivado no art. 20 do Regulamento[353]. Ele consiste, basicamente, no direito do titular dos dados de "[...] receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática", bem como de "[...] transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir" (art. 20.1.), inclusive que "[...] os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível" (art. 20.2.). Ou seja, trata-se de faculdade ao titular dos dados, mas uma obrigação para o responsável pelo tratamento.

Bebendo fortemente da influência do grupo de trabalho intitulado *Data Portability Project*, criado no final de 2007 nos EUA, o direito à portabilidade de dados pessoais também visa possibilitar que o usuário recupere o controle sobre suas próprias informações pessoais cedidas a uma empresa da sociedade da informação durante o curso de sua relação – usualmente, de consumo – com a mesma[354].

Em que pese se possa alegar que tal direito nada mais é que o desenvolvimento da figura do direito de acesso às informações pessoais, ou de um direito à autodeterminação informativa e do princípio do consentimento, a possibilidade de o usuário requerer que seus dados sejam fornecidos a um terceiro (inclusive com as informações "num formato estruturado, de uso corrente e de leitura

---

[352] UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[353] SAMANIEGO, Javier Fernández; LONGORIA, Paula Fernandez. El derecho a la portabilidad de los datos. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 257-274.

[354] Ibid.

automática" – art. 20.1.) consiste, inegavelmente, em uma inovação trazida por esse direito[355].

Reitera-se que esse direito, em que pese instigar tal conduta, não obriga o responsável pelo tratamento de utilizar ou manter sistemas de tratamento tecnicamente compatíveis (Considerando 68). Portanto, a faculdade de o titular requerer que os dados sejam diretamente transmitidos para terceiros nem sempre poderá ser atendida em razão de eventual incompatibilidade (até por isso a utilização do vocábulo "sempre que tal seja tecnicamente possível" – art. 20.2.), mas nada impede que ele recebe tais informações e repasse, posteriormente, a um terceiro, nos termos do art. 20.1.

Analisando-se o Considerando 68, identifica-se que esse direito se presta a "reforçar o controle [do titular] sobre os seus próprios dados". Ademais, ele explicita que tal direito é aplicável somente quando o tratamento for realizado com base no consentimento do titular dos dados, ou para fins de cumprimento de um contrato. Outra limitação a esse direito é quando ele esbarra nos direitos e liberdades de terceiros (art. 20.4.); assim, quando as informações não disserem respeito somente ao titular dos dados, só serão fornecidas aquelas que não afetem negativamente terceiros[356].

Ainda sob abrigo do art. 20.4., é possível que o responsável pelo tratamento não realize a portabilidade dos dados que possam violar seus direitos de propriedade intelectual. Ou seja, aqueles dados adquiridos por meio do cruzamento de informações, especialmente a partir do uso de algoritmos, não são de fornecimento obrigatório pelo responsável pelo tratamento (por exemplo, o *score* gerado por ferramentas de *creditscore*)[357]. Tal exceção também pode encontrar respaldo no art. 20.1.*b.*, que permite que se impeça a portabilidade no caso de tratamento "realizado por meios automatizados".

No que concerne à responsabilidade do responsável pelo tratamento, ela pode ser penal, administrativa e civil, não havendo prejuízo na cumulação da

---

[355] SAMANIEGO, Javier Fernández; LONGORIA, Paula Fernandez. El derecho a la portabilidad de los datos. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 257-274.

[356] Ibid.

[357] A sistemática do *credit scoring* será enfrentada no terceiro capítulo desta dissertação.

responsabilidade civil com a administrativa ou a penal, conforme o caso concreto. Em termos de Regulamento, ele prevê a aplicação de algumas multas ("coimas") administrativas (art. 83), que podem variar de 10.000.000 a 20.000.000 de euros ou de 2% a 4% do volume de negócios do exercício financeiro anterior em nível mundial, bem como dá margem aos Estados membros para que estabeleçam sanções aos casos em que o Regulamento não previu a aplicação de multa, podendo ser de natureza penal ou administrativa, porém sempre de caráter efetivo, dissuasório e proporcional (art. 84)[358].

Em que pese a importância da responsabilidade penal, que se dá (ao menos em termos de Espanha), pelo acesso, alteração ou transmissão de dados pessoais de forma dolosa e não autorizada[359], enfocar-se-á, no presente estudo, as searas administrativa e civil. O Regulamento dispõe, em seu art. 24, que o responsável pelo tratamento deve aplicar "[...] medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento". Do disposto, conclui-se que: a ele cabe o ônus de comprovar que adotou as medidas adequadas a um tratamento seguro e as medidas a serem adotadas. As medidas a serem adotadas devem observar um critério de proporcionalidade às atividades de tratamento, especialmente no que concerne sua "[...] natureza, o âmbito, o contexto e as finalidades"[360].

---

[358] ÁLVAREZ, Luis Felipe López. La responsabilidad del responsable. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 275-294.

[359] Ibid.

[360] "Artigo 24º Responsabilidade do responsável pelo tratamento
1.Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.
2. Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o nº 1 incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento.
3. O cumprimento de códigos de conduta aprovados conforme referido no artigo 40º ou de procedimentos de certificação aprovados conforme referido no artigo 42º pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento." UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

As “coimas” dispostas no art. 83 correspondem à violação de obrigações impostas ao responsável pelo próprio Regulamento (*vide* arts. 8º, 11, 25 a 39 e 42), a violação dos princípios de tratamento (*vide* arts. 5º, 6º, 7º e 9º), a violação de direitos do titular dos dados (*vide* arts. 12 a 22), ou a inobservância de alguma restrição imposta por uma autoridade de controle. Importante lembrar que, nesse caso, se responsabilizam ações dolosas (quando há a intenção), assim como culposas (especialmente nas figuras da negligência e da imprudência) – *vide* art. 83. 2[361].

Por fim, a responsabilidade civil do responsável pelo tratamento pode se dar de duas formas. A primeira é quando ocorre do descumprimento do Regulamento que, por si só, gera o dever de indenizar o dano[362]. A segunda, por sua vez,

---

[361] Artigo 83. Condições gerais para a aplicação de coimas
[...]
2. Consoante as circunstâncias de cada caso, as coimas são aplicadas para além ou em vez das medidas referidas no artigo 58.o, n. 2, alíneas a) a h) e j). Ao decidir sobre a aplicação de uma coima e sobre o montante da coima em cada caso individual, é tido em devida consideração o seguinte:
a) A natureza, a gravidade e a duração da infração tendo em conta a natureza, o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos por eles sofridos;
b) O caráter intencional ou negligente da infração;
c) A iniciativa tomada pelo responsável pelo tratamento ou pelo subcontratante para atenuar os danos sofridos pelos titulares;
d) O grau de responsabilidade do responsável pelo tratamento ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos 25º e 32.o;
e) Quaisquer infrações pertinentes anteriormente cometidas pelo responsável pelo tratamento ou pelo subcontratante;
f) O grau de cooperação com a autoridade de controlo, a fim de sanar a infração e atenuar os seus eventuais efeitos negativos;
g) As categorias específicas de dados pessoais afetadas pela infração;
h) A forma como a autoridade de controlo tomou conhecimento da infração, em especial se o responsável pelo tratamento ou o subcontratante a notificaram, e em caso afirmativo, em que medida o fizeram;
i) O cumprimento das medidas a que se refere o artigo 58.o, nº 2, caso as mesmas tenham sido previamente impostas ao responsável pelo tratamento ou ao subcontratante em causa relativamente à mesma matéria;
j) O cumprimento de códigos de conduta aprovados nos termos do artigo 40º ou de procedimento de certificação aprovados nos termos do artigo 42.o; e
k) Qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como os benefícios financeiros
obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração.” UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[362] Considerando 146: “(146) O responsável pelo tratamento ou o subcontratante deverão reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o presente regulamento responsável pelo tratamento. O responsável pelo tratamento ou o subcontratante pode ser exonerado da responsabilidade se provar que o facto que causou o dano

demanda a verificação de dolo ou culpa, cabendo ao responsável o ônus de comprovar que adotou todas as medidas técnicas e organizativas que determina o art. 24 do Regulamento[363], lembrando que elas sempre devem ser proporcionais às especificidades do tratamento realizado e do risco a ele inerente[364], Ou seja, trata-se de seara de responsabilidade intimamente ligada às responsabilidades civil e administrativa, mas que, por vezes, pode ocorrer de forma autônoma e independente dessas[365].

---

não lhe é de modo algum imputável. O conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do presente regulamento. Tal não prejudica os pedidos de indemnização por danos provocados pela violação de outras regras do direito da União ou dos Estados-Membros. Os tratamentos que violem o presente regulamento abrangem igualmente os que violem os atos delegados e de execução adotados nos termos do presente regulamento e o direito dos Estados-Membros que dê execução a regras do presente regulamento. Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido. Sempre que os responsáveis pelo tratamento ou os subcontratantes estiverem envolvidos no mesmo tratamento, cada um deles deverá ser responsabilizado pela totalidade dos danos causados. Porém, se os processos forem associados a um mesmo processo judicial, em conformidade com o direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido. Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento". UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[363] Considerando 74: "(74) Deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares". Ibid.

[364] A esse propósito o Considerando 84 dispõe que: "(84) A fim de promover o cumprimento do presente regulamento **nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação**, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. **Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas** a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. **Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais**". [Grifo nosso]. Ibid.

[365] ÁLVAREZ, Luis Felipe López. La responsabilidad del responsable. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 275-294.

Ademais, o Considerando 74 dispõe que o responsável responde por qualquer tratamento feito por si ou por sua conta. A responsabilidade do responsável ou do subcontratante (quando não se isenta da mesma) é solidária (art. 82.4), cabendo eventual ação de regresso no que concerne à respectiva parcela do prejuízo causado pelo outro responsável ou subcontratante (art. 82.5.)[366]. Dos Considerandos 74 e 146 depreende-se, ainda, que o ônus da prova não recai sobre o indivíduo lesado, mas sobre o responsável do tratamento, que terá que demonstrar que o fato causador do dano não lhe é imputável.

A própria construção da responsabilidade do responsável pelo tratamento visa que se adotem medidas preventivas e não reparativas. Ou seja, o que se busca é evitar a ocorrência de eventos danosos, trabalhando-se sempre sob uma ótica de minimização dos riscos (ainda que não seja possível eliminá-los completamente), estabelecendo medidas a serem adotadas e recomendando a adoção de códigos de conduta[367].

Outro ponto de grande relevância, não só por seu caráter inovador em termos de regulação, mas principalmente pelo impacto que gera sobre as mídias e redes sociais, consiste nos princípios de proteção de dados de privacidade desde a concepção (*privacy by design*) e privacidade por defeito (*privacy by default*)[368].

---

[366] "Artigo 82º Direito de indemnização e responsabilidade
[...]
4.Quando mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, estejam envolvidos no mesmo tratamento e sejam, nos termos dos nºs 2 e 3, responsáveis por eventuais danos causados pelo tratamento, cada responsável pelo tratamento ou subcontratante é responsável pela totalidade dos danos, a fim de assegurar a efetiva indemnização do titular dos dados.
5.Quando tenha pago, em conformidade com o nº4, uma indemnização integral pelos danos sofridos, um responsável pelo tratamento ou um subcontratante tem o direito de reclamar a outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento a parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano em conformidade com as condições previstas no nº 2." UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[367] ÁLVAREZ, Luis Felipe López. La responsabilidad del responsable. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 275-294.

[368] No que toca aos princípios de *privacy by design* e *privacy by default,* utilizar-se-á os termos em inglês porque a tradução proposta na versão em português do regulamento pode dar margem a interpretações errôneas destes princípios.

Em que pese novidade em termos de legislação da UE, o princípio de *privacy by design* é desenvolvido desde a década de 90, especialmente pela doutrina norte-americana[369]. Parte da percepção que "[...] o futuro da privacidade não pode ser assegurado por *compliance* e quadros regulatórios; antes, a garantia da privacidade deve se tornar, idealmente, um modo padrão de operação de uma organização"[370].

Ou seja, percebe-se no desenvolvimento desse princípio (assim como do *privacy by default*) que a tecnologia deve desempenhar papel central na defesa da privacidade e da proteção de dados pessoais[371]. Não apenas na abordagem convencional das PETs (*Privacy Enhancing Technologies*), mas a partir de uma postura mais positiva e funcional em relação aos problemas, uma PET *plus*, em que se tem um sistema totalmente funcional que afasta as pretensas dicotomias e os eventuais *trade offs* como privacidade e segurança[372].

Trabalhando sempre sob uma ótica proativa (preventiva e não reativa)[373], o *privacy by design* demanda que as questões relativas à privacidade devem ser enfrentadas no próprio momento em que se desenha o sistema que envolva o tratamento de dados, não como algo incorporado posteriormente ao *design* do

---

[369] Em 2012, a própria *Federal Trade Comission* (FTC) reconheceu o princípio do *privacy by design* como um dos três pilares de seu quadro de *privacy*, visando melhores práticas das empresas que desempenham atividades de tratamento de dados pessoais. FTC. **Protecting consumer privacy in an era of rapid change**: recommendations for businesses and policymakers. Mar. 2012. Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>. Acesso em: 06 out. 2017.

[370] "*Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.*" [Tradução livre]. CAVOUKIAN, Ann. **Privacy by design**: the 7 foundation principles. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>. Acesso em: 06 out. 2017.

[371] CALÉS, Rosario Duaso. Los princípios de protección de datos desde el diseño y protección de datos por defecto. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 295-320.

[372] "*Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS Plus — taking a positive-sum (full functionality) approach, not zero-sum. That's the 'Plus' in PETS Plus: positive-sum, not the either/or of zero-sum (a false dichotomy)* […]
Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both." [Tradução livre]. CAVOUKIAN, op cit.

[373] Até por trabalhar sob uma ótica de uma gestão responsável da informação, a partir de uma *accountability*. Nesse sentido, ver: CALÉS, op. cit.

produto, mas como verdadeiro componente do *design* mesmo[374]. Com isso, facilita-se o processo de garantia da proteção da informação pessoal em todo o seu "ciclo de vida" dentro do sistema – ou seja, desde a coleta até o apagamento do dado[375].

Como bem aponta Calés[376], integrar a privacidade na própria arquitetura de todo sistema ou aplicativo, assim como no próprio desenho daqueles processos que pressupõem o tratamento de dados, constitui uma resposta capaz de contribuir fortemente para o cumprimento dos princípios de proteção de dados estabelecidos por lei. Mais do que isso, o próprio sistema já pode cumprir de forma automatizada algumas dessas determinações – por exemplo, apagar os dados depois que transcorrido o prazo máximo de armazenamento ou depois de atingida a finalidade para a qual o dado foi coletado, ou garantir que apenas as pessoas autorizadas tenham acesso aos dados pessoais, permitindo sua visualização somente após a identificação do usuário mediante *login* e senha.

Consoante se depreende do Considerando 78, as medidas a serem adotadas em observância aos princípios da *privacy by design* e *privacy by default* podem incluir a minimização do tratamento de dados pessoais, a pseudoanonimização e possiblidade de controle do tratamento pelo próprio titular. Ademais, o Considerando 108 dispõe que esses princípios deverão ser levados em conta quando da transferência de dados para um país terceiro juntamente com os demais princípios gerais da proteção de dados pessoais (*vide* art. 47.2.*d*). Por fim, o art. 25 do Regulamento determina a aplicação dos princípios do *privacy by design* (art. 25.1.) e *privacy by default* (art. 25.2.)[377].

---

[374] CAVOUKIAN, Ann. **Privacy by design**: the 7 foundation principles. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>. Acesso em: 06 out. 2017.

[375] Nesse sentido, a resolução sobre *privacy by design* de 2010, realizada pela 32ª Conferência Internacional sobre Proteção de Dados e Comissão de Privacidade em Israel dispõe que: "*Recognizing that embedding privacy as the default into the design, operation and management of ICT and systems, across the entire information life cycle, is necessary to fully protect privacy*; […]." 32ND INTERNATIONAL Conference of Data Protection and Privacy Commissioners. **Resolution on privacy by design**. Jerusalem, Israel, 27-29 oct. 2010. p. 1.

[376] ÁLVAREZ, Luis Felipe López. La responsabilidad del responsable. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 275-294.

[377] UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

A esse respeito Calés[378] aponta a grande aproximação entre a operacionalização do princípio do *privacy by design* e a do o princípio da precaução, sustentando que aquele pode ser interpretado como uma aplicação deste. Inclusive, vale-se da construção de Poullet[379] ao defender a aplicação do princípio da precaução no âmbito tecnológico. Segundo Poullet, em ambos é preciso avaliar o risco ou potencial lesivo da atividade a ser desempenhada ou tecnologia a ser implantada (*in casu* o tratamento de dados pessoais) e adotar medidas de precaução a fim de evitar os resultados não desejados.

A bem da verdade, desdobra-se do princípio do *privacy by design* o próprio princípio do *privacy by default*[380]. Esse consiste, basicamente, na ideia de que a configuração padrão dos sistemas, produtos e conteúdos seja a mais protetiva possível ao usuário. Isto é,

> [...] ainda que os titulares dos dados pessoais não empreendam nenhum tipo de ação para proteger seus dados, o sistema, por sua própria arquitetura baseada na privacidade, seja, em todo caso, a configuração predeterminada.[381]

Tomando as redes sociais como exemplo, o princípio da *privacy by default* faz com que o menor número possível dos dados pessoais do usuário seja acessível ao

---

[378] "*El concepto de Privacy by Design, por tener su aplicación en el momento de la creación de la propria tecnología, teniendo por objetivo que la privacidad esté integrada en el sistema o solución tecnológica para deducir al máximo la posibilidad de que los riesgos que en matéria de protección de datos pudean materializarse, podría verse como una manifestación de la aplicación del principio de precaución*." CALÉS, Rosario Duaso. Los princípios de protección de datos desde el diseño y protección de datos por defecto. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 295-320.

[379] POULLET, Yves. Internet et Sciences Sociales ou <<Comment comprendre l'invisible>>?>>. **Revue des Questions Scientifiques.** 2011. 184 (4). Pp. 377-398, apud CALÉS, op. cit.

[380] Nesse sentido, Cavoukain elenca sete princípios básicos da *privacy by design,* sendo o segundo deles: "2. *Privacy as the Default Setting. We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default*". CAVOUKIAN, Ann. **Privacy by design**: the 7 foundation principles. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>. Acesso em: 06 out. 2017.

[381] "*El concepto de Privacy by Default integrado en el sistema, garantiza que aunque los titulares de los datos personales no emprendan ningún tipo de acción para proteger sus datos, el sistema por su própria arquitectura basada en la privacidade, va a garantizar la confidencialidade de toda información de caráter personal*." CALÉS, op. cit., p. 304.

público em geral. Para que possa tornar seu perfil público, ele teria que mexer nas configurações do mesmo, invertendo a lógica costumeira das redes sociais em que, para aumentar a privacidade do perfil do usuário, é preciso alterar os padrões de privacidade nas configurações da página ou do aplicativo.

Inclusive, o próprio Regulamento traz alguns mecanismos de operacionalização desses dois princípios (*privacy by default* e *privacy by design).* A possiblidade de uso de mecanismos de certificação e até mesmo o uso de selos e marcas que demonstrem o cumprimento do Regulamento e o respeito à proteção de dados pessoais (*vide* art. 25.3 c/c arts. 42 e 43)[382]. A pseudononimização dos dados pessoais o mais cedo possível, a minimização do tratamento de dados de caráter pessoal, a possiblidade de o próprio titular controlar o tratamento de suas informações, transparência no tratamento e nas suas finalidades, e adoção de medidas de segurança também são outros mecanismos elencados pelo Regulamento no intuito do cumprimento desses princípios, inclusive no âmbito dos contratos públicos (*vide* Considerando 78)[383].

Cabe, ainda, fazer menção às pertinentes observações tecidas pela Comissão Belga de Proteção da Vida Privada, que, em 2012, já apontava para a importância da inserção dos princípios da *privacy by design* e *privacy by default* no

[382] "Artigo 25º Proteção de dados desde a concepção e por defeito
3. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas nos nº 1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42º." UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[383] "(78) A defesa dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige a adoção de medidas técnicas e organizativas adequadas, a fim de assegurar o cumprimento dos requisitos do presente regulamento. Para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a concepção e da proteção de dados por defeito. Tais medidas podem incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança. No contexto do desenvolvimento, concepção, seleção e utilização de aplicações, serviços e produtos que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções, haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e concepção e, no devido respeito pelas técnicas mais avançadas, a garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados. Os princípios de proteção de dados desde a concepção e, por defeito, deverão também ser tomados em consideração no contexto dos contratos públicos." Ibid.

texto do Regulamento, porém, sempre sublinhando que a obrigação de observância desses princípios não deveria recair apenas sobre o responsável pelo tratamento, mas principalmente sobre os desenvolvedores de *softwares* e programas que envolvam o tratamento de dados pessoais. Consoante bem observado pela comissão, a observância desses princípios é ainda mais importante na fase de desenvolvimento, do desenho e da concepção desses produtos do que na fase de aplicação e operacionalização dos mesmos, devendo-se tais princípios serem aplicados aos próprios desenvolvedores de tecnologias[384].

Tal apontamento foi devidamente reconhecido no Considerando 78, ao dispor que:

> **No contexto do desenvolvimento, concepção, seleção e utilização de aplicações, serviços e produtos** que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções, **haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e concepção** e, no devido respeito pelas técnicas mais avançadas, a garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados.[385] [Grifo nosso].

Ou seja, é perceptível na construção de todo o Regulamento, em especial na formulação desses dois princípios, uma abordagem baseada no controle de riscos – *risk-based approach*. Em que pese não se tratar de mecanismo inovador, vez já existir uma preocupação com a figura do risco na própria Diretiva 95/46/CE (*vide* arts. 8º, 17 e 20)[386], certamente o modo pelo qual se faz essa abordagem e a própria importância que é dada à figura do risco são muito distintas no regulamento[387].

---

[384] COMMISSION DE LA PROTECTION DE LA VIE PRIVEÉ. **Avis n°12/35 du 15 mai 2012 concernant la demande de l'asbl l'équipe relative à la candidature de madame isabelle de schutter aux fonctions de conseiller en sécurité.** (COA-A-2012-015). Belgique, Bruxelles, apud CALÉS, Rosario Duaso. Los princípios de protección de datos desde el diseño y protección de datos por defecto. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 295-320.

[385] UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[386] Segundo o Grupo de Trabalho do Artigo 29: "*The so-called 'risk-based approach' is not a new concept, since it is already well known under the current Directive 95/46/EC especially in the security (Article 17) and the DPA prior checking obligations (Article 20). The legal regime*

Nessa ceara, a introdução de uma imposição de uma avaliação prévia do impacto de eventual tratamento de dados pessoais por parte do responsável pelo tratamento é um dos principais mecanismos dessa nova abordagem baseada no risco e na gestão responsável da informação[388]. Em que pese não trazer um conceito de risco, depreende-se do Regulamento que ele é verificado a partir de dois parâmetros: a probabilidade de ocorrência de um dano[389] e, principalmente, a potencialidade lesiva de eventual dano[390].

Consoante se depreende do art. 35 do Regulamento, a avaliação de impacto das operações de tratamento de dados pessoais deve ser realizada previamente ao início do tratamento quando ele "[...] em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares". Ainda no mesmo artigo, determina-se a obrigatoriedade da realização da avaliação de impactos nos casos de:

> [...] a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem

---

applicable to the processing of special categories of data (Article 8) can also be considered as the application of a risk-based approach: strengthened obligations result from processing which is considered risky for the persons concerned." UNIÃO Europeia. **Article 29**. Data Protection Working Party. Statement on the role of a risk-based approach in data protection legal frameworks. Brussels, Belgium, 30 maio 2014. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>. Acesso em: 10 out. 2017.

387 A esse respeito sustenta o grupo de trabalho do artigo 29 que: "*However, the risk-based approach has gained much more attention in the discussions at the European Parliament and at the Council on the proposed General Data Protection Regulation. It has been introduced recently as a core element of the accountability principle itself (Article 22). In addition to the obligation of security (Article 30) and the obligation to carry out an impact assessment (Article 33) already prescribed in the draft regulation, the risk-based approach has been extended and reflected in other implementation measures such as the data protection by design principle (Article 23), the obligation for documentation (Article 28) and the use of certification and codes of conduct (Articles 38 and 39). It is apparent therefore that the draft Regulation already contains the tools – for example in Article 33 relating to impact assessment – to provide for a reliable and relatively objective assessment of risk.*" Ibid.

388 GAYO, Miguel Recio. Aproximación baseada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 351-366.

389 A probabilidade do dano é utilizada como parâmetro, especialmente no que concerne às medidas a serem adotadas para a mitigação do mesmo.

390 Nesse sentido, Gayo aponta que a própria sensibilidade dos dados pessoais e as possíveis consequências danosas de um tratamento não adequado são parâmetros traçados pelo próprio regulamento para taxar o tratamento como sendo de alto risco. GAYO, op. cit.

> efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
>
> b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9º, nº 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º; ou
>
> c) Controle sistemático de zonas acessíveis ao público em grande escala.[391]

Ainda, as autoridades de controle nacionais, por exemplo, a Agência Nacional de Proteção de Dados da Espanha, podem elaborar uma lista – de caráter público – dos tipos de operações de tratamento em que se faz necessária a elaboração da avaliação prévia de impacto (art. 35.4) e uma lista de tipos de operações em que a análise prévia não é obrigatória (art. 35.5), estando ambas as listas sujeitas à vistoria do Comité.

Como exceção, o art. 35.10 dispõe que tratamentos efetuados para cumprimento de obrigação jurídica (art. 6º.1.*c*) ou tratamentos necessários para efeito dos interesses legítimos do responsável pelo tratamento ou de terceiros, tendo fundamento jurídico o direito da União ou Estado Membro a que está sujeito o responsável pelo tratamento, "[...] e esse direito regular a operação ou as operações de tratamento específicas em questão, e se já tiver sido realizada uma avaliação de impacto sobre a proteção de dados no âmbito de uma avaliação de impacto geral no contexto da adoção desse fundamento jurídico" não se faz necessária a realização da análise de impacto – prevista no art. 35.1 a 7 –, salvo em caso de disposição expressa do Estado Membro[392].

Ainda que de caráter exemplificativo ou não taxativo, o Regulamento traz alguns parâmetros para a realização da avaliação de impacto do tratamento. Nos termos do art. 35.7:

---

[391] UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[392] "Artigo 35º **Avaliação de impacto sobre a proteção de dados** 10.Se o tratamento efetuado por força do artigo 6º, nº 1, alínea c) ou e), tiver por fundamento jurídico o direito da União ou do Estado-Membro a que o responsável pelo tratamento está sujeito, e esse direito regular a operação ou as operações de tratamento específicas em questão, e se já tiver sido realizada uma avaliação de impacto sobre a proteção de dados no âmbito de uma avaliação de impacto geral no contexto da adoção desse fundamento jurídico, não são aplicáveis os nºs 1 a 7, salvo se os Estados-Membros considerarem necessário proceder a essa avaliação antes das atividades de tratamento." Ibid.

