GUILHERME BERTI DE CAMPOS GUIDI

PROTEÇÃO DE DADOS PESSOAIS:
A COMPOSIÇÃO DE SISTEMAS PELO DIREITO INTERNACIONAL

Tese de Doutorado

Orientador: Professor Associado Dr. Wagner Menezes

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO
São Paulo-SP
2021

GUILHERME BERTI DE CAMPOS GUIDI

PROTEÇÃO DE DADOS PESSOAIS:
A COMPOSIÇÃO DE SISTEMAS PELO DIREITO INTERNACIONAL

Tese apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para obtenção do título de Doutor em Direito, na área de concentração Direito Internacional, sob a orientação do Professor Associado Dr. Wagner Menezes.

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO
São Paulo-SP
2021

Catalogação da Publicação
Serviço de Biblioteca e Documentação
Faculdade de Direito da Universidade de São Paulo

Guidi, Guilherme Berti de Campos
Proteção de dados pessoais: a composição de sistemas pelo direito internacional ; Guilherme Berti de Campos Guidi ; orientador Wagner Menezes - - São Paulo, 2021.
217 f.
Tese (Doutorado - Programa de Pós-Graduação em Direito Internacional) - Faculdade de Direito, Universidade de São Paulo, 2021.

1. Proteção de dados pessoais. 2. Dados pessoais. 3. Direito internacional. I. Menezes, Wagner , orient. II. Título.

FOLHA DE APROVAÇÃO

Nome: Guilherme Berti de Campos Guidi

Título: Proteção de dados pessoais: a composição de sistemas pelo direito internacional

Natureza: Tese de Doutorado

Instituição: Faculdade de Direito da Universidade de São Paulo

Orientador: Professor Associado Dr. Wagner Menezes

Área de Concentração: Direito Internacional Público

Data da Banca: _____

Banca Examinadora

Professor Associado Dr. Wagner Menezes (Orientador)

_____

_____

_____

_____

_____

AGRADECIMENTOS

O que era sonho distante se concretiza e a realidade demora a ser apreendida. Não poderia ter alcançado uma fração do que cumpri nos últimos anos sem o apoio incondicional de diversas pessoas que lutaram comigo essa batalha.

Primeiramente, à Luana, minha eterna companheira, pelo incentivo, carinho e dedicação em longos anos de trabalho, enfrentando comigo novamente um projeto tão desafiante e tão exigente. Sem você nada disso faria sentido.

Aos meus pais, Fernanda e Homero, agradeço por sua confiança e pelos ensinamentos que me trouxeram até aqui. À minha irmã, Carolina, pela permanente compreensão e carinho.

Aos amigos, agradeço especialmente pela paciência, pela compreensão frente aos convites recusados e pelo apoio que, mesmo distante em tempos tão conturbados, foi essencial.

Por fim, agradeço, em especial, a meu orientador, o Professor Wagner Menezes, por acreditar que eu seria capaz de produzir algo que parecia impossível. Pelo apoio, dado nos momentos mais críticos em que a vida se interpõe no caminho. Pela amizade, que certamente marcou estes anos sob sua orientação. Pelos ensinamentos, que carregarei para toda a vida. Obrigado a todos.

Para Luana.

GUIDI, Guilherme Berti de Campos. *Proteção de dados pessoais*: a composição de sistemas pelo direito internacional. 2021. 217f. Tese (Doutorado). Faculdade de Direito da Universidade de São Paulo, São Paulo, 2021.

RESUMO

Os regimes possíveis de proteção de dados pessoais encontram dois grandes modelos no mundo moderno, o da União Europeia e o dos Estados Unidos da América. Tais sistemas de proteção de dados apresentam-se, à primeira vista, como bastante distintos, principalmente em razão da natureza do direito de privacidade em cada um desses sistemas jurídicos. Apesar da crença geral de que tais sistemas são por natureza incompatíveis, o presente trabalho objetiva justamente avaliar, em uma perspectiva jurídica, se tal alegação é correta. Adicionalmente, o trabalho busca entender em qual medida tais sistemas convergem e divergem, avaliando também o impacto passado e a capacidade futura do Direito Internacional na composição desses sistemas. O estudo baseia-se na comparação sistemática e funcional entre os dois sistemas de proteção de dados pessoais, e análise documental e doutrinária.

Palavras-chave: Proteção de Dados Pessoais, Privacidade, Estados Unidos, União Europeia, Direito Internacional.

GUIDI, Guilherme Berti de Campos. *Personal data protection*: the composition of systems by International Law. 2021. 217p. PhD Thesis, Faculty of Law, University of São Paulo, São Paulo, 2021.

ABSTRACT

The possible regimes for protection of personal data find two major models in the modern world, that of the European Union and that of the United States of America. These data protection systems appear, at first glance, to be quite different, mainly due to the nature of the right to privacy in each of these legal systems. Despite the general belief that these systems are incompatible by nature, this paper aims to assess, from a legal perspective, whether this claim is correct. Additionally, the paper seeks to understand to what extent these systems converge and diverge, and to assess the past impact and future capacity of international law in the composition of these systems. The study is based on a systematic and functional comparison between the two systems of personal data protection, and documentary and doctrinal analysis.

Key Words: Personal Data Protection, Privacy, United States, European Union, International Law.

GUIDI, Guilherme Berti de Campos. *Protection des données personnelles*: la composition des systèmes par le droit international. 2021. 217f. Thèse (Doctorat). Faculté de droit de l'Université de São Paulo, São Paulo, 2021.

RÉSUMÉ

Les régimes de protection des données personnelles trouvent deux grandes modèles dans le monde moderne, celui de l'Union Européenne et celui des États-Unis. Ces systèmes de protection des données se présentent comme assez distinctifs au premier abord, surtout en raison de la nature du droit à la vie privée de chacun de ces systèmes juridiques. Malgré la croyance générale selon laquelle ces systèmes sont incompatibles par essence, cet article a pour objectif d'analyser la véracité de cet affirmation sous une perspective juridique. En plus, on cherche à comprendre dans quelle mesure ces systèmes convergent et divergent, en analysant l'impact du droit international dans le passé et sa capacité future dans la composition de ces systèmes. L'étude est basée sur la comparaison systématique et fonctionnelle entre les deux systèmes de protection des donnés personnelles et sur l'analyse documentaire et doctrinaire.

Mots-clés: Protection des Données Personnelles; Privacité; États-Unis; Union Européenne; Droit International.

SUMÁRIO

INTRODUÇÃO 10

CAPÍTULO 1. PREMISSAS CONCEITUAIS SOBRE PROTEÇÃO DE DADOS 17

1.1. Considerações iniciais 17

1.2. Dado, informação, dados pessoais 18

1.2.1. Informação e dado 18

1.2.2. Sujeito: titular dos dados 24

1.2.3. Dados públicos e dados privados 26

1.3. Sociedade da Informação e Dados Pessoais 27

1.4. Da privacidade aos dados pessoais 43

1.5. Interdependência, globalismo e *soft law* 46

CAPÍTULO 2. PROTEÇÃO DE DADOS NO SISTEMA DA UNIÃO EUROPEIA 52

2.1. Considerações iniciais 52

2.2. Introdução sobre o sistema legal da União Europeia 52

2.3. O histórico da Proteção de Dados Pessoais na União Europeia 56

2.4. O direito à proteção dos dados pessoais 67

2.4.1. Origem: o direito à privacidade 67

2.4.2. Da privacidade à autodeterminação informática 71

2.4.3. A consolidação de um direito fundamental 77

2.5. Desenho normativo 81

2.5.1. A Convenção 108 do Conselho da Europa 82

2.5.2. Regulamento Geral de Proteção de Dados 83

2.5.3. Diretiva 2002/58/CE e a *e-Privacy Directive* 86

2.5.4. O Tribunal de Justiça da União Europeia 87

2.6. Considerações sobre proteção de dados no sistema europeu 93

2.6.1. Abrangência 94

2.6.2. Condicionantes do Tratamento de Dados 95

2.6.3. Direitos do titular e tutela 97

2.6.4. Responsabilidade, *accountability* e segurança 100

CAPÍTULO 3. PROTEÇÃO DE DADOS NO SISTEMA DOS ESTADOS UNIDOS DA AMÉRICA 103
3.1. Considerações iniciais 103
3.2. Introdução sobre o sistema legal dos Estados Unidos 103
3.3. O histórico da *privacy* nos Estados Unidos 107
3.4. Privacidade e responsabilidade civil: *torts* 114
3.5. *Fair Information Privacy Principles* e normas estatutárias 121
3.6. Proteção de dados e autorregulação 135
3.7. A FTC e os *Consent Decrees* 137
3.8. Propostas para leis abrangentes sobre proteção de dados 141
3.9. Considerações sobre proteção de dados no sistema norte-americano 145
3.9.1. Setorização, consentimento e autorregulação 145
3.9.2. Padrões de boas práticas ou lei? 149

CAPÍTULO 4. PRIVACIDADE E PROTEÇÃO DE DADOS NO CONTEXTO COMPARADO E NO DIREITO INTERNACIONAL 151
4.1. Considerações iniciais 151
4.2. Sistemas de proteção 152
4.3. Análise comparativa 163
4.3.1. Comparação detalhada 163
4.3.2. Convergências, divergências e globalismo 174
4.4. Compatibilidade: espaços para convergência 186
4.5. Direito internacional: *soft-law* e composição progressiva 191
4.6. Efeitos da composição de sistemas para o Brasil e o mundo 198

CONCLUSÃO 201

REFERÊNCIAS 205

INTRODUÇÃO

A privacidade e a proteção de dados pessoais, também chamada de *data privacy*, são temas que têm ocupado espaços cada vez maiores, não mais apenas nos congressos acadêmicos e painéis de discussão, mas também na grande mídia[1]. O cidadão comum, alheio talvez aos grandes debates teóricos, se não tem ainda completa ciência da proteção que pode reclamar para seus dados pessoais, tem no mínimo maiores chances de ser exposto ao assunto. Na Constituição Federal do Brasil, a proteção à privacidade, inserida no artigo 5º, inciso X, representa um direito fundamental. O texto adota uma diferenciação entre intimidade e vida privada, ao que podemos adotar uma conceituação mais restrita para o primeiro termo e mais ampla para o segundo. A distinção no texto legal leva Marcelo Pereira a definir como intimidade "o mais [recôndito] mais interior da pessoa, seus pensamentos, ideias, emoções etc", uma zona nuclear e reservada, de caráter espiritual, livre de ingerências. Ao mesmo tempo, o autor confina ao conceito de vida privada "tudo o que não pertença a esse âmbito íntimo, mas que, por sua vez, não transpasse à esfera pública."[2]

A inclusão da proteção de dados pessoais como parte do direito à privacidade vem do início do século XX, com mudança do Estado liberal para o Estado de bem estar social e seu reconhecimento como direito fundamental inicia-se já nos primeiros anos do século XXI, com a inclusão deste em constituições e tratados internacionais sobre o tema. No Brasil, por exemplo, discute-se o Projeto de Emenda à Constituição nº 17 de 2019 que pretende adicionar expressamente o direito à proteção de dados pessoais ao rol dos direitos fundamentais. Na União Europeia, tal direito fundamental está previsto no artigo oitavo da Carta de Direitos Fundamentais da União Europeia, desde o texto original de 2000.

O que se percebe, das mais diversas abordagens ao direito à proteção de dados pessoais, é que apesar de ter sua base primeira no direito à privacidade, a proteção de dados

---

[1]A tal respeito, confira-se, por exemplo: RONCOLATO, Murilo. Por que debater a Lei de Proteção de Dados Pessoais? *O Estado de S. Paulo Online*, 28 jan. 2015. Disponível em: http://link.estadao.com.br/noticias/geral,por-que-debater-a-lei-de-protecao-de-dados-pessoais,10000029762. Acesso em: 19 jan. 2019. PEDUZZI, Pedro. MJ finaliza nova versão de anteprojeto sobre proteção de dados na internet. *Agência Brasil EBC*, 19 out. 2015. Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2015-10/mj-finaliza-nova-versao-de-anteprojeto-sobre-protecao-de-dados-na-internet. Acesso em: 19 jan. 2019. ANGWIN, Julia. Protecting your digital privacy is not as hard as you might think. *Consumer Reports*, 20 Sept. 2016. Disponível em: http://www.consumerreports.org/privacy/protecting-your-digital-privacy-is-not-as-hard-as-you-might-think/. Acesso em: 19 jan. 2019.

[2]PEREIRA, Marcelo Cardoso. *Direito à intimidade na internet*. 1. ed. 6. impr. Curitiba: Juruá, 2011. p. 111-117.

hoje já é vista como merecedora de normatização específica, constituindo um direito fundamental por si só. Tal tendência significa, do ponto de vista prático, que a proteção de dados, ainda que ligada à privacidade, deve ser regida por normas próprias, com seus princípios e regras específicos,[3] não sendo possível apenas "remendar" as leis em vigor através da modificação legislativa ou interpretação extensiva (em realidade, *criativa*, dada a ausência de menções claras sobre dados pessoais).

Em relação aos modelos regulatórios adotados para lidar com a proteção de dados pessoais, a maioria deles tem grande foco em legislação garantista, protetiva, que impõe igualmente diversos deveres aos interessados nos dados alheios. Outros, por sua vez, relegam a tutela de direitos à autorregulação, ao direito contratual e ao Judiciário.

Tal discussão, geralmente, traz um viés essencialmente protetivo ao usuário, sem considerar, por outro lado, os interesses econômicos e o interesse geral no desenvolvimento tecnológico e na inovação. Desse modo, não é possível uma abordagem enviesada, considerando apenas os interesses de uma parcela dos envolvidos, ainda que tal parcela represente a parte mais "fraca" da transação, pois não se trata aqui de simples relação particular, mas também de algo que interessa às políticas públicas, sobretudo no que diz respeito ao acesso à informação, liberdade econômica e incentivo à inovação.

Esse equilíbrio é abordado e definido de formas razoavelmente diferentes pelos dois sistemas preponderantes de proteção de dados: o estabelecido na União Europeia e o estabelecido nos Estados Unidos da América. Enquanto aquele modelo baseia-se na tradição do *Civil Law*, este é radicado na *Common Law* e, como seria de se esperar, apresentam grandes divergências sobre o enquadramento do direito à proteção dos dados (e mesmo sua existência, em certas situações), sua extensão e as obrigações daí advindas para terceiros com quem negociem os titulares dos dados pessoais.

Dada a vocação transnacional da proteção de dados pessoais, tendo em conta a crescente digitalização das interações sociais por vias como a Internet, questiona-se se o direito à tutela dos dados é razoavelmente homogêneo ao redor do mundo ou pelo menos nos grandes mercados (o que não parece ser o caso à primeira vista).

---

[3]"O tratamento da proteção de dados pessoais de forma autônoma é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos. Os desdobramentos e efeitos do tratamento automatizado de informações pessoais, mais do que justificar mudanças e atualizações pontuais no ordenamento jurídico, formam as bases daquilo que vem sendo tratado, hoje, como um direito fundamental à proteção de dados." DONEDA, Danilo. O direito fundamental à proteção dos dados pessoais. *In*: MARTINS, Guilherme Magalhães (Org.). *Direito privado e internet*. São Paulo: Atlas, 2014. p. 66.

Ora, parece ser a concepção geral de que os direitos dos Estados Unidos e da União Europeia não estão em total harmonia no que diz respeito ao assunto da proteção de dados pessoais. Isso se extrai não só da prática cotidiana, mas também de uma simples análise superficial dos dois sistemas. O sistema norte-americano é bastante claro em sustentar que o uso dos dados pessoais para atividades econômicas é uma exigência da vida moderna e, portanto, não se há de regular algo que deve ser deixado à própria liberdade contratual das partes (o que se extrai da própria ausência de normativas federais gerais sobre o tema, exceto em áreas muito particulares como instituições de saúde e proteção ao crédito). Enquanto isso, o sistema europeu é profícuo na produção e adaptação de normas, nacionais e supranacionais, sobre o tema, mantendo a preocupação com o livre fluxo de dados pessoais entre os Estados-Membros, como seria de se esperar, mas estabelecendo também níveis gerais mínimos de proteção que, em realidade, já se mostram razoavelmente custosos em termos de esforços necessários para a conformidade de instituições e iniciativas comerciais.

Não sendo tais modelos protetivos homogêneos, resta avaliar como tais sistemas podem ser aproximados e possivelmente integrados, de modo a prover certas garantias mínimas ao titular dos dados. Considerando-se que o Direito Internacional é, provavelmente, o instrumento de excelência para a convergência de sistemas nacionais distintos, recorreremos a ele nesta pesquisa, para avaliar se e como ele pode desempenhar seu papel de integração.

O direito à proteção de dados é percebido de modo diferente nos sistemas da Common Law e da Civil Law, e a ausência, ao menos aparente, de um centro comum, mínimo, dificulta a garantia de direitos em sistemas diferentes, principalmente em um campo fático tão sujeito à remoção de fronteiras operada pela tecnologia. Assim a primeira pergunta a ser respondida deve ser: (i) quais são os fundamentos e contornos do sistema de proteção de dados pessoais da União Europeia e dos Estados Unidos da América? Essa pergunta inicial nos levará a estabelecer as bases comparativas necessárias para continuidade do estudo.

Mais que o conflito de sistemas, no entanto, buscamos avaliar a possibilidade de integração especificamente entre Estados Unidos e União Europeia no campo dos dados pessoais, dada a relevância dos dois mercados para o comércio mundial, mas também dado o poder atrativo que ambos possuem para influenciar outros estados na concepção de suas próprias legislações. Assim, a segunda pergunta a ser respondida deve ser: (ii) mesmo que haja divergências entre os sistemas, existem espaços para se criar convergência – o que

chamaremos de compatibilidade – entre os sistemas da União Europeia e dos Estados Unidos?

Por fim, a pesquisa tem como objetivo primário analisar *se* e *como* o Direito Internacional pode exercer uma função de conciliação e integração entre os sistemas predominantes de proteção a dados pessoais, representados pelos Estados Unidos e pela União Europeia e, nesse passo, ampliar o grau universal de proteção. Assim, as perguntas a serem respondidas devem ser: (iii) o Direito Internacional foi e é capaz de aproximar os dois sistemas de proteção de dados? E (iv) como pode o Direito Internacional atuar para aproximar os dois sistemas de proteção de dados?

A pesquisa desenvolver-se-á com o objetivo de fornecer resposta ao problema identificado e, em consequência, verificar a validade da hipótese preliminar elaborada. Para tanto, o presente trabalho adota a abordagem dialética, adequada aos estudos comparativos pela exposição de pontos contraditórios (ainda que parcialmente), com análise posterior (síntese). O estudo proposto, entretanto, por não se limitar à comparação de sistemas ou institutos, demandará também uma abordagem dedutiva, utilizada na fase de análise do Direito Internacional e seu papel na conciliação e integração dos diferentes sistemas.

A metodologia comparativa a ser empregada no presente trabalho merece algum detalhamento adicional. René David, em sua obra *Os grandes sistemas do Direito Contemporâneo,* de 1978, pode resumir de maneira perfeita o cabimento e a necessidade do método comparativo.[4]

Segundo as correntes majoritárias, a comparação de direitos pode ser dar em nível macro (sistemas) ou em nível micro (institutos). Pela metodologia da macro comparação, em resumo, busca-se analisar o quadro geral de determinado sistema jurídico para nele identificar fatores ou traços que o assemelhem a outros sistemas jurídicos, de modo a assim

---

[4]"O direito comparado tem uma função de primeiro plano a desempenhar na ciência do direito. Tende, com efeito, em primeiro lugar, a esclarecer os juristas sobre a função e a significação do Direito, utilizando, para este fim, a experiência de todas as nações. Visa, por outro lado, num plano mais prático, facilitar a organização da sociedade internacional, fazendo ver as possibilidades de acordo e sugerindo fórmulas para a regulamentação de relações internacionais. Permite, em terceiro lugar, aos juristas de diversas nações, no que respeita aos seus direitos internos, considerar o seu aperfeiçoamento, libertando-os da rotina.
Para que o direito comparado cumpra a função que lhe compete, é necessário que os juristas deixem de se concentrar unicamente sobre o estudo do seu direito nacional, e é necessário que, na ocasião própria, falam uso do método comparativo. (...)
É normal que os práticos do direito, na sua actividade quotidiana, limitem o seu horizonte ao direito nacional; pelo contrário, não existe ciência do direito que não seja universal. O direito comparado é um dos elementos deste universalismo, particularmente importante na nossa época, que desempenha e é chamado a desempenhar, mais ainda, uma função de primeira ordem para o conhecimento e o progresso do direito." DAVID, René. *Os grandes sistemas do direito contemporâneo*. 2. ed. Lisboa: Meridiano, 1978. p. 40-41.

poder incluí-lo dentre uma determinada “família” de direitos. A macro comparação tem amplo apelo não só pela possibilidade de encontrar convergências ou semelhantes entre diferentes sistemas quanto às grandes questões do direito, mas também por apresentar grande valor comparativo quando se avaliam os traços culturais e históricos de determinado sistema jurídico. Tal comparação, aprofundada, geralmente prescinde da análise de institutos específicos e prefere antes comparar abordagens, metodologia de aplicação do direito e mesmo as formas de *pensar* o direito.

A micro comparação, por seu lado, também chamada de comparação funcional, busca respostas para perguntas específicas na comparação entre dois sistemas. Antes de se concentrar em traços gerais, a micro comparação geralmente busca comparar institutos específicos, paralelos em funcionalidade (dentro do possível), para que se possa compreender não só a *natureza* de determinado sistema jurídico, mas sim como dois ou mais sistemas jurídicos tratam na prática determinada questão, quais regras são criadas e aplicadas para resolver determinado conflito. A micro comparação, note-se, é dita *funcionalista* pois não se preocupa necessariamente com *nomes* de institutos, mas sim com sua função social e jurídica na solução de situações juridicamente relevantes para identificar institutos semelhantes que mereçam e permitam comparação.

Enquanto as metodologias aqui expostas podem parecer de simplicidade excessiva em sua alternância, nosso trabalho não pode prescindir de nenhuma delas, uma vez que nem uma nem outra são, sozinhas, adequadas e suficientes ao presente estudo.

O método macro comparativo, por si só, teria pouco a contribuir com o presente estudo, pois apesar de já se ter noção razoável sobre as divisões clássicas entre Estados Unidos, da tradição da *Common Law*, e União Europeia, cujos sistemas jurídicos em sua maioria têm raízes romano-germânicas, a comparação a ser realizada não pode se satisfazer apenas com contornos gerais sobre como cada polo trata a questão dos dados pessoais, uma vez que a diferença cultural por trás das diferenças funcionais na regulação do assunto é bastante conhecida e razoavelmente definida.

Isso não quer dizer que a macro comparação não terá papel importante no trabalho, pois antes que se inicie o trabalho micro comparativo, é necessário sim estabelecer um contexto seguro para tal comparação, o que neste trabalho fazemos justamente pelo método macro comparativo ao avaliarmos as raízes e caminhos do direito da proteção de dados em cada país/bloco ao longo das últimas décadas, de modo a enquadrar toda a comparação em

contornos sociais claros que têm suas próprias consequências sobre a base jurídica de todo a discussão.

A micro comparação, por seu lado, também não seria suficiente como metodologia única deste trabalho, uma vez que podemos comparar institutos de proteção de dados entre Estados Unidos e União Europeia e apontar semelhanças e divergências em tais pontos, mas sem um contexto claro que nos permita verificar não só pontos de convergência, mas a própria possibilidade de convergência – o que chamaremos de *compatibilidade* – , o trabalho não poderia alcançar os objetivos anteriormente delineados. Assim, usaremos também a micro comparação para, após o desenho geral do quadro normativo de cada país/bloco, verificar quais institutos parecem já apresentar certa integração ou semelhanças, e quais demandariam maior esforço integrativo para aproximar os sistemas analisados.

Uma vez realizadas as comparações, o presente trabalho realizará a análise de tais resultados frente ao cenário atual do Direito Internacional, considerando as normas existentes sobre o tema e os espaços para atuação eventualmente identificados.

A técnica de pesquisa proposta, considerando o problema e a hipótese adotados, assim como a abordagem geral da pesquisa, é a do levantamento documental e bibliográfico.

Feitas as considerações cabíveis sobre a metodologia empregada no presente trabalho, cabe explanar brevemente como este trabalho se divide para alcançar seus objetivos.

Em um primeiro capítulo, serão exploradas algumas premissas centrais para o trabalho, o que inclui o próprio conceito de dado e de informação, a relação entre privacidade e proteção de dados, considerações sobre a chamada "sociedade da informação". Exploraremos também os conceitos importados das Relações Internacionais de "globalismo" e "interdependência", que nos auxiliarão, ao fim do trabalho, a talvez entender o *porquê* de certos movimentos globais na regulação da proteção de dados pessoais. Ainda, exploraremos também o conceito de *soft law*, este oriundo de fato do Direito Internacional, que será de extrema importância para a compreensão de *como* pôde e pode o Direito Internacional atuar em certas frentes para aproximar sistemas de proteção de dados tão distintos quanto os da União Europeia e dos Estados Unidos.