> 7. A avaliação inclui, **pelo menos**:
>
> a) Uma **descrição sistemática das operações de tratamento previstas e a finalidade do tratamento**, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;
>
> b) Uma **avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos**;
>
> c) Uma **avaliação dos riscos para os direitos e liberdades dos titulares** dos direitos a que se refere o nº 1; e
>
> d) As **medidas previstas para fazer face aos riscos**, incluindo as garantias, medidas de segurança e **procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento**, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.[393] [Grifo nosso].

Ademais, Gayo[394] aponta que essa análise de impacto também deve levar em consideração o cumprimento de códigos de conduta, tanto pelos responsáveis pelo tratamento como pelos encarregados do mesmo *(vide* art. 35.8), e a opinião dos titulares dos dados ou representantes desses, sem prejuízo da defesa de interesse de natureza comercial, pública ou de segurança do tratamento *(vide* art. 35.9), enfatizando que o dano a ser considerado não se resume ao direito fundamental à proteção de dados pessoais, mas a qualquer direito e liberdade fundamental do titular.

Realizada a análise de impacto e identificado, pelo responsável pelo tratamento, um risco elevado caso não se adote medidas necessárias para sua mitigação, incumbe ao responsável pelo tratamento a realização de uma consulta prévia junto à autoridade de controle (art. 36). Trata-se de inovação do Regulamento e que, em que pese não vincular diretamente o encarregado pelo tratamento, acaba

---

[393] UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[394] GAYO, Miguel Recio. Aproximación baseada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 351-366.

fazendo por forma indireta, a partir do dever de colaboração que o encarregado tem para com o responsável[395].

Essa consulta deve conter informações como quem são os responsáveis pelo tratamento e qual a repartição de responsabilidade entre eles (contratantes e subcontratantes), finalidade do tratamento e o meio pelo qual será realizado, medidas e garantias de segurança e de respeito aos direitos dos titulares dos dados, e a própria avaliação do impacto do tratamento realizada (*vide* art. 36.3)[396].

Em não entendendo suficiente as medidas apontadas pelo responsável para fins de mitigação do risco, a autoridade de controle pode, dentro de oito semanas (prorrogáveis por mais seis semanas se devidamente justificado pela autoridade de controle, e/ou suspendidos se solicitada alguma informação complementar) a contar do recebimento do pedido de consulta, efetuar, por escrito, orientações ao responsável e, quando houver, ao subcontratante, podendo se valer de todos os seus poderes dispostos no art. 58 (*vide* art. 36.2)[397].

Ainda, o art. 36.5. dispõe que "[...] o direito dos Estados-Membros pode exigir que os responsáveis pelo tratamento consultem a autoridade de controlo e dela obtenham uma autorização prévia em relação ao tratamento por um responsável no exercício de uma missão de interesse público"[398], até mesmo nos casos de tratamento para fins de proteção social ou saúde pública.

Por sua vez, a questão da transferência internacional de dados, em que pese não ser novidade trazida pelo Regulamento, é tratada de forma muito mais detalhada do que o fora feito na Diretiva. Essa dedicava apenas dois artigos à temática (arts. 25 e 26), enquanto aquele dedica sete artigos (arts. 44 a 50). Tal dado, *per si,* demonstra a importância atribuída ao fluxo internacional de

---

[395] GAYO, Miguel Recio. Aproximación baseada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 351-366.

[396] UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[397] Os poderes da autoridade de controle serão enfrentados em momento posterior neste trabalho.

[398] UNIÃO Europeia, op. cit.

informações pessoais e o reconhecimento da necessidade de uma regulação mais clara e detalhada dessa questão[399].

Assim como na Diretiva, em nenhum momento busca-se obstaculizar a circulação dos dados pessoais em nível internacional[400]. Consoante se depreende dos Considerandos 6 e 101 e do art. 44 do Regulamento, o objetivo é incrementar a circulação dos dados, inclusive por meio de novas tecnologias, porém, sempre se assegurando um elevado nível de proteção dos dados pessoais, até como forma de legitimar tal fluxo de dados e fortalecer o comércio e a cooperação internacional.

Ou seja, é possível a transmissão de dados sempre que houver juízo de adequação sobre o país terceiro, podendo ser feito, também, apenas sobre setor específico ou território dentro do país (art. 45.3); ou, na ausência dessa decisão, quando sejam oferecidas garantias suficientes a assegurar o alto nível de proteção perseguido pelo Regulamento (art. 46.1). Outrossim, o art. 49 traz algumas exceções para casos específicos[401], sendo que tais disposições são aplicáveis não só ao responsável pelo tratamento como ao encarregado do mesmo (art. 44).

---

[399] PIÑAR MAÑAS, Jose Luis. Transferencias de datos personales a terceros países u organizaciones internacionales. In: _____ (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 427-460.

[400] Como bem aponta Piñar Mañas, "[...] *el fujo transfronterizo de datos es no sólo imprescindible en la actualidad, sino que aumenta día a día. Intentar bloquear o restringir sin razón tales flujos en aras de la protección de datos puede estar aocado al más sonoro de los fracasos. Pero tales movimentos internacionales no pueden poner en riesgo la privacidade tan larga y costosamente conseguida en la Unión Europea, por lo que, como ya ocurría en la Directiva 95/46/CE, lo que se exige es que las transferências se lleven a cabo sólo si se assegura la protección de datos* [...]. *En consecuencia, el RGPD expressa por un lado el convencimento de que las transferências internacionales son no sólo una realidade, sino que son imprescindibles* [...]". Ibid., p. 430.

[401] "Artigo 49º Derrogações para situações específicas
1.Na falta de uma decisão de adequação nos termos do artigo 45.o, nº 3, ou de garantias adequadas nos termos do artigo 46.o, designadamente de regras vinculativas aplicáveis às empresas, as transferências ou conjunto de transferências de dados pessoais para países terceiros ou organizações internacionais só são efetuadas caso se verifique uma das seguintes condições:
a) O titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas;
b) A transferência for necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;
c) A transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados, entre o responsável pelo seu tratamento e outra pessoa singular ou coletiva;
d) A transferência for necessária por importantes razões de interesse público;

Vale lembrar que, ao se falar em transferência internacional, está se trabalhando com o que o Regulamento denominou de transferência de dados pessoais a um país terceiro (*Transfers of personal data to third countries*), isto é, quando as informações são enviadas a país não membro da União Europeia, ou a uma organização internacional. Em se tratando de transferência para outro país membro, o regulamento optou pelo termo "tratamento transfronteiriço" (*vide* art. 4.23 do Regulamento)[402].

---

e) A transferência for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial;
f) A transferência for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento;
g) A transferência for realizada a partir de um registo que, nos termos do direito da União ou do Estado-Membro, se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo, mas apenas na medida em que as condições de consulta estabelecidas no direito da União ou de um Estado-Membro se encontrem preenchidas nesse caso concreto.
Quando uma transferência não puder basear-se no disposto no artigo 45º ou 46º, incluindo nas regras vinculativas aplicáveis às empresas, e não for aplicável nenhuma das derrogações previstas para as situações específicas a que se refere o primeiro parágrafo do presente número, a transferência para um país terceiro ou uma organização internacional só pode ser efetuada se não for repetitiva, apenas disser respeito a um número limitado de titulares dos dados, for necessária para efeitos dos interesses legítimos visados pelo responsável pelo seu tratamento, desde que a tais interesses não se sobreponham os interesses ou os direitos e liberdades do titular dos dados, e o responsável pelo tratamento tiver ponderado todas as circunstâncias relativas à transferência de dados e, com base nessa avaliação, tiver apresentado garantias adequadas no que respeita à proteção de dados pessoais. O responsável pelo tratamento informa da transferência a autoridade de controlo. Para além de fornecer a informação referida nos artigos 13º e 14º, o responsável pelo tratamento presta informações ao titular dos dados sobre a transferência e os interesses legítimos visados.
2.As transferências efetuadas nos termos do nº 1, primeiro parágrafo, alínea g), não envolvem a totalidade dos dados pessoais nem categorias completas de dados pessoais constantes do registo. Quando o registo se destinar a ser consultado por pessoas com um interesse legítimo, as transferências só podem ser efetuadas a pedido dessas pessoas ou se forem elas os seus destinatários.
3.O nº 1, primeiro parágrafo, alíneas a), b) e c), e segundo parágrafo, não é aplicável a atividades levadas a cabo por autoridades públicas no exercício dos seus poderes.
4.O interesse público referido no nº 1, primeiro parágrafo, alínea d), é reconhecido pelo direito da União ou pelo direito do Estado-Membro a que o responsável pelo tratamento se encontre sujeito.
5Na falta de uma decisão de adequação, o direito da União ou de um Estado-Membro podem, por razões importantes de interesse público, estabelecer expressamente limites à transferência de categorias específicas de dados para países terceiros ou organizações internacionais. Os Estados-Membros notificam a Comissão dessas disposições.
6.O responsável pelo tratamento ou o subcontratante documenta a avaliação, bem como as garantias adequadas referidas no nº 1, segundo parágrafo, do presente artigo, nos registos a que se refere o artigo 30º." UNIÃO Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

[402] Importante apontar que os países do EEE (Espaço Econômico Europeu), nos termos do regulamento, são considerados países terceiros, sendo que o mesmo ocorre com a Grã-Bretanha em razão do Brexit. PIÑAR MAÑAS, Jose Luis. Transferencias de datos personales a terceros países u organizaciones internacionales. In: _____ (Dir.). **Reglamento General de Protección**

Contudo, ele não traz nenhuma definição do que se entende por transferência de dados pessoais a um país terceiro, tampouco o fizera a Diretiva que lhe precedia. O que se tem mais de concreto nesse sentido é a Sentença do Tribunal de Justiça da EU, em 6 de novembro de 2003, do caso *Lindqvist*, que, segundo Piñar, pode levar à conclusão de que a transferência consistiria no efetivo

> [...] *envío de información a un país terceiro o a una organización internacional. En este sentido, facilitar, poner, bajar, volcar información en internet no implicaria una transferencia de datos pero la prestación de servicios de comutación en la nube o claud computing si, pues en este caso sí estamos ante tratamentos de tatos que exigen el envío de la información, en su caso a terceiros países*.[403]

Ainda, o autor complementa sustentando que eventual matização a ser realizada na interpretação da sentença (que deve ser feita nos termos e a partir do caso concreto enfrentado), especialmente no que toca à ampliação do conceito de transferência, deve ser muito bem ponderada em razão da complexidade do tema e das potenciais consequências dessa nova interpretação. Para Piñar, o art. 49.1.*g* do regulamento é um bom parâmetro para tal interpretação, vez que considera legítima a transferência de informações pessoais para países terceiros quando esta "[...] nos termos do direito da União ou do Estado-Membro, se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo". Ou seja, "[...] *no se mueve en la lógica de envío de la informacíon sino de la puesta a disposición de los datos para su consulta*"[404].

De suma importância, também, é a figura da autoridade independente de controle. Questão já abordada pela Diretiva 95/46/CE, a autoridade de controle se mostra imprescindível ao bom funcionamento de qualquer regulação não só enquanto órgão fiscalizador, mas até mesmo consultivo. A ela se soma ainda a figura do encarregado da proteção de dados pessoais (*delegado de protección de*

---

de Datos: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 427-460.

[403] PIÑAR MAÑAS, Jose Luis. Transferencias de datos personales a terceros países u organizaciones internacionales. In: _____ (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 427-460. p. 433.

[404] Ibid.

datos ou *data protection officer*), inovação trazida pelo NRPDP que seria uma espécie de "meio campo" entre a Administração Pública e a empresa, atuando especialmente na supervisão do cumprimento do Regulamento e em cooperação com a autoridade de controle, ainda que com autonomia funcional, tanto em relação à empresa, como à autoridade pública (arts. 38.3 e 39)[405].

Em relação à autoridade de controle, o Regulamento extinguiu a obrigação de notificação da criação ou modificação de ficheiros de tratamento de dados pessoais prevista na Diretiva 95/46 e na LOPDP Espanhola. Tal obrigação foi substituída pelo dever de registro das atividades de tratamento (art. 30)[406], ressalvando-se os casos que envolvem um alto risco no tratamento de dados pessoais, os quais demandam consulta prévia à autoridade de controle (art. 36).

Tal construção evidencia a função de fiscalização e controle desenhada para essas autoridades de controle (art. 51.1.). Essas devem atuar com total independência no exercício de suas atribuições e poderes (art. 52), havendo um dever de cooperação entre as diferentes autoridades de controle e a Comissão (art. 51.2.). Assim, parece que a experiência enfrentada pelas agências de proteção de dados pessoais (APDP), desde o início da década de 90, foram levadas em consideração para o *modus operandi* proposto no Regulamento. Consoante apontou Bennett[407] em seu estudo sobre as APDP, aquelas que atuavam em um controle fiscalizatório *a posteriori* eram mais eficientes que aquelas que faziam um controle prévio, exigindo autorizações para a realização de tratamentos de dados pessoais. Nesse sentido, valorizar uma atuação proativa do responsável pelo tratamento, incentivando, inclusive, a autorregulação, é uma opção que melhor se adapta ao volume de fluxo de informações existente, limitando-se a atuação prévia dessas autoridades aos casos que envolvem um alto risco no tratamento de dados.

Dentre os poderes da autoridade de controle está a possiblidade da aplicação de sanções econômicas significativas e de impor a limitação temporária ou definitiva do tratamento de dados como mecanismos capazes de dar eficácia à atuação das

---

[405] REIGADA, Antonio Troncoso. Autoridades de control independientes. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 461-512.

[406] Ibid.

[407] BENNETT, Colin J. **Regulating privacy**: data protection and public policy in Europe and the United States. New York: Cornell University Press, 2011.

autoridades (art. 58.2.*f* e *i*). Inclusive, o Regulamento busca reduzir a desigualdade de atuação das autoridades de controle, seja na atividade inspetora, como na gravidade das sanções que essas podiam impor. Dedicando 8 artigos ao tema, ele visa uma sistematização das autoridades de controle de forma muito mais detalhada que a Diretiva 95/46 (que dedicava apenas o art. 28 ao tema)[408].

A Comissão já havia assinalado sobre a carência de ações coercitivas por parte das autoridades de controle resultando em uma baixa aplicabilidade da Diretiva 95/46. Tomando a AEPDP como modelo, verificou-se que as demais não tinham o costume de realizar inspeções para fiscalizar o cumprimento da Diretiva, sendo ainda mais raras as inspeções detalhadas e aprofundadas. Ademais, somente Espanha e Portugal tinham o costume de impor sanções econômicas, as quais eram consideradas como "último recurso" pelas demais autoridades europeias[409].

No que toca ao tratamento de dados pessoais pelo Judiciário, vale lembrar que esse se submete ao Regulamento, mesmo que no exercício de suas funções. Nada obstante, o Poder Judiciário não está sujeito ao controle de uma autoridade de controle; essa fiscalização fica a cargo do encarregado da proteção de dados pessoais (vez que há uma obrigatoriedade de sua designação pelas autoridades públicas – art. 37.1.a) e do próprio judiciário, que deve criar organismos específicos para esse controle – art. 55.3 e Considerando 20. Assim, respeita-se a autonomia do judiciário a quem cabe o controle sobre a autoridade de controle e não o contrário[410].

A autoridade de controle pode agir mediante uma reclamação, a qual pode ser feita por uma pessoa singular, uma associação, organização, de ofício, ou mediante notificação de outra autoridade de controle ou autoridade pública. Outrossim, é possível identificar um caráter consultivo da autoridade de controle quando da elaboração da lista de requisitos para a avaliação de impacto no tratamento de dados (art. 57.1.*k*); da prestação de informações a qualquer titular de dados sobre seus direitos (art. 57.1.*e*); do aconselhamento ao "[...] governo e outras instituições e organismos a respeito das medidas legislativas e administrativas relacionadas com a defesa dos direitos e liberdades das pessoas singulares no que

[408] REIGADA, Antonio Troncoso. Autoridades de control independientes. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 461-512.
[409] Ibid.
[410] Ibid.

diz respeito ao tratamento" (art. 57.1.*c*); ou da realização de "[...] orientações sobre as operações de tratamento previstas no artigo 36, nº 2 (art. 57.1.*l*)"[411].

Traçado o panorama desses dois modelos, cabe enfrentar a proteção de dados pessoais dentro do ordenamento jurídico brasileiro, o que será realizado a partir de um enfoque especial na figura do *profiling*, ainda que sem lançar mão das demais nuances da sistemática da proteção de dados pessoais.

[411] REIGADA, Antonio Troncoso. Autoridades de control independientes. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 461-512.

3 O *PROFILING* A PARTIR DE UMA SISTEMÁTICA BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS

O reconhecimento de um direito à proteção de dados pessoais, no ordenamento jurídico pátrio, é pacífico na doutrina nacional. Nada obstante, o fundamento desse direito não o é. Em que pese a concordância de que esse direito tem origem no direito à privacidade, o enquadramento dele como um aspecto da privacidade ou como um direito autônomo ainda é objeto de debates doutrinários.

Trabalhando-se sob o prisma da privacidade, sua abordagem jurídica demanda certo pragmatismo. Em que pese válidas, as diversas tentativas de conceituação do direito à privacidade não são suficientes para o esgotamento do tema, em especial porque a tutela da privacidade deve contemplar uma multiplicidade de interesses identificados nas mais diversas manifestações do indivíduo[412]. Ainda assim, é possível extrair o que Rodotà chama de eixo da privacidade, o qual "[...] não se estrutura mais em torno do eixo 'pessoa-informação-segredo', no paradigma da *zero-relationship,* mas sim em um eixo 'pessoa-informação-circulação-controle'"[413].

Seguindo tal construção, o direito à privacidade estaria ligado a um direito geral da personalidade como um todo, evidenciando a sua relação com as noções de autonomia e de livre arbítrio[414]. Ou seja, trabalha-se a proteção de dados a partir da *informational privacy,* aproximando a privacidade à *privacy* americana e a um direito geral da personalidade.

Ocorre que, como bem salientam Sarlet, Marinoni e Mitidiero[415], as especificidades da estrutura constitucional pátria, notadamente no que toca ao

---

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

[413] RODOTÀ, Stefano. **Tecnologie e diritti***,* cit., p. 102, apud DONEDA, op. cit., p. 23.

[414] WESTIN, Alan. **Privacy and freedom***,* cit. p. 34, apud DONEDA, op. cit.

[415] "Como já referido, diversamente de outras ordens constitucionais, a Constituição Federal não reconheceu apenas um genérico direito à privacidade (ou vida privada), mas optou por referir tanto a proteção da privacidade, quanto da intimidade, como bens autônomos, tal como no caso da honra e da imagem. Todavia, o fato de a esfera da vida íntima (intimidade) ser mais restrita que a da privacidade, cuidando-se de dimensões que não podem pura e simplesmente ser dissociadas, recomenda um tratamento conjunto de ambas as situações. Por outro lado, é preciso reconhecer que, dadas as peculiaridades da ordem constitucional brasileira, especialmente à vista do reconhecimento de outros direitos pessoais no plano constitucional e da cláusula geral

reconhecimento da dignidade da pessoa humana enquanto cláusula geral e de outros direitos pessoais, tornam a abrangência do *right to privacy* norte-americano incompatível com a ordem constitucional brasileira.

De fato, é preciso reconhecer que, da funcionalização da proteção à privacidade, surge a necessidade de se regular a proteção de dados pessoais. Essa seria um tipo de continuação da privacidade, porém tutelando interesses, cuja relevância aumentou significativamente na sociedade pós-industrial. Tal cenário implica a adoção de características próprias da proteção de dados pessoais no que toca à tutela dos interesses que protege, bem como em referência à vinculação a valores e a direitos fundamentais distintos[416].

Outrossim, também é verdade que esse nexo de continuidade não obsta que o direito à proteção de dados pessoais tutele valores próprios e seja dotado de características próprias, as quais são desvinculadas da própria noção de privacidade. Enquanto a tutela constitucional da privacidade, a partir do emprego dos vocábulos vida privada e intimidade, ecoa na teoria alemã das esferas (ou círculos concêntricos), ela acaba não se desvinculando da dicotomia entre as noções de esfera pública e esfera privada. Nesse sentido, "[...] aplica-las à atual problemática dos dados pessoais, por exemplo, somente poderia ser feito com um raciocínio extensivo – o que, por si só, mitigaria os pressupostos de sua existência"[417].

---

representada pela dignidade da pessoa humana, o direito à privacidade – a exemplo do que ocorre também em Portugal – não merece a abrangência que lhe foi dada no direito constitucional norte-americano, em que assumiu a função equivalente a um direito geral de personalidade." SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017. p. 446.

[416] A esse respeito Rodotà assevera que "[...] a distinção entre o direito ao respeito da vida privada e familiar e o direito à proteção dos dados pessoais não é bizantina. O direito ao respeito da vida privada e familiar reflete, primeira e principalmente, um componente individualista: este poder basicamente consiste em impedir a interferência na vida privada e familiar de uma pessoa. Em outras palavras, é um tipo de proteção estático, negativo. Contrariamente, a proteção de dados estabelece regras sobre mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas – i.e. um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos". RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 17.

[417] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 111.

Fazendo uma analogia à crítica de Andrade[418] a propósito do uso desmesurado da dignidade da pessoa humana, e o consequente risco de sua banalização, praticamente equiparar o direito à privacidade a um direito geral da personalidade, nos moldes do ordenamento jurídico brasileiro, implicaria o esvaziamento do (já conturbado) conceito de privacidade. Destarte, em que pese se reconheça a íntima relação entre o direito à privacidade e o direito à proteção de dados pessoais, os quais, de fato, se confundem em determinados aspectos, não é possível trabalhá-los sob o mesmo instituto, em razão dos diferentes valores que cada um tutela.

Posto isso, cabe reconhecer que não há previsão expressa a um direito à proteção de dados pessoais na Constituição brasileira de 1988. O mais próximo dessa consiste na inviolabilidade da comunicação de dados consagrada no art. 5º, inciso XII[419], e no reconhecimento do *habeas data* – art. 5º, inciso LXXII[420].

É, portanto, do caráter instrumental da proteção de dados[421], especificamente no que toca ao resguardo da personalidade, da igualdade, da autonomia e da

---

[418] Defendendo o reconhecimento de um direito geral da personalidade, Andrade sustenta que ele seria um "[...] instrumentário apto a tutelar de forma efetiva a personalidade humana em todas as suas potencialidades [...]" prescindindo da evocação, em todos os casos do princípio da dignidade humana. Ainda, complementa o autor que "[...] a invocação exclusiva do princípio da dignidade humana pode conduzir ao risco de sua banalização, pois ele passa a ser aplicado em uma ampla gama de situações em que, por exemplo, não estaria presente, *prima facie,* a implicação do mínimo existencial". ANDRADE, Fábio Siebeneichler de. O desenvolvimento da tutela dos direitos da personalidade nos dez anos de vigência do Código Civil de 2002. In: LOTUFO, Renan; NANNI, Giovanni Ettore; MARTINS, Fernando Rodrigues (Coord.). **Temas relevantes do direito civil contemporâneo**: reflexões sobre os 10 anos do Código Civil. São Paulo: Atlas, 2012. p. 51-85. p. 57-58.

[419] "[...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [...]."BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 05 mar. 2017.

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

[421] Doneda sustenta que, havendo uma tutela constitucional da privacidade, poder-se-ia estendê-la a proteção de dados pessoais ao se inserir este direito como subespécie do direito à privacidade. Não obstante, corre-se o risco de limitar a tutela dos dados pessoais ao se trabalhar com essa fundamentação deveras simplista. Ainda, nas palavras do autor: "Em suma, a proteção de dados pessoais é uma garantia de caráter instrumental, derivada da tutela da privacidade, porém não limitada a esta, e que faz referência a um leque de garantias fundamentais que se encontram no

privacidade, que se extrai o amparo constitucional desse direito, ao qual se soma os aspectos já mencionados no parágrafo anterior[422].

Outrossim, consoante se verificou da experiência estrangeira, há uma tendência ao reconhecimento de um direito fundamental à proteção de dados pessoais[423]. Inclusive, é no âmbito internacional que se identifica a manifestação brasileira mais contundente no sentido de se reconhecer um direito fundamental à proteção de dados pessoais. Trata-se da Declaração de Santa Cruz de La Sierra, de 15 de novembro de 2003, documento oriundo da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, da qual o Brasil é signatário e que dispõe no seu item 45:

> 45. Estamos também conscientes de que **a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras iberoamericanas para proteger a privacidade dos cidadãos**, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade.[424] [Grifo nosso].

Nesse sentido, cabe referir que a aplicabilidade imediata dos direitos fundamentais – prevista no §1º do art. 5º da nossa Constituição – alcança desde os direitos fundamentais previstos no Catálogo do art. 5º, até direitos fora do catálogo – por exemplo, aqueles previstos em tratados internacionais – como se pode extrair da concepção aberta de direitos fundamentais positivada no §2º do referido artigo[425].

---

ordenamento brasileiro". DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 326.

[422] "No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada." Id. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2. p. 91-108, jul./dez. 2011. p. 103.

[423] Ibid.

[424] CUMBRA Iberoamericana. XIII CIMEIRA IBERO-AMERICANA DE CHEFES DE ESTADO E DE GOVERNO. **Declaração de Santa Cruz de la Sierra**, 14 e 15 de novembro de 2003. Disponível em: <http://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf>. Acesso em: 21 out. 2017.

[425] "[...] a aplicabilidade imediata (por força do art. 5, §1º, de nossa Lei Fundamental) de todos os direitos fundamentais constantes do Catálogo (arts. 5º a 17), bem como dos localizados em outras partes do texto constitucional e nos tratados internacionais. Aliás, a extensão do regime material

No âmbito infraconstitucional, chama a atenção a ausência de uma regulação específica acerca da proteção de dados. Dignos de menção o Projeto de Lei do Senado nº 181/2014 e o Projeto de Lei nº 5.276/2016, cujo objeto é a regulação do direito à proteção de dados pessoais; todavia, desde 2012 (PL nº 4.060/2012), tem-se a tramitação de um projeto de lei com esse objeto, sem maiores pretensões de aprovação a curto prazo.

Desta feita, a sistemática brasileira, a exemplo da norte-americana, acaba marcada por seu caráter fragmentado[426]. A proteção de dados no Brasil é composta por inúmeras disposições esparsas, dentre as quais destacam-se: o Código de Defesa do Consumidor – Lei nº 8.070/90; a Lei do Cadastro Positivo – Lei nº 12.414/2011; a Lei nº 9.507/97, que regulamenta a ação constitucional do *habeas data*; a Lei Complementar nº 105/2001, que diz respeito ao sigilo bancário; a lei de acesso à informação – Lei nº 12.527/2011; e o marco civil da internet – Lei nº 12.965/2014.