Em um segundo capítulo, será analisado atentamente o sistema de proteção de dados pessoais estabelecido na União Europeia. Essa análise passa pela compreensão das origens de tal movimento, do histórico do direito à proteção de dados pessoais naquele bloco e o

histórico da própria criação das normas centrais do sistema de proteção. Ainda explanaremos brevemente como tal sistema é composto, em termos normativos, e analisaremos os principais requisitos e institutos de proteção de dados na União Europeia, com base no *General Data Protection Regulation*, o famigerado GDPR.

Em um terceiro capítulo, será abordado o sistema de proteção de dados pessoais existente nos Estados Unidos da América, analisando as origens do direito à privacidade naquele país, os limites de tal direito, e como esse direito é aplicado, de forma adaptada, para proteção dos dados pessoais. Avaliaremos também algumas leis federais setoriais que tratam diretamente do tema dos dados pessoais, bem como algumas iniciativas interessantes, estaduais e federais, que poderiam aproximar os sistemas dos EUA e da UE.

Por fim, em um quarto capítulo, proceder-se-á à análise comparativa dos dois sistemas visitados, buscando ponto de convergência, divergências e buscando definir um grau de "compatibilidade" entre os sistemas. Ainda nesse capítulo, avaliaremos as iniciativas do Direito Internacional sobre dados pessoais e como tais iniciativas podem ter afetado cada um dos sistemas, analisando por fim se há de fato compatibilidade suficiente entre os sistemas estudados para que o Direito Internacional aja de forma efetiva para promover sua composição.

Nosso objetivo maior neste trabalho é avaliar se a aproximação dos sistemas de proteção de dados da União Europeia e dos Estados Unidos é obstada de fato por razões jurídicas, como geralmente se alega e como o próprio autor já chegou a crer, ou se tal oposição é meramente política, havendo de fato espaço para convergências e possibilidade real de desenvolver tais convergências. A mera resposta genérica, baseada geralmente em apenas uma observação superficial e em fatos geopolíticos, não atende aos requisitos de rigor científico demandados para que se faça uma afirmação tão séria de que os sistemas são ou não incompatíveis por natureza. Buscamos assim responder a tal questão de modo técnico, verificável, para que uma questão jurídica tão relevante não seja relegada ao mero "achismo", buscando no caminho entender quais seriam as consequências, positivas e negativas, de tal aproximação entre União Europeia e Estados Unidos não só para os países envolvidos, mas para o Brasil e para o mundo.

CAPÍTULO 1. PREMISSAS CONCEITUAIS SOBRE PROTEÇÃO DE DADOS

1.1. Considerações iniciais

O escopo do presente trabalho demanda, antes que se proceda ao exercício comparativo entre os sistemas eleitos e à consequente análise à luz do Direito Internacional, a exploração de conceitos e premissas básicas para tal tarefa. Esse esforço se justifica na medida em que o presente estudo parte de uma base comum de conhecimento sobre proteção de dados, mas tais preceitos fundamentais não serão explorados de modo aprofundado ao longo da exposição. Desta forma, cabe antes estabelecer as bases conceituais da discussão que será conduzida nos capítulos seguintes.

A exploração, no entanto, não se pretende exaustiva, dada a imensa quantidade de diferentes conceitos de grande relevância em cada um dos sistemas. O presente capítulo tende então a buscar justamente aqueles conceitos e premissas mais essenciais e que trespassam ambos sistemas, necessários portanto à compreensão da matéria da proteção de dados pessoais como um todo.

Dentre os conceitos a serem sumariamente apresentados, primeiro envidaremos esforços para elucidar o que é um dado pessoal e por que motivo ele reclama tamanha relevância no mundo atual. Na sequência, avaliaremos os contornos gerais da proteção de dados pessoais como instituto jurídico e sua relação com o direito à privacidade. Não se busca, naturalmente, uma descrição *total* de um sistema de proteção de dados, visto que tal esforço nos levaria a justamente descrever um ou outro sistema, mas antes à ilustração de alguns pontos que são geralmente relevantes na regulação de tal matéria.

Em seguida, traremos os conceitos de globalismo e *soft law*, que serão essenciais na análise dos resultados da comparação entre os sistemas escolhidos à luz do Direito Internacional, provendo uma fundação sólida para compreensão do fenômeno que se desenha hoje na regulamentação dos dados pessoais. Notamos já neste ponto que os conceitos não podem se confundir pois pertencem a campos diferentes, considerando as relações internacionais e o direito internacional, respectivamente. Mas, como veremos,

ambos nos auxiliam a explicar o *porquê* e o *como* dos movimentos que se percebem no cenário internacional de proteção de dados.

1.2. Dado, informação, dados pessoais

Uma primeira questão a ser necessariamente abordada diz respeito à delimitação do objeto de estudo do presente trabalho. O conceito jurídico típico de privacidade, na maioria dos sistemas, evoluiu para abarcar também a defesa daqueles atributos da personalidade e, mais especificamente, da vida privada do indivíduo que passaram a ser "destacáveis" da própria pessoa, encontrando suporte físico distinto, mas ainda assim mantendo uma relação de continência com o indivíduo que descreve. Falamos aqui dos dados pessoais.

1.2.1. Informação e dado

A expressão dado pessoal traz em si mesmo boa parte de seu conceito jurídico. "Dados", segundo o Dicionário Jurídico de Maria Helena Diniz, são, no campo do Direito de Informática, "informações que identificam ou quantificam coisas".[5] Alain Bensoussan remete o significado do termo à "representação de uma informação em uma forma convencional destinada a facilitar seu tratamento", frisando a irrelevância do suporte em que se insira.[6]

Com tal significado já se exclui a equivocada ideia de que dados pessoais dizem respeito apenas à identificação de seu titular (tendo então a abrangência reduzida a informações como nome, endereço e números de identificação), uma vez que não são apenas aqueles suficientes para identificar, mas também aqueles que exprimem características do objeto da informação.

Já "pessoal", em sua acepção do Direito Civil, refere-se ao que é "pertinente à pessoa" ou "exclusivo de certa pessoa".[7] Combinados os termos, temos já uma noção de *dados pessoais* em que estão abrangidos todos os dados, informações, sobre determinada

---

[5]DINIZ, Maria Helena. *Dicionário jurídico*. 3. ed. São Paulo: Saraiva, 2008. t. 2, verbete "Dados", p. 3-4.
[6]BENSOUSSAN, Alain. *Informatique, télécoms, internet*: réglementation, contrats, fiscalité, assurance, santé, fraude, communications électroniques. 5. ed. Levallois: Editions Francis Lefebvre, 2013. p. 89.
[7]DINIZ, Maria Helena. *op. cit.*, t. 3, verbete "Pessoal", p. 641.

pessoa – geralmente chamada *titular dos dados* – que deem conta de sua *(i)* identificação, *(ii)* suas características físicas, morais, psicológicas e de sua personalidade (traços de personalidade, gostos, hábitos); e *(iii)* sua vida privada, familiar e pessoal.

O conjunto de informações que podem ser considerados dados pessoais deve abranger toda a vida do indivíduo pela simples razão de que, sejam características pessoais ou mesmo acontecimentos que o envolveram, tais informações dão notícia do desenvolvimento da própria vida do titular dos dados. Adriano de Cupis, ainda em época anterior ao surgimento do conceito de dados pessoais, já defendia tal ideia,[8] quando sustentava que o direito ao resguardo deveria ter tal alcance.

Os dados pessoais não são coisa nova. Apesar de sua relevância hoje decorrer principalmente de escândalos envolvendo violações ocorridas em grandes empresas de tecnologia e vazamento de informações privadas na Internet, desde antes dela já se podia falar de dados pessoais, quando qualquer tipo de sistema automatizado ou observação manual e sistemática fosse mencionada, uma vez que o dado pessoal não se define pelo suporte, digital ou físico, em que se fixa, mas antes se constitui da separação de tal informação, parte da intimidade de um indivíduo, de sua pessoa, vindo a ser fixada em determinado suporte.

Segundo a Convenção de Estrasburgo, de 1981, informação pessoal é "qualquer informação relativa a um indivíduo identificado ou identificável" (art. 2º). Tal conceito é repetido incessantemente por diversas outras normas, como a Diretiva 95/46/CE e o Regulamento 2016/679 que a sucedeu na União Europeia e normatizam o assunto para aquele bloco, bem como a própria Lei Geral de Proteção de Dados brasileira.

Diversas outras leis, que antecederam inclusive a Convenção de Estrasburgo e a Diretiva de Privacidade de Dados, já adotavam definição semelhante e até mais detalhada. A lei francesa de proteção de dados, a chamada *Loi informatique et libertés*[9] define, por exemplo, os dados pessoais em seu artigo 2º como "qualquer informação relativa a uma

---

[8]"Além disto, a pessoa tem direito a conservar a discrição mesmo em torno dos acontecimentos e do desenvolvimento da sua vida. Experiências, lutas, paixões pessoais, estão-lhe intimamente ligadas, não podendo, por isso, conceder-se livre acesso à curiosidade do público. Aquele que deixou uma parte de si mesmo em certos acontecimentos, é naturalmente levado a considerá-los incluídos na sua esfera de reserva pessoal, e a não tolerar indiscrições alheias. A tendência manifesta do direito para conferir tutela ao bem do resguardo pessoal, faz com que esta aspiração possa considerar-se acolhida pela ordem pública." DE CUPIS, Adriano. *Os direitos da personalidade*. Campinas: Romana, 2004. p. 156.

[9]RÉPUBLIQUE FRANCAISE. Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés. *Journal Officiel de la République Française*, 7 janv. 1978. Disponível em: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/.

pessoa física identificada ou que possa ser identificada, direta ou indiretamente, por referência a um número de identificação ou a um ou mais elementos que lhe são próprios".[10]

A lei federal alemã de proteção de dados, a *Bundesdatenschutzgesetz,*[11] traz conceito muito semelhante em seu parágrafo 3º: dados pessoais seriam "informações específicas sobre as circunstâncias pessoais ou de fato de uma pessoa singular identificada ou identificável".

A doutrina acolheu o conceito básico de dados pessoais,[12] concentrando-se as discussões mais atuais em questões como a limitação quanto aos titulares desses dados (se apenas pessoas naturais ou se pessoas jurídicas também tem direito à proteção), à abrangência do conceito no tocante à possibilidade de identificação do titular nos casos de dados tornados anônimos e às diversas distinções quanto à sensibilidade dos dados.

Para Marcelo Cardoso Pereira, por exemplo, dados pessoais são "informações referentes a determinados aspectos da vida das pessoas",[13] enquanto para Danilo Doneda é importante diferenciar o *dado,* informação em potencial visto que não foi interpretado ou comunicado, da *informação*, que representa "algo além da representação contida no dado, chegando ao limiar da cognição".[14]

Por seu lado, Anderson Schreiber ao analisar a evolução do conceito de privacidade, inscreve na sigla de dados pessoais "características físicas, código genético, estado de

---

[10]Traduzido livremente do original:
"Article 2
(…)
Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne."

[11]BUNDESREPUBLIK DEUTSCHLAND. *Bundesdatenschutzgesetz. Bundesgesetzblatt I (BGBI),* 27 Jan. 1977.

[12]A esse respeito, confira-se por exemplo a obra de Danilo Doneda, Anderson Schreiber e Carlos Bruno Ferreira da Silva.

[13]PEREIRA, Marcelo Cardoso. *op. cit*., p. 141.

[14]"Em relação à utilização dos termos "informação" e "dado", é necessário notar preliminarmente que o conteúdo de ambos os vocábulos se sobrepõe em várias circunstâncias, o que justifica uma certa promiscuidade na sua utilização. Ambos os termos servem a representar um fato, um determinado aspecto de uma realidade. Não obstante, cada uma carrega um peso particular a ser levado em conta.
Assim, o "dado" apresenta conotação um pouco mais primitiva e fragmentada, como observamos por exemplo em um autor [Raymond Wacks, em seu *Personal information]* que o entende como uma informação em estado potencial, antes de ser transmitida; o dado estaria associado a uma espécie de "pré-informação", anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição, e mesmo nos efeitos que esta pode apresentar para o seu receptor." DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 152.

saúde, crença religiosa e qualquer outra informação pertinente à pessoa",[15] enquanto Pedro Asensio considera pessoais "os dados que permitem estabelecer um vínculo com a identidade do usuário".[16]

Os dados pessoais podem incluir: o nome, números de identificação (Números do Registro Geral (RG), do Cadastro de Pessoa Física (CPF), e do Título de eleitor), endereço, endereço eletrônico, idade, data de nascimento, senhas de acesso, localização, nacionalidade, origem racial ou étnica, convicções religiosas, políticas ou filosóficas, locais visitados, ligações pessoais, ligações familiares, números de telefone e celular, profissão, relações profissionais, empregadores, filiação sindical, informações médicas e sobre saúde em geral, traços físicos e informações biométricas, preferências de conteúdo, preferências de consumo, hábitos do dia a dia, hábitos de navegação na Internet, preferências e orientação sexual, gênero, endereço IP, informações bancárias, sobre histórico de consumo, histórico de crédito, patrimônio, informações sobre o dispositivo que utiliza para acessar a Internet, entre tantos outros que surgem com a criação de novas formas de monitoramento do usuário.