A partir de tais legislações busca-se delinear o direito à proteção de dados no ordenamento jurídico pátrio, contrapondo os textos legais com casos paradigmáticos, bem como contextualizando algumas questões pontuais concernentes à questão do *profiling*. Vale lembrar que, para além das legislações nacionais existentes, não se pode ignorar a convergência em âmbito internacional a propósito dos princípios basilares da proteção de dados pessoais. Como bem aponta Mendes:

> A convergência internacional estabelecida acerca dos princípios é marcante: mesmo os ordenamentos jurídicos mais diversos preveem praticamente os mesmos princípios de proteção de dados, com mínimas diferenças. Esse quadro comum de princípios é conhecido por "*Fair Information Principles*" e

da aplicabilidade imediata aos direitos fora do catálogo não encontra qualquer óbice no texto constitucional, harmonizando, para além disso, com a concepção materialmente abera dos direitos fundamentais consagrada, entre nós, no art. 5, §2º, da CF [...] (além dos direitos sociais, econômicos e culturais, por expressamente excluídos do regime) todos os direitos, liberdades e garantias de natureza análoga, ainda que localizados fora do texto da Constituição, constituem normas diretamente aplicáveis." SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado, 2015. p. 263.

[426] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2. p. 91-108, jul./dez. 2011.

> teve sua origem na década de 70 de forma quase simultânea nos Estados Unidos, Inglaterra e Alemanha.[427]

Dessa feita, com grande acerto Ruaro e Molinaro[428] sustentam que esses princípios específicos da proteção de dados se consubstanciam em verdadeiros vetores para a garantia desse direito, principalmente no Brasil, onde há uma carência legislativa na matéria. Seguindo tal raciocínio, os autores identificam cinco princípios basilares da disciplina da proteção de dados pessoais, quais sejam: princípio da publicidade, princípio da exatidão, princípio da finalidade, princípio do livre acesso e princípio da segurança física e lógica.

Posto isso, enfatiza-se que não se tem a pretensão de esgotar a temática da proteção de dados no Brasil. O que se pretende, *in casu*, é traçar algumas linhas a propósito do estado atual da arte, trazendo provocações críticas à ineficiente tutela existente no ordenamento jurídico pátrio, enfocando, especialmente, a figura do *profiling*.

3.1 *PROFILING:* APROXIMAÇÕES INICIAIS

Antes de enfrentar a questão de fundo deste capítulo, julga-se pertinente realizar uma breve conceituação do que se entende por *profiling* e do porquê da sensível preocupação em relação a essa temática. Dessa forma, é possível traçar uma delimitação do enfoque do presente estudo, facilitando a compreensão e a adequação desta pesquisa.

O *profiling* consiste na elaboração de perfis de comportamento de um indivíduo ou de um grupo de indivíduos a partir de suas informações pessoais, as quais podem ser disponibilizadas por ele mesmo, ou coletadas pelo responsável

---

[427] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online. p. 68.

[428] RUARO, Regina Linden; MOLINARO, Carlos Alberto. Conflito real ou aparente de interesses entre o direito fundamental à proteção de dados pessoais e o livre mercado. In: RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (Org.). **Privacidade e proteção de dados pessoais na sociedade digital**. [recurso eletrônico]. Porto Alegre: Fi, 2017. p. 13-46.

pelo tratamento dos dados. O perfil do indivíduo (ou do grupo) é traçado com base no cruzamento das informações coletadas e na comparação dessas com dados estatísticos. Logo, não é raro que o tratamento conte com o suporte de algoritmos e de mecanismos e de técnicas de inteligência artificial, a fim de se obter uma "metainformação". Essa "metainformação", por sua vez, consiste em uma "síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa"[429], podendo ser utilizada para as mais diversas finalidades[430].

Sob uma perspectiva comercial, Elmer define o *profiling* como um "[...] processo econômico e instrumental que enfoca na coleta, armazenamento, cruzamento, diagnóstico e alocação de informações demográficas e psicográficas", em que se distribui e se cataloga informações a respeito de "[...] desejos, hábitos e localização de indivíduos ou grupos, a fim de se diferenciar, racionalizar e prever o comportamento dos consumidores"[431].

Em sentido semelhante, Mendes assevera que

> [...] a construção de perfis compreende a reunião de inúmeros dados sobre uma pessoa, com a finalidade de se obter uma imagem detalhada e confiável, visando, geralmente, à previsibilidade de padrões de comportamento, de gostos, hábitos de consumo e preferências do consumidor.[432]

---

[429] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 173.

[430] Doneda aponta que o *profiling* pode ser usada tanto no âmbito público (no controle alfandegário, por exemplo), como no âmbito privado (para fins de publicidade comportamental). BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Elaboração Danilo Doneda. Brasília: SDE/DPDC, 2010. Disponível em: <http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf>. Acesso em: 23 jul. 2017.

[431] "*In the second definition, however, profiling is discussed as an instrumental and economic process that focuses on the collection, storage, networking, diagnosis, and deployment of demographic and psychographic information. This kind of profiling is broadly defined as an ongoing distribution and cataloguing of information about desires, habits, and location of individuals and groups. This instrumental approach is, in other words, much more concerned with segmenting, rationalizing, and predicting consumer behavior* […]." ELMER, G. **Profiling machines**: mapping the personal information economy. Cambridge, Mass: The MIT Press, 2004. p. 9.

[432] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online. p. 111.

Tal operação permite que o responsável pelo tratamento de informações pessoais trace um padrão ou uma tendência de comportamento do titular dos dados nos mais variados campos da vida em sociedade[433]. Reitera-se que tal tendência pode ser traçada tanto para um indivíduo em específico, como para uma determinada coletividade[434].

Na sociedade da informação, esse perfil criado transmuta-se em uma réplica virtual do indivíduo, pois será a única representação desse diante de uma gama de sujeitos. Ou seja, ele acaba, por vezes, substituindo o próprio indivíduo no ambiente virtual, repercutindo diretamente no dia a dia da pessoa[435].

Tal situação é constatada por diversos autores, sendo inúmeras as denominações dadas a esse fenômeno: *corpo eletrônico, digital persona*, *avatar, data shadow, pessoa virtual*, *réplicas virtuais,* dentre outros[436]. Em todos, identifica-se a mesma preocupação: a substituição da pessoa por uma representação virtual nem sempre precisa ter o condão de determinar como esse indivíduo vai interagir com a própria sociedade em que se insere[437].

O *profiling* surge como técnica que facilita o processo de massificação das relações, em especial a consumerista, sem que se abra mão da personalização. A estagnação dos mercados de massas demandava uma nova lógica econômica das empresas, uma economia de produção flexível, baseada na "individualização e flexibilização em massa", a fim de permitir a oferta de produtos em volumes mais

---

[433] A técnica pode ser utilizada desde para um controle aduaneiro no que toca ao fluxo de indivíduos de determinado país para outro, até para seleção de candidatos em uma vaga de emprego, ou de clientes que buscam acesso a crédito.

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

[435] Nesse sentido, Doneda aponta que "[...] um perfil assim obtido pode se transformar numa verdadeira representação virtual da pessoa, pois pode ser o seu único aspecto visível a uma séria de outros sujeitos. Este perfil estaria, diversas vezes, fadado a confundir-se com a própria pessoa". Ibid., p. 174.

[436] BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013; DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006; ELMER, G. **Profiling machines**: mapping the personal information economy. Cambridge, Mass: The MIT Press, 2004; GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010; LEMOS, André; LÉVY, Pierre. **O futuro da internet**: em direção a uma ciberdemocracia planetária. São Paulo: Paulus, 2010.

[437] DONEDA, op. cit.

reduzidos, porém destinados a um público-alvo específico[438]. Com isso, dinamiza-se o mercado de consumo e se contribui para uma gestão administrativa mais eficiente.

Nada obstante, também se abre margem para novas técnicas de vigilância[439]. Tal problemática é tão alarmante que Rodotà[440], ao invés de falar em uma sociedade da informação, optou por trabalhar uma sociedade da vigilância, marcada por uma sistemática de classificação, de segmentação (ou discriminação) e de classificação.

No âmbito do mercado, é possível identificar que essa economia de informação pessoal remonta à década de 70[441]. Nesse sentido, Rodotà[442] chama atenção para os meios de coleta dessas informações pessoais. Segundo o autor, a própria utilização de bens e serviços serve como objeto de coleta de dados dos usuários. Os terminais e as máquinas se prestam ao monitoramento dos trabalhadores, e, cada vez mais, o controle e a sistemática de vigilância diluem-se no cotidiano das pessoas, valendo-se de mecanismos que, *a priori*, não são criados para esse fim, mas que, em razão dos incrementos tecnológicos, também acabam atendendo a tal finalidade.

"Concretamente, isso significa que a contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações". [443] Ou seja, não há apenas uma apropriação de uma parcela do patrimônio do indivíduo, mas uma apropriação de parte de sua própria *persona.*

Uma vez coletada, essa informação ganha "vida própria", auferindo novas aplicações e novas utilidades, consoante os interesses daqueles que a manipulam.

---

[438] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online.

[439] BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

[440] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

[441] MENDES, op. cit.

[442] RODOTÀ, op. cit.

[443] Ibid., p. 113.

Assim, a mesma informação serve para inúmeros negócios com propósitos distintos, seja no setor privado, seja no público[444].

Em termos de mercado, a nova lógica econômica demanda uma constante vigilância sobre os consumidores, protagonizada pela captação e tratamento de seus dados pessoais. Isto se dá sob uma lógica de gerenciamento e distribuição dos riscos socialmente, o que acarreta um ciclo infindável de obtenção de mais informações, as quais geram mais insegurança, que demanda mais vigilância[445].

No âmbito estatal, a sociedade de vigilância estaria diretamente associada ao uso político das informações como meio de controle social, sendo marcadas por seu caráter autoritário e até mesmo ditatorial. Não por acaso, o "homem de vidro" que se materializa nessa sociedade é uma ideia proveniente do regime nazista. Nessa seara, a sociedade da informação, sob um apelo de uma transparência (unilateral), torna-se a sociedade da vigilância[446].

Como bem pontua Beck:

> Em minha primeira publicação, em 1986, eu descrevi a Sociedade de Risco como "uma condição estrutural inescapável da industrialização avançada" – e critiquei a "moral matematicisada" de pensamentos de experts e do discurso público de "profiling de riscos". Enquanto avaliações políticas orientadas a partir do risco propõem o gerenciamento dos riscos, eu apontei que "mesmo a conta mais contida e objetivista-moderada de implicações de riscos envolvem uma política, uma ética e uma moral encobertas". Risco "não é reduzível a um produto de probabilidade de ocorrência multiplicado pela intensidade e a abrangência de um mal em potencial". Ao contrário, é um fenômeno construído socialmente, em que algumas pessoas têm maior capacidade de definir riscos que outras. Nem todos os atores [sociais] se beneficiam da gestão do risco – apenas aqueles com o escopo de definir seus próprios riscos. A exposição ao risco está substituindo as classes como a principal desigualdade da sociedade moderna, porque como o risco é gerido e definido por atores [sociais]: "Em sociedades do risco relações de definição são concebidas analogamente as relações de produção de Marx". As desigualdades de definições possibilitam atores poderosos a maximizar os riscos para os "outros" e minimizar os riscos para "si mesmos". A definição do risco, essencialmente, é um jogo de poder. Isso é especialmente verdade para uma sociedade global do risco em que

[444] GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010.

[445] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online.

[446] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

> governos ocidentais ou fortes atores econômicos definem os riscos para os outros.[447]

Destarte, o *profiling* denota um potencial lesivo muito severo se não utilizado com a devida cautela. Sendo a única representação de indivíduos para terceiros – inclusive para o próprio Estado –, essas técnicas de previsão de comportamentos, ou de padrões de comportamento podem significar a diminuição da esfera de liberdade de inúmeros indivíduos[448]. Os perfis eletrônicos não levam em consideração as reais intenções do sujeito, eles sempre partem do pressuposto de que ele adotará determinado comportamento tido como padrão para aquela categoria de indivíduos[449].

É preciso encarar o mecanismo do *profiling* com franqueza, vez que o cerne do mesmo é a discriminação. Basicamente, ele identifica padrões de comportamento e classifica o indivíduo a partir de categorias pré-estabelecidas – geralmente por meio do Big Data –, tudo com base no uso de dados pessoais. Tal prática consiste em uma discriminação racional, em que o indivíduo pode ser privado do acesso a

---

[447] "*In my first publication, in 1986, I described Risk Society as 'an inescapable structural condition of advanced industrialization' – and criticized the 'mathematicized morality' of expert thinking and public discourse on 'risk profiling'. While policyoriented risk assessment posited the manageability of risks, I pointed out that 'even the most restrained and moderate-objectivist account of risk implications involves a hidden politics, ethics and morality'. Risk 'is not reducible to the product of probability of occurrence multiplied with the intensity and scope of potential harm'. Rather, it is a socially constructed phenomenon, in which some people have a greater capacity to define risks than others. Not all [social] actors really benefit from the reflexivity of risk – only those with real scope to define their own risks. Risk exposure is replacing class as the principal inequality of modern society, because of how risk is reflexively defined by [social] actors: 'In risk society relations of definition are to be conceived analogous to Marx's relations of production'. The inequalities of definition enable powerful actors to maximize risks for 'others' and minimize risks for 'themselves'. Risk definition, essentially, is a power game. This is especially true for world risk society where Western governments or powerful economic actors define risks for others.*" BECK, Ulrich. World risk society. In: OLSEN, J. K. B.; PEDERSEN, S. A.; HENDRICKS, V. F. (Ed.). **A companion to the philosophy of technology**. Oxford: Blackwell Publishing Ltd, 2009. p. 495-499. p. 496.

[448] "Os mais diversos tipos de entidades realizam a vigilância de cidadãos, consumidores e empregados no dia a dia. A consequência disso é a classificação das pessoas em categorias de acordo com a avaliação de seus riscos e a discriminação do acesso a determinados bens e serviços, de modo a afetar significativamente as suas chances de vida." MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online. p. 91.

[449] "A partir do momento em que o perfil eletrônico é a única parte da personalidade de uma pessoa visível a outrem, as técnicas de previsão de padrões de comportamento podem levar a uma diminuição de sua esfera de liberdade, visto que vários entes com os quais ela se relaciona partem do pressuposto de que ela adotará um comportamento predefinido, acarretando uma efetiva diminuição de escolha". DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 174.

bens e a serviços, ou até mesmo ser objeto de perseguição estatal a partir de meios automatizados de tratamento de informações.

O próprio modo de operacionalização do *profiling* evidencia não só o caráter impessoal dessa ferramenta, mas a fragilidade das regulações existentes. Grande parte desse processo sequer trabalha com dados pessoais, como é o caso da *Data Analysis,* da *Data Mining* e da *Machine Learning* que operam basicamente sobre a Big Data e com dados anônimos ou anonimizados, fugindo, assim, ao âmbito material de legislações de proteção de dados pessoais (a exemplo do Regulamento 2016/679 UE)[450]. Ademais, a carência de uma definição legal de *profiling* no Brasil, na Europa e nos Estados Unidos corrobora para essa fragilização na proteção do indivíduo quando do uso desse tipo de mecanismo de tratamento de dados pessoais, que demanda algum tipo de regulação ou abordagem legal específica[451].

3.2 PROTEÇÃO DE DADOS, ESTADO E INDIVÍDUO

A partir de uma análise da legislação vigente no ordenamento jurídico pátrio, é possível identificar uma construção protetiva em torno de dados sensíveis. Aquelas informações que dizem respeito à intimidade, à vida privada, à honra e à imagem dos indivíduos são sempre tratadas como sigilosas – art. 5º, inciso XXXIII, CF c/c art. 23 da Lei dos Arquivos Públicos[452].

Soma-se a tal estrutura a proteção contra a interceptação e a utilização desses dados (sensíveis) por terceiros não autorizados. Outrossim, o princípio do *need to know* (necessidade de conhecer) – pode ser identificado nos art. 4º, inciso XIII e art. 37, inciso I do Decreto nº 4.553/02 – que determina que somente terá

---

[450] DÖHMANN, Indra Spiecker Genannt; TAMBOU, Olivia; BERNAL, Paul; et. al. The Regulation of Commercial Profiling – A Comparative Analysis. **European Data Protection Law Review.** Berlin, v. 2, n. 4, p. 535-554, 2016.

[451] DÖHMANN, Indra Spiecker Genannt; TAMBOU, Olivia; BERNAL, Paul; et. al. The Regulation of Commercial Profiling – A Comparative Analysis. **European Data Protection Law Review.** Berlin, v. 2, n. 4, p. 535-554, 2016.

[452] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007.

acesso a informações sigilosas aquele agente público que necessita dela para o desempenho de suas funções[453].

A ausência de uma disciplina sistematizada e de uma regulação específica implica a falta de uma proteção jurídica eficaz em relação aos bancos de dados informatizados. O instituto do *habeas data,* não obstante, é o mais próximo que se tem, hoje, dessa necessária tutela jurídica[454].

A ação constitucional do *habeas data* é prevista no art. 5º, inciso LXXII da CF, sendo posteriormente regulada pela Lei nº 9.507/97. Trata-se de remédio constitucional cabível sempre que o impetrante tenha o interesse de conhecer informações a seu respeito, "constantes de registros ou bancos de dados de entidades governamentais ou de caráter público" – art. 5º, inciso LXXII, *a* –, ou queria retificar tais informações – art. 5º, inciso LXXII, *b*.

Trata-se de instituto surgido no Brasil, na própria Constituição da República Federativa do Brasil de 1988, servindo de modelo para diversos países latino-americanos. Não por acaso, o *habeas data* desenvolveu-se em "[...] sociedades recém-saídas de regimes ditatoriais, como era o panorama de muitos países latino-americanos na década de 1980, em cuja sociedade civil persistia o trauma pelo uso autoritário da informação"[455].

Ainda que não seja inspirado em nenhum modelo existente, pode-se identificar forte influência das Constituições espanhola e portuguesa (que também saíram de longas e rígidas ditaduras), no que toca à tratativa de informações. Ainda, vale ressaltar que, mesmo antes de 1988, já havia legislações de âmbito estatal – especificamente, Rio de Janeiro e de São Paulo –, que dispunham a propósito do direito de acesso e de retificação de informações de cunho pessoal, e que já apresentavam alguns elementos até hoje não identificados na normativa federal (ao menos não expressamente), como é o caso dos princípios da finalidade e do consentimento informado[456].

---

[453] Ibid.
[454] LIMBERGER, Têmis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.
[455] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 327.
[456] Ibid.

Com carga semântica similar à do *habeas corpus*, Frosini valeu-se do termo *habeas data* em face da necessidade de se reconhecer o "[...] direito do cidadão de dispor dos próprios dados pessoais, assim como ele tem o direito de dispor livremente do próprio corpo"[457].

Entretanto, o alcance da proteção do *habeas data* é muito restrito, limitando-se a bancos de dados públicos ou de caráter público. Assim, o "[...] impetrante fica com a proteção jurídica fragilizada, do ponto de vista da aplicabilidade da norma, sempre que estiver diante de entidade de caráter privado e numa relação que não seja de consumo"[458].

Outrossim, em que pese seu grande valor teórico e dogmático, o instituto do *habeas data,* em termos de prática jurídica, é pouco operacionalizável. Em face dessa estreita margem de uso, foi objeto de crítica por parte da doutrina, que o taxa de um remédio constitucional essencialmente simbólico[459]. A ausência de elementos capazes de tornar a ação ágil e eficaz somada aos empecilhos impostos à sua impetração, como a necessidade de um advogado e a comprovação da recusa do fornecimento das informações, fazem do *habeas data* um "[...] instrumento que proporciona uma tutela completamente anacrônica e ineficaz à realidade das comunicações e tratamentos de dados pessoais na Sociedade da Informação"[460].

A bem da verdade, é preciso levar em consideração que o *habeas data* foi editado como um remédio para uma questão específica de seu tempo: a falta de transparência dos arquivos ditatoriais. Não obstante, o instituto serviu para a positivação, em sede constitucional, dos direitos de acesso e de retificação dos dados pessoais[461], embora impondo algumas limitações aos mesmos[462].

---

[457] FROSINI, Vitorio. La protezione della riservatezza nella società informática. In: **Informatica e Diritto**. fascículo 1º, janeiro-abril, 1981, p. 9-10.), apud DONEDA, op. cit., p. 331.

[458] LIMBERGER, Têmis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007. p. 189.

[459] É o que pode se extrair dos posicionamentos de Luís Roberto Barroso e José Carlos Barbosa Moreira, os quais apontam que o mandado de segurança seria suficiente para remediar as questões que são objeto do *habeas data*. DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[460] Id. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2. p. 91-108, jul./dez. 2011. p. 104.

[461] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017.

[462] Das limitações impostas, destacam-se a restrição da ação a bancos de dados públicos ou de caráter público, a necessidade de impetração por advogado e a necessidade de tentativa de

Para além do *habeas data,* é possível trabalhar, sob o prisma da proteção de dados pessoais, a questão do sigilo fiscal e bancário e a inviolabilidade das comunicações. Tal abordagem, entrementes, parte do pressuposto de que há, em alguns aspectos, a superposição do direito à proteção de dados pessoais em relação a outros direitos fundamentais[463].

Os sigilos fiscal e bancário são trabalhados majoritariamente pela doutrina como um aspecto dos direitos à privacidade e à intimidade[464], em que pese discutível sua fundamentalidade[465]. No que concerne ao âmbito de proteção desse direito, inexiste distinção no que toca à natureza das informações constantes de cadastros fiscais e bancários, importando a proteção desses dados na sua integralidade[466].

Naturalmente, não se trata de direito absoluto, sendo possível a determinação da quebra do sigilo bancário, desde observados alguns parâmetros para assegurar sua legitimidade e constitucionalidade. Em que pese sua limitação seja amplamente

---

acesso ou retificação prévia pela via administrativa. Como bem descreve Doneda: "[...] além do seu perfil estar demasiadamente associado à proteção de liberdades negativas, algo que se percebe em vários dos seus pontos estruturais, como a necessidade de sua interposição por meio de advogado ou então a necessidade de demonstração de recusa de fornecimento dos dados por parte do administrador de banco de dados". DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental, op. cit., p. 104.

463 Como bem lecionam Sarlet, Marinoni e Mitidiero, "[...] dada a sua proximidade e mesmo, a depender do caso, a parcial superposição com o âmbito de proteção de outros direitos fundamentais, a determinação da esfera autônoma de incidência do direito à proteção dos dados nem sempre é fácil, pois a utilização de determinados dados pode violar simultaneamente mais de um direito". SARLET; MARINONI; MITIDIERO, op. cit., p. 473.

464 Nesse sentido, ver: RUARO, Regina Linden. Direito fundamental à privacidade: o sigilo bancário e a fiscalização da Receita Federal do Brasil. **Interesse Público**, Belo Horizonte, v. 17, n. 90, p. 103-125, mar./abr. 2015; FERRAZ JÚNIOR, Tercio Sampaio. Sigilo bancário – privacidade e liberdade. In: SARAIVA FILHO, Oswaldo Othon de Pontes; GUIMARÃES, Vasco Branco (Coord.). **Sigilos bancário e fiscal**. Homenagem ao Jurista José Carlos Moreira Alves. 2. ed. rev. ampl. Belo Horizonte: Fórum, 2015. p. 85-110; MARTINS, Ives Gandra da Silva. Sigilo bancário e privacidade. In: SARAIVA FILHO; GUIMARÃES, op. cit., p. 67-84; SANCHES, Jose Luis Saldanha; GAMA, João Taborda da. Sigilo bancário – crónica de uma morte anunciada. In: SARAIVA FILHO; GUIMARÃES, op. cit., p. 243-264.

465 Em que pese não se aprofundar na discussão a propósito da fundamentalidade ou não do direito ao sigilo bancário e fiscal, Sarlet, Marinoni e Mitidiero apontam que é possível sim encarar tal situação com reservas e que se tal direito se trata, ao menos, de "[...] uma dimensão relativamente mais fraca da proteção da vida privada, visto que se tem admitido uma ampla possiblidade de intervenções legítimas". SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017. p. 451.

466 Ibid.

aceita pela jurisprudência e pela doutrina, a definição dos parâmetros para essa relativização gera grande controvérsia[467].

Nesse aspecto, o debate a propósito da constitucionalidade da Lei Complementar (LC) nº 105/2001 teve grande repercussão. A incorporação, pela LC nº 105, da tendência mundial de quebra do sigilo sem a observância de reserva de jurisdição, ou seja, prescindindo de autorização judicial, foi objeto de apreciação pelo Plenário do Supremo Tribunal Federal (STF), por meio do Recurso Extraordinário (RE) nº 601.314/SP.

Sob relatoria do Ministro Edson Fachin, a Suprema Corte entendeu, por maioria, que o art. 6º da LC nº 105/01[468] não viola o direito ao sigilo bancário, pois não haveria uma quebra de sigilo, mas sim uma transferência do mesmo. Apesar de não ser isenta de críticas[469], a decisão deu solução ao debate existente sobre a legitimidade da transferência do sigilo bancário para o sigilo fiscal.

Para além da administração tributária, porém, a reserva de jurisdição vem sendo mantida pelo STF. Assim, o Ministério Público, o Banco Central, a autoridade policial e outros órgãos do Poder Executivo (por exemplo, os Tribunais de Contas) não estariam legitimados a proceder à quebra do sigilo fiscal e bancário. Tal conjuntura demonstra que, na prática, o STF acabou "[...] consagrando uma espécie

---

[467] RUARO, Regina Linden. Direito fundamental à privacidade: o sigilo bancário e a fiscalização da Receita Federal do Brasil. **Interesse Público**, Belo Horizonte, v. 17, n. 90, p. 103-125, mar./abr. 2015.

[468] "Art. 6º As autoridades e os agentes fiscais tributários da União, dos Estados, do Distrito Federal e dos Municípios somente poderão examinar documentos, livros e registros de instituições financeiras, inclusive os referentes a contas de depósitos e aplicações financeiras, quando houver processo administrativo instaurado ou procedimento fiscal em curso e tais exames sejam considerados indispensáveis pela autoridade administrativa competente." BRASIL. Lei complementar nº 105, de 11 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. **Diário Oficial da União**, Brasília, 11 jan. 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm>. Acesso em: 14 out. 2017.

[469] No que concerne à decisão do STF, ver: MACHADO, Fernando Inglez de Souza; KRONBAUER, Eduardo Luís. Proteção de dados e quebra do sigilo bancário para fins tributários: retrocesso em matéria de direitos fundamentais em prol de uma maior eficiência na administração pública. In: CONPEDI; UNICURITIBA (Org.). **Direito tributário e financeiro II**. 1. ed. Florianópolis: CONPEDI, 2016. v. 1. p. 47-66; e RUARO, Regina Linden. Direito fundamental à privacidade: o sigilo bancário e a fiscalização da Receita Federal do Brasil. **Interesse Público**, Belo Horizonte, v. 17, n. 90, p. 103-125, mar./abr. 2015.

de reserva de jurisdição relativa, objetivando um maior controle e rigor no campo das intervenções na esfera do sigilo fiscal e bancário"[470].

Por sua vez, o direito fundamental à inviolabilidade das comunicações, sejam elas via correspondência, telegráficas, telefônicas ou de dados, está materialmente ligado ao direito à privacidade e instrumentalmente ligado ao direito à liberdade de expressão e de comunicação[471]. Trata-se de direito expressamente previsto na Constituição – art. 5º, inciso XII[472] –, que abrange todos os meios de comunicação pessoal, estendendo sua proteção não só ao conteúdo, mas a tudo que permeia essa comunicação (a forma da comunicação, a data, o horário, o local, a identidade das pessoas que estão se comunicando, dentre outros)[473].

Digno de nota, ainda, o Marco Civil da Internet – Lei nº 12.965, de 23 de abril de 2014 – que, como era de se esperar, não enfrentou de forma minuciosa a questão dos dados pessoais, até mesmo porque não é objeto dessa lei[474]. Assim, o texto normativo apenas contém algumas menções pontuais à proteção de dados pessoais, porém sempre remetendo à uma lei específica, vez que o projeto de lei que deu origem ao Marco Civil da Internet foi encabeçado concomitantemente com o projeto de lei de proteção de dados pessoais até agora não aprovado pelo legislativo brasileiro. Dessa feita, a aplicação dessa lei simultaneamente ao CDC permite compendiar um direito à proteção de dados pessoais dos consumidores no âmbito virtual, o que, apesar de não ser suficiente, já é um grande avanço para o cenário brasileiro de proteção de dados[475].

---

[470] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017. p. 453.

[471] Ibid.

[472] "[...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [...]. " BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 05 mar. 2017.

[473] SARLET; MARINONI; MITIDIERO, op, cit.

[474] Trata-se de lei que "[...] estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil". BRASIL. Lei nº 12.965, de 24 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 out. 2017.

[475] MENDES, Laura Schertel. O diálogo entre o marco civil da internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 106, p. 37-69, jul./ago. 2016.

Do Marco Civil da Internet depreende-se que o uso da internet deve observar a “proteção da privacidade” – art. 3º, inciso II – e a “proteção de dados pessoais, na forma da lei” – art. 3º, inciso III – (em que pese, até agora, inexista essa lei). Ademais, é assegurada ao usuário a inviolabilidade de sua vida privada, proporcionando-se a devida indenização por eventuais danos (materiais ou morais) sofridos – art. 7º, inciso I – e a inviolabilidade do fluxo de suas comunicações via internet ou armazenadas, salvo em caso de determinação judicial – art. 7º, incisos II e III. Destaca-se, ainda, que alguns princípios do direito à proteção de dados também são recepcionados na lei. É o caso do não fornecimento dos dados do usuário para terceiros, inclusive registro de conexões – art. 7º, inciso VII; o princípio da transparência e da finalidade, ao se assegurar o direito de informação clara e precisa sobre o tratamento de dados do usuário e condicionar o tratamento apenas aos casos que “[...] justifiquem sua coleta, não sejam vedados pela legislação e estejam especificados no contrato” – art. 7º, inciso VIII; o princípio do consentimento, que deverá ser expresso e estar destacado das demais cláusulas do contrato – art. 7º, inciso IX; e o direito de apagamento de dados – art. 7º, inciso X[476].

Por fim, em termos de vigilância policial (ou político-policial), é prudente ter um olhar céptico com os discursos inflamados que clamam por transparência. É preciso grande cuidado na implementação de medidas invasivas, sob a justificativa (ou pretexto) de (in)seguridade nacional. Nem sempre elas se prestam ao fim anunciado, ou podem não ser tão eficientes quanto aparentam. Contudo, elas mantêm a característica de mecanismos de vigilância político-policial, marcados por atributos típicos de regimes totalitários e não democráticos[477].

---

[476] No que toca à exclusão dos dados, entende-se que a disposição legal: “[...] 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;” não deveria ter condicionado a exclusão dos dados ao requerimento do usuário. Uma vez que não há mais pertinência na conservação dos dados, entende-se que sua conservação seria violaria o “direito ao esquecimento”. Melhor seria a fixação de um prazo razoável de conservação dos dados, a exemplo do que se tem na experiência Europeia. BRASIL. Lei nº 12.965, de 24 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 out. 2017.

[477] Nesse sentido, Whitaker aponta que: “[...] *la vigilancia político-policial a escala internacional sólo remite a un uso (o mal uso) de los servicios de inteligencia*”. Já no que toca à sua aplicação em âmbito nacional, o autor entende que essa se faz muito mais pertinente, mas ainda muito perigosa pois essa sistemática de “[...] *represión de la discidencia y de los dissidentes; el control de las clases turbulentas y peligrosas; la conformidade política compulsiva, y la penetrante y*

3.3 *PROFILING* NAS RELAÇÕES DE CONSUMO

O fenômeno da sociedade da informação, especialmente no que concerne à digitalização de informações a partir de uma linguagem universal – o código binário –, ensejou um significativo aumento nas aplicações e nas utilidades dos mecanismos de estatística e de tratamento de dados pessoais. Hoje, o *Big Data* permite que se encontre um padrão para praticamente todos os fatos da vida social, inclusive no que toca ao comportamento humano[478]. Em tal cenário, o consumidor não é apenas o responsável pela demanda, mas objeto de consumo de uma nova lógica do mercado[479]. O tratamento de dados pessoais permite às empresas refinarem a previsibilidade do comportamento de consumo e reduzirem os riscos na alocação de recursos e investimentos, bem como trabalharem com a diferenciação de produtos e serviços a partir de uma maior interação com o consumidor[480].

Em termos de consumo, o *profiling* é identificado de forma mais saliente no âmbito das relações creditícias e das estratégias de *marketing* e publicidade, mas não se pode ignorar que afeta até questões como a definição de estratégias, investimento em produtos e locação de pontos de venda[481]. No Brasil, o Código de

---

omnipresente vigilancia y regulación de la vida cotidiana" acaba manchando um Estado liberal com elementos autoritários e antidemocráticos. WHITAKER, Reg. **El fin de la privacidad**: como la vigilancia total se está convirtiendo en realidad. Traducción Luis Prat Clarós. Barcelona: Paidos, 1999. p. 32.

478 A fim de visualizar as aplicações do *Big Data*, ver: CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang (Org.). **New horizons for a data-driven economy**: a roadmap for usage and exploitation of big data in Europe. Cham (Suiça): Springer Open, 2016.

479 Como bem aponta Mendes, a "[...] informação transformou-se em insumo da produção, possuindo um papel tão importante quanto a força de trabalho e o capital. A partir dessa constatação, pode-se concluir que existe na economia atual um imperativo de vigilância dos consumidores". MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online. p. 91.

480 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online.

481 "Vivemos em uma economia da informação pessoal desde a década de 70, na qual a informação constitui-se como a fonte motriz. Tal fenômeno ultrapassa as áreas de proteção ao crédito e marketing direto, pois atualmente grandes empresas de varejo tomam as suas decisões de investimento referentes a estratégias, produtos e locação de pontos de venda baseadas em refinadas análises a respeito da renda, preferências e comportamento dos seus clientes." Ibid., p. 84.

Defesa do Consumidor (CDC)[482] enfrentou as duas primeiras questões de forma pontual, bebendo fortemente da experiência norte-americana no que concerne aos cadastros de créditos, havendo, também, o aporte de legislação específica a respeito dos cadastros positivos – Lei nº 12.414/2011[483].

O *Fair Credit Reporting Act* (FCRA), aprovado pelo Congresso americano em abril de 1971, foi a mais forte influência sobre a regulação dos "Bancos e Cadastros dos Consumidores", prevista nos arts. 43 e 44 do CDC. A lei norte-americana veio como resposta aos abusos praticados pelos *crédit bueraus* que, já em 1969, eram amplamente utilizados em todo o território estadunidense[484].

No período de 1965 a 1970, das diversas audiências realizadas pelos três Comitês do Congresso a propósito das práticas desses *crédit bueraus,* verificou-se a falta de transparência na coleta e no tratamento das informações pessoais. Inclusive, constatou-se que a própria existência desses departamentos era de pouco ou de nenhum conhecimento dos consumidores em geral[485].

Somada a essa falta de transparência, especialmente o fato de a política dos *credit bureaus* não permitirem o acesso dos consumidores a suas próprias informações, averiguou-se que inúmeras das informações coletadas não atendiam nenhum critério de razoabilidade, no que concerne à finalidade para qual foram coletadas: análise de crédito. Com especial destaque aos testemunhos do professor Alan Westin, as audiências coordenadas pelo Congresso norte-americano revelaram que não só dados relativos a operações financeiras eram objeto de coleta e

---

[482] BRASIL. Lei nº 8.078, de 12 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**, Brasília, DF, 12 set. 1990. p. 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 30 out. 2017.

[483] Id. Lei nº 12.414, de 10 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União**, Brasília, 10 jun. 2011. p. 2. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 30 out. 2017.

[484] GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010.

[485] GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010.

tratamento, mas dados relativos a hábitos sexuais, a opiniões políticas, à vida matrimonial, dentre outros[486].

Como resultado, o FCRA foi aprovado, determinando que nenhum *credit bureau* pudesse manter sua existência em sigilo. Ademais, a lei garantiu aos consumidores o direito de acesso às suas informações constantes em bancos de dados para fins de análise de crédito e o direito de contestar eventuais informações imprecisas, errôneas ou desatualizadas, possibilitando que o consumidor inserisse sua versão dos eventos anotados[487].

A aprovação do FCRA, em que pese se tratar de significativo avanço na temática da proteção de dados pessoais, não foi suficiente para remediar a questão das anotações de informações errôneas ou desatualizadas. Em 1991, James Williams, da *Consolidated Information Service*, uma firma de registros de hipotecas em New York analisou 1.500 relatórios dessas três maiores empresas de *credit report* americanas e constatou que em 43% dos arquivos analisados havia informações errôneas. No mesmo ano, o sistema da TRW classificou como *tax delinquents* (irregulares com os impostos) cerca de 1.400 proprietários de imóvel em uma cidade de aproximadamente 3.000 habitantes, tudo em face de uma anotação equivocada do pessoal que coleta informações de hipotecas em domicílios – "*tax bill on town records as tax aliens*"[488].

Outrossim, o já mencionado *Code Fair Information Practices* também norteou o aporte legislativo brasileiro referente à matéria de concessão de crédito, inclusive, a ponto de parte da doutrina nacional identificar nesse tópico do CDC um marco normativo nacional concernente aos princípios de proteção de dados pessoais[489].

---

[486] "[...] *testifying before Congress in March 1970, Professor Alan Westin said that the files 'may include 'facts, statistics, inacuracies and rumors' about virtually every phase of a person's life: his marital troubles, jobs, school history, childhood, sex life, and political activities.' Apparently, business leaders of the time thought that a person beat his spouse or engaged in certain sexual practices, he probably couldn't be trusted to pay back a loan. Not surprisingly, businesses were afraid of letting the public discover just what kind of information was being collected on Americans*." Ibid., p. 22.

[487] Ibid.

[488] GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010. p. 28.

[489] BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Elaboração Danilo Doneda. Brasília: SDE/DPDC, 2010. Disponível em:

Valendo-se da experiência norte-americana, o art. 43 do CDC[490] estipulou inúmeros deveres para os responsáveis por bancos de dados de consumidores, bem como alguns direitos aos titulares dos dados. Dentre tais determinações, destacam-se: o dever de notificação (art. 43, §2º), o direito de acesso às informações (art. 43, *caput*, §§1º e 6º), o direito ao esquecimento (art. 43, §1º), o direito de correção das informações (art. 43, §§eº e 5º). Outrossim, ele equiparou esses bancos de dados àqueles de caráter público (art. 43, §4º), abrindo margem para a utilização da já referida ação constitucional do *habeas data*[491].

Trata-se de uma das normativas brasileiras mais modernas e eficazes no que concerne à questão dos bancos de dados. Inclusive, Doneda aponta que o CDC vem marcando significativamente o ordenamento civil brasileiro, irradiando sua disciplina para além da relação consumerista, servindo como parâmetro interpretativo em razão de sua eficácia limitada às relações de consumo e sendo responsável pelo preenchimento de inúmeras lacunas existentes no ordenamento brasileiro, notadamente no que toca à ausência de um marco regulatório específico a propósito da proteção de dados pessoais[492].

<http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf>. Acesso em: 23 jul. 2017.

[490] "Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor." Id. Lei nº 8.078, de 12 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**, Brasília, DF, 12 set. 1990. p. 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 30 out. 2017.

[491] A esse respeito ver: LIMBERGER, Têmis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

[492] BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Elaboração Danilo Doneda. Brasília: SDE/DPDC, 2010. Disponível em:

As disposições do CDC vieram regular os serviços de proteção de crédito – dos quais destacam-se o SPC e o SERASA. Nesse sentido, a lei foi essencial para conformar os cadastros negativos com a proteção do consumidor, servindo de base, ademais, para a consolidação do entendimento do Superior Tribunal de Justiça (STJ) no sentido de que a inscrição negativa do consumidor, ou o protesto indevido em seu nome, quando inexistente anotação anterior, configura dano moral *in re ipsa* (Súmula 385 do STJ)[493].

O aporte legislativo do Código, contudo, não foi suficiente para a solução de questões envolvendo o chamado cadastro positivo, o que só ocorreu com a edição da Lei nº 12.414/2011, também chamada de Lei do Cadastro Positivo. Tendo enfoque específico na "[...] formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito" (art. 1º), a lei trouxe uma série de determinações ao "gestor" do banco de dados e direitos ao "cadastrado"[494], a fim de garantir a proteção do consumidor quando do acesso ao crédito.

Da análise da lei, é possível identificar inúmeros princípios da proteção de dados pessoais: o dever de objetividade e clareza das informações armazenadas (art. 3º, §1º); a vedação de anotações de informações excessivas, consubstanciada no princípio da adequação (art. 3º, §3º, inciso I); a vedação de anotações sensíveis (art. 3º, §3º, inciso II); o princípio do consentimento informado (arts. 4º, 9º e 11); os direitos de acesso às informações e de retificação das mesmas (art. 5º, incisos II e III); o princípio da finalidade (art. 5º, inciso VII, e art. 7º), e o dever de apagamento dos dados (art. 14). Com base nessa análise, destarte, é possível afirmar que a Lei

---

<http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf>. Acesso em: 23 jul. 2017.

493 Súmula 385, STJ: "Da anotação irregular em cadastro de proteção ao crédito, não cabe indenização por dano moral, quando preexistente legítima inscrição, ressalvado o direito ao cancelamento". Id. Superior Tribunal de Justiça. **Súmula nº 385**. Da anotação irregular em cadastro de proteção ao crédito, não cabe indenização por dano moral, quando preexistente legítima inscrição, ressalvado o direito ao cancelamento. Julgamento: 27 de maio de 2009. RSTJ v. 214 PG: 00541. Súmulas STJ. Disponível em: <http://www.stj.jus.br/docs_internet/SumulasSTJ.pdf>. Acesso em: 3 nov. 2017.

494 São utilizados os termos "gestor" em vez do vocábulo "responsável" e "cadastrado" em vez de "titular dos dados", a fim de se adequar a nomenclatura utilizada pela lei. *Vide* art. 2º, II e III. Id. Lei nº 12.414, de 10 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União**, Brasília, 10 jun. 2011. p. 2. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 30 out. 2017.

do Cadastro Positivo está em harmonia com um direito à proteção dos dados pessoais, não só em termos de Brasil, mas de União Europeia[495].

Para além da Lei do Cadastro Positivo, o uso de sistemas de *scoring* também foi objeto de grande controvérsia no ordenamento jurídico pátrio. Só no Tribunal de Justiça do Estado do Rio Grande do Sul (TJRS), existiam cerca de 80 mil recursos pendentes de julgamento, cujo objeto da ação versava a propósito da licitude e dos limites da utilização do sistema do *Credit Scoring*[496]. Diante de tal repercussão, a questão foi objeto de apreciação pelo Superior Tribunal de Justiça (STJ), a partir do Recurso Especial nº 1.419.679-RS[497], o qual fora afetado pelo rito de recurso repetitivo.

Cumpre referir que o sistema de *Credit Scoring* é produto da massificação das relações de consumo e do consequente aumento da procura de crédito. Trata-se de um mecanismo de *profiling* que enfoca especificamente a análise de crédito de pequenos valores[498]. Criado com a finalidade de garantir maior segurança e agilidade às operações de crédito, o sistema opera atribuindo uma pontuação ao consumidor que pleiteia crédito, com base em técnicas estatísticas, mais especificamente por meio de um algoritmo. Tal pontuação, por sua vez, serve como um indicativo ao proponente do crédito acerca do risco (de inadimplemento) que a operação envolve[499].

---

[495] O modelo europeu de proteção de dados pessoais foi enfrentado no segundo capítulo deste trabalho.

[496] Informação do Núcleo de Recursos Repetitivos e Repercussão Geral – NURER – do TJRS. BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.419.679-RS**. Relator: Ministro Paulo de Tarso Sanseverino. Segunda Seção, julgado em 12/11/2014, DJe 17/11/2014, Brasília, DF, 12 nov. 2014. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201303862850&dt_publicacao=17/11/2014>. Acesso em: 20 nov. 2017.

[497] Ibid.

[498] MARQUEZ, Javier. **An introduction to credit scoring for small and medium size enterprizes**. World Bank, 2008. Disponível em: <http://siteresources.worldbank.org/EXTLACOFFICEOFCE/Resources/870892-1206537144004/MarquezIntroductionCreditScoring.pdf>. Acesso em: 30 jul. 2017.

[499] A elaboração do *Credit Scoring* perpassa pela estipulação e definição dos "[...] mercados e produtos de crédito para os quais serão desenvolvidos o sistema; finalidades de uso; tipos de clientes; conceito de inadimplência a ser adotado; horizonte de previsão do modelo. Identificação das variáveis potenciais: caracterização do proponente ao crédito; caracterização da operação; seleção das variáveis significativas para o modelo; análise das restrições a serem consideradas em relação às variáveis. Planejamento amostral e coleta de dados: seleção e dimensionamento da amostra; coleta dos dados; montagem da base de dados. Determinação da fórmula de escoragem através de técnicas estatísticas, como por exemplo, a análise discriminante ou regressão logística. Determinação do ponto de corte, a partir do qual o cliente é classificado como adimplente ou bom

Destarte, trata-se de mecanismo que pressupõe o tratamento de dados pessoais e que visa à classificação do consumidor a partir de seu comportamento e de seu histórico de crédito[500]. A partir dele, as empresas pautam-se para definir não só as condições de acesso ao crédito, mas a própria possibilidade de acessá-lo, bem como a quantia que será disponibilizada[501].

Forçoso apontar, também, que os sistemas de *scoring*, não apenas na área do crédito, mas de forma geral, figuram como uma avaliação objetiva de consumidores, identificando os consumidores de maior interesse às empresas e os de menor interesse, seja em termos de menor risco de inadimplência ou de maior capacidade econômica. Assim, o consumidor "ruim" acaba sendo privado de ofertas e até mesmo do acesso a bens e serviços em consequência de sua classificação[502].

Voltando ao Recurso Especial nº 1.419.679-RS, o julgado contou com a realização de audiência pública a pedido do próprio relator Ministro Paulo de Tarso Sanseverino e teve como objeto duas questões: a compatibilidade do sistema de *scoring* com os direitos do consumidor e a configuração ou não de danos morais no uso desse sistema. A lide que serviu de base para tal caso consistia na ação de indenização por danos morais ajuizada por Anderson Guilherme Prado Soares, tendo como parte ré Boa Vista Serviços, motivada por uma negativa de crédito, em que pese a inexistência de qualquer inscrição negativa contra o autor.

Após posicionamento favorável ao demandante nas duas instâncias ordinárias, indicada a abusividade da prática comercial de escoragem, o STJ, por maioria, deu parcial provimento ao recurso especial interposto pela parte

---

pagador". ARAÚJO, Elaine Aparecida. **Risco de crédito**: desenvolvimento de modelo Credit Scoring para a gestão da inadimplência de uma instituição de microcrédito. Ipea Caixa, 2006. Disponível em: <http://www.esaf.fazenda.gov.br/assuntos/premios/premios-1/premios-realizados/pasta-premio-ipea-caixa/premio-ipea-caixa-2006/profissionais/tema-3/2-lugar-tema-3-profissionais>. Acesso em: 31 jul. 2017.

500 Nesse sentido, o próprio SCPC *Score Crédito* afirma que o *Credit Scoring* visa agrupar os "[...] consumidores em faixas de risco, tendo como parâmetro o comportamento médio esperado em termos de inadimplência baseado no histórico de informações de mercado compartilhadas" nos bancos de dados da empresa. BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.419.679-RS**. Relator: Ministro Paulo de Tarso Sanseverino. Segunda Seção, julgado em 12/11/2014, DJe 17/11/2014, Brasília, DF, 12 nov. 2014. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201303862850&dt_publicacao=17/11/2014>. Acesso em: 20 nov. 2017.

501 ARAÚJO, op. cit.

502 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online.

demandada. O Tribunal Superior entendeu que, no caso em comento, o uso do sistema do *credit scoring* não configurou dano moral que ensejasse a reparação pretendida[503].

A fim de motivar a decisão supracitada, o voto do Ministro Relator Paulo de Tarso Sanseverino desenvolveu cinco teses, que sustentavam, em suma: 1) o sistema *credit scoring* é um sistema de avaliação de risco para concessão de crédito, baseado em modelos estatísticos, composto por diversas variáveis que se prestam a determinar a pontuação (*score*) do consumidor; 2) o uso desse sistema é uma prática comercial lícita, autorizada pelo art. 5º, inciso IV, e art. 7º, inciso I da Lei nº 12.414/2011; 3) o uso desse sistema e as avaliações do risco de crédito em geral devem obedecer aos limites postos pelo sistema de proteção ao consumidor, nos termos do CDC e da Lei nº 12.414/2011; 4) o consentimento do consumidor não é requisito indispensável à utilização desse sistema, não obstante, a ele é ressalvado os direitos de acesso e de esclarecimento no que concerne a suas informações

---

503 "RECURSO ESPECIAL REPRESENTATIVO DE CONTROVÉRSIA (ART. 543-C DO CPC). TEMA 710/STJ. DIREITO DO CONSUMIDOR. ARQUIVOS DE CRÉDITO. SISTEMA 'CREDIT SCORING'. COMPATIBILIDADE COM O DIREITO BRASILEIRO. LIMITES. DANO MORAL.
I - TESES: 1) O sistema 'credit scoring' é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito).
2) Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo).
3) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011.
4) Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas.
5) O desrespeito aos limites legais na utilização do sistema 'credit scoring', configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.
II - CASO CONCRETO: 1) Não conhecimento do agravo regimental e dos embargos declaratórios interpostos no curso do processamento do presente recurso representativo de controvérsia;
2) Inocorrência de violação ao art. 535, II, do CPC.
3) Não reconhecimento de ofensa ao art. 267, VI, e ao art. 333, II, do CPC.
4) Acolhimento da alegação de inocorrência de dano moral 'in re ipsa'.
5) Não reconhecimento pelas instâncias ordinárias da comprovação de recusa efetiva do crédito ao consumidor recorrido, não sendo possível afirmar a ocorrência de dano moral na espécie.
6) Demanda indenizatória improcedente.
III - NÃO CONHECIMENTO DO AGRAVO REGIMENTAL E DOS EMBARGOS DECLARATÓRIOS, E RECURSO ESPECIAL PARCIALMENTE PROVIDO." BRASIL. Superior Tribunal de Justiça. **Acórdão no REsp nº 1.419.697/RS**. Relator: Paulo de Tarso Sanseverino. Publicado no DJe de 17 nov. 2014. RSTJ vol. 236, p. 368. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201303862850&dt_publicacao=17/11/2014>. Acesso em: 30 jul. 2017.

constantes nos bancos de dados da empresa, bem como o direito de saber a fonte das mesmas; 5) a inobservância dos limites legais na utilização do *credit scoring* configura abuso de direito, ensejando a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte das informações e do consulente nos casos de utilização de informações excessivas e/ou sensíveis, ou no caso de recusa de crédito com base em dados desatualizados ou incorretos[504].

Com grande acerto a decisão reconheceu a licitude, *a priori,* da utilização das sistemáticas de "escoragem", em específico o mecanismo do *credit scoring*. Inclusive, merece destaque a humildade do Ministro Sanseverino no que toca à realização de audiência pública, a fim de ganhar maior familiaridade com esse método de avaliação dos riscos de crédito[505].

Nada obstante, entende-se pertinente tecer duas ressalvas à decisão do Tribunal Superior. A primeira delas recai no fato de que, em nenhum momento, a decisão enfrenta a questão da possibilidade de se requerer a revisão da decisão de negativa do crédito prevista no art. 5º, inciso VI da Lei nº 12.414/2011[506]. Trata-se de dispositivo que, apesar do conteúdo sensivelmente distinto daquele previsto no ordenamento europeu[507], assemelha-se muito à proteção trazida pelo novo regulamento de proteção de dados pessoais da comunidade europeia[508], e que não se tem, ao certo, um parâmetro para a produção de seus efeitos.

---

[504] BRASIL. Superior Tribunal de Justiça. **Acórdão no REsp nº 1.419.697/RS**. Relator: Paulo de Tarso Sanseverino. Publicado no DJe de 17 nov. 2014. RSTJ vol. 236, p. 368. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201303862850&dt_publicacao=17/11/2014>. Acesso em: 30 jul. 2017. p. 36-37

[505] LUPION, Ricardo. O caso do sistema "*Credit Scoring"* do Cadastro Positivo. **Revista da AJURIS**, Porto Alegre, v. 42, n. 137, p. 431-449, mar. 2015.

[506] "Art. 5º São direitos do cadastrado: VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; [...]." BRASIL. Lei nº 12.414, de 10 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União**, Brasília, 10 jun. 2011. p. 2. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 30 out. 2017.

[507] Enquanto o dispositivo brasileiro permite apenas um pedido de revisão, a legislação europeia permite que o titular dos dados não se sujeite a uma decisão baseada exclusivamente no tratamento automatizado dos dados.

[508] O Considerado 71 do Regulamento (UE) 2016/679 dispõe que: "O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrônica ou práticas de recrutamento eletrônico sem qualquer intervenção humana". UNIÃO Europeia. Parlamento e Conselho.

A segunda ressalva, por sua vez, refere-se à questão da prescindibilidade do consentimento do consumidor para a utilização do sistema do *credit scoring.* Em que pese a Lei nº 12.414/2011 prever expressamente a necessidade do consentimento para fins de cadastros para análise do risco de crédito (art. 4º, *caput*)[509], o STJ entendeu que "[...] não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico", ainda que esse sistema deva obedecer às disposições previstas tanto no CDC como na Lei do Cadastro Positivo[510].

Nada obstante, da leitura do art. 5º da lei se depreende que são direitos do titular dos dados: "[...] IV – conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial"; bem como "[...] V – ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento"[511]. Destarte, para que se prescinda do consentimento do cadastrado, a utilização desse sistema automatizado de tratamento de dados deve estar prevista expressamente no termo de consentimento informado que anui com a abertura do cadastro. Não sendo esse o caso, faz-se necessária a obtenção de um novo consentimento para operacionalização desses mecanismos de avaliação de risco, sob pena de se violar o princípio do consentimento informado. Uma vez dado o consentimento, contudo, não se faz necessária a realização de um novo para utilizações posteriores do sistema.

Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

509 "Art. 4º A abertura de cadastro requer autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada." BRASIL. Lei nº 12.414, de 10 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União**, Brasília, 10 jun. 2011. p. 2. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 30 out. 2017.