Esses dados, por sua vez, podem ser contidos em diversos meios físicos: jornais, revistas, catálogos, notas, diários, cartas, fotografias, fitas magnéticas, discos rígidos, pendrives, CD-ROMs, DVDs, entre outros. Ainda, esses dados poderiam atender a finalidades diversas, limitadas apenas pela inventividade daquele que se utiliza deles.

Além disso, os dados estão inseridos em um determinado meio, um contexto no qual são coletados, transferidos, processados e utilizados. Esses atributos, em conjunto ou individualmente, podem apresentar um critério para determinar se a regulação normativa dos dados pessoais deve ser uma, ou se merece atenção específica a determinados setores.

Analisando a primeira faceta - o conteúdo dos dados - podemos identificar, com base na profundidade da compreensão que permitem do sujeito a que aqueles dados se referem, certos grupos de dados que poderiam merecer maior proteção. A distinção entre graus de intimidade não é nova, de modo que se nota facilmente que dados médicos e dados que dizem respeito a convicções políticas ou religiosas de um indivíduo, por exemplo, são muito mais sensíveis do que informações sobre sua carreira profissional.

Não obstante, ainda que a identificação de categorias de dados mais sensíveis seja de certa utilidade, um escalonamento geral de categorias de dados não parece ser um esforço

---

[15]SCHREIBER, Anderson. *Direitos da personalidade*. 2. ed. São Paulo: Atlas, 2013. p. 137.
[16]MIGUEL ASENSIO, Pedro Alberto de. *Derecho privado de internet*. 4. ed. Madrid: Civitas, 2011. p. 294.

produtivo. Nem sempre, por exemplo, dados bancários de uma pessoa serão mais importantes que suas preferências afetivas e sexuais. Tampouco se pode afirmar que estas serão sempre mais importantes que simples informações de contato como número de telefone e endereço residencial. Afinal, afora a inexata distinção entre as diversas camadas da privacidade, como valorar em tantos detalhes tantas informações?

Uma segunda faceta dos dados pessoais diz respeito à finalidade para a qual é realizada a coleta, processamento, transmissão e utilização de tais dados. Como adiantado, os interesses na coleta de dados pessoais podem ser os mais variados.

Dentre tantos outros fins, os dados pessoais podem ser utilizados para criar perfis que permitam a um anunciante direcionar anúncios publicitários a um público-alvo extremamente específico; ou utilizar tais dados como forma de fazer previsões na variação de preços de bilhetes aéreos; identificar a propagação de doenças contagiosas em determinadas regiões com grande agilidade; identificar tendências políticas em determinados grupos da sociedade em certo momento; ou ainda, de formas eticamente e legalmente questionáveis, fornecer meios para a implementação de controle social, através de cadastros políticos, étnicos ou biológicos, policiamento ideológico, entre outros.

Interessa aqui notar que podemos separar tais utilidades, de modo geral, em dois grupos: os usos legítimos e os usos ilegítimos dos dados pessoais. Tal distinção é decisiva para a regulação dos dados pessoais, pois, apesar de não apresentar todas as respostas para a regulação do tema, estabelece um critério fundamental a ser utilizado para distinguir situações em que é possível a coleta e processamento de dados pessoais, daquelas em que o direito à privacidade deve prevalecer.

Em uma terceira faceta, os meios em que se fixam os dados pessoais parecem ter alguma relevância ao modo como a proteção legal é estabelecida. Pode-se argumentar que dados pessoais contidos em meios de comunicação (revistas ou jornais, por exemplo) merecem maior proteção, dado que há maior potencial para que esses dados tornem-se de conhecimento público, tornando-se conhecidos de milhares de pessoas, uma vez que a edição de um periódico é publicada e ofertada ao público.

O mesmo não ocorreria, no entanto, com um diário pessoal, ao qual o indivíduo confidencia informações de cunho personalíssimo. Nesse caso, ainda que seu conteúdo seja potencialmente mais delicado (sentimentos pessoais, preferências afetivas, segredos), o risco de violação, de acesso não autorizado ou divulgação ampla, de um diário pessoal é muito

reduzido em relação a uma publicação midiática. Não obstante, é falsa a afirmação de que o fator relevante, neste caso, é o suporte físico do dado pessoal. A avaliação do risco de violação não diz respeito ao suporte em si, mas ao contexto em que se insere.

Para chegar a tal afirmação, basta que se imagine o furto e divulgação do mencionado diário pessoal e seu conteúdo nos meios de comunicação. A informação, não importa onde esteja contida, pode estar sujeita à publicidade, independentemente se fixada em uma foto, um manuscrito, um vídeo ou uma carta.

Tal constatação nos leva à quarta faceta dos dados pessoais: o contexto em que esses dados são gerados, coletados e processados. O ponto fulcral da evolução tecnológica não está nas novas ferramentas, que são criadas para resolver novos e velhos problemas, mas sim na mudança que ela causa na sociedade.

Através dos anos, o sistema de registro utilizado pelo homem evoluiu, dos simples desenhos rupestres, para o registro escrito, para o registro por imagens detalhadas, para linguagens cada vez mais complexas, para a prensa, para fotografias, para a captura do movimento em filme, para as formas mecânicas de escrita, para as formas eletrônicas de registro e finalmente para a digitalização da informação.

Cada etapa desse desenvolvimento causou enormes alterações no modo como as pessoas se comunicam, como as pessoas se relacionam, como conduzem seus negócios, como vivem suas vidas em geral.

O registro escrito, por exemplo, permitiu o desenvolvimento estável dos registros históricos, do comércio e da comunicação à distância. O registro fotográfico, por sua vez, alterou o modo como as pessoas escolhem registrar determinados momentos de sua vida para posterior recordação, bastando notar como hoje é comum que uma viagem de dois dias a uma praia próxima com sua família ou amigos renda a uma pessoa muitas fotos dos momentos agradáveis da ocasião. Mais icônico ainda foi o impacto da prensa de Gutenberg na difusão do conhecimento, com a facilitação da reprodução de obras que antes exigiam extenso trabalho de um copista para que se produzisse um único novo exemplar.[17]

Ocorre que com os avanços das últimas décadas em matéria de transmissão e armazenamento de dados e a evolução dos serviços e produtos digitais de uma instância onde

[17]A respeito do impacto da tecnologia na sociedade e no Direito, confira-se LINZER, Peter. From the Gutenberg bible to net neutrality - how technology makes law and why english majors need to understand it. *McGeorge Law Review*, v. 39, n. 1, 2008. Disponível em: https://faculty.mcgeorge.edu/documents/Publications/_03b_Linzer_MasterMLR39.pdf.

o usuário não só consome informação (por exemplo, apenas lendo notícias) para uma onde o usuário também gera conteúdo (publicando textos, fotos e vídeos em redes sociais, blogs e sites pessoais, por exemplo), a quantidade de informações armazenadas e em circulação cresce exponencialmente, no seio do que se convencionou chamar de "*Web 2.0",* hoje já um conceito antigo.[18]

Os quatro aspectos aqui citados são importantes porque a regulação deve considerar todos de forma a estabelecer níveis equilibrados de proteção e ainda considerar os possíveis cenários mais comuns em que dados, informações e dados pessoais tenham relevância jurídica, seja por seu valor econômico ou pelo valor moral que possuem para seus respectivos titulares.

1.2.2. Sujeito: titular dos dados

Como visto, a doutrina e mesmo a legislação adotam um conceito de dados pessoais que faz referência apenas aos dados de pessoas naturais. Neste trabalho seguiremos tal orientação e optaremos por analisar a proteção de dados pessoais apenas das pessoas naturais, por três simples razões.

Em primeiro lugar, sendo parte da nossa proposta a análise da legislação europeia sobre proteção de dados e tendo a maioria das leis (nacionais e comunitárias) daquela região adotado um conceito que exclui os dados pessoais das pessoas coletivas (jurídicas), não seria produtivo avaliar tal aspecto da proteção de dados pela falta de elementos para comparação.

Em segundo lugar, a expressão *dados pessoais* na acepção normalmente aceita teria pouca relevância para as pessoas coletivas. Uma vez que os dados pessoais da pessoa coletiva não podem se confundir com os dados pessoais dos indivíduos que a compõem, restaria apenas uma pequena quantidade de dados que poderia ser objeto de proteção.

Em terceiro lugar, mesmo tais dados pessoais da pessoa coletiva, que não se confundem com os de seus componentes, diriam respeito a matérias melhor tratadas pelo

---

[18]"Aunque de utilidad discutible y de perfiles inciertos, el término Web 2.0 ha alcanzado notoriedad para haver referencia a las características de ciertos servicios que han contribuido a la rápida transformación que ha experimentado el modo como el conjunto de los usuarios interactúan con la Red (y no sólo con la web), algunas de cuyas manifestaciones más representativas son los blogs (weblogs) y las redes sociales, así como en general los sevicios que permiten compartir y difundir contenidos generados por los propios usuarios." MIGUEL ASENSIO, Pedro Alberto de. *op. cit.*, p. 36.

Direito Comercial, como seria o caso da identificação da pessoa coletiva (tutelado pelo direito de marcas, nomes comerciais e sinais distintivos,[19] além do direito concorrencial),[20] das características de seu funcionamento, de seus produtos e serviços, e de seus bancos de dados (tutelados pelo direito concorrencial e pelo direito da propriedade intelectual)[21] e das características únicas do negócio (tuteladas pelo direito concorrencial e enquadráveis como *trade secrets*).[22]

Neste ponto é importante notar que a diferença entre a tutela dos dados de pessoas singulares e pessoas coletivas advém de um grande abismo entre a finalidade de cada uma: a tutela dos dados pessoais da pessoa coletiva atendem a um interesse mercantil ou mercadológico[23] (aqui incluindo também as pessoas sem fins lucrativos), enquanto a tutela dos dados da pessoa singular visa quase exclusivamente a proteção da personalidade do indivíduo.[24]

É certo que em casos limítrofes pode ser desejável certa proteção a dados pessoais de entes coletivos, mas a regra geral da proteção de dados (que aqui se pretende discutir) deve ser direcionada à pessoa natural, sendo de aplicação subsidiária às pessoas coletivas e apenas no que com elas for compatível.

---

[19]Confira-se a Lei nº 9.279 de 1996, em especial o Título III, "Das Marcas". BRASIL. *Lei nº 9.279 de 14 de maio de 1996*. Regula direitos e obrigações relativos à propriedade industrial. Diário Oficial da União, Brasília, DF, 15 de maio de 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm.

[20]Confira-se a Lei nº 12.529 de 2011, com especial menção ao artigo 36. BRASIL. *Lei nº 12.529 de 30 de novembro de 2011*. Estrutura o Sistema Brasileiro de Defesa da Concorrência (...). Diário Oficial da União, Brasília, DF, 01 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12529.htm.

[21]Confira-se a Lei nº 9.610 de 1998. BRASIL. *Lei nº 9.610 de 19 de fevereiro de 1998*. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Diário Oficial da União, Brasília, DF, 20 de fevereiro de 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9610.htm.

[22]Nos dizeres de Gama Cerqueira, "A divulgação ou exploração de *segredos de fábrica* e a divulgação ou utilização de *segredos de negócio* são capitulados como crimes de concorrência desleal [atualmente previsto no artigo 195, incisos XI e XII da Lei nº 9.279/1996]. A expressão *segredo de fábrica*, nesta matéria, possui sentido específico: muitas vezes um industrial, em lugar de requerer privilégio para novo processo de sua invenção, prefere explorá-lo secretamente em seu estabelecimento, com a dupla vantagem de não revelá-lo em virtude do pedido de patente e de beneficiar-se com a proteção indefinida resultante do seu uso secreto." CERQUEIRA, João da Gama. *Tratado da propriedade industrial*. 3. ed. Rio de Janeiro: Lumen Juris, 2012. v. 2, t. 2, p. 287.

[23]"La législation relative aux données à caractère personnel ne protège pas les personnes morales. Lors du vote de la loi, la notion de données à caractère personnel concernant uniquement des personnes physiques a été dégagée en deuxième lecture à l'Assemblée nationale qui a considéré que le droit d'accès à des informations concernant des *personnes morales* risquait de donner lieu à des violations du secret professionnel et commercial." BENSOUSSAN, Alain. *op. cit.*, p. 498.

[24]Nos dizeres de Caio Mario ao avaliar o direito à intimidade, (que, como veremos adiante, é o fundamento para a proteção dos dados pessoais): "O direito à privacidade, cujas ofensas crescem em virtude das novidades tecnológicas, ganha consagração explícita no artigo 21 do Código Civil, impondo ao juiz a adoção das providências necessárias, a requerimento da parte ofendida. O dispositivo exclui a pessoa jurídica, já que quanto a esta não se pode referir a vida privada, como aspecto que é da dignidade humana." PEREIRA, Caio Mario da Silva. *Instituições de direito civil*. 22. ed. Rio de Janeiro: Forense, 2008. v. 1, p. 259.

Assim, por titular dos dados entende-se a pessoa física a quem os dados digam respeito ou sobre quem revelem uma informação sobre sua realidade física, mental, emocional ou ideológica. Os dados podem dizer respeito a mais de uma pessoa (por exemplo, a informação de que João e Maria são irmãos), e nesse caso ambos serão considerados titulares (independentes) de tal dado, se ambos puderem ser identificados.

1.2.3. Dados públicos e dados privados

Uma grande discussão do tema geral da proteção de dados que não encontra real paralelo no direito mais tradicional da privacidade é a que envolve o caráter público dos dados pessoais.

No direito tradicional de privacidade o caráter público de uma informação é um aspecto central para a definição de estar tal informação adstrita ou não à esfera de controle e sigilo mantida pela pessoa em questão. É dizer, então, que a escolha de determinado indivíduo por tornar pública determinada informação, se não há qualquer tipo de limitação no ato de divulgação ou se não há uma intenção razoavelmente objetiva em tal divulgação que limite de alguma forma a publicidade da informação, é fato central para determinar que o indivíduo não tem mais controle para *negar em absoluto* o acesso a tal informação. Obviamente, ainda é razoável que se coíba o abuso de direito no uso de tal informação, agora pública, punindo-se e garantindo a indenização por danos causados pelo mau uso da informação pública. O que não se tem, entretanto, é a faculdade de tornar tal informação novamente privada nem de exigir sobre tal informação pública as mesmas restrições que seriam aplicáveis às informações privadas.

O debate que parece inviável no direito tradicional à privacidade, entretanto, tem campo fértil na proteção de dados pessoais, uma vez que claramente se reconhece que um dado é pessoal e por isso protegido independentemente do seu caráter público ou do seu grau de publicidade.

É assim, por exemplo, que o nome de um indivíduo, mesmo que seja absolutamente público em razão de sua figura pública, de sua atuação profissional ou mesmo pelo simples fato de que ele possui perfis em diferentes redes sociais que são acessíveis publicamente,

permanece um dado pessoal e seu tratamento está submetido aos mesmos requisitos de qualquer outro dado pessoal.

Em outras palavras, o nome, um dado publicamente acessível, continua só podendo ser tratado mediante uma justificativa legal mínima – uma hipótese legal, comumente conhecida como "base legal de tratamento", que autorize seu uso - , para finalidades específicas e mediante aplicação das medidas de segurança e transparência corretas e adequadas à situação. Interessa razoavelmente pouco que tal dado possa ser coletado livremente de diversas fontes; interessa muito que, uma vez coletado, tal dado é um dado pessoal e deve ser tratado como tal.

Assim, como relevante premissa do estudo ora desenvolvido, mesmo que as regras nos modelos comparados sejam diferentes no tratamento dos dados pessoais públicos, nossa abordagem considerará o dado como pessoal pelos critérios que o assim definem, independentemente do seu grau de publicidade ou de acessibilidade, tendo tal grau mínimo de proteção como referência.

Igualmente, não nos prenderemos, ao menos não de maneira específica, nas diferenciações possíveis entre "dados públicos", "dados publicamente acessíveis" ou "dados tornados públicos", uma vez que tal debate, ainda que de grande interesse, escapa ao objeto maior deste estudo.

1.3. Sociedade da Informação e Dados Pessoais

Expostas as premissas básicas relacionadas à qualificação dos dados pessoais, duas perguntas centrais devem ser postas nesse momento: *(i)* Quais são os interesses envolvidos na questão da privacidade e dos dados pessoais que justificam tal preocupação?; e *(ii)* Qual a relevância da evolução social e tecnológica para a proteção dos dados pessoais? A tecnologia, em verdade, é fator determinante. Para responder às perguntas acima, consideremos algumas hipóteses.

Do mesmo modo como diversos institutos de estatística podem coletar informações sobre certo segmento da população, através de entrevistas pessoais feitas por pesquisadores que abordam pessoas aleatórias nas ruas de uma cidade, a Internet nesse cenário faria o papel dos entrevistadores, dos questionários e do próprio local onde as pessoas são entrevistadas.

Arnaud Belleil nos brinda com uma ilustração bastante instrutiva e, ao mesmo tempo, sombria em que vendedores nos acompanhariam a todos os lugares tentando vender seus produtos, detetives tomassem notas sobre cada movimento nosso dentro de um mercado e uma consulta médica fosse registrada e divulgada a todo um grupo de pessoas. O autor compara tal cenário à famosa obra *1984* de George Orwell, mas num caso em que o governo totalitário se visse substituído pela tirania comercial, sem que isso representasse qualquer melhora na ambientação sombria da obra de Orwell, o que não deixaria a dever em nada a como atualmente funcionam a maioria dos serviços da Internet.[25]

Diversos fatores contribuíram para o crescimento da Internet nas últimas décadas; muitos outros também foram essenciais para o surgimento de um efetivo interesse nos dados pessoais que circulam pela Internet.

O primeiro deles foi a redução dos custos de armazenamento, o aumento da capacidade de processamento dos computadores e a redução geral dos custos de efetivamente coletar e armazenar informações. As tecnologias de armazenamento de dados deram grandes saltos nas últimas décadas, sendo que hoje é comum que se encontre computadores domésticos que possuem muitas vezes a capacidade de armazenamento vista há poucos anos em grandes computadores empresariais.[26]

A capacidade de processamento evoluiu também a grande velocidade, permitindo que mesmo os mais simples computadores pessoais atuais sejam capazes de processar muito mais dados com maior velocidade que computadores de apenas dois ou três anos atrás.

Com a redução dos custos de processamento digital de dados, os custos da coleta e tratamento desses dados, antes conduzidos com o trabalho de diversas pessoas e através de métodos automáticos primitivos, também foram reduzidos sensivelmente, uma vez que agora dependem muito menos da intervenção humana no processo.

Com a facilitação do armazenamento e tratamento de informações através de computadores, a lógica por trás dessas práticas se inverteu, preferindo-se armazenar o dado para a eventualidade de se descobrir uma utilidade para ele, ao invés de coletar apenas o absolutamente necessário. O registro tornou-se regra e o anonimato a exceção.[27]

---

[25]BELLEIL, Arnaud. *@-Privacidade*: o mercado dos dados pessoais, proteção da vida privada na internet. Lisboa: Instituto Piaget, 2002. p. 52.

[26]SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional*: teoria e prática na Alemanha, Espanha e Brasil. Belo Horizonte: Arraes, 2014. p. 9-10.

[27]SILVA, Carlos Bruno Ferreira da. *op. cit*., p. 14-15.

Cresceu assim a ideia de que, quanto mais informações certa empresa possui sobre o mercado e sobre seus consumidores, mais valor ela consegue criar, através do desenvolvimento de produtos e serviços, do direcionamento destes e da definição de estratégias de atuação. Esse conceito foi apelidado de *data-hoarding*[28] e representa basicamente um interesse geral de determinado ator do mercado de reunir a maior quantidade de informações possíveis, mesmo que estas não se apresentem úteis à primeira vista, na esperança de que todas elas possam lhe fornecer uma vantagem competitiva.[29]

No entanto, não haveria tamanho interesse econômico na exploração da atividade se, apesar da capacidade de processamento, não houvesse também uma grande massa de indivíduos de onde tais informações pudessem ser extraídas. Assim, outro fator determinante para o desenvolvimento do setor foi a adoção em massa da Internet como meio de comunicação pela sociedade.

Tal expansão deveu-se, sobretudo, ao barateamento do acesso à rede e dos equipamentos necessários para tanto.[30] Mais recentemente, com o salto dos dispositivos móveis e redes celulares, o número de dispositivos conectados à Internet cresceu de modo assustador,[31] assim como a constância do uso da Internet, tornando-se ela uma ferramenta essencial para o estilo de vida atual.[32]

---

[28]MARR, Bernard. 5 signs you are a big data hoarder. *Data Informed*, Aug. 12, 2015. Disponível em: http://data-informed.com/5-signs-you-are-a-big-data-hoarder/. Acesso em: 08 fev. 2019.

[29]"Neste novo mundo, podemos analisar muito mais dados. Em alguns casos, podemos até mesmo processar *tudo* o que está relacionado com determinado fenômeno. Desde o século XIX, a sociedade depende do uso de amostragens quando se trata de grandes quantidades. Mas a necessidade dessas amostragens remonta a um período de escassez de informações, produto dos limites naturais de se interagir com as informações numa era analógica. Antes do domínio das tecnologias digitais de alto desempenho, não percebíamos a amostragem como algo artificial, mas como algo comum. Usar todos os dados permite que vejamos detalhes nunca antes vistos quando estávamos limitados a quantidades menores. O big data nos dá uma visão clara do que é granular: subcategorias e submercados que as amostragens não alcançam." MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data*: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Rio de Janeiro: Elsevier, 2013. p. 8.

[30]Para comparação, o preço de um computador IBM 610, lançado em 1957, chegava à marca dos US$ 55.000 (cinquenta e cinco mil dólares americanos). Hoje em dia, nas principais lojas de varejo encontram-se computadores a partir de R$ 1.000 (mil reais).

[31]A esse respeito, um relatório da CISCO, empresa especializada em tecnologia de redes de comunicação, estima que o tráfego diário de dados em toda a Internet, que em 2014 era de 16.400 GB por segundo, passara a marca dos 50.000 GB por segundo. CISCO Systems Inc. The Zettabyte era: trends and analysis. *Cisco Annual Internet Report*, May 2015. Disponível em: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.pdf. Acesso em: 03 fev. 2019.

[32]Tal é a importância da Internet no mundo atual que em alguns países surgiu até mesmo a discussão se a conexão à rede deveria ser considerada uma utilidade fundamental. Confira-se: PRAMUK, Jacob. FCC votes to classify internet as a public utility. *CNBC Online*, Feb. 26, 2015. Disponível em: http://www.cnbc.com/2015/02/26/fcc-votes-to-classify-the-internet-as-a-public-utility.html. Acesso em: 05 abr. 2019.

Como explica Bill Schmarzo, a informação hoje é tratada pelo meio empresarial como um verdadeiro ativo, uma matéria-prima. A combinação entre informação e clientela permite a uma empresa fidelizar seus clientes, adequar seus produtos para maximizar seus lucros, criar novas oportunidades de negócios e concorrer de uma forma mais eficiente e efetiva em seu ramo de atuação.[33]

O conflito aparente de interesses surge na medida em que as empresas, supostamente, têm o maior interesse possível em coletar e tratar a maior quantidade possível de dados que lhes sejam úteis, enquanto o indivíduo, titular dos dados coletados, supostamente tem total interesse na manutenção de sua privacidade, evitando que outras pessoas tomem conhecimento de sua vida e de sua intimidade. Essa, no entanto, é uma visão demasiado simplista da questão.

É o que se percebe, por exemplo, quando avaliamos o início dos "serviços de Internet". Em seus primórdios, inclusive pelos valores imbuídos em seu desenvolvimento, a Internet já apresentava um caráter libertário. As primeiras incursões comerciais na Internet também, em grande medida, apostaram na gratuidade dos serviços oferecidos como modo de atrair usuários e amplificar a adoção da Internet.

Até hoje, inúmeros serviços são oferecidos gratuitamente na Internet. Para possibilitar tal modelo de negócios, os fornecedores de tais serviços apostaram na troca do serviço por informações do usuário a fim de financiar sua operação.[34] É assim, por exemplo, que o Google se sustentou por muitos anos: publicidade. Até hoje, inclusive, a receita advinda da plataforma de publicidade do Google, que liga anunciantes (que escolhem o perfil do público-alvo de certo anúncio) a consumidores (que são então selecionados pelo próprio Google com base em suas informações pessoais e recebem o dito anúncio), representa uma parcela considerável de sua receita total.[35]

---

[33]"In the end, it's all about the data. Insight-hungry organizations are liberating the data that is buried deep inside their transactional and operational systems, and integrating that data with data that resides outside the organizations's four walls (such as social media, mobile, service providers, and publicly available data). These organizations are discovering that data - and the key insights buried inside the data - has the power to transforme how organizations understand their customers, partners, suppliers, products, operations, and market. In the process, leading organizations are transforming their thinking on data, transitioning from treating data as an operational cost to be minimized to a mentality that nurtures data as a strategic asset that needs to be acquired, cleansed, transformed, enriched and analyzed to yield actionable insights." SCHMARZO, Bill. *Big data*: understanding how big data powers big business. Indianapolis: Wiley, 2013. p. 3.

[34]SILVA, Carlos Bruno Ferreira da. *op. cit.*, p. 14.