510 Id. Superior Tribunal de Justiça. **Acórdão no REsp nº 1.419.697/RS**. Relator: Paulo de Tarso Sanseverino. Publicado no DJe de 17 nov. 2014. RSTJ vol. 236. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201303862850&dt_publicacao=17/11/2014>. Acesso em: 30 jul. 2017.

511 BRASIL. Lei nº 12.414, de 10 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União**, Brasília, 10 jun. 2011. p. 2. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 30 out. 2017.

Inclusive, é justamente o princípio do consentimento que legitima esse tipo de tratamento de dados pessoais, ao garantir que o indivíduo exerça seu direito à autodeterminação informativa[512]. Traçando um comparativo com a LOPD (Lei Orgânica de Proteção de Dados) espanhola, constata-se a importância de um marco regulatório específico a propósito da proteção dos dados pessoais. Na experiência espanhola, o art. 5º da LOPD dispõe que o titular dos dados deve ser informado não só sobre a existência e a finalidade do tratamento de informações pessoais, mas o caráter facultativo ou obrigatório do fornecimento desses dados e os possíveis reflexos desse consentimento ou recusa ao tratamento em relação ao contrato que se pretende firmar[513].

Ainda em termos de escoragem na Espanha, destaca-se que o direito de oposição a decisões automatizadas previstas no novo regulamento de proteção de dados europeu não seria, *a priori*, aplicável. Tal direito se limita a decisões tomadas exclusivamente por meios automatizados, e, no caso dos sistemas de análise e concessão de crédito, não só os mecanismos de escoragem, mas os próprios ficheiros são apenas algumas das ferramentas (e não a única) utilizadas para a análise de concessão de crédito[514].

No cenário brasileiro, percebe-se que a proteção do consumidor é notoriamente reparativa e não preventiva e acaba exigindo que a pessoa lesada recorra ao judiciário para a reparação do dano sofrido. Trata-se de construção notoriamente insatisfatória que não atende a realidade mundial, onde é possível identificar uma atuação administrativa estatal a partir de agências de proteção de dados (modelo europeu de proteção de dados).

Apenas a título de exemplo, aponta-se que o estudo dirigido pela *Consumer Federation of America* (CFA) e pela *National Credit Reporting Association* (NCRA), em 2002, tendo como objeto 500.000 *credit scores* e 1.700 *credit reports* apontara que 20% dos consumidores americanos foram prejudicados em suas classificações

---

[512] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

[513] Inclusive há uma preocupação no que toca ao acesso a essas informações, que só poderão ser fornecidas a um terceiro com quem se pretenda realizar um contrato de crédito ou que envolva uma relação creditícia (vide arts. 29, 37 e ss. da LOPD espanhola). ARIAS, Ignacio San Martín. **Protección de datos en el crédito al consumo**. Madrid: Thomson Reuters, 2015.

[514] ARIAS, Ignacio San Martín. **Protección de datos en el crédito al consumo**. Madrid: Thomson Reuters, 2015.

nas categorias de riscos devido a *scores* imprecisos. A pesquisa demonstrou, ainda, que o prejuízo gerado chegava aos U$ 124.000,00 por consumidor, nos casos de crédito imobiliário (hipoteca)[515]. Tal quadro demonstra a necessidade de uma atuação proativa das próprias empresas, a fim de reduzir o risco no uso dessas ferramentas, bem como do próprio Estado em termos de fiscalização desse tipo de mecanismo.

Para além do caso do *Credit Scoring*, a obrigatoriedade do fornecimento de dados é aspecto preocupante à vulnerabilidade do consumidor, enquanto acirra a assimetria informacional entre as partes, e a própria fragilidade do instituto do consentimento informado, uma vez que esse se torna um requisito ao acesso a determinados bens ou serviços. A esse respeito, Rodotà[516] aponta que ganha especial relevância, nesse jogo de interesses, a figura daqueles indivíduos que podem sofrer uma "perda de dignidade", ou de autonomia quando o acesso a determinados bens e serviços é condicionado ao consentimento de fornecimento de informações pessoais. Segundo o autor, nesses casos é preciso

> [...] registrar de forma realista os limites do consentimento individual, inevitáveis quando em presença de fortes desníveis de poder nas relações de mercado, e de determinar os *standards* mínimos para a proteção efetiva de direitos fundamentais.[517]

Outra temática também sensível aos mecanismos de *profiling,* no âmbito do direito do consumidor, é a questão do *marketing* e da publicidade. O já referido modelo de economia flexível demandou uma alteração na lógica não só de produção, mas do *marketing*, esse também passou de um público de massas para grupos menores, com algum tipo de identidade (e identificação), ou até mesmo consumidores individualizados[518]. Nesse sentido, a própria dinâmica da sociedade

---

[515] **CREDIT Score Accuracy and Implications for Consumers**. December 17, 2002. Disponível em: <http://www.consumerfed.org/pdfs/121702CFA_NCRA_Credit_Score_Report_Final.pdf>. Acesso em: 14 nov. 2017.

[516] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 101.

[517] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 101-102.

[518] "Diferentemente da produção de massa, o modelo flexível compreende que as empresas devem investir na diferenciação dos produtos e serviços para adquirir vantagens competitivas e aumentar a lucratividade. Por consequência, tal concepção de produção exige uma alteração também da

da informação enseja novos meios de se atingir o consumidor. O fluxo de informações possibilita novos meios de seleção do público-alvo, a partir de novas formas de abordagem desse público, notadamente através do chamado *target marketing* ou *marketing* direcionado.

Nesse aspecto, é preciso levar em consideração a própria estrutura de interação social nessa sociedade em rede. Tomando-se como base a *Web* 2.0, também chamada de *Web* participativa, identifica-se que o próprio usuário é o gerador do conteúdo, especilamente a partir do compartilhamento de suas ideias e de suas informações pessoais[519]. Tal modelo não exclui, mas se soma ao anterior, em que o usuário acessa algum conteúdo por meio de conexão a um *site* ou um *blog*, porém até mesmo na *Web* clássica (*Web* 1.0) o usuário acaba fornecendo dados pessoais a cada *click* que realiza[520].

A tendência e, até mesmo, o ímpeto de auto-exposição[521], são encarados pelo mercado como uma oportunidade para a criação de um novo nicho no mercado. Retomando a percepção de Rodotà, no sentido de a própria utilização de bens e serviços servir como fonte de informações pessoais dos usuários, passível de tratamento para diversas finalidades[522], percebe-se na construção de aplicativos "grátis" uma nova logística para a geração de lucro.

Tomando o *Facebook* e o *WhatsApp* como exemplo (ou até mesmo o *Google*), é possível verificar que a remuneração dessas ferramentas não advém de uma contraprestação em espécie do usuário. Sua renda, na verdade, decorre da

---

forma de realização do marketing. Afinal, o marketing de massa convinha para uma produção em massa. Já uma produção diferenciada e segmentada pressupõe igualmente um marketing diferenciado e segmentado." MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online. p. 87.

519 EX2. **Web 1.0, Web 2.0 e Web 3.0...** Enfim o que é Isso? 2013. Disponível em: <http://www.ex2.com.br/blog/web-1-0-web-2-0-e-web-3-0-enfim-o-que-e-isso/>. Acesso em: 28 mar. 2017.

520 Os modos de coleta dos dados pessoais durante a navegação serão enfrentados no decorrer deste capítulo.

521 BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

522 RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

exploração publicitária que circunscreve sua utilização[523]. Ou seja, o consumidor não paga com dinheiro, mas com a disponibilização de seus dados pessoais.

Os meios de coleta dessas informações são os mais variados. Hoje é comum a oferta de sorteios, brindes, benefícios ou prêmios para aqueles que se dispõem ao preenchimento de uma ficha de cadastro. Os cartões fidelidades, comuns desde supermercados até loja de roupas, também concedem benefícios ao seu usuário – descontos, meios facilitados de pagamento ou pontos –, a fim de possibilitarem o monitoramento individualizado do consumidor[524].

A esse respeito, Mendes[525] aponta como principais fontes de informações pessoais dos consumidores: 1. as transações comerciais, caso em que a coleta deve observar invariavelmente os princípios da finalidade e do consentimento informado; 2. os censos e registros públicos – caso em que o uso dessas informações para fins de *marketing* é uma afronta em potencial ao princípio da finalidade; 3. as pesquisas de mercado e de estilo de vida – sendo a primeira marcada pelo anonimato e a segunda, geralmente utilizada por empresas que se valem do *geomarketing,* é marcada por uma exatidão e precisão de dados questionável; 4. sorteios e concursos – situações que na prática denunciam a falta de observância do princípio do consentimento informado; 5. comercialização de dados; e 6. as tecnologias de vigilância da internet. Toda essa coleta sistemática de informações pessoais gera um nicho próprio do mercado que gira em torno dos dados pessoais, especialmente a partir da chamada publicidade comportamental[526]. Trabalha-se, assim, uma ideia

---

523 "*The current economic drivers of big data usage are large companies with access to complete infrastructures. These include sectors like advertising at Internet companies and sensor data from large infrastructures (e.g. smart grids or smart cities) or for complex machinery (e.g. airplane engines). In the latter examples, there is a trend towards even closer integration of data usage at large companies as the big data capabilities remain with the manufactures (and not the customers), e.g. when engines are only rented and the big data infrastructure is owned and managed by the manufacturers.*" CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang (Org.). **New horizons for a data-driven economy**: a roadmap for usage and exploitation of big data in Europe. Cham (Suiça): Springer Open, 2016. p. 146.

524 ELMER, G. **Profiling machines**: mapping the personal information economy. Cambridge, Mass: The MIT Press, 2004.

525 MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online. p. 95 et seq.

526 "*The analysis of prevalent trends in commercial and popular iconography (on screen, in print, or on strategically placed billboards) is placed within a digitized and networked information economy that increasingly requires consumers to exchange demographic and psychographic information for commodities and services. In an era where two-thirds of all commercial campaigns ask for some degree of feedback from consumers (via sweepstakes entry forms, bar-coded discounts cards, special club enrollments forms, online membership forms, and so on)* […]." ELMER, G. **Profiling**

de *marketing one-to-one,* trabalhada na coleta de informações pessoais e na interatividade com o consumidor[527].

Essa alta exposição do consumidor pode, entrementes, ensejar diversos problemas, dentre os quais destacam-se: a clonagem de cartões de crédito (*identity theft)*[528], o lixo eletrônico (*junk mail*), e as ligações inconvenientes, ou as mensagens de texto de *telemarketing*[529]. Em contrapartida, a utilização de dados pessoais pelas empresas permite não só a criação de novos mercados, como um aprimoramento dos já existentes. Ferramentas e métodos estatísticos capazes de processar grandes volumes de informação permitem uma abordagem diferenciada de *marketing* direcionado (*user-especific advertisement*), além de pesquisas de mercado em geral[530].

Nessa seara, o mercado baseado em informações pessoais se apresenta como uma dualidade complexa. O que começa com "[...] 'recompensas' (como uma camiseta grátis por solicitações de cartões de crédito) pode facilmente se tornar 'castigos' (como lixo eletrônico, irritantes pedidos em ligações, fraude de identidade e comprometimento de crédito)"[531].

---

machines: mapping the personal information economy. Cambridge, Mass: The MIT Press, 2004. p. 4.

527 "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 a maior quantidade de clientes possível. O marketing "*one-to-one*" insere-se em uma estratégia mais ampla de relacionamento entre a empresa e o cliente, conhecida como *customer relation management* – CRM (gerenciamento da relação com o cliente)." MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online. p. 89-90.

528 A propósito do *Identity Theft* ver: GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010.

529 BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Elaboração Danilo Doneda. Brasília: SDE/DPDC, 2010. Disponível em: <http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf>. Acesso em: 23 jul. 2017.

530 CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang (Org.). **New horizons for a data-driven economy**: a roadmap for usage and exploitation of big data in Europe. Cham (Suiça): Springer Open, 2016.

531 "*What's more, given the ubiquity and complexity of today's personal-information economy, initial 'rewards' (such as free T-shirts for credit-card applications) can easily later turn into 'punishments' (such as junk mail, irritating phone solicitations, identity fraud, and compromised and damaged credit). Such rewards and punishments of consumer profiling indicate the continuous and increasing attempts of producers to improve both quantitatively and qualitatively their consumer 'intelligence' gathering – to track and integrate the everyday behavior of consumers into other*

Em termos de internet, o *online profiling* é o principal mecanismo para operacionalização do *target marketing*[532], usualmente por meio do *online advertising* e do *online behavioral advertising*. Em junho de 2000, a *Federal Trade Comission* (FTC), cujo enfoque é na autorregulação, elaborou um relatório específico sobre a prática do *online profiling*, realizando uma contraposição entre os benefícios e os problemas que essa atividade apresenta[533].

Grande parte dessa publicidade *online* é feita por meio dos *banner ads*, que aparecem nas margens das páginas da internet, contendo alguma mensagem publicitária. Normalmente, porém, não é o provedor do conteúdo da página visitada que seleciona qual o anúncio exposto por esses *banners*, mas uma empresa que trabalha especificamente com *network advertising* (publicidade na internet). Essa não só fornece o anúncio constante do *banner*, como coleta dados a propósito do consumidor, a fim de selecionar qual publicidade será exposta para determinado indivíduo[534].

Tal publicidade comportamental (*behavioral advertising*) é objeto de grande controvérsia quanto aos limites de sua utilização, por gerar inúmeros riscos à figura do consumidor e por esbarrar na garantia constitucional de inviolabilidade da comunicação de dados[535]. Segundo Mendes[536], sua utilização deveria ser condicionada à obtenção de um consentimento claro, informado, específico e de fácil revogação, bem como à adoção de medidas técnicas de segurança como a

---

production, sales, and distribution data." [Tradução livre]. ELMER, G. **Profiling machines**: mapping the personal information economy. Cambridge, Mass: The MIT Press, 2004. p. 8.

[532] De 1996 a 1999 a receita proveniente do *online advertising* nos EUA cresceu de 301 milhões de dólares para 4,62 bilhões de dólares, ganhando uma projeção de 11,5 bilhões de dólares para 2003. FTC. **Online profiling**: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commission-report-congress-june-2000/onlineprofilingreportjune2000.pdf>. Acesso em: 26 nov. 2016.
Em 2017, a renda proveniente de *digital advertising* chegou à marca de 19.6 bilhões de dólares só no primeiro quadrimestre do ano, sendo que há uma tendência de crescimento desse mercado de aproximadamente 23% ao ano. IAB. Internet Advertising Revenue Report Conducted by PricewaterhouseCoopers (PWC). **Digital Advertising Revenues Hit $19.6 Billion in Q1 2017, Climbing 23% Year-Over-Year, According to IAB**. New York: 14 jun. 2017. Disponível em: <https://www.iab.com/news/adrevenues-hit-19-6b/>. Acesso em: 7 ago. 2017.

[533] FTC, op. cit.

[534] FTC. **Online profiling**: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commission-report-congress-june-2000/onlineprofilingreportjune2000.pdf>. Acesso em: 26 nov. 2016.

[535] MENDES, Laura Schertel. O diálogo entre o marco civil da internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 106, p. 37-69, jul./ago. 2016.

[536] Ibid.

anonimização e a pseudononimização, a fim de resguardar os direitos do consumidor.

No que toca à coleta de informações pessoais, os *cookies*[537] e os *web bugs*[538] são mecanismos que permitem rastrear as ações do indivíduo na internet. Eles permitem a coleta de dados como: quais páginas foram visitadas pelo consumidor, a duração de cada sessão na internet, qual foi tempo gasto em cada página, termos pesquisados em ferramentas de busca, compras *online,* e quais anúncios foram "clicados"[539].

Para além desses dois instrumentos (*cookies* e os *web bugs*), ainda é possível mencionar os *mail bugs*[540] e o *spyware*[541]. Eles também se prestam à coleta de informações sobre o usuário de forma praticamente desapercebida, sendo uma

---

[537] "*A cookie is a small text file placed on a consumer's computer hard drive by a Web server. The cookie transmits information back to the server that placed it and, in general, can be read only by that server*." FTC, op. cit., p. 3.
Acerca dos *cookies* e dos diferentes tipos existentes ver: FULLANA, Antonia Paniza. Protección de datos, cookies y otros instrumentos de navegación. In: COMESAÑA, Julio Costas et al. **Publicidad, defensa de la competencia y protección de datos**. Pamplona (Espanha): Thomson Reuters, 2010. p. 32-57.

[538] "*'Web bugs' are also known as 'clear GIFs' or '1-by-1 GIFs.' Web bugs are tiny graphic image files embedded in a Web page, generally the same color as the background on which they are displayed which are invisible to the naked eye. The Web bug sends back to its home server (which can belong to the host site, a network advertiser or some other third party): the IP (Internet Protocol) address of the computer that downloaded the page on which the bug appears; the URL (Uniform Resource Locator) of the page on which the Web bug appears; the URL of the Web bug image; the time the page containing the Web bug was viewed; the type of browser that fetched the Web bug; and the identification number of any cookie on the consumer's computer previously placed by that server. Web bugs can be detected only by looking at the source code of a Web page and searching in the code for 1-by-1 IMG tags that load images from a server different than the rest of the Web page. At least one expert claims that, in addition to disclosing who visits the particular Web page or reads the particular email in which the bug has been placed, in some circumstances, Web bugs can also be used to place a cookie on a computer or to synchronize a particular email address with a cookie identification number, making an otherwise anonymous profile personally identifiable*." FTC, op. cit., p. 3.

[539] FTC. **Online profiling**: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commission-report-congress-june-2000/onlineprofilingreportjune2000.pdf>. Acesso em: 26 nov. 2016.

[540] Com estrutura muito semelhante as dos *web bugs*, os *mail bugs* também são "imagens" que passam desapercebidas ao usuário, para fins de coleta de informações do mesmo para empresas publicitárias, porém eles não são associados a uma página ou a um arquivo, mas a um correio eletrônico (e-mail). Trata-se de instrumento frequentemente utilizado para verificar a veracidade de um e-mail, inclusive para fins de envio de *junk mail*. FULLANA, Antonia Paniza. Protección de datos, cookies y otros instrumentos de navegación. In: COMESAÑA, Julio Costas et al. **Publicidad, defensa de la competencia y protección de datos**. Pamplona (Espanha): Thomson Reuters, 2010. p. 32-57.

[541] Os *spyware,* como o próprio nome diz, consiste em um programa espião. O programa é instalado e executado sem o conhecimento do usuário, servindo, normalmente, para coletar informações inseridas no computador que está instalado, porém sem danificar o sistema, para além desse propósito, o *spyware* já fora utilizado para controle de *copyrights* por empresas como a Sony. A esse respeito ver: Ibid.

potencial ameaça à privacidade do usuário e ao seu direito à proteção de dados pessoais[542].

Interessante notar que existem formas de *network advertising* anonimizadas, em que os perfis traçados estão ligados a um número constante de um *cookie* ou ao computador em si (e não a um indivíduo em específico). Essas informações são chamadas de *non-personally indetifiable information* (*non-PII*). Para além dessas, existem aquelas em que o consumidor está devidamente identificado, as chamadas *personally identifiable information* (*PII*) operam quando a atividade do usuário na internet é associada à identificação do consumidor. Essa identificação pode se dar pelo fornecimento por parte de um *site*, por exemplo, o *Facebook*, das informações pessoais de determinado indivíduo à empresa publicitária, ou quando os dados pessoais são processados pelo *site* de forma a armazenar e incorporar essas informações na própria URL *string*, sendo automaticamente transmitida para a empresa publicitária[543].

Nada obstante, ainda que se trate de *non-PII*, precisa-se trabalhar com as noções de pessoa identificada e pessoa identificável. Ou seja, dependendo da informação ou da forma como essa é armazenada, o fato de ela não estar diretamente relacionada à identidade de uma pessoa não afasta o seu caráter de dado pessoal. Quando for possível adquirir informações adicionais sobre aquele indivíduo sem um esforço desmesurado, e que o cruzamento de tais informações permita a identificação do titular dos dados, considera-se aquela informação um dado pessoal, vez que ele diz respeito a uma pessoa identificável[544].

---

[542] Ibid.

[543] "*The information gathered by network advertisers is often, but not always, anonymous, i.e., the profiles are frequently linked to the identification number of the advertising network's cookie on the consumer's computer rather than the name of a specific person. This data is generally referred to as non-personally identifiable information ('non-PII'). In some circumstances, however, the profiles derived from tracking consumers activities on the Web are linked or merged with personally identifiable information ('PII'). This generally occurs in one of two ways when consumers identify themselves to a Web site on which the network advertiser places banner ads.15 First, the Web site to whom personal information is provided may, in turn, provide that information to the network advertiser. Second, depending upon how the personal information is retrieved and processed by the Web site, the personally identifying information may be incorporated into a URL string16 that is automatically transmitted to the network advertiser through its cookie*." FTC. **Online profiling**: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commission-report-congress-june-2000/onlineprofilingreportjune2000.pdf>. Acesso em: 26 nov. 2016. p. 4-5.

[544] "[...] • Consideram-se dados pessoais os dados relativos a uma pessoa identificada ou, pelo menos, identificável: o titular dos dados ou a pessoa em causa

Tomando como exemplo os *cookies* anônimos (quando não se identifica o usuário), é preciso verificar quais são os dados armazenados e coletados por esse dispositivo. Por exemplo, se esse *cookie* possibilita a coleta do IP (estática) do computador do usuário, o Grupo de Trabalho sobre o artigo 29 já se manifestou no sentido de que se está diante de dados pessoais[545].

Uma vez coletada a informação, ela pode ser cruzada com outras constantes do próprio banco de dados da empresa de publicidade *online* ou com informações provenientes de terceiros. Essas informações tratadas resultam em um

> [...] perfil detalhado que busca prever os gostos, as necessidades, os hábitos de compras do consumidor e permite que os computadores das empresas de publicidade tomem decisões em frações de segundo sobre como dirigir anúncios diretamente direcionadas aos interesses específicos daquele consumidor.[546]

• Considera-se que uma pessoa é identificável se for possível obter informações adicionais, sem um esforço desproporcionado, que permitam a identificação do titular dos dados." AGÊNCIA dos Direitos Fundamentais da União Europeia. **Manual da Legislação Europeia sobre a Proteção de Dados**. Luxemburgo: Serviço das Publicações da União Europeia, 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 05 out. 2016. p. 36.

545 "[…] *el Grupo de Trabajo sobre el artículo 29 en su Dictamen sobre cuestiones de protección de datos de 4 de abril de 2008 en relación con los buscadores afirma que: <<Cuando una cookie contiene una ID de usuario única, esta ID es claramente un dato personal. La utilización de cookies permanentes o de dispositivos similares con una ID de usuario permite el seguimento de los usuários de un ordenador concreto incluso cuando se utilizan direcciones Ip dinâmicas. Los datos de comportamento que se generan mediante la utilización de estos dispositivos permiten centrarse más en las características personales de la persona em cuestión>>.*" FULLANA, Antonia Paniza. Protección de datos, cookies y otros instrumentos de navegación. In: COMESAÑA, Julio Costas et al. **Publicidad, defensa de la competencia y protección de datos**. Pamplona (Espanha): Thomson Reuters, 2010. p. 32-57. p. 40.

546 "*Once collected, consumer data can be analyzed and combined with demographic and 'psychographic' 18 data from third-party sources, data on the consumer's offline purchases, or information collected directly from consumers through surveys and registration forms. This enhanced data allows the advertising networks to make a variety of inferences about each consumer's interests and preferences. The result is a detailed profile that attempts to predict the individual consumer's tastes, needs, and purchasing habits and enables the advertising companies' computers to make splitsecond decisions about how to deliver ads directly targeted to the consumer's specific interests*." [Tradução livre]. FTC. **Online profiling**: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commission-report-congress-june-2000/onlineprofilingreportjune2000.pdf>. Acesso em: 26 nov. 2016.

A esse respeito, de grande valia é a advertência de Fullana[547], no sentido de que, dependendo do tipo de utilização da internet, os próprios dados pessoais podem figurar como dados sensíveis. Trazendo o exemplo do histórico de navegação, depende dos *sites* visitados pelo usuário é possível identificar sua orientação política, filosófica ou até mesmo religiosa, o que demanda toda uma lógica de proteção distinta.

Forçoso notar, porém, que os *cookies* não só servem às empresas de *online advertising*, sendo úteis, também, ao próprio consumidor. A partir deles, é possível o armazenando de diversas informações que se prestam a facilitar a interação do usuário com as páginas e os serviços oferecidos *online*, inclusive para fins de personalização dos serviços e de sugestões para o usuário, além de permitir que o provedor otimize o *layout* das páginas e o fornecimento do serviço de forma geral[548].

Em termos de Brasil, desconhece-se qualquer disposição legal que enfrente a temática dos *cookies,* dos *web bugs* e similares. Buscando amparo no direito alienígena, contudo, é possível identificar nos Considerandos 24 e 25 da Diretiva 2002/58 do Conselho Europeu que o equipamento terminal e as informações nele constantes "[...] constituem parte integrante da esfera privada dos utilizadores e devem ser protegidos", sendo a que a "[...] utilização desses dispositivos [como *spyware* e *web bugs*] deverá ser autorizada unicamente para fins legítimos, com o conhecimento dos utilizadores em causa" (Considerando 24)[549]. Ademais, garante-

---

[547] FULLANA, Antonia Paniza. Protección de datos, cookies y otros instrumentos de navegación. In: COMESAÑA, Julio Costas et al. **Publicidad, defensa de la competencia y protección de datos**. Pamplona (Espanha): Thomson Reuters, 2010. p. 32-57.

[548] "*Cookies can store these names and passwords so that consumers do not need to sign in each time they visit the site. In addition, many sites allow consumers to set items aside in an electronic shopping cart while they decide whether or not to purchase them; cookies allow a Web site to remember what is in a consumer's shopping cart from prior visits. Cookies also can be used by Web sites to offer personalized home pages or other customized content with local news and weather, favorite stock quotes, and other material of interest to individual consumers*." FTC, op. cit., p. 8-9.

[549] "(24) O equipamento terminal dos utilizadores de redes de comunicações electrónicas e todas as informações armazenadas nesse equipamento constituem parte integrante da esfera privada dos utilizadores e devem ser protegidos ao abrigo da Convenção Europeia para a Protecção dos Direitos Humanos e das Liberdades Fundamentais. Os denominados «gráficos espiões», «programas-espiões», («spyware»), «gráficos-espiões» («web bugs») e «identificadores ocultos» («hidden identifiers») e outros dispositivos análogos podem entrar nos terminais dos utilizadores sem o seu conhecimento a fim de obter acesso a informações, armazenar informações escondidas ou permitir a rastreabilidade das actividades do utilizador e podem constituir uma grave intrusão na privacidade desses utilizadores. A utilização desses dispositivos deverá ser autorizada unicamente para fins legítimos, com o conhecimento dos utilizadores em causa." UNIÃO Europeia. Parlamento Europeu e Conselho. Directiva 2002/58/CE, de 12 de julho de 2002. Relativa ao tratamento de

se aos usuários a possiblidade de "[...] recusarem que um testemunho de conexão (<<cookie>>) ou um outro dispositivo análogo seja armazenado no seu equipamento terminal (Considerando 25)"[550].