[35]Segundo o anúncio de resultados do ano fiscal de 2020 da companhia, as receitas referentes à plataforma de publicidade nos *websites* do Google e em *websites* parceiros corresponde a mais de 80% da receita total da empresa. ALPHABET Announces fourth quarter and fiscal year 2020 results. *Mountain View*, Feb. 2, 2021. Disponível em: https://abc.xyz/investor/static/pdf/2020Q4_alphabet_earnings_release.pdf. Acesso em: 01 abr. 2021.

Nota-se, então, que há também um interesse do próprio usuário de oferecer seus dados pessoais a fim de acessar determinado serviço ou produto na Internet. Isso é resultado de uma avaliação pessoal do consumidor sobre o *trade-off* que a situação lhe apresenta. Mesmo quando não usados como moeda de troca, o rápido crescimento das redes sociais demonstra que há um interesse do usuário em compartilhar alguns dados pessoais, parte de sua vida, de sua intimidade, com pessoas que lhe são próximas.

Tal constatação encontra coro no ensinamento de Anderson Schreiber, para quem em uma séria de situações socialmente admitidas, ainda que não previstas em lei, o indivíduo deseja e aceita limitar o exercício de algum atributo da sua personalidade de forma pontual. É o caso do escritor que concede uma entrevista, revelando detalhes da sua vida particular ao público que, naquela situação específica, deixa de exercer seu direito à reclusão, a negar acesso a tal público às informações sobre sua vida privada. Essa limitação, defende o autor, ligada expressamente à vontade do titular, não deve ser reprimida pois objetiva justamente a realização da dignidade humana daquele indivíduo, dirige-se à sua realização como indivíduo de sua personalidade.[36]

Segundo o autor, a limitação, pela vontade do indivíduo, de um direito da personalidade não pode ser objeto de repulsa pelo Direito quando tal limitação "atenda genuinamente ao propósito de realização da personalidade do seu titular."[37] É exatamente o que se nota nesse caso.

Ainda por outra faceta, com a elevação das questões sobre privacidade e dados pessoais aos holofotes da mídia, a atividade empresarial que respeita e preserva a privacidade de seus clientes passou a ser uma imagem desejada e perseguida por grande parte do mercado. Ainda outras propostas que visam incentivar as empresas a adotar manuais de boas práticas, com a concessão de certificados e selos relativos ao cumprimento de regras de privacidade já são previstos na maioria da legislação sobre o tema, em um claro sinal de incentivo à autogestão e autorregulação.

Dada a complexidade dos interesses em jogo nas atividades que envolvam a privacidade e os dados pessoais dos usuários da Internet, parece assim ser prudente responder à primeira pergunta com uma sugestão para a busca de equilíbrio. Já alertava Rodotà que o

---

[36]SCHREIBER, Anderson. *op. cit.*, p. 27.
[37]*Id. Ibid*., p. 27.

debate da privacidade na sociedade hoje deve ser inserido no contexto do poder econômico,[38] o que nos induz a concluir que uma solução adequada deve balancear esses interesses, não através da tutela excessivamente paternalista, mas pelo empoderamento da parte vulnerável: o coletivo de usuários, consumidores, indivíduos.[39]

No aspecto prático, a segunda questão nos permite compreender exatamente como os afamados termos como "coleta" e "tratamento" realmente se concretizam no dia a dia. A *web* não é apenas o meio por onde circulam os dados, mas a própria ferramenta de coleta e o contexto. Resta saber o que tal informação quer realmente dizer. Podemos dividir nossa explicação em três partes, abordando *(i)* a coleta de dados, *(ii)* o processamento de dados e *(iii)* o emprego prático desses dados processados.

Em uma primeira situação, um usuário deseja comprar um produto através do *website* de uma loja em que confia. Para isto, escolhendo o produto, para formalizar o pedido ele é encaminhado a uma página que requer que ele faça um cadastro no site da loja, onde, para concluir a compra, ele *necessariamente* deve fornecer seu nome, sua data de nascimento, seu endereço de e-mail, seu CPF, seu gênero, informações de pagamento e seu endereço completo, além de criar uma senha, que juntamente ao seu endereço de e-mail, será utilizada para fazer *log in* na página (acessar sua página personalizada, acompanhar seus pedidos, atualizar seus dados, etc). Após preencher todos os dados, ele deve assinalar uma caixa na tela em que consigna que leu os termos de uso da loja virtual e com eles concorda. Terminado o cadastro, ele pode confirmar o pedido e finalizar a compra.

Em um segundo momento, tendo recebido o produto, o usuário percebe que este apresenta alguns problemas que ele não sabe identificar como defeitos de fabricação ou simples características falhas do produto. Para saber se outros consumidores também encontraram o mesmo defeito, como consertá-lo ou como proceder junto ao fabricante para

---

[38]"Às novas formas de coleta e tratamento de informações, possibilitadas sobretudo pelo recurso a computadores, adicione-se a crescente necessidade de dados por parte das instituições públicas e privadas: como não é imaginável uma ação que vá de encontro a esta tendência, comum a todas as organizações sociais modernas, é necessário considerar de forma realista tal situação, analisando as transformações que causa na distribuição e no uso do poder pelas estruturas públicas e privadas. Somente assim será possível desfazer o nó das relações entre a tutela das liberdades individuais e a eficiência administrativa e empresarial." RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Org., sel. e apres. de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008. p. 24.

[39]"Para identificar corretamente a perspectiva na qual todo o problema deve ser proposto não basta, portanto, uma avaliação da situação e dos poderes dos sujeitos sobre os quais se coletam informações: é necessário valorar diretamente a posição e o significado da nova "infra-estrutura informativa". Superando o tempo das denúncias apocalípticas e dos comportamentos genéricos de recusa, nos quais somente grupos marginais da opinião pública insistem, permanece garantido de qualquer forma o fato de que estamos diante de questões que, pelo conjunto de meios empregados e pelo número de sujeitos interessados, podem ser corretamente propostas somente em termos coletivos." RODOTÀ, Stefano. *op. cit.*, p. 38.

providenciar o reparo ou a troca do produto, o usuário então decide fazer uma busca *online.* Para isso, acessando a Internet através de seu navegador, ele vai até a página do buscador Google e digita sua pesquisa. Ele navega por algumas páginas e não consegue resultados precisos. Ele altera os termos de busca e tenta novamente, ao que encontra algumas páginas que contêm tutoriais para consertar o problema em questão, outras que aconselham o contato com o fabricante.

Em um terceiro momento, o usuário encontra uma outra página que parece conter a solução definitiva para o problema, mas as instruções estão bloqueadas: é necessário realizar um cadastro no novo *website* para ter acesso ao texto. Mas dessa vez, é possível pular o preenchimento do cadastro ao autorizar o acesso da página que quer consultar ao perfil do Facebook do usuário, permitindo que o *website* tenha acesso às informações pessoais, à lista de amigos e à lista de interesses desse indivíduo contidas no Facebook. Por ser o caminho mais rápido, o usuário autoriza tal acesso e chega finalmente ao texto com a solução para seu problema. O usuário, satisfeito, consegue consertar sozinho o problema, sem de nada suspeitar.

Nas semanas seguintes, no entanto, passa a receber dois ou três e-mails diários da loja em que fez a compra com produtos em promoção, além de outros e-mails promocionais de outras lojas nas quais não fez compras; ao mesmo tempo, suas pesquisas no Google passam a exibir muitos resultados promocionais em que figuram produtos semelhantes ao que usuário adquiriu; ainda, seus amigos começam a reclamar, pois passaram a receber mensagens de *spam* de uma conta de e-mail que alegam ser de propriedade do usuário.

Uma vez que os atos de *coleta*, *processamento* e *utilização* têm uma grande abrangência e certa dificuldade de compreensão por conta dos detalhes técnicos inerentes à tecnologia informacional, estando geralmente incluídos na definição de "tratamento de dados pessoais",[40] acreditamos que a compreensão desse processo é melhor buscada nos exemplos. Consideremos, portanto, a crônica narrada.

Dados pessoais são coletados todo o tempo durante o uso da Internet por determinado indivíduo. A coleta é o ato pelo qual um interessado - que pode ser uma empresa, um grupo de pessoas, um governo ou até um outro indivíduo - recebe de um indivíduo dados pessoais,

[40]O conceito pouco varia nas leis sobre o assunto, por isso podemos fazer referência à definição adotada pelo Regulamento Geral de Proteção de Dados da União Européia, em seu artigo 4º: "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição".

podendo esses dados serem fornecidos de modo consciente ou inconsciente, intencional ou não intencional, livremente ou sob coação. A definição não contribui de modo muito relevante para o entendimento. Isso porque na lei e na doutrina convencionou-se chamar *coleta* a uma infinidade de tipos de ação,[41] abrangendo-se desde o fornecimento livre, consciente e voluntário de dados até atividades ilícitas, como a ação de crackers que invadem redes e sistemas para obter dados sensíveis que lhes tragam alguma vantagem (informações bancárias, credenciais de acesso, documentos pessoais, apenas para nomear alguns).

A história narrada é muito comum à maioria das pessoas hoje e, justamente por isso, tão relevante como exemplo prático. Ocorre que nos três momentos descritos[42] houve a coleta de dados pessoais, por vezes com o conhecimento do usuário, por outras não; de modo voluntário ou não.

Na primeira situação, ao acessar o *website* da loja, o usuário já começa a compartilhar informação com ele, pois o *website* passa a monitorar os produtos procurados e visualizados, os tipos de produtos de interesse, o tipo de computador sendo utilizado para acessar o *website* (se um PC, um *tablet PC* ou um *smartphone*) e até mesmo a localização, ainda que aproximada, do usuário. Essa informação é coletada e armazenada como vinculada àquele computador específico através de pequenos arquivos chamados *cookies* que são criados pelo *website* e inseridos no computador do usuário.

Mesmo que este não tenha um cadastro na loja online, da próxima vez que acessar sua página, esta poderá ler a informação gravada nos *cookies* e identificar, com base em visitas anteriores, quais os interesses e preferências desse consumidor em potencial.

Ainda na primeira situação, o usuário fornece de forma voluntária seus dados para efetuar seu cadastro na loja virtual e confirmar sua compra. A partir disso, sempre que visitar tal *website* o usuário terá todas as informações sobre produtos visitados e seus interesses pessoais coletadas e vinculadas àquela conta. A empresa que controla a página da loja virtual já possui então uma grande quantidade de informações e, principalmente, dados pessoais do usuário depois de apenas uma ou duas horas de interação, incluindo-se ai tudo o que foi fornecido diretamente e voluntariamente pelo usuário e o que foi coletado sem seu

[41] A esse respeito, confiram-se tanto o Regulamento Geral de Proteção de Dados europeu quanto a Lei Geral de Proteção de Dados brasileira.

[42] Quando o usuário adquire o produto, quando faz pesquisas na Internet através de um buscador, quando permite a um site qualquer que acesse suas informações contidas em uma rede social.

conhecimento (apesar de provavelmente autorizado pelos “termos de uso” que o usuário declara, na ocasião do registro, que leu e aceita).

Nesse primeiro momento e também no segundo, a coleta de dados inicia-se com o simples interagir com o navegador de Internet. Muitos desses programas atualmente possuem mecanismos que possibilitam ao usuário personalizar a aparência e o funcionamento da aplicação, inclusive com alguns benefícios extras com a criação de uma conta junto à empresa que fornece o *software.*

O navegador Chrome, por exemplo, é fornecido gratuitamente pelo Google e permite que usuário identifique-se com o *log in* naquela conta no próprio navegador, permitindo que as configurações e preferências do usuário sejam sincronizadas para todos os outros lugares em que utiliza o mesmo software.[43] Ocorre que o próprio navegador coleta dados do usuário, mais especificamente dados de uso da aplicação: como o usuário usa o navegador, por quanto tempo, acessando que tipos de páginas, etc.

Mais que isso, ao utilizar um buscador (como Google, Yahoo, Bing) para fazer pesquisas na Internet, esses *websites* criam um histórico de todas as buscas feitas, onde foram feitas, quais os tipos de resultados foram mais úteis, entre diversos outros.[44] Assim, no exemplo dado, o buscador identificou que o usuário tinha interesse por um determinado produto através da simples interação com a página para finalidade outra que não o fornecimento direto de dados.

Ainda nesse segundo momento, boa parte dos *websites* visitados pelo usuário, enquanto este buscava a solução para seu problema, provavelmente utilizava também algum tipo de serviço de monitoramento, possibilitando ao *website* saber quais partes da página foram exibidas, em quais links o visitante clicou e como ele interagiu com a página em geral.

Já no terceiro momento, veja-se que além de todo o monitoramento a que o usuário já está normalmente sujeito, o *website* malicioso condiciona a exibição de seu conteúdo a uma contrapartida: o acesso a dados pessoais contidos em um outro *website.* No caso específico, uma rede social é um alvo perigoso para esse tipo de ação, pois tais serviços são criados especificamente para o compartilhamento de conteúdo entre o usuário e seus amigos.

---

[43]Para melhor ilustrar tal funcionalidade, se o usuário navega na Internet com o navegador X em seu computador pessoal, em seu computador de trabalho e em seu *smartphone*, ao fazer o *log in* na aplicação, todos os três lugares estarão sempre atualizados com as últimas páginas visitadas, as senhas salvas e os *websites* marcados como favoritos, seja qual for o aparelho efetivamente utilizado para navegar na Internet.

[44]A exemplo disto, encontramos o Google Trends, que compila os termos mais buscados por região, país, dia e hora. GOOGLE Trends. Disponível em: https://trends.google.com/. Acesso em: 02 abr. 2021.

Nesse conteúdo podem incluir-se fotos, textos próprios, vídeos, interesses pessoais e informações sobre sua vida: a postagem de fotos de suas últimas férias, o anúncio orgulhoso da aquisição de um novo carro ou da conquista de um novo emprego, lugares que visita com frequência. Todos esses dados, apesar de não terem o caráter de segredo, dão a um observador a capacidade de conhecer muitos detalhes da vida de um indivíduo, esferas da intimidade normalmente reservadas aos amigos mais próximos.

No entanto, no exemplo, todas essas informações, compartilhadas através da rede social tendo como alvo um círculo de amigos, são cedidas também a um *website* duvidoso, sem qualquer notícia sobre a utilização de tais dados, sua finalidade e seus limites.

Um modo de coleta de dados que merece menção é a obtenção forçada. Tal tipo de coleta - termo que aqui é aplicado no limiar de seu significado - consiste na invasão de uma rede ou dispositivo e subsequente coleta ilegal de dados pessoais.

Tal invasão pode ser feita por diversas vias, como a violação física (acesso direto e presencial ao computador da vítima), a interceptação de dados em trânsito (quer pelo acesso físico aos cabos de transmissão ou pelo desvio feito através de falhas do sistema), o acesso remoto através de *software* malicioso (frequentemente chamados de *vírus de computador* ou *malware*, que permitem a invasão do dispositivo à distância, através da rede) ou pelo roubo de credenciais de autenticação (o roubo do nome de usuário e senha para acesso a um dispositivo ou serviço *online*, como uma conta de e-mail).

Os meios pelos quais um criminoso pode obter dados pessoais são determinados apenas por sua imaginação, mas normalmente se utilizam de falhas na rede, no sistema ou *software* e, mais comumente, falhas humanas (como nos casos de engenharia social)[45].

São diversos os modos pelos quais a coleta de dados pessoais pode ser feita: através da solicitação direta, pelo monitoramento constante das ações do usuário enquanto na Internet, por armadilhas maliciosas ou pela coerção representada por conteúdo "registre-se para ver" que chamaremos de "*datawalls*".[46]

---

[45]Engenharia social é um método utilizado por fraudadores em que este consegue convencer a vítima que se trata de um contato legítimo, fazendo com que a vítima sinta-se à vontade para compartilhar informações que geralmente não compartilharia e que são utilizadas então para fraudes subsequentes. Um exemplo comum é o golpista que se passa por um atendente de uma instituição financeira e liga para a vítima solicitando uma atualização de dados cadastrais e às vezes até o fornecimento de senhas bancárias. O golpista então usa tais informações para, em contato com a instituição financeira verdadeira, se passar pela vítima.

[46]O termo *paywall* aplica-se à barreira estabelecida por alguns *websites* na qual todo ou parte do conteúdo necessita de uma subscrição paga para ser acessado. Analogicamente, adotamos a expressão *datawall* para o

Na situação inicialmente descrita, em um primeiro momento, os dados coletados pela aplicação de navegação na Internet, os dados gerados pelas buscas *online* e os dados gerados pelas visitas a diversos *websites* são separados e catalogados pelos diferentes serviços ou empresas que os coletaram. Assim, os dados que o navegador coletou seriam compilados em uma lista de diferentes *websites* visitados, a localização aproximada do dispositivo, os identificadores de rede (número de IP), hora e data da utilização da aplicação e alguns outros dados.

Os dados coletados pelo *website* da loja virtual são compilados levando em consideração os hábitos de consumo do usuário, valor médio dos produtos, categorias e marcas de produtos visualizados e adquiridos, além de padrões de comportamento para a compra de determinado produto.[47]

Os dados coletados pelo *website* do buscador seriam compilados com os termos de busca utilizados, que tipos de resultados (*websites*, documentos, imagens, vídeos) foram de maior interesse para tais buscas, informações sobre hora e local da conexão, identificadores de rede, entre outros. Em todos os casos, se o usuário é registrado ou possui um perfil em um serviço conectado (por exemplo o cliente que já possui um cadastro na loja virtual ou um usuário do navegador Google Chrome que fez *log in* com sua conta do Google), essas informações são associadas a essas contas existentes e servem para formar um perfil identificado que possibilita à empresa responsável pela coleta e processamento dos dados não só identificar padrões anônimos, mas associar tais padrões a uma pessoa específica.

O uso de meios eletrônicos de coleta de dados pode aparentar estar "apenas" adstrito ao uso efetivo de equipamentos eletrônicos conectados à internet, frase por si só enganosa, pois ignora uma realidade básica e atual de que o acesso à internet, em termos absolutos, avançou significativamente. Segundo estatísticas da UIT, hoje quase dois terços da

---

bloqueio de conteúdo que pode ser removido com o fornecimento de dados pessoais do usuário, seja por um registro (com o preenchimento de um formulário) ou pela requisição de acesso a dados pessoais já existentes em outro serviço (como no caso de uma rede social como o Facebook). Esse tipo de abordagem para monetização de conteúdo existe, por exemplo, nos *websites* de jornais famosos, como o Estado de São Paulo, a Folha de São Paulo e o Valor Econômico. Sobre o tema, confira-se também: SILVA, Carlos Bruno Ferreira da. *op. cit.*, p. 14.

[47]Muitas lojas virtuais como Amazon.com e BestBuy, ambas com sede nos Estados Unidos, podem determinar a probabilidade de que um usuário compre determinado produto pelo número de vezes e pela frequência com que o cliente visita a página do produto, sendo comum concederem descontos para tais produtos para incentivar a compra.

população global acessa com regularidade a Internet, enquanto 72% das residências urbanas no mundo dispõe de acesso à internet (contra 37% das residências rurais).[48]

Isto dito, é necessário reconhecer que tal acesso já permite, por si só, a coleta de dados pessoais, o que torna a regulação da proteção de dados não só um interesse abstrato de toda a sociedade (como deve ser), mas um interesse de consequências concretas para parcela considerável da população mundial que pode estar sujeita diariamente a monitoramento, por empresas ou mesmo por governos, sem seu conhecimento.

Talvez a etapa mais delicada da cadeia econômica dos dados pessoais seja a *utilização* desses dados. Referimo-nos a utilização à falta de uma palavra mais específica que possa abranger as inúmeras maneiras de emprego dos dados coletados e processados. Podemos entender por utilização, de maneira genérica, a etapa que sucede o processamento em que os dados serão analisados, em conjunto e individualmente, para criar informação sobre a qual a empresa que coleta/processa/adquire os dados pode agir. Os dados são utilizados para obter informações: de um determinado segmento do mercado, dos hábitos de determinado setor da sociedade, da recepção a um produto ou serviço.

A partir da compilação desses dados, dada a escala maciça da prática nos dias de hoje, o modo de processar esses dados varia infinitamente: combinar diferentes categorias de dados para descobrir padrões; criar perfis socioeconômicos e de consumo com base em informações como número de carros possuídos ou o número de viagens ao exterior por ano; criar divisões no coletivo com base em certos critérios como idade, gênero, ideologia política, crença religiosa, renda; buscar padrões comportamentais baseados até mesmo em fatos externos, como o aumento de compras de produtos para gestantes em certas épocas do ano, entre tantas outras possibilidades.

A grande quantidade de dados hoje coletada e processada permite diversos tipos de análise que não seriam possíveis com campos amostrais menores, uma vez que os cientistas de dados e os algoritmos por eles criados buscam sempre conexões não aparentes entre diferentes tipos de dados. Assim, por exemplo, é fácil imaginar que dados sobre o nível de renda de uma pessoa, seus interesses pessoais e seus hábitos de consumo poderiam prover informações para o desenvolvimento de produtos para determinada fatia do mercado com precisão milimétrica.

---

[48]Confira-se o estudo INTERNATIONAL TELECOMMUNICATION UNION. *Measuring digital development*: facts and figures 2020. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Pages/ff2020interactive.aspx. Acesso em: 03 abr. 2021.

O que pouco se vê, no entanto, são as conexões possíveis nos lugares em que não são esperadas. Isso porque a ciência de dados ultrapassou o viés causal da pesquisa científica e pode assentar-se em correlações. Em uma situação em que poucos dados estão disponíveis, buscar a causa para que o consumidor compre um livro de Ernest Hemingway e em seguida um livro de F. Scott Fitzgerald pode ter utilidade à empresa que os vende, a fim de que possa oferecer o segundo livro a quem se interessar pelo primeiro, e vice-versa.

No entanto, com a multiplicação dos dados disponíveis para análise, a utilidade da simples correlação entre dois produtos (até mesmo de gênero diferentes, como um livro e uma torradeira) ultrapassa a da busca de relações causais e representa esforço mais simples e passível de ser automatizado.[49]

Dessa maneira, por exemplo, o pesquisador Oren Etzioni desenvolveu em 2003 uma ferramenta que podia prever, com base em uma amostragem de 12 mil preços de passagens obtida junto a *websites* de viagens ao longo de 41 dias, a variação de preço de passagens aéreas.

Do mesmo modo, em 2009 o Google desenvolveu um algoritmo que conseguia identificar, com base apenas nos dados coletados das pesquisas feitas por seus usuários, focos de disseminação de gripe com um atraso de apenas um dia, enquanto as pesquisas oficiais do Centro de Doenças Contagiosas dos Estados Unidos levavam cerca de uma semana para chegar às mesmas conclusões.[50] Os exemplos só se tornam mais complexos e surpreendentes com o passar do tempo, permitindo supostas "maravilhas" pelo simples processamento estatístico.

Um fator agravante desse cenário é que, assim como o tratamento de dados pode ser feito de modo descentralizado através da subcontratação, nem sempre é a própria empresa que coletou os dados que se utiliza deles, sendo comum a monetização da própria atividade de coleta e tratamento: empresas especializadas recolhem e armazenam imensas quantidades de dados pessoais e criam bancos de dados para fins específicos que são então oferecidos a outras empresas que não possuem infraestrutura própria de coleta, possibilitando a elas o uso

---

[49]MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *op. cit.*, p. 35-36.

[50]"Já não precisamos necessariamente de uma hipótese válida de um fenômeno para compreendermos o mundo. Assim, não precisamos desenvolver uma ideia a respeito de quais termos as pessoas buscam em relação a quando e onde a gripe se dissemina. Não precisamos saber como as empresas aéreas determinam preços. Não precisamos nos preocupar com os gostos culinários dos consumidores do Walmart. Em vez disso, podemos sujeitar o big data à análise de correlações e deixar que eles nos digam quais buscas são as melhores para a previsão da gripe, se os preços das passagens aéreas vai aumentar ou o que famílias ansiosas querem comer durante uma tempestade. Em vez da abordagem com base em hipóteses, podemos usar uma abordagem com base em dados. Os resultados podem ser menos tendenciosos e mais precisos e quase sempre mais rápidos." MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *op. cit.*, p. 37-38.

dessas informações para, por exemplo, análise de perfis de consumidores, geomarketing e modelagem estatística.

Assim funciona, por exemplo, o serviço Mosaic, fornecido pela empresa Serasa Experian, que oferece a qualquer empresa disposta a pagar acesso a dados pessoais de potenciais clientes, pré-analisados e divididos em grupos como "Elites Brasileiras", "Juventude Trabalhadora Urbana" e "Massa Trabalhadora Urbana". Esses grupos apresentam subdivisões em subgrupos como "Elite Urbana Qualificada", que reúne adultos maduros, altamente qualificados e com altíssima escolaridade, com boa renda e um bom padrão de vida, compondo a elite instruída do país.