Ainda que inexistente lei federal, os Estados Unidos também tendem a uma regulação semelhante à europeia, proibindo-se a instalação de *softwares* que alterem o computador ou que coletem informações pessoais do usuário, salvo se atendidos diversos requisitos que buscam resguardar a *user's privacy*. Destacam-se, nesse sentido, as leis estaduais *Spyware Control Act*, de Utah e a *Consumer Protection Against Computer Spyware Act*, da Califórnia, vez que pioneiras na matéria[551].

Merecem atenção, ainda, outros mecanismos de tratamento da informação que não o *profiling*. O *data warehousing* (depósito de dados) consiste em um sistema informatizado capaz de armazenar uma enorme quantidade de dados de forma ordenada, facilitando a análise e o cruzamento dessas informações de caráter pessoal, ou seja, é "[...] uma grande base de dados, integrada, orientada pelo sujeito, com dimensão temporal, e não volátil", que permite a organização dos dados

---

dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). **Jornal Oficial das Comunidades Europeias**, L 201/37. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT>. Acesso em: 25 jul. 2017.

550 "(25) Todavia, esses dispositivos, por exemplo os denominados testemunhos de conexão («cookies»), podem ser um instrumento legítimo e útil, nomeadamente na análise da eficácia da concepção e publicidade do sítio web, e para verificar a identidade dos utilizadores que procedem a transacções em linha. Sempre que esses dispositivos, por exemplo os testemunhos de conexão («cookies»), se destinem a um fim legítimo, como por exemplo a facilitar a prestação de serviços de informação, a sua utilização deverá ser autorizada, na condição de que sejam fornecidas aos utilizadores informações claras e precisas, em conformidade com a Directiva 95/46/CE, acerca da finalidade dos testemunhos de conexão («cookies») ou dos dispositivos análogos por forma a assegurar que os utilizadores tenham conhecimento das informações colocadas no equipamento terminal que utilizam. Os utilizadores deveriam ter a oportunidade de recusarem que um testemunho de conexão («cookie») ou um dispositivo análogo seja armazenado no seu equipamento terminal. Tal é particularmente importante nos casos em que outros utilizadores para além do próprio têm acesso ao equipamento terminal e, consequentemente, a quaisquer dados que contenham informações sensíveis sobre a privacidade armazenadas no referido equipamento. A informação e o direito a recusar poderão ser propostos uma vez em relação aos diversos dispositivos a instalar no equipamento terminal do utente durante a mesma ligação e deverá também contemplar quaisquer outras futuras utilizações do dispositivo durante posteriores ligações. As modalidades para prestar as informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão conviviais quanto possível. O acesso ao conteúdo de um sítio web específico pode ainda depender da aceitação, com conhecimento de causa, de um testemunho de conexão («cookie») ou dispositivo análogo, caso seja utilizado para um fim legítimo." Ibid.

551 FULLANA, Antonia Paniza. Protección de datos, cookies y otros instrumentos de navegación. In: COMESAÑA, Julio Costas et al. **Publicidad, defensa de la competencia y protección de datos**. Pamplona (Espanha): Thomson Reuters, 2010. p. 32-57.

com base nos critérios que melhor atendem os interesses das empresas e a utilização de inúmeras técnicas de tratamento de dados[552].

O *data mining* (mineração de dados) é uma das técnicas que se pode aplicar no *data warehousig* ou diante de grandes volumes de dados (*Big Data*). Trata-se de ferramenta capaz de selecionar rapidamente informações úteis em meio a inúmeras nem sempre utilizáveis, detectando padrões de informação, permitindo sua classificação. Trata-se de mecanismo de processamento de dados com grande potencial de uso, uma vez que permite uma otimização e rapidez no tratamento e, por isso mesmo, imbuído de grande risco[553].

O *Online Analytical Processing* – OLAP – Processamento Analítico *Online* – é outra técnica aplicável em *data warehouses.* Como o próprio nome anuncia, ela serve para análise de processamento de informações contidas em bancos de dados tanto para fins de pesquisas como para apresentação de informações que relacionem os dados de forma automatizada[554].

Por fim, a *Machine Learning* é uma espécie interdisciplinar de inteligência artificial, a *exemplo do Data Mining.* Comumente, a *machine learning* é tratada como a habilidade fazer com que computadores e máquinas em geral possam aprender, prescindindo de uma nova programação. Em que pese ser difícil diferenciar a *Data Mining* da *Machine Learning,* pode-se afirmar que a primeira "foca principalmente na análise e exploração enquanto [a segunda] foca em tomada de decisões"[555]. Vale lembrar que, mesmo que tais mecanismos de tratamento de dados pessoais não se confundam com o *profiling,* eles acabam compondo a ferramenta do profiling, vez

---

[552] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online. p. 108.

[553] Em razão de seu uso para fins de classificação e segmentação, Mendes chama atenção para os riscos na utilização dessa ferramenta e seu possível uso para fins discriminatórios. Ademais, a autora aponta que as possiblidades de uso desse mecanismo ainda não são compreendidas por completo, gerando riscos especialmente no que toca a transparência do tratamento e o princípio da finalidade. Ibid., p. 108.

[554] Ibid.

[555] DÖHMANN, Indra Spiecker Genannt; TAMBOU, Olivia; BERNAL, Paul; et. al. The Regulation of Commercial Profiling – A Comparative Analysis. **European Data Protection Law Review.** Berlin, v. 2, n. 4, p. 535-554, 2016. p. 538.

que proporcionam as informações necessárias para a criação de um perfil capaz de prever tendências ou comportamentos.[556]

Seguindo o raciocínio de dualidade entre benefícios e malefícios trazidos pelos incrementos tecnológicos, importa asseverar que o *online profiling,* geralmente, é o que subsidia a manutenção de páginas de conteúdo livre na internet. Outrossim, ele possibilita a criação de novos produtos e serviços e a atuação de pequenas empresas em novos nichos personalizados do mercado (criação de nichos empresariais). Contudo, ele é uma prática que passa praticamente desapercebida aos olhos do consumidor e que traz consigo uma gama de problemas em potencial[557].

O primeiro é a própria falta de transparência nesses mecanismos de coleta de informações pessoais, particularmente no que toca à própria existência desses mecanismos[558] e à própria extensão dos mesmos[559]. Outra questão inquietante é que a internet deixa de ser um espaço de atuação "anônima" para se tornar um em que todas as ações do usuário são monitoradas e gravadas. Em termos de consumo em si, o *online profiling* dá margem à prática do *weblining*, em que as condições (financeiras, de saúde etc.) do indivíduo vêm afetar as condições de acesso a determinados bens e serviços, inclusive havendo variação de preço para um mesmo produto[560].

---

[556] DÖHMANN, Indra Spiecker Genannt; TAMBOU, Olivia; BERNAL, Paul; et. al. The Regulation of Commercial Profiling – A Comparative Analysis. **European Data Protection Law Review.** Berlin, v. 2, n. 4, p. 535-554, 2016.

[557] FTC. **Online profiling**: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commission-report-congress-june-2000/onlineprofilingreportjune2000.pdf>. Acesso em: 26 nov. 2016.

[558] Em uma pesquisa realizada por volta dos anos 2000, a Comissão da FTC verificou que cerca de 57% das páginas na *Web* permitiam a inserção de *coookies* na página por terceiros, mas apenas 22% dos *sites* mencionavam que permitiam o uso de *cookies* ou outros mecanismos de coleta de dados, sendo que, se tomado como base os 100 maiores *sites* da internet, esses números subiam para 78% e 51%, respectivamente. Ibid.

[559] "*The second most persistent concern expressed by commenters was the extensive and sustained scope of the monitoring that occurs. Unbeknownst to most consumers, advertising networks monitor individuals across a multitude of seemingly unrelated Web sites and over an indefinite period of time. The result is a profile far more comprehensive than any individual Web site could gather. Although much of the information that goes into a profile is fairly innocuous when viewed in isolation, the cumulation over time of vast numbers of seemingly minor details about an individual produces a portrait that is quite comprehensive and, to many, inherently intrusive*." Ibid. p. 12.

[560] "*These commenters expressed concern that companies could use profiles to determine the prices and terms upon which goods and services, including important services like life insurance, are offered to individuals (for example, products might be offered at higher prices to consumers whose profiles indicate that they are wealthy, or insurance might be offered at higher prices to consumers whose profiles indicate possible health risks). This practice, known as 'weblining', raises many of*

Por fim, é de se notar que há um grande problema em relação ao consentimento no uso dos mecanismos de *online profiling*. A ausência de um mecanismo de objeção contra esse tratamento de dados pessoais ou de uma ferramenta de *opt-out* são contrapostas a uma realidade em que a maioria dos consumidores aparentam serem contrários à sua sujeição a esta prática[561].

3.4 PROTEÇÃO DE DADOS E O JUDICIÁRIO

A ausência de sistematização da disciplina da proteção de dados pessoais e a necessidade de um exercício interpretativo para sua identificação na Constituição Federal abre margem a interpretações temerárias dessa temática. Doneda[562] chama atenção às nuances de um sistema constitucional que garante, de forma expressa, a inviolabilidade da vida privada e da intimidade (art. 5º, inciso X) e a inviolabilidade da comunicação de dados (art. 5º, inciso XII), mas não a proteção dos dados em si. Segundo o autor, tais disposições abrem margem para uma leitura extremamente permissiva no que toca à utilização das informações pessoais, e é o que se identifica em diversos casos no judiciário brasileiro.

Em decisão do STF, de lavra do Ministro relator Sepúlveda Pertence, entendeu-se que não haveria uma garantia constitucional de inviolabilidade de

---

the same concerns that 'redlining' and 'reverse redlining' do in offline financial markets". Ibid., p. 13.

561 "*In particular, surveys show that consumers are not comfortable with profiling. A Business Week survey conducted in March of this year found that 89% of consumers are not comfortable having their browsing habits and shopping patterns merged into a profile that is linked to their real name and identity. If that profile also includes additional personal information such as income, driver's license, credit data and medical status, 95% of consumers express discomfort. Consistent with the comments received in connection with the Public Workshop, consumers are also opposed to profiling even when data are not personally identifiable: sixty-three percent of consumers say they are not comfortable having their online movements tracked even if the data is not linked to their name or real-world identity. An overwhelming 91% of consumers say that they are not comfortable with Web sites sharing information so that they can be tracked across multiple Web sites*." FTC. **Online profiling**: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commission-report-congress-june-2000/onlineprofilingreportjune2000.pdf>. Acesso em: 26 nov. 2016. p. 14-15.

562 BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Elaboração Danilo Doneda. Brasília: SDE/DPDC, 2010. Disponível em: <http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf>. Acesso em: 23 jul. 2017.

dados armazenados em computador. Na oportunidade do julgamento do RE 418416/SC, em 10/05/2006, o STF entendeu, por maioria, que "[...] a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador"[563].

Tal decisão fortalece a tese de Ferraz Júnior de que o ordenamento brasileiro tutela tão somente a inviolabilidade das comunicações, e não das informações em si[564], fragilizando toda uma construção doutrinária de proteção de dados pessoais

---

[563] "I. Decisão judicial: fundamentação: alegação de omissão de análise de teses relevantes da Defesa: recurso extraordinário: descabimento. Além da falta do indispensável prequestionamento (Súmulas 282 e 356), não há violação dos art. 5º, LIV e LV, nem do art. 93, IX, da Constituição, que não exige o exame pormenorizado de cada uma das alegações ou provas apresentadas pelas partes, nem que sejam corretos os fundamentos da decisão; exige, apenas, que a decisão esteja motivada, e a sentença e o acórdão recorrido não descumpriram esse requisito (v.g., RE 140.370, 1ª T., 20.4.93, Pertence, DJ 21.5.93; AI 242.237 - AgR, 1ª T., 27.6.00, Pertence, DJ 22.9.00). II. Quebra de sigilo bancário: prejudicadas as alegações referentes ao decreto que a determinou, dado que a sentença e o acórdão não se referiram a qualquer prova resultante da quebra do sigilo bancário, tanto mais que, dado o deferimento parcial de mandado de segurança, houve a devolução da documentação respectiva. III. Decreto de busca e apreensão: validade. 1. Decreto específico, que somente permitiu que as autoridades encarregadas da diligência selecionassem objetos, dentre aqueles especificados na decisão e na sede das duas empresas nela indicadas, e que fossem 'interessantes à investigação' que, no caso, tinha pertinência com a prática do crime pelo qual foi efetivamente condenado o recorrente. 2. Ademais não se demonstrou que as instâncias de mérito tenham invocado prova não contida no objeto da medida judicial, nem tenham valorado qualquer dado resultante da extensão dos efeitos da decisão determinante da busca e apreensão, para que a Receita Federal e a 'Fiscalização do INSS' também tivessem acesso aos documentos apreendidos, para fins de investigação e cooperação na persecução criminal, 'observado o sigilo imposto ao feito'. IV - Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a conseqüente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. **Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve 'quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial'. 4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270)**. V - Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º e 114, II; e Súmula 497 do Supremo Tribunal)." [Grifo nosso]. BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 418416/SC. Relator: Min. Sepúlveda Pertence. Brasília, DF, 10 de maio de 2006. **Diário da Justiça**, Brasília, DF, 10 maio 2006. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790>. Acesso em: 25 nov. 2017.

[564] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 88, p. 439-459, 1993. Disponível em: <https://www.revistas.usp.br/rfdusp/article/download/67231/69841>. Acesso em: 10 set. 2017.

em termos de Brasil. Ademais, o julgado evidencia a dificuldade de se tratar a temática dos dados pessoais, ainda analisada sob as dicotomias entre sigilo e transparência; e entre público e privado, as quais são insuficientes para dar conta da complexidade da temática[565], consoante já denunciado no primeiro capítulo deste trabalho ao se justificar a necessidade de diferenciação entre direito à privacidade e direito à proteção de dados pessoais.

Percebe-se que a problemática do tratamento de dados pessoais não é ignorada pelo Poder Judiciário. Em 1995, o Ministro Ruy Rosado de Aguiar já externava, em um de seus votos como relator do STJ (REsp 22.337-9/RS), sua preocupação com o fluxo de informações pessoais e o armazenamento dessas em bancos de dados informatizados. Segundo o Ministro:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da Informática e a possibilidade de controle unificados das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão, objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir ao Estado ou ao particular para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica.[566]

Nada obstante, a ausência de uma regulação específica do direito à proteção de dados pessoais e até mesmo o desconhecimento acerca do mesmo dão margem a decisões equivocadas, as quais fragilizam a proteção do indivíduo. Ao menos, é o que se depreende da decisão prolatada pelo TJRS na Apelação Cível nº

---

[565] BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Elaboração Danilo Doneda. Brasília: SDE/DPDC, 2010. Disponível em: <http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf>. Acesso em: 23 jul. 2017.

[566] Id. Superior Tribunal de Justiça. REsp 22.337-9/RS. Quarta Turma. Relator: Min. Ruy Rosado de Aguiar. Brasília, 13 de fevereiro de 1995. **Diário de Justiça**, Brasília, DF, 20 mar. 1995, p. 138. Disponível em: <https://ww2.stj.jus.br/processo/ita/documento/mediado/?num_registro=199200114466&dt_publicacao=20-03-1995&cod_tipo_documento=>. Disponível em: 01 nov. 2017. p. 138.

70069420503, julgada pela Sexta Câmara Cível, sob relatoria do Des. Ney Wiedemann Neto. Segue a ementa do aludido Acórdão:

> Apelação cível. Responsabilidade civil. Ação coletiva. SPC BRASIL. Marketing service. Divulgação de dados. Ausência de ofensa a direitos da personalidade. Hipótese em que os dados divulgados não são sigilosos, pois se trata de informação fornecida nas relações negociais cotidianas. Inexistência de dados sensíveis. Apelos providos.[567]

O processo teve origem em ação coletiva ajuizada pelo Ministério Público do Rio Grande do Sul (MPRS) em face da Confederação Nacional de Dirigentes Lojistas – SPC Brasil (posteriormente ingressou na lide a SERASA S/A enquanto terceira interessada, assumindo o papel de assistente litisconsorcial), sob a alegação de que a venda de dados e informações pessoais dos consumidores sem sua prévia anuência consistiria em prática abusiva. O MPRS sustentou, ainda, que essa prática tinha como público-alvo empresas que buscam a prospecção de clientes e que utilizam esses dados para fins de *marketing* e *telemarketing.* Dentre os dados comercializados é possível destacar: nome completo, número de telefone, endereço completo, número de documentos de identificação, data de nascimento, nomes dos pais (filiação), endereço de *e-mail*, dentre outros.

Em primeira instância, a ação foi julgada procedente[568]. Irresignadas com a sentença, a SPC Brasil e a SERASA S/A apelaram. Em segundo grau, a Sexta

---

[567] RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível Nº 70069420503**. Sexta Câmara Cível. Comercialização de dados cadastrais de consumidores. Apelante: Confederação Nacional de Dirigentes Lojistas (SPC Brasil); SERASA S.A. Apelado: Ministério Público. Relator: Ney Wiedemann Neto, Porto Alegre, 25 de agosto de 2016. Disponível em: <http://www.tjrs.jus.br/busca/search?q=&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=*&aba=juris&entsp=a__politica-site&wc=200&wc_mc=1&oe=UTF-8&ie=UTF-8&ud=1&sort=date%3AD%3AS%3Ad1&as_qj=&site=ementario&as_epq=&as_oq=&as_eq=&partialfields=n%3A70069420503.%28s%3Acivel%29&as_q=+#main_res_juris>. Acesso em: 7 dez. 2017.

[568] Como dispositivo da sentença, extrai-se: "Isso posto, JULGO PROCEDENTES os pedidos formulados pelo Ministério Público em desfavor de CONFEDERAÇÃO NACIONAL DE DIRIGENTES LOJISTAS, tendo a SERASA como assistente litisconsorcial (e que não poderá discutir no porvir os fundamentos de fato e de direito decididos), resolvendo o mérito na forma do art. 269, inc. I do CPC, para o fim de, com abrangência nacional da sentença:
a) determinar que a ré cancele, no prazo de 30 dias, o registro de consumidores que não tenham expressamente autorizado a inserção de seus dados cadastrais e informações pessoais no banco de dados de responsabilidade da ré, sob pena de multa de R$ 100,00, por cada exclusão descumprida, a ser revertida para o Fundo de Reconstituição dos Bens Lesados;
b) determinar que a ré se abstenha de registrar e/ou divulgar e/ou comercializar dados cadastrais e informações pessoais de consumidores, sem prévia autorização destes, sob pena de multa de R$ 200,00 por cada descumprimento, a ser revertida para o Fundo de Reconstituição dos Bens Lesados.

Câmara Civil do TJRS, sob relatoria do Des. Ney Widemann Neto, concluiu por dar provimento aos recursos interpostos, entendendo pela legitimidade da conduta da empresa ré (e da SERASA S/A).

Em suma, sustentou-se no Acórdão que os dados de identificação ou dados cadastrais são considerados dados públicos, tratando-se daqueles "[...] que quase todos os cidadãos comuns fornecem ao praticar dados da vida civil, não sendo dados sigilosos. São dados menos invasivos e não necessitam de prévia autorização para divulgação [...]"[569]. Estabeleceu-se, assim, uma distinção entre dados sensíveis e dados de identificação, aos quais não haveria proteção legal quanto a sigilo ou à autorização prévia de utilização, fundamentando tal tese no art. 1º da Lei nº 9.507/97[570]. Ainda é possível extrair do Acórdão:

> Na realidade, os dados cadastrais abrangem informações de caráter relativamente público, revelando-se imprescindíveis para a própria

---

c) condenar a ré genericamente e mediante apuração em liquidação de sentença ao pagamento de indenização por danos materiais e morais causados aos consumidores individualmente considerados, e lesados em decorrência da divulgação e comercialização de seus dados cadastrais, sem prévia autorização, cujas quantias deverão ser corrigidas monetariamente pelo IGP-M, e acrescidas de juros legais de 1% (um por cento) ao mês, ambos a contar da citação;
d) condenar a ré ao pagamento de indenização pelos danos morais coletivos no valor de R$ 70.000,00 (setenta mil reais), corrigida pelo IGP-M desde a data desta sentença, e acrescida de juros de mora de 1% ao mês, a contar da citação. Tal valor deverá ser revertido ao Fundo de Reconstituição de Bens Lesados (art. 13 da Lei 7.347/85).
e) determinar que, para ciência da presente decisão aos interessados, deverá a demandada publicar - duas vezes, em intervalo de dez dias - às suas expensas, no prazo de 15 dias após o trânsito em julgado da sentença, às suas custas, nos jornais Zero Hora, O Sul, Correio do Povo, Jornal do Comércio e Diário Gaúcho, nas dimensões de 15cm x 15cm, a parte dispositiva da sentença condenatória.
Condeno a ré ao pagamento das custas processuais, sendo incabível a condenação de honorários advocatícios ao Ministério Público." RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível Nº 70069420503**. Sexta Câmara Cível. Comercialização de dados cadastrais de consumidores. Apelante: Confederação Nacional de Dirigentes Lojistas (SPC Brasil); SERASA S.A. Apelado: Ministério Público. Relator: Ney Wiedemann Neto, Porto Alegre, 25 de agosto de 2016. Disponível em: <http://www.tjrs.jus.br/busca/search?q=&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=*&aba=juris&entsp=a__politica-site&wc=200&wc_mc=1&oe=UTF-8&ie=UTF-8&ud=1&sort=date%3AD%3AS%3Ad1&as_qj=&site=ementario&as_epq=&as_oq=&as_eq=&partialfields=n%3A70069420503.%28s%3Acivel%29&as_q=+#main_res_juris>. Acesso em: 7 dez. 2017.

[569] Ibid., p. 7-8

[570] "Art. 1º (VETADO)
Parágrafo único. Considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações." BRASIL. Lei nº 9.507/97, de 13 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. **Diário Oficial da União**, Brasília, 13 nov. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9507.htm>. Acesso em: 30 nov. 2017.

> convivência em sociedade. Ademais, não há como olvidar que tais dados podem ser facilmente obtidos por qualquer pessoa das mais variadas formas.
>
> Ocorre que, se de um lado existe a necessidade de se proteger o direito fundamental à privacidade destes consumidores, de outro, deve-se preservar a garantia de livre acesso às informações da entidade privada que pretende repassar os dados, direito fundamental que, como já visto, inclui a liberdade de receber e transmitir informações por quaisquer meios, sem interferências. No caso em tela, os dados fornecidos pela parte agravante, ainda que privativos, são próprios do próprio das relações intersociais existentes, não possuindo, no caso específico, proteção sigilosa.[571]

Buscando amparo nas lições de Tércio Sampaio Ferraz Júnior, o Tribunal reconhece o caráter privativo dos dados, porém sustenta a ausência de qualquer caráter sigiloso e confidencial dos mesmos e que, por isso, inexistiria "[...] qualquer ofensa à privacidade ou a qualquer outro direito fundamental dos consumidores"[572].

Primeiro, a própria passagem citada de Tércio Sampaio Ferraz Júnior é nebulosa. O autor nitidamente faz uma confusão entre os direitos da personalidade que, no texto, são indistinguíveis uns dos outros, como se todos fossem parte de um direito à privacidade[573]. Segundo, ignora-se por completo a figura do direito à

---

[571] RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível Nº 70069420503**. Sexta Câmara Cível. Comercialização de dados cadastrais de consumidores. Apelante: Confederação Nacional de Dirigentes Lojistas (SPC Brasil); SERASA S.A. Apelado: Ministério Público. Relator: Ney Wiedemann Neto, Porto Alegre, 25 de agosto de 2016. Disponível em: <http://www.tjrs.jus.br/busca/search?q=&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=*&aba=juris&entsp=a__politica-site&wc=200&wc_mc=1&oe=UTF-8&ie=UTF-8&ud=1&sort=date%3AD%3AS%3Ad1&as_qj=&site=ementario&as_epq=&as_oq=&as_eq=&partialfields=n%3A70069420503.%28s%3Acivel%29&as_q=+#main_res_juris>. Acesso em: 7 dez. 2017. p. 9

[572] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 88, p. 439-459, 1993. Disponível em: <https://www.revistas.usp.br/rfdusp/article/download/67231/69841>. Acesso em: 10 set. 2017.

[573] "Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos – como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial, etc. –, condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido. Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores usados nas relações de convivência, as quais só dizem respeito aos que convivem. Dito de outro modo, os elementos de identificação só são protegidos quando compõem relações de convivência privativas: a proteção é para elas, não para eles. Em conseqüência, simples cadastros de elementos identificadores (nome, endereço, RG, filiação, etc.) não são protegidos. Mas cadastros que envolvam relações de convivência privadas (por exemplo, nas relações de clientela, desde quando é cliente, se a relação foi interrompida, as razões pelas quais isto ocorreu, quais os interesses peculiares do cliente, sua capacidade de satisfazer aqueles interesses, etc.)

proteção de dados pessoais, a tese de que essas "[...] são informações, em tese, de domínio público, que não transcendem a individualidade moral da pessoa"[574] é equivocada. É preciso distinguir informações de caráter público (em termos de acesso) e informações de uso público (em termos de tratamento e transmissão). Pensar as informações pessoais ainda sob a dicotomia entre o que é público ou privado implica negligenciar o potencial lesivo do uso de dados considerados de caráter público. Vale lembrar, como bem aponta Doneda[575], que até uma informação de identificação como o nome da pessoa pode ser um dado sensível, basta se pensar em nomes que são típicos de uma origem étnica ou religiosa, por exemplo, Davi ou Mohamed. Um dado pessoal, ainda que acessível ao público, não perde seu caráter privativo[576].

Outro ponto sustentado pelo TJRS é a licitude da criação e manutenção de bancos de dados, os quais possuem amparo no CDC (art. 43) e na Lei do Cadastro

---

estão sob proteção. Afinal, **o risco à integridade moral do sujeito, objeto do direito à privacidade, não está no nome, mas na exploração do nome, não está nos elementos de identificação que condicionam as relações privadas, mas na apropriação dessas relações por terceiros a quem elas não dizem respeito. Pensar de outro modo seria tornar impossível, no limite, o acesso ao registro de comércio, ao registro de empregados, ao registro de navio, etc., em nome de uma absurda proteção da privacidade. Por último, a honra e a imagem. A privacidade, nesse caso, protege a informação de dados que envolvam avaliações (negativas) do comportamento que, publicadas, podem ferir o bom nome do sujeito, isto é o modo como ele supõe e deseja ser visto pelos outros. Repita-se que o direito à privacidade protege a honra, o direito à inviolabilidade do sigilo de dados protege a comunicação referente a avaliações que um sujeito faz sobre outro e que, por interferir em sua honra, comunica restritivamente, por razões de interesse pessoal**. É o caso, por exemplo, de cadastros pessoais que contêm avaliações negativas sobre a conduta (mau pagador, devedor impontual e relapso, etc.). **No tocante à imagem, para além do que ela significa de boa imagem, assimilando-se, nesse sentido, à honra, a proteção refere-se a dados que alguém fornece a alguém e não deseja ver explorada (comercialmente, por exemplo) por terceiros**." [Grifo nosso]. FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 88, p. 439-459, 1993. p. 447, apud RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível Nº 70069420503**. Sexta Câmara Cível. Comercialização de dados cadastrais de consumidores. Apelante: Confederação Nacional de Dirigentes Lojistas (SPC Brasil); SERASA S.A. Apelado: Ministério Público. Relator: Ney Wiedemann Neto, Porto Alegre, 25 de agosto de 2016. Disponível em: <http://www.tjrs.jus.br/busca/search?q=&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=*&aba=juris&entsp=a__politica-site&wc=200&wc_mc=1&oe=UTF-8&ie=UTF-8&ud=1&sort=date%3AD%3AS%3Ad1&as_qj=&site=ementario&as_epq=&as_oq=&as_eq=&partialfields=n%3A70069420503.%28s%3Acivel%29&as_q=+#main_res_juris>. Acesso em: 7 dez. 2017. p. 9-10.