Já o subgrupo "Jovens Dependentes do Interior" reúne jovens de cidades do interior que moram com parentes, possuem escolaridade e renda médias, em muitos casos residentes do estado de São Paulo, que buscam a independência financeira através do trabalho. Ainda, no subgrupo "Trabalhadores manuais de baixa remuneração" estão cadastradas pessoas entre 30 e 55 anos, casadas, dependentes de ajuda governamental, com baixas renda e escolaridade e geralmente residentes de "bairros pobres e afastados".[51]

Apenas a título de exemplo, tal cenário é agravado no Brasil por iniciativas que se consolidaram nos últimos anos, como a centralização dos bancos de dados governamentais[52] e a criação do cadastro positivo.[53] Pela primeira iniciativa, o governo buscou consolidar recursos informáticos para reduzir custos e simplificar o acesso à informação, levantando questionamentos, entretanto, sobre a necessidade da imensa quantidade de informações detidas sobre cada cidadão para cada serviço público oferecido. Pela segunda iniciativa, além dos tradicionais cadastros negativos de crédito, que há décadas listam indivíduos em situação de inadimplência, foi iniciado o compartilhamento de dados de instituições financeiras para bureaus de crédito, com a finalidade de se criarem ratings para melhor classificar o risco de crédito a cada indivíduo. Ambas as iniciativas, apesar do racional econômico aparentemente razoável que as fundamentou, traz seus próprios questionamentos, que entretanto não são

---

[51]Mais informações e outros exemplos de seleção e categorização de pessoas com base em dados pessoais podem ser encontrados no *website* da empresa: SERASA EXPERIAN. Disponível em: https://www.serasaexperian.com.br/solucoes/mosaic/. Acesso em: 03 abr. 2021.

[52]BRASIL. *Decreto nº 10.046 de 9 de outubro de 2019*. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Diário Oficial da União, Brasília, DF, 10 de outubro de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm.

[53]BRASIL. *Lei nº 12.414 de 9 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de possas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial da União, Brasília, DF, 10 de junho de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.

objeto deste estudo. Cabe notar, ainda assim, que tais iniciativas aumentaram em muito a exposição do indivíduo a coletas mandatórias de dados, cenário que se repete em outros países do mundo.

Hoje, praticamente toda empresa possui um banco de dados considerável sobre seus clientes, mas não apenas com informações colhidas na relação normal entre as partes, mas também uma gama aparentemente não relacionada de dados que permite o desenvolvimento de novos produtos, análises sobre como o público interage com determinados produtos da empresa, análise de risco de crédito, dentre tantos outros.

Isso veio acompanhado do crescimento dos chamados "bureaus de dados", um jogo de palavras com o tradicional bureau de crédito, empresas com dados específicos sobre histórico de adimplência e inadimplência que indica muito bem como os dados estão à disposição de quer estiver disposto a pagar por eles. Enquanto o modelo de negócio não é objeto específico deste estudo, fica claro pelo crescimento de tal setor que o tratamento de dados pessoais pode ser uma atividade lucrativa e, como todo ramo econômico com alto retorno, exige atenção adicional para que não sejam cruzados os limites da legalidade.

Como já se tornou chavão, se nas últimas décadas se dizia que "tempo é dinheiro", hoje o que vale ouro é a informação. Dentro dessa infinidade de possibilidades, as empresas que investem na coleta e processamento de dados podem utilizá-los de diversas maneiras, e algumas com especial frequência.

O primeiro uso típico dos dados pessoais é a criação de perfis socioeconômicos que permitam a uma empresa melhor desenvolver e direcionar seus produtos. Assim, identificando certas preferências e comparando-as com os caracteres pessoais de um segmento da massa de indivíduos, a empresa pode optar por oferecer produtos com determinadas características, ou ainda utilizar tais informações para definir o preço de seu produto ou ainda alterar e manipular a percepção da marca por aquele segmento específico do mercado. Esse estudo do mercado e a análise do desenvolvimento de uma marca e de produtos em geral são afeitos ao *marketing*. Tal ramo de estudo teve um grande impulso com a era da Big Data, dado que a informação sobre o mercado é considerada hoje vital para o desenvolvimento de um negócio.

Os dados podem ser usados também, de um modo mais direto, em ações publicitárias. Tomemos como exemplo o Google e o Facebook. Em ambos os *websites*, sua interação com a página gera um grande número de dados para a respectiva empresa. Esses dados têm

inúmeros destinos, mas um deles é a disponibilização dos perfis criados a partir deles a anunciantes que desejem abordar um segmento específico do público daquele *website*.

Assim, por exemplo, pessoas que pesquisam ou postam sobre pesca esportiva, que estão na casa dos 25 a 40 anos, que falam sobre pesca com seus amigos e residem em uma determinada área provavelmente receberão, nas próprias páginas do Google e do Facebook, anúncios de produtos para pesca esportiva de uma loja local. Isso funciona pois as empresas criam perfis com base nesses dados e as empresas anunciantes, comprando a ideia de que esses *websites* são capazes de direcionar seus produtos a determinados segmentos, pagam ao *website* determinada remuneração pelo anúncio.

Esta é a mecânica, por exemplo, por trás do AdWords do Google. Os perfis não-anônimos (ou seja, ligados a um nome ou nome de usuário) não são vendidos aos anunciantes, mas utilizados pelos intermediários para vender um serviço ao anunciante. É assim que muitos serviços "gratuitos" podem ser oferecidos aos usuários sem custo, através da monetização de seu banco de dados ou de seus próprios usuários.

Os dados pessoais coletados e processados podem ser objeto de cessão ou venda[54], mas esse não é o único uso possível e talvez atualmente não mais o mais comum. Em uma era em que dados e informações estão disponíveis em grande quantidade, o desafio das empresas passa ser a disputa pela *atenção* do usuário.[55] Nesse aspecto, o uso dos dados pessoais colabora justamente para maximizar a atratividade de determinado conteúdo ao corretamente direcioná-lo a quem por ele provavelmente se interessaria.

Por fim, é necessário reconhecer que todo o processo pelo qual os dados passam, desde sua coleta até seu emprego prático, não é necessariamente linear ou realizado por uma mesma empresa, em um mesmo local. Muito se discute hoje sobre qual o caráter jurídico da rede mundial, sobre a competência para sua regulamentação e sobre a aplicabilidade de leis nacionais sobre os dados armazenados e em trânsito.[56] Tais objeções podem ser objeto de

---

[54]"La commercialisation de fichiers est devenue une des activités essentielles de certaines entreprises, telles les entreprises de courtage, et constitue par ailleurs une activité annexe das toute société disposant d'un fichier quelconque. Le fichier constitue en effet aujourd'hui un outil indispensable à la stratégie commerciale des entreprises ainsi qu'un nouvel élément du patrimoine de l'entreprise, assurant le suivi de son activité et le support des opérations de relance. Les informations contenues dans le fichier susceptibles d'intéresser d'autres organismes, confèrent en outre à ce dernier une valeur marchande." BENSOUSSAN, Alain. *op. cit.*, p. 540.

[55]KEOHANE, Robert O.; NYE, Joseph S. Power and interdependence in the information age. *Foreign Affairs*, v. 77, n. 5, p. 87-91, Sep./Oct. 1998.

[56]Sobre a persistência de tais discussões, confira, por exemplo, a discussão travada ao longo do trâmite legislativo da Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/2018).

estudos posteriores, mas interessa aqui o reconhecimento de que as informações, ao contrário dos meios físicos, não estão, em absoluto, restritas às fronteiras nacionais usuais.

Já é comum que uma empresa tenha sua sede em um país, seu centro industrial em outros três e representantes comerciais ao redor de todo o mundo. Empresas que possuem uso intensivo de dados não são diferentes, mas tal interação transfronteiras é ainda mais complexa. Muitas vezes possuem sua sede em um país, seus *data centers*, onde armazenam os dados de seus usuários, em outros países-chaves e oferecem seu serviço ao mundo todo.

Também não raro é a fragmentação vertical de determinados negócios, contando uma empresa que oferece determinado serviço ao público com serviços *de meio* prestados por outras empresas, como no caso do tratamento e armazenamento dos dados, seguindo o mesmo modelo da indústria tradicional.

Por tais razões, é importante ter em mente, ao se analisar a tutela dos dados pessoais, que estes estarão sujeitos não apenas a um processamento local, mas podem ser submetidos a diversas transferências internacionais - e consequentemente a diversos regimes jurídicos diferentes - e trocar de mãos pela venda de bancos de dados ou pela simples terceirização de alguma etapa do processamento dos dados.

1.4. Da privacidade aos dados pessoais

Tendo explorado como os dados pessoais são utilizados na atual instância da sociedade da informação e por que motivos merecem proteção, cabe um pequeno adendo sobre a relação entre a proteção de dados pessoais e o direito maior à privacidade, comparando seus elementos e aspectos jurídicos. Tal diferenciação é relevante para que possamos começar a explorar, na União Europeia e nos Estados Unidos, como tal domínio evoluiu e pode evoluir no futuro próximo.

Em apertada síntese, a privacidade *stricto sensu* é aquela privacidade tradicional, conhecida e estudada, que visitamos em obra anterior,[57] caracterizada primariamente pelo

[57]GUIDI, Guilherme Berti de Campos. *A proteção dos dados pessoais na internet*: contribuições da experiência europeia ao modelo brasileiro. 2016. Dissertação (Mestrado) – Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de São Paulo, São Paulo, 2016.

poder de exclusão de outras pessoas do conhecimento de suas características pessoais (físicas, mentais, psicológicas, sociais) e dos acontecimentos de sua vida privada.

A proteção da privacidade em sentido estrito se dá por três vias: o isolamento, a tutela inibitória e a tutela compensatória. Pela primeira via, a tutela da privacidade é exercida pelo próprio indivíduo, que pode abster-se de divulgar sua própria vida, negar o acesso de estranhos ao seu convívio privado e aos seus espaços particulares. Pela segunda via, o indivíduo busca que terceiro que se encontre violando sua privacidade cesse tal comportamento. Pela terceira, busca-se a reparação de danos, morais ou patrimoniais, causados pela intromissão alheia. Nos últimos dois casos, a tutela normalmente se dá pelo recurso ao Poder Judiciário.

A proteção dos dados pessoais, por sua vez, surge como resultado direto do advento da evolução tecnológica e ganha especial tração com o avanço da computação e da Internet, além do surgimento de modelos de negócio baseados, justamente, em dados, em informações. O instituto não se aplica apenas ao que ocorre exclusivamente na Internet, mas passa a abranger cada vez mais situações, dado que novas tecnologias de comunicação – em geral derivadas ou que se utilizam da Internet – passam a se integrar cada vez mais ao cotidiano físico. Como exemplo basta que se cite a chamada Internet das Coisas[58] ou as tecnologias vestíveis.[59]

O primeiro fator de diferenciação diz respeito ao objeto da tutela jurídica. Enquanto a privacidade em sentido estrito tem como objeto imediato a intimidade e a vida privada do indivíduo, na proteção dos dados pessoais esse é o objeto mediato, enquanto o objeto imediato são os dados em si, informações coletadas e organizadas sobre a vida de um indivíduo que descrevem, identificam ou qualificam tal pessoa (em seus aspectos físicos, mentais, psicológicos e sociais) e sua vida (compreendendo fatos, acontecimentos e comportamentos do indivíduo).

---

[58]Do inglês, *Internet of Things*, a expressão descreve a interconexão que equipamentos como fogão, geladeira, sistema de som, sistemas de iluminação e sistemas de segurança em breve terão. A conexão de tais equipamentos à Internet permitirá que o usuário se utilize deles sem estar necessariamente presente, controlando-os à distância, além de adicionar diversas outras funções. Um exemplo sempre citado diz respeito a uma geladeira capaz de inventariar seu conteúdo, avisar seu dono que o leite acabou através de um e-mail em seu celular, e apresentar um relatório nutricional do que aquele usuário vem consumindo.

[59]Do inglês, *Wearable Tech*, a expressão designa equipamentos de uso pessoal que podem ser *vestidos* pelo usuário, como relógios e óculos, que apresentam funções avançadas e interconectividade (com o *smartphone* do usuário ou diretamente com a Internet). Como exemplos mais comuns, podemos citar os *smartwatches* (relógios de pulso que normalmente se conectam a um *smartphone* para exibir notificações de e-mail e SMS, além de outras informações) e os monitores de atividade física (braceletes utilizados para medir quantidade e intensidade de exercícios físicos, ritmo cardíaco, entre outros).

O segundo fator de diferenciação encontra-se na estrutura do direito. Enquanto o direito à privacidade em sentido estrito tem caráter negativo, que importa na abstenção de terceiros de condutas que invadam a intimidade do indivíduo contra sua vontade, a proteção de dados pessoais tem, sobretudo, um caráter de controle e fiscalização.

Diferentemente da forma mais tradicional da privacidade, a proteção aos dados pessoais garante ao indivíduo o direito de fiscalizar a legitimidade e a legalidade na utilização de seus dados por terceiros, controlando ainda as finalidades dessa utilização, a qualidade e correção dos dados e as garantias de sigilo e segurança destes. Essa diferenciação estrutural nasce, sobretudo, de diferentes expectativas de privacidade: diferentemente do conceito tradicional, a proteção de dados pessoais deve considerar que a privacidade absoluta