574 Ibid., p. 14.

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

576 Inclusive, no próprio acórdão se reconhece a natureza privativa dos dados. RIO GRANDE DO SUL, op. cit., p. 9.

Positivo. Nesse ponto, inclusive, se vale de passagem de Benjamin que, em verdade, não se coaduna com o sustentado no Acórdão[577].

Entendem os Desembargadores que, *in casu,* o princípio da finalidade estaria devidamente observado, uma vez que as informações dos consumidores são "[...] disponibilizadas tão somente a pessoas jurídicas e profissionais liberais assinantes do serviço, com a finalidade, indiscutivelmente, apenas empresarial"[578]. Porém, contraditoriamente, reconhecem que a atuação da empresa destoa de sua finalidade original, ao sustentarem a não sujeição ao dever de notificação previsto no art. 43, §2º do CDC, "[...] uma vez que não se trata propriamente de atuação como órgão de restrição ao crédito, mas de disponibilização de dados dos consumidores"[579]. O princípio da finalidade, conforme já enfrentado no segundo capítulo deste trabalho, limita tanto a coleta de dados (somente os necessários para atender tal fim), como o uso dos dados (os dados só podem ser usados para o fim que foram inicialmente

---

[577] Transcreve-se a passagem de Benjamin:
"O CDC, ao contrário da Diretiva 95/46/CE e do Fair Credit Reporting Act, não determina explicitamente que a informação não deve ser excessiva e, ainda, que esteja diretamente vinculada aos propósitos dos bancos de dados. Não obstante, análise sistemática do ordenamento jurídico leva exatamente à mesma conclusão.
A CF garante, no art. 5.º, X, a inviolabilidade do direito à honra e à vida privada - cujo um dos seus principais aspectos é justamente o controle de dados pessoais. Embora fundamentais, os direitos não são ilimitados. Admite-se que algumas informações negativas e integrantes da privacidade pessoal, considerando circunstâncias fáticas que envolvem tensão ou conflito com outros valores, possam, licitamente, ser tratadas por bancos de dados de proteção ao crédito.
Todavia, a atuação das referidas entidades, em constante confronto com os valores honra e privacidade, deve sempre ser vista como situação excepcional, cuidando o intérprete de evitar a imposição de sacrifício desarrazoado aos direitos da personalidade, sob pena de inconstitucionalidade do resultado hermenêutico. Em outros termos, a atividade dos bancos de dados de proteção ao crédito legitima-se na exata medida em que os valores honra e privacidade - de gênese constitucional - devam ceder diante de outros valores do mesmo grau.
Em outros termos, objetiva-se preservar o núcleo essencial do direito à privacidade. Não é por outra razão que, no exterior, há disposições expressas no sentido de que os bancos de dados possuam objetivos específicos, previamente determinados, e as informações não sejam excessivas, além de estarem vinculadas aos propósitos da entidade arquivista. No Brasil, conclusão diversa esbarraria na Constituição Federal." BENJAMIN, Antonio Hermann V; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe. **Manual de direito do consumidor** *[livro eletrônico].* 1. ed. São Paulo: Revista dos Tribunais, 2013, apud RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível Nº 70069420503**. Sexta Câmara Cível. Comercialização de dados cadastrais de consumidores. Apelante: Confederação Nacional de Dirigentes Lojistas (SPC Brasil); SERASA S.A. Apelado: Ministério Público. Relator: Ney Wiedemann Neto, Porto Alegre, 25 de agosto de 2016. Disponível em: <http://www.tjrs.jus.br/busca/search?q=&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=*&aba=juris&entsp=a__politica-site&wc=200&wc_mc=1&oe=UTF-8&ie=UTF-8&ud=1&sort=date%3AD%3AS%3Ad1&as_qj=&site=ementario&as_epq=&as_oq=&as_eq=&partialfields=n%3A70069420503.%28s%3Acivel%29&as_q=+#main_res_juris>. Acesso em: 7 dez. 2017. p. 12-13.

[578] RIO GRANDE DO SUL, op. cit.

[579] Ibid., p. 14.

coletados, salvo no caso de consentimento). Nesse ponto, esclarecedora é a passagem de Ruaro e Molinaro:

> [...] em matéria de proteção de dados pessoais o princípio da finalidade resulta que os dados pessoais ao serem coletados são ou devem ser a título de um fim específico, ou seja, "indica a correlação necessária que deve existir entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta dos dados". Esse princípio resguarda o titular dos dados de uso por terceiros não legitimados na relação estabelecida com quem coleta os dados pessoais. Assim, por exemplo, se a coleta dos dados pessoais tem por finalidade a formação de um banco de dados finalidade de proteção ao crédito para o mercado (SPC e SERASA), ainda que possa ser disseminada para aqueles que têm a mesma finalidade, não poderá sê-lo para fins alheios ao objetivo [de proteção de crédito] sem o prévio consentimento livre, informado e específico.[580]

Outrossim, sustenta-se no Acórdão que o "[...] banco de dados mantido apenas com informações pessoais não se sujeita ao prévio consentimento do consumidor avaliado (art. 4º, Lei nº 12.414, de 2011)"[581]. Não obstante, o referido artigo dispõe exatamente o contrário, *in verbis*:

> Art. 4º A abertura de cadastro requer autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada.
>
> § 1º Após a abertura do cadastro, a anotação de informação em banco de dados independe de autorização e de comunicação ao cadastrado.
>
> § 2º Atendido o disposto no caput, as fontes ficam autorizadas, nas condições estabelecidas nesta Lei, a fornecer aos bancos de dados as

[580] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 100-101, apud RUARO, Regina Linden; MOLINARO, Carlos Alberto. Conflito Real ou Aparente de Interesses entre o Direito Fundamental à Proteção de Dados Pessoais e o Livre Mercado. in: RUARO, Regina Linden; Mañas, José Luis Piñar; MOLINARO, Carlos Alberto (Org). **Privacidade e Proteção de Dados Pessoais na Sociedade Digital.** [recurso eletrônico]. Porto Alegre, RS: Editora Fi, 2017. p. 32.

[581] RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível Nº 70069420503**. Sexta Câmara Cível. Comercialização de dados cadastrais de consumidores. Apelante: Confederação Nacional de Dirigentes Lojistas (SPC Brasil); SERASA S.A. Apelado: Ministério Público. Relator: Ney Wiedemann Neto, Porto Alegre, 25 de agosto de 2016. Disponível em: <http://www.tjrs.jus.br/busca/search?q=&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=*&aba=juris&entsp=a__politica-site&wc=200&wc_mc=1&oe=UTF-8&ie=UTF-8&ud=1&sort=date%3AD%3AS%3Ad1&as_qj=&site=ementario&as_epq=&as_oq=&as_eq=&partialfields=n%3A70069420503.%28s%3Acivel%29&as_q=+#main_res_juris>. Acesso em: 7 dez. 2017. p. 13-14.

> informações necessárias à formação do histórico das pessoas cadastradas.[582]

Nos termos da Lei, o consentimento do consumidor é prescindível apenas para anotações posteriores em banco de dados cujo cadastro já existe, ou seja, para cadastros que já obtiveram o consentimento do consumidor quando da sua abertura. Aos demais cadastros demanda-se "[...] autorização prévia do potencial cadastrado [leia-se titular dos dados], *mediante consentimento informado*"[583]. [Grifo nosso].

A desnecessidade de consentimento do titular dos está atrelada à finalidade do cadastro criado e ainda assim não suprime o dever de notificação do titular dos dados. Assim, existem determinadas atividades que pressupõem o tratamento de dados pessoais e que, em razão de sua importância, prescindem do consentimento, exemplo disso é o próprio caso dos cadastros de consumidores para fins de proteção do crédito regrados pelo já estudado art. 43 do CDC. Porém, tal situação não se estende a qualquer fim (por exemplo, prospecção de clientes), devendo-se observar os valores em conflito em cada caso concreto[584].

Por fim, traçando um comparativo com a Espanha (e a União Europeia de forma geral), a questão da ilicitude da transferência de informações pessoais para fins diversos do que foram coletados (comerciais), sem anuência do titular dos dados sequer é objeto de debate. Até mesmo nos casos de consentimento como

---

[582] Ibid.

[583] RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível Nº 70069420503**. Sexta Câmara Cível. Comercialização de dados cadastrais de consumidores. Apelante: Confederação Nacional de Dirigentes Lojistas (SPC Brasil); SERASA S.A. Apelado: Ministério Público. Relator: Ney Wiedemann Neto, Porto Alegre, 25 de agosto de 2016. Disponível em: <http://www.tjrs.jus.br/busca/search?q=&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=*&aba=juris&entsp=a__politica-site&wc=200&wc_mc=1&oe=UTF-8&ie=UTF-8&ud=1&sort=date%3AD%3AS%3Ad1&as_qj=&site=ementario&as_epq=&as_oq=&as_eq=&partialfields=n%3A70069420503.%28s%3Acivel%29&as_q=+#main_res_juris>. Acesso em: 7 dez. 2017.

[584] A esse respeito, Ruaro e Molinaro sustentam que: "O SPC e o SERASA, é sabido, foram criados para proteger as empresas da inadimplência dos consumidores, são órgãos de proteção ao crédito e por sua natureza, para esta finalidade, prescindem de autorização do consumidor para coleta de dados pessoais que nesta categoria não se consideram como sigilosos podendo ser coletados e de caráter público dentre os associados aos sistemas devendo preservar sua natureza apenas informacional. Assim, usá-lo para fins de prospecção de clientes, marketing, etc, constitui-se em finalidade alheia à sua natureza e portanto torna-se inconstitucional." RUARO, Regina Linden; MOLINARO, Carlos Alberto. Conflito real ou aparente de interesses entre o direito fundamental à proteção de dados pessoais e o livre mercado. In: RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (Org.). **Privacidade e proteção de dados pessoais na sociedade digital**. [recurso eletrônico]. Porto Alegre: Fi, 2017. p. 13-46. p. 38.

condicionante de acesso ao serviço, a normativa alienígena dispõe "[...] *que no son válidas las tachaduras de cláusulas que en algunos casos los clientes realizan (por ejemplo, la cesión de datos a terceiros para fines publicitários, en lugar de simplemente rellenar la casilla que al efecto contienen los contratos)*"[585]. Ou seja, o titular dos dados tem sempre o direito de se opor à cessão de suas informações para terceiros para fins de publicidade e ao recebimento de ofertas comerciais da própria empresa responsável pelo tratamento, inclusive a anuência de tais cláusulas além de não poder ser condicionante ao acesso ao serviço deve se dar, em se tratando de contrato por via eletrônica, por meio do sistema de *opt in*[586] e não de *opt out*[587].

É preciso atentar para o que Solove[588] chamou de "indústria de bancos de dados". Dados pessoais são verdadeiras mercadorias, objetos de comercialização ou cessão entre empresas, as quais se beneficiam amplamente de tal atividade e geram significativo risco aos consumidores.

Reconhece-se a necessidade de circulação das informações de caráter pessoal, porém, essa deve se harmonizar com o respeito aos direitos do consumidor e a proteção de dados pessoais. Nesse sentido, Mendes[589] aponta os critérios da LOPD (Lei de Proteção de Dados espanhola) como parâmetro para a verificação da legitimidade da transferência desses dados, são eles: *a existência de consentimento prévio do consumidor*; ou quando a *transferência é necessária para atender uma finalidade que se relaciona diretamente com atividades legítimas da empresa* que transfere e da empresa que recebe os dados, ambos ignorados no presente caso.

A proteção de dados pessoais tem em sua essência a chamada autodeterminação informativa. Consoante já mencionado no segundo capítulo, essa consiste em direito fundamental e da personalidade e se presta a garantir ao

---

[585] ARIAS, Ignacio San Martín. **Protección de datos en el crédito al consumo**. Madrid: Thomson Reuters, 2015. p. 22.

[586] O sistema de *opt in* é aquele em que o usuário deve preencher o campo em que consta a cláusula para anuir com a mesma. Geralmente, abre-se uma caixa de diálogo em que ele deve clicar, marcando com um "X" que concorda com determinada cláusula. O sistema de *opt out*, por sua vez, é justamente o contrário, neste caso, a caixa de diálogo já está marcada, sendo necessário que o usuário desmarque a opção que já vem pré-selecionada com a anuência.

[587] ARIAS, Ignacio San Martín. **Protección de datos en el crédito al consumo**. Madrid: Thomson Reuters, 2015.

[588] SOLOVE, Daniel. **The Digital Person**. p. 19, apud MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online. p. 117.

[589] MENDES, op. cit.

cidadão o controle de suas próprias informações, evitando, assim, o uso discriminatório dessas ou alguma forma de controle social amparado em bancos de dados[590].

[590] RUARO, Regina Linden; MOLINARO, Carlos Alberto. Conflito real ou aparente de interesses entre o direito fundamental à proteção de dados pessoais e o livre mercado. In: RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (Org.). **Privacidade e proteção de dados pessoais na sociedade digital**. [recurso eletrônico]. Porto Alegre: Fi, 2017. p. 13-46.

CONCLUSÃO

O enfrentamento das temáticas do direito à proteção de dados pessoais e do *profiling* consiste em um verdadeiro desafio. A intensidade das mudanças tecnológicas e a velocidade com que mecanismos considerados “de ponta” se tornam obsoletos, em especial no âmbito das TICs, dificultam qualquer tentativa de construção pontual na matéria. Nesse sentido, percebe-se a importância de uma abordagem calcada em construções principiológicas e em critérios norteadores para a adequação e conformação de interesses juridicamente tuteláveis que, inevitavelmente, entram em colisão. Em um cenário jurídico marcado pela falta de uma regulação específica são esses pilares interpretativos que possibilitam a articulação de interesses conflitantes sob uma estrutura hermenêutica harmonizada com os direitos fundamentais e com a própria Constituição da República Federativa do Brasil de 1988.

Buscando exatamente contribuir para a identificação e a consolidação desses pilares interpretativos, este trabalho enfrentou a temática do *profiling* no cenário jurídico brasileiro. Partindo da premissa de que o direito à proteção de dados é um direito fundamental reconhecido pelo ordenamento jurídico pátrio, verificaram-se quais são os limites no uso dessa ferramenta de tratamento de dados pessoais, notadamente no que toca ao respeito à autonomia e à privacidade do titular dos dados.

Do exposto, conclui-se que o direito à privacidade não se esgota em sua primeira formulação enquanto um *right to be let alone.* Esse direito a ser deixado só é apenas uma das inúmeras faces que o direito à privacidade apresenta. É preciso encarar o direito à privacidade como um direito fundamental e, como tal, dotado de um núcleo essencial inviolável, tendo em si uma expressão da dignidade da pessoa humana. Forçoso reconhecer que esse direito é dotado não só de uma dimensão negativa, da qual se extrai um dever de abstenção, mas também de uma dimensão positiva, da qual decorre um dever prestacional, de proteção e promoção da privacidade.

Outrossim, é preciso observar que tal direito também consiste em um direito da personalidade, dotado das características inerentes a tal categoria de direitos. Destarte, trata-se de um direito inalienável e intransmissível, que não pode sofrer uma limitação que venha a interferir com o livre desenvolvimento da personalidade.

O direito fundamental à privacidade apresenta, também, um caráter informacional. Consoante apontado no primeiro capítulo, os avanços tecnológicos, especialmente nas TICs, influenciaram diretamente na construção desse direito e nas mutações que ele sofreu no decorrer do tempo. Em que pese ainda manter seu aspecto de *right to be let alone,* é a privacidade informacional que ganha maior evidência na sociedade da informação. Essa noção de que o indivíduo tem o direito de determinar quais informações ele pretende manter privadas e quais pretende expor ao público consiste na dimensão do direito à privacidade que mais esbarra em outros interesses juridicamente tuteláveis. Inclusive, é a partir do desenvolvimento dessa formulação do direito à privacidade que surge o chamado direito à proteção de dados pessoais.

A esse respeito, impossível ignorar o grande desenvolvimento da temática nos âmbitos europeu e norte-americano, ambos considerados modelos de referência em termos de proteção de dados pessoais. Do estudo realizado no segundo capítulo, percebe-se que, em que pese sensivelmente distintas, é possível identificar diversos pontos de conexão entre as duas sistemáticas de proteção de dados pessoais. Apesar de partirem de abordagens distintas, o propósito delas é o mesmo: a proteção do indivíduo, resguardando a sua privacidade e, mais do que isso, sua autonomia. Com isso, diversos princípios estruturais de uma disciplina de proteção de dados pessoais acabam convergindo.

O princípio da transparência desdobra-se na vedação de sigilo a respeito da existência de um banco de dados pessoais e no dever de esses bancos de dados prestarem informações claras e precisas acerca dos dados a serem coletados, de como serão tratados e para qual finalidade. O princípio da finalidade irradia a noção de *fair use* a toda a sistemática de proteção de dados. Segundo ele, o tratamento deve atender a uma finalidade específica e as informações pessoais só podem ser coletadas quando necessárias para atingir tal finalidade. Ou seja, é justamente o fim almejado que justifica e legitima toda a coleta e tratamento dos dados pessoais. Do

princípio da exatidão, por sua vez, pode-se extrair, de um lado, o dever do responsável pelo tratamento de verificar a veracidade e atualidade das informações utilizadas e, de outro, o direito de acesso e de retificação dos dados por parte do titular.

Percebem-se, em tais princípios, pontos de contato entre os modelos norte-americano e o europeu, os quais permitem extrair um norte para uma sistemática brasileira de proteção de dados pessoais. Ademais, é possível identificar maior proximidade do sistema brasileiro em relação ao modelo europeu do que em relação ao modelo estadunidense, o que facilita a utilização de outros aspectos desse modelo como referência à estrutura jurídica brasileira na temática da proteção de dados pessoais, porém, sem refutar a possiblidade de fazê-lo em relação ao modelo norte-americano.

No último capítulo, por fim, inferiu-se que o direito à proteção de dados pessoais consiste em um direito fundamental e autônomo, que recebe guarida no ordenamento jurídico pátrio, em razão do seu caráter instrumental no que concerne ao resguardo do livre desenvolvimento da personalidade e de outros direitos fundamentais. Em que pese inexista uma regulação específica, é possível extrair uma sistemática brasileira de proteção de dados pessoais a partir das disposições legislativas esparsas que abordam a matéria – destacando-se as disposições constantes na Constituição Federal, no Código de Defesa do Consumidor e na Lei do Cadastro Positivo (Lei nº 12.414/2011) – e da convergência em nível internacional dos “princípios básicos” do direito à proteção de dados pessoais – por exemplo, o princípio da finalidade, o princípio da publicidade, o princípio do livre acesso, o princípio da segurança e o princípio da exatidão.

No que toca à figura do *profiling,* constata-se que essa ferramenta possibilita que o processo de massificação e de globalização das relações interpessoais não implique uma perda de customização e de personalização. Ela permite a dinamização do mercado e uma gestão (pública ou privada) eficiente, facilitando uma melhor alocação e utilização de recursos. Não obstante, essa técnica incrementa o risco de relações desumanizadas, uma vez que o perfil virtual passa a ser a única representação da pessoa perante inúmeros agentes sociais. Assim, as interações sociais perdem o caráter pessoal, e o indivíduo acaba reduzido a um

conglomerado de informações, ou a um *score* que representa uma previsão de comportamento, ou um indicativo de risco, respectivamente.

Tal situação é identificável nas sistemáticas de análise de crédito a partir dos mecanismos de *credit scoring*, as quais foram objeto de apreciação pelo STJ no que concerne à licitude e aos limites de sua utilização. Reconheceu-se, assim, que a utilização desses indicativos, *per si*, não violaria os direitos dos titulares dos dados, cabendo apenas a observância ao direito à proteção de dados pessoais nos termos da Lei do Cadastro Positivo.

Outra situação marcante é a da utilização do *profiling* para fins de *marketing* direcionado, em especial nas figuras do *online profiling* e do *behavioral advertising.* Os problemas na utilização desses mecanismos perpassam não só pela forma como os dados são tratados, mas principalmente na maneira pela qual são coletados (*coockies, web bugs, spywares,* dentre outros). O monitoramento do consumidor a partir de seu comportamento é uma das questões mais preocupantes na sociedade da informação, em razão da falta de transparência que permeia a utilização desses mecanismos de coleta de dados. Todavia, a utilização de mecanismos como o consentimento informado supriria esses riscos ao indivíduo, legitimando o uso de grande parte dessas ferramentas de coleta de informações pessoais.

Por fim, verificou-se que a falta de uma regulação específica abre espaço a uma interpretação temerária a propósito do direito à proteção de dados pessoais. A falta de conhecimento sobre a temática possibilita que o próprio judiciário convalide abusos no tratamento de dados pessoais, fragilizando a proteção do indivíduo. Exemplo disso é a decisão do TJRS na Apelação Cível nº 70069420503, na qual uma análise ainda calcada na dicotomia do que seriam “dados públicos” ou “dados privados” deu margem à comercialização de dados pessoais sem o consentimento do titular e para fins de prospecção de clientes.

Tão importante quanto a proteção exercida pelo judiciário é a atuação na esfera administrativa. Em 2011, Bennet[591] já evidenciou a necessidade de uma atuação de fiscalização e de controle por uma autoridade competente, dotada de

[591] Bennet realizou uma pesquisa com base nas agências de proteção de dados europeias e nas agências de regulação norte-americanas para verificar qual a abordagem mais eficiente por parte dessas agências de regulação. BENNETT, Colin J. **Regulating privacy**: data protection and public policy in Europe and the United States. New York: Cornell University Press, 2011.

autonomia, demonstrando maior eficiência daquelas autoridades que fazem um controle de fiscalização em relação às que trabalham com uma autorização prévia. Ademais, as figuras da *accountability* e do *compliance* surgem no modelo europeu de proteção de dados pessoais como mecanismos complementares ao modelo tradicional de atuação das agências de proteção de dados pessoais. Ou seja, o *risk-based approach* é complementar à atuação fiscalizatória do Estado, há uma combinação entre a autorregulação e o controle estatal. Daí a insistência na elaboração de um marco regulatório específico que preveja, inclusive, a criação de uma agência de proteção de dados brasileira[592].

Portanto, conclui-se que o *profiling* é uma ferramenta lícita, mas que demanda grande atenção, em face do risco inerente à sua utilização. Dessa feita, a adoção de medidas suficientes para a minimização desse risco, bem como para garantir que eventual dano seja devidamente reparado, é imprescindível. Com isso, legitima-se a utilização desses mecanismos de tratamento de dados pessoais, sem que implique na fragilização da proteção da pessoa humana, notadamente na figura do titular dos dados.

[592] No caso do Projeto de Lei nº 5.276/2016 prevê-se a designação de um órgão com poder fiscalizatório e a criação do Conselho Nacional de Proteção de Dados e da Privacidade, ao passo que o Projeto de Lei do Senado nº 181, de 2014, imputa à União, aos Estados, ao Distrito Federal e aos Municípios a incumbência de fiscalização da lei. Ou seja, nenhum dos projetos de lei propõe a criação de uma agência de proteção de dados com autonomia em sua atuação. BRASIL. Projeto de Lei da Câmara de Deputados nº 5.276/2016, de 13 de maio de 2016. **Congresso Nacional**, Brasília, 13 maio 2016. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 25 de nov. 2017.

REFERÊNCIAS

32ND INTERNATIONAL Conference of Data Protection and Privacy Commissioners. **Resolution on privacy by design**. Jerusalem, Israel, 27-29 oct. 2010.

AGÊNCIA dos Direitos Fundamentais da União Europeia. **Manual da Legislação Europeia sobre a Proteção de Dados**. Luxemburgo: Serviço das Publicações da União Europeia, 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 05 out. 2016.

AGUIAR JÚNIOR, Ruy Rosado de (Coord. Científico). **Jornadas de direito civil I, III, IV e V**: enunciados aprovados. Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2012.

ÁLVAREZ, Luis Felipe López. La responsabilidad del responsable. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 275-294.

ANDRADE, Fábio Siebeneichler de. O desenvolvimento da tutela dos direitos da personalidade nos dez anos de vigência do Código Civil de 2002. In: LOTUFO, Renan; NANNI, Giovanni Ettore; MARTINS, Fernando Rodrigues (Coord.). **Temas relevantes do direito civil contemporâneo**: reflexões sobre os 10 anos do Código Civil. São Paulo: Atlas, 2012. p. 51-85.

ARAÚJO, Elaine Aparecida. **Risco de crédito**: desenvolvimento de modelo Credit Scoring para a gestão da inadimplência de uma instituição de microcrédito. Ipea Caixa, 2006. Disponível em: <http://www.esaf.fazenda.gov.br/assuntos/premios/premios-1/premios-realizados/pasta-premio-ipea-caixa/premio-ipea-caixa-2006/profissionais/tema-3/2-lugar-tema-3-profissionais>. Acesso em: 31 jul. 2017.

ARIAS, Ignacio San Martín. **Protección de datos en el crédito al consumo**. Madrid: Thomson Reuters, 2015.

BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BECK, Ulrich. World risk society. In: OLSEN, J. K. B.; PEDERSEN, S. A.; HENDRICKS, V. F. (Ed.). **A companion to the philosophy of technology**. Oxford: Blackwell Publishing Ltd, 2009. p. 495-499.

BELTRÃO, Silvio Romero. **Direitos da personalidade**: de acordo com o novo Código Civil. São Paulo: Atlas, 2005.

BENNETT, Colin J. **Regulating privacy**: data protection and public policy in Europe and the United States. New York: Cornell University Press, 2011.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed. São Paulo: Saraiva, 2015.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 05 mar. 2017.

_____. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Elaboração Danilo Doneda. Brasília: SDE/DPDC, 2010. Disponível em: <http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf>. Acesso em: 23 jul. 2017.

_____. Lei complementar nº 105, de 11 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. **Diário Oficial da União**, Brasília, 11 jan. 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm>. Acesso em: 14 out. 2017.

_____. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, seção 1, Brasília, DF, a. 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/CCivil_03/leis/2002/L10406.htm>. Acesso em: 20 mar. 2017.

_____. Lei nº 12.414, de 10 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União**, Brasília, 10 jun. 2011. p. 2. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 30 out. 2017.

_____. Lei nº 12.965, de 24 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 out. 2017.

_____. Lei nº 8.078, de 12 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**, Brasília, DF, 12 set. 1990. p. 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 30 out. 2017.

_____. Lei nº 9.507/97, de 13 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. **Diário Oficial da União**, Brasília, 13 nov. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9507.htm>. Acesso em: 30 nov. 2017.

_____. Projeto de Lei da Câmara de Deputados nº 5.276/2016, de 13 de maio de 2016. **Congresso Nacional**, Brasília, 13 maio 2016. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 25 de nov. 2017.

_____. Superior Tribunal de Justiça. **Acórdão no REsp nº 1.419.697/RS**. Relator: Paulo de Tarso Sanseverino. Publicado no DJe de 17 nov. 2014. RSTJ vol. 236. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201303862850&dt_publicacao=17/11/2014>. Acesso em: 30 jul. 2017.

_____. Superior Tribunal de Justiça. **Recurso Especial nº 1.419.679-RS**. Relator: Ministro Paulo de Tarso Sanseverino. Segunda Seção, julgado em 12/11/2014, DJe 17/11/2014, Brasília, DF, 12 nov. 2014. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201303862850&dt_publicacao=17/11/2014>. Acesso em: 20 nov. 2017.

_____. Superior Tribunal de Justiça. Recurso Especial nº 418416/SC. Relator: Min. Sepúlveda Pertence. Brasília, DF, 10 de maio de 2006. **Diário da Justiça**, Brasília, DF, 10 maio 2006. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790>. Acesso em: 25 nov. 2017.

_____. Superior Tribunal de Justiça. REsp 22.337-9/RS. Quarta Turma. Relator: Min. Ruy Rosado de Aguiar. Brasília, 13 de fevereiro de 1995. **Diário de Justiça**, Brasília, DF, 20 mar. 1995, p. 138. Disponível em: <https://ww2.stj.jus.br/processo/ita/documento/mediado/?num_registro=199200114466&dt_publicacao=20-03-1995&cod_tipo_documento=>. Disponível em: 01 nov. 2017.

_____. Superior Tribunal de Justiça. Súmula n° 227. A pessoa jurídica pode sofrer dano moral. **Diário de Justiça**, seção 2, Brasília, DF, p. 126, 08 out. 1999.

_____. Superior Tribunal de Justiça. **Súmula nº 385**. Da anotação irregular em cadastro de proteção ao crédito, não cabe indenização por dano moral, quando preexistente legítima inscrição, ressalvado o direito ao cancelamento. Julgamento: 27 de maio de 2009. RSTJ v. 214 PG: 00541. Súmulas STJ. Disponível em: <http://www.stj.jus.br/docs_internet/SumulasSTJ.pdf>. Acesso em: 3 nov. 2017.

CALÉS, Rosario Duaso. Los princípios de protección de datos desde el diseño y protección de datos por defecto. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 295-320.

CANOTILHO, José Joaquim Gomes. **“Reality shows” e liberdade de programação**. Portugal: Coimbra, 2003.

CARO, María Álvarez. El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas. In: PIÑAR MAÑAS, José Luis(Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 227-240.

CARULLA, Santiago Ripol. Aplicación territorial del reglamento. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 77-186.

CASTELLS, Manuel. **A galáxia internet**. Reflexões sobre internet, negócios e sociedade. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

_____. **La era de la información**: economía, sociedad y cultura. La sociedad red. México, D.F.: Siglo Veintiuno, 2008. v. I.

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

CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang (Org.). **New horizons for a data-driven economy**: a roadmap for usage and exploitation of big data in Europe. Cham (Suiça): Springer Open, 2016.

_____. The big data value opportunity. In: _____ (Org.). **New horizons for a data-driven economy**: a roadmap for usage and exploitation of big data in Europe. Cham (Suiça): Springer Open, 2016. p. 3-11.

CAVOUKIAN, Ann. **Privacy by design**: the 7 foundation principles. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>. Acesso em: 06 out. 2017.

CONTE, Julen Fernández; BURGOS, Diego León. Antecedentes y processo de reforma sobre protección de datos en la Unión Europea. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 35-50.

COSTA JR., Paulo José Da. **O direito de estar só**: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1970.

CREDIT Score Accuracy and Implications for Consumers. December 17, 2002. Disponível em: <http://www.consumerfed.org/pdfs/121702CFA_NCRA_Credit_Score_Report_Final.pdf>. Acesso em: 14 nov. 2017.

CUMBRA Iberoamericana. XIII CIMEIRA IBERO-AMERICANA DE CHEFES DE ESTADO E DE GOVERNO. **Declaração de Santa Cruz de la Sierra**, 14 e 15 de novembro de 2003. Disponível em: <http://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf>. Acesso em: 21 out. 2017.

CUPIS, Adriano de. **Os direitos da personalidade**. Tradução Afonso Celso Furtado. Campinas: Romana, 2004.

DELGADO, Mário Luiz. Big Brother Brasil: reality shows e os direitos da personalidade. **Revista Jurídica Consulex**, Brasília, a. VIII, n. 169, p. 24-26, jan. 2004. Disponível em: <https://marioluizdelgado.files.wordpress.com/2014/04/mario-luiz-delgado-3.pdf>. Acesso em: 13 jun. 2017.

DELSON, Ferreira. **Manual de sociologia**: dos clássicos à sociedade da informação. São Paulo: Atlas, 2003.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2. p. 91-108, jul./dez. 2011.

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

_____. Os direitos da personalidade no Código Civil. **Revista da Faculdade de Direito de Campos**, Rio de Janeiro, a. VI, n. 6, p. 71-99, jun. 2005. Disponível em: <http://www.uniflu.edu.br/arquivos/Revistas/Revista06/Docente/03.pdf >. Acesso em: 10 abr. 2017.

DÖHMANN, Indra Spiecker Genannt; TAMBOU, Olivia; BERNAL, Paul; HU, Margaret; MOLINARO, Carlos Alberto; NEGRE, Elsa; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; WITZLEB,Normann; YGER, Florian. The Regulation of Commercial Profiling – A Comparative Analysis. **European Data Protection Law Review.** Berlin, v. 2, n. 4, p. 535-554, 2016.

DOURADO, Maria de Fátima Abreu Marques. **Fundamentos do direito à intimidade**. Porto Alegre: Sergio Antonio Fabris, 2008.

ELMER, G. **Profiling machines**: mapping the personal information economy. Cambridge, Mass: The MIT Press, 2004.

EPIC. **Electronic Communications Privacy Act** (ECPA). Disponível em: <https://epic.org/privacy/ecpa/>. Acesso em: 06 jul. 2017.

_____. **Video protection privacy act**. Disponível em: <https://epic.org/privacy/vppa/>. Acesso em: 05 jul. 2017.

EUROPEAN Commission. Article 29 Data Protection Working Party. **Statement on the role of a risk-based approach in data protection legal frameworks**. Brussels, Belgium, 30 maio 2014. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>. Acesso em: 10 out. 2017.

EX2. **Web 1.0, Web 2.0 e Web 3.0...** Enfim o que é Isso? 2013. Disponível em: <http://www.ex2.com.br/blog/web-1-0-web-2-0-e-web-3-0-enfim-o-que-e-isso/>. Acesso em: 28 mar. 2017.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 88, p. 439-459, 1993. Disponível em: <https://www.revistas.usp.br/rfdusp/article/download/67231/69841>. Acesso em: 10 set. 2017.

_____. Sigilo bancário – privacidade e liberdade. In: SARAIVA FILHO, Oswaldo Othon de Pontes; GUIMARÃES, Vasco Branco (Coord.). **Sigilos bancário e fiscal**. Homenagem ao Jurista José Carlos Moreira Alves. 2. ed. rev. ampl. Belo Horizonte: Fórum, 2015. p. 85-110.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 31. ed. Tradução Raquel Ramalhete. Petrópolis: Vozes, 2006.

FREITAS, Juarez. A hermenêutica jurídica e a ciência do cérebro: como lidar com os automatismos mentais. **Revista da AJURIS**, Porto Alegre, v. 40, n. 130, p. 223-244, jun. 2013.

FTC. **Online profiling**: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commission-report-congress-june-2000/onlineprofilingreportjune2000.pdf>. Acesso em: 26 nov. 2016.

_____. **Protecting consumer privacy in an era of rapid change**: recommendations for businesses and policymakers. Mar. 2012. Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>. Acesso em: 06 out. 2017.

_____. Staff Report. **Self-regulatory principles for online behavioral advertising**. 2009. Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>. Acesso em: 25 nov. 2016.

FULLANA, Antonia Paniza. Protección de datos, cookies y otros instrumentos de navegación. In: COMESAÑA, Julio Costas et al. **Publicidad, defensa de la competencia y protección de datos**. Pamplona (Espanha): Thomson Reuters, 2010. p. 32-57.

GANDY JR., Oscar H. Consumer protection in cyberspace. **CC:** Creative Commons License, v. 9, n. 2, 2011. Disponível em: <http://triplec.at/index.php/tripleC/article/viewFile/267/241>. Acesso em: 26 nov. 2016.

GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010.

GAYO, Miguel Recio. Aproximación baseada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 351-366.

IAB. Internet Advertising Revenue Report Conducted by PricewaterhouseCoopers (PWC). **Digital Advertising Revenues Hit $19.6 Billion in Q1 2017, Climbing 23% Year-Over-Year, According to IAB**. New York: 14 jun. 2017. Disponível em: <https://www.iab.com/news/adrevenues-hit-19-6b/>. Acesso em: 7 ago. 2017.

JIN, Julia. Luddism during the Industrial Revolution. In: **WESTERN Civilization II guides**. 24 abr. 2012. Disponível em: <http://westerncivguides.umwblogs.org/2012/04/24/luddism-during-the-industrial-revolution/>. Acesso em: 30 maio 2017.

LANDA, Iñaki Uriarte. Ámbito de aplicación material. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia un nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 63-76.

LEGAL Information Institute. **18 U.S. Code**. Disponível em: <https://www.law.cornell.edu/uscode/text/18/2721>. Acesso em: 05 jul. 2017.

LEGAL Information Institute. Disponível em: <https://www.law.cornell.edu/uscode/text/18/2721>. Acesso em: 05 jul. 2017.

LEMOS, André; LÉVY, Pierre. **O futuro da internet**: em direção a uma ciberdemocracia planetária. São Paulo: Paulus, 2010.

LEONARDI, Marcel. Vigilância tecnológica, bancos de dados, Internet e privacidade. **Revista Jus Navigandi**, Teresina, a. 9, n. 499, 18 nov. 2004. Disponível em: <https://jus.com.br/artigos/5899>. Acesso em: 3 abr. 2017.

LIMBERGER, Têmis. Mutações da privacidade e a proteção dos dados pessoais. In: RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (Org.). **Privacidade e proteção de dados pessoais na sociedade digital**. Porto Alegre: Fi, 2017. p. 145-168.

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

LUPION, Ricardo. O caso do sistema "*Credit Scoring"* do Cadastro Positivo. **Revista da AJURIS**, Porto Alegre, v. 42, n. 137, p. 431-449, mar. 2015.

MACHADO, Fernando Inglez de Souza; KRONBAUER, Eduardo Luís. Proteção de dados e quebra do sigilo bancário para fins tributários: retrocesso em matéria de direitos fundamentais em prol de uma maior eficiência na administração pública. In: CONPEDI; UNICURITIBA (Org.). **Direito tributário e financeiro II**. 1. ed. Florianópolis: CONPEDI, 2016. v. 1. p. 47-66.

MACHADO, Marta Rodriguez de Assis. **Sociedade do risco e direito penal**: uma avaliação de novas tendências político-criminais. São Paulo: IBCCRIM, 2005.

MAQUIAVEL, Nicolau. **O príncipe**. 4. ed. São Paulo: Edipro, 2015.

MARQUEZ, Javier. **An introduction to credit scoring for small and medium size enterprizes**. World Bank, 2008. Disponível em: <http://siteresources.worldbank.org/EXTLACOFFICEOFCE/Resources/870892-1206537144004/MarquezIntroductionCreditScoring.pdf>. Acesso em: 30 jul. 2017.

MARTINS, Ives Gandra da Silva. Sigilo bancário e privacidade. In: SARAIVA FILHO, Oswaldo Othon de Pontes; GUIMARÃES, Vasco Branco (Coord.). **Sigilos bancário e fiscal**. Homenagem ao Jurista José Carlos Moreira Alves. 2. ed. rev. ampl. Belo Horizonte: Fórum, 2015. p. 67-84.

MATTELART, Armand. **História da sociedade da informação**. Tradução Nicolás Nyimi Campanário. São Paulo: Loyola, 2002.

MAY, Christopher. **The information society**: a sceptical view. Cambridge: Polity, 2002.

MCNEIL, Sonia. Privacy and the modern grid. **Harvard Journal of Law & Technology**, v. 25, fall 2011. Disponível em: <https://ssrn.com/abstract=1928254>. Acesso em: 21 abr. 2017.

MENDES, Laura Schertel. O diálogo entre o marco civil da internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 106, p. 37-69, jul./ago. 2016.

_____. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. Série IDP – Linha de Pesquisa Acadêmica. Vital Source Bookshelf Online.

MILLS, John L. **Privacy**: the lost right. New York: Oxford University, 2008.

OECD. **Exploring data-driven innovation as a new source of growth** – mapping the policy issues raised by “Big Data.” Rep. from OECD, 2013. Disponível em: <http://dx.doi.org/10.1787/5k47zw3fcp43-en>. Acesso em: 20 abr. 2017.

ONU. **Declaração Universal dos Direitos Humanos**. Adotada e proclamada pela resolução 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Disponível em: <http://unesdoc.unesco.org/images/0013/001394/139423por.pdf>. Acesso em: 9 mar. 2017.

ORWELL, George. **1984**. Tradução Alexandre Hubner, Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

PAESANI, Liliana Minardi. **Direito e internet**: liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2000.

PATON, H. J. **The categorical imperative**: a study in Kant's moral philosophy. Chicago: The University of Chicago, 1948.

PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia un nuevo modelo europeo de privacidade. Madrid: Reus, 2016.

_____. Introducción: hacia un nuevo modelo europeo de protección de datos. In: _____ (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 15-22.

_____. Transferencias de datos personales a terceros países u organizaciones internacionales. In: _____ (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 427-460.

PONTES DE MIRANDA. **Tratado de direito privado**. Atualizado por Rosa Maria Barreto Borriello de Andrade Nery. São Paulo: Revista dos Tribunais, 2012. t. VII.

POU, María Arias. Definiciones a efecto del reglamento general de protección de datos. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 115-134.

PROSSER, William L. Privacy. **California Law Review**, v. 48. i. 3, ago. 1960. Disponível em: <http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1>. Acesso em: 28 jun. 2017.

REIGADA, Antonio Troncoso. Autoridades de control independientes. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 461-512.

RIO GRANDE DO SUL. Tribunal de Justiça. **Apelação Cível Nº 70069420503**. Sexta Câmara Cível. Comercialização de dados cadastrais de consumidores. Apelante: Confederação Nacional de Dirigentes Lojistas (SPC Brasil); SERASA S.A. Apelado: Ministério Público. Relator: Ney Wiedemann Neto, Porto Alegre, 25 de agosto de 2016. Disponível em: <http://www.tjrs.jus.br/busca/search?q=&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=*&aba=juris&entsp=a__politica-site&wc=200&wc_mc=1&oe=UTF-8&ie=UTF-8&ud=1&sort=date%3AD%3AS%3Ad1&as_qj=&site=ementario&as_epq=&as_oq=&as_eq=&partialfields=n%3A70069420503.%28s%3Acivel%29&as_q=+#main_res_juris>. Acesso em: 7 dez. 2017.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODRIGUEZ, Daniel Piñeiro. **O direito fundamental à proteção de dados pessoais**: as transformações da privacidade na sociedade de vigilância e a decorrente necessidade de regulação. Dissertação (Mestrado em Direito) – Faculdade de Direito, Programa de Pós-Graduação em Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2010.

RODRÍGUEZ, Ofelia Tejerina. Interrelación con la directiva sobre protección de datos por autoridades competentes. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 97-114.

ROUVROY, Antoinette e POULLET, Yves. The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. In: GUTWIRTH, Serge et al. **Reinventing data protection?** Rotterdam, Netherlands: Sispringer, 2009. p. 45-76.

RUARO, Regina Linden. Direito fundamental à privacidade: o sigilo bancário e a fiscalização da Receita Federal do Brasil. **Interesse Público**, Belo Horizonte, v. 17, n. 90, p. 103-125, mar./abr. 2015.

_____. Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância? **Arquivo Jurídico**, Teresina, v. 2, n. 1, p. 41-60, jan./jul. 2015.

RUARO, Regina Linden; MACHADO, Fernando Inglez de Souza. Ensaio a propósito do direito ao esquecimento: limites, origem e pertinência no ordenamento jurídico brasileiro. **Revista do Direito Público**, Londrina, v. 12, n. 1, p.204-233, abr. 2017.

RUARO, Regina Linden; MOLINARO, Carlos Alberto. Conflito real ou aparente de interesses entre o direito fundamental à proteção de dados pessoais e o livre mercado. In: RUARO, Regina Linden; PIÑAR MAÑAS, José Luis; MOLINARO, Carlos Alberto (Org.). **Privacidade e proteção de dados pessoais na sociedade digital**. [recurso eletrônico]. Porto Alegre: Fi, 2017. p. 13-46.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais: uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro. **Direitos Fundamentais e Justiça**, Porto Alegre, n. 11, p. 163-180, abr./jun. 2010.

SAMANIEGO, Javier Fernández; LONGORIA, Paula Fernandez. El derecho a la portabilidad de los datos. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 257-274.

SANCHES, Jose Luis Saldanha; GAMA, João Taborda da. Sigilo bancário – crónica de uma morte anunciada. In: SARAIVA FILHO, Oswaldo Othon de Pontes; GUIMARÃES, Vasco Branco (Coord.). **Sigilos bancário e fiscal**. Homenagem ao Jurista José Carlos Moreira Alves. 2. ed. rev. ampl. Belo Horizonte: Fórum, 2015. p. 243-264.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 12. ed. Porto Alegre: Livraria do Advogado, 2015.

_____. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. Porto Alegre: Livraria do Advogado, 2001.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme, MITIDIERO, Daniel. **Curso de direito constitucional**. 6. ed. São Paulo: Saraiva, 2017.

SARMENTO, Daniel; GOMES, Fábio Rodrigues. A eficácia dos direitos fundamentais nas relações entre particulares: o caso das relações de trabalho. **Rev. TST**, Brasília, v. 77, n. 4, p. 60-101, out./dez. 2011.

SAS Institute. **Big data**: o que é e por que é importante? Disponível em: <https://www.sas.com/pt_br/insights/big-data/what-is-big-data.html#>. Acesso em: 16 ago. 2017.

SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014.

SCHWABE, Jürgen; MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Berlim: Konrad-

Adenauer-Stifung E.V., 2005. Disponível em: <http://www.kas.de/wf/doc/kas_7738-544-4-30.pdf>. Acesso em: 12 jul. 2017.

SILVA, Virgílio Afonso da. **Direitos fundamentais**: conteúdo essencial, restrições e eficácia. 2. ed. São Paulo: Malheiros, 2011.

SILVEIRA, Alessandra. Democracia e tecnologias da informação. In: VII ENCONTRO INTERNACIONAL DO CONPEDI, Portugal, Braga, 7 set. 2017.

SOARES, Flaviana Rampazzo. **Responsabilidade civil por dano existencial**. Porto Alegre: Livraria do Advogado, 2009.

STOUT, Martha. **The sociopath next door**. New York: Bradway Books, 2005.

STUNTZ, William J. Privacy's problem and the law of criminal procedure. **Michigan Law Review**, n. 93, p. 1016-1078, 5 mar. 1995. Disponível em: <go.galegroup.com/ps/i.do?p=AONE&sw=w&u=capes&v=2.1&id=GALE%7CA17353728&it=r&asid=1e4616fcc39ef94467d7cab05b3a9c80>. Acesso em: 27 jun. 2017.

SBROGIO GALIA, Susana. **Mutações constitucionais interpretativas e proteção do núcleo essencial dos direitos fundamentais**. 2006. 191 f. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2006.

THE UNITED States. **DOJ guide to the freedom of information act**. Disponível em: <https://www.justice.gov/oip/doj-guide-freedom-information-act>. Acesso em: 05 jul. 2017.

TURNER, David e MUÑOZ, Jesus. **Para os filhos de nossos filhos**: uma visão da sociedade internet. São Paulo: Plexus, 1999.

TURNER, V., GANTZ, J. F., REINSEL, D. & MINTON, S. **The digital universe of opportunities**: rich data and the increasing value of the internet of things. Rep. from IDC EMC. 2014. Disponível em: <https://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf>. Acesso em: 5 abr. 2017.

TZU, Sun. **A arte da guerra**. Tradução Sueli Barros Cassal. Porto Alegre: L&PM, 2006.

UNIÃO Europeia. Agência dos Direitos Fundamentais da União Europeia. **Manual da Legislação Europeia sobre a Proteção de Dados**. Luxemburgo: Serviço das Publicações da União Europeia, 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 05 out. 2016.

_____. **Article 29**. Data Protection Working Party. Statement on the role of a risk-based approach in data protection legal frameworks. Brussels, Belgium, 30 maio 2014. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>. Acesso em: 10 out. 2017

_____. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119, 4.5.2016, p. 1-88.

_____. Parlamento Europeu e Conselho. Directiva 2002/58/CE, de 12 de julho de 2002. Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). **Jornal Oficial das Comunidades Europeias**, L 201/37. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT>. Acesso em: 25 jul. 2017.

_____. Parlamento Europeu e Conselho. Directiva 2016/680, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**, L 119/89. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT>. Acesso em: 1 ago. 2017.

_____. Parlamento Europeu e Conselho. Directiva 95/46/CE, de 24 de outubro de 1995. **Jornal Oficial das Comunidades Europeias**, L 281/31. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 13 jul. 2017.

_____. Parlamento Europeu, o Conselho e a Comissão. Carta dos Direitos Fundamentais da União Europeia. **Jornal Oficial das Comunidades Europeias**, 2000/C 364/01. Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 30 jul. 2017.

_____. Tribunal de Justiça (Grande Secção). Comunicações eletrônicas. **Diretiva 2006/24/CE** – Serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações – Conservação de dados gerados ou tratados no contexto da oferta desses serviços – Validade – Artigos 7.°, 8.° e 11.° da Carta dos Direitos Fundamentais da União Europeia. Acórdão do Tribunal de Justiça, C-293/12 e C-594/12 (processos apensos). Digital Rights Ireland Ltd. contra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General, 08 de abr. 2014. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=671099>. Acesso em: 15 set. 2017.

USA. **Cable Communications Policy Act. 47 U.S.C. ch. 5, subch. V–A To** (1) establish a national policy cable television. (2) establish franchise procedures and standards which encourage the growth and development of cable systems and which assure that cable systems are responsive to the needs and interests of the local community; "(3) establish guidelines for the exercise of Federal, State, and local authority with respect to the regulation of cable systems; "(4) assure that cable

communications provide and are encouraged to provide the widest possible diversity of information sources and services to the public; "(5) establish an orderly process for franchise renewal which protects cable operators against unfair denials of renewal where the operator's past performance and proposal for future performance meet the standards established by this title; and "(6) promote competition in cable communications and minimize unnecessary regulation that would impose an undue economic burden on cable systems. Washington, DC, 30 out. 1984. Disponível em: <https://transition.fcc.gov/Bureaus/OSEC/library/legislative_histories/1286.pdf>. Acesso em: 08 jul. 2017.

_____. Department of Justice. **DOJ Guide to the Freedom of Information Act**. Washington, DC, 23 Jul. 2014. Disponível em: <https://www.justice.gov/oip/doj-guide-freedom-information-act>. Acesso em: 05 jul. 2017.

_____. Department of Justice. **The Freedom of Information Act. 5 U.S.C. § 552 (2000)**. Vol. XVII, n. 4, 1996. Disponível em: <https://www.justice.gov/oip/blog/foia-update-freedom-information-act-5-usc-sect-552-amended-public-law-no-104-231-110-stat>. Acesso em: 10 jul. 2017.

_____. Department of Justice. **The Privacy Act of 1974 5 U.S.C. § 552a (2012)**. Establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. Washington, DC, 01 maio 1974. Disponível em: <https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition>. Acesso em: 04 jul. 2017.

_____. **Family Educational Rights and Privacy Act. 20 U.S.C. 1221e–3(a)(1), 1232h**. To set out requirements for the protection of privacy of parents and students under section 444 of the General Education Provisions Act, as amended. Washington DC, 11 abr. 1988. Disponível em: <https://www.gpo.gov/fdsys/pkg/CFR-2010-title34-vol1/pdf/CFR-2010-title34-vol1-part99.pdf>. Acesso em: 07 jul. 2017.

_____. **Health Insurance Portability and Accountability Act. H.R. 3103. 42 USC 201**. To improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes. Washington, DC, 21 ago. 1996. Disponível em: <https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>. Acesso em: 10 jul. 2017.

_____. **Right to Finantial Privacy Act. Sec. 1108, Right to Financial Privacy Act of 1978, 92 Stat. 3697 et seq., 12 U.S.C. 3401 et seq.; (5 U.S.C. 301)**. To authorize Departmental units to request financial records from a financial institution pursuant to the formal written request procedure authorized by section 1108 of the Act, and to set forth the conditions under which such requests may be made. Washington, DC, 20 mar. 1979. Disponível em: <https://www.gpo.gov/fdsys/pkg/CFR-2011-title31-vol1/pdf/CFR-2011-title31-vol1-part14.pdf>. Acesso em: 06 jul. 2017.

_____. Supreme Court. **Katz v. United States, 389 U.S. 347, 360 (1967)**. Washington, DC, 18 dez. 1967. Disponível em: <https://supreme.justia.com/cases/federal/us/389/347/case.html>. Acesso em: 21 abr. 2017.

VARELA, Borja Adsuara. El consentimiento. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos**: hacia um nuevo modelo europeo de privacidade. Madrid: Editorial Reus, 2016. p. 151-170.

VEIGA, Armando; RODRIGUES, Benjamim Silva. A monitorização de dados pessoais de tráfego nas comunicações eletrônicas. **Raízes Jurídicas**, Curitiba, v. 2, n. 2, p. 59-110, jul./dez. 2007. Disponível em: <http://ojs.up.com.br/index.php/raizesjuridicas/article/viewFile/168/140>. Acesso em: 22 ago. 2017.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris, 2007.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, dec. 1890. Disponível em: <http://www.jstor.org/stable/1321160>. Acesso em: 06 abr. 2017.

WHITAKER, Reg. **El fin de la privacidad**: como la vigilancia total se está convirtiendo en realidad. Traducción Luis Prat Clarós. Barcelona: Paidos, 1999.

Pontifícia Universidade Católica do Rio Grande do Sul
Pró-Reitoria de Graduação
Av. Ipiranga, 6681 - Prédio 1 - 3º. andar
Porto Alegre - RS - Brasil
Fone: (51) 3320-3500 - Fax: (51) 3339-1564
E-mail: prograd@pucrs.br
Site: www.pucrs.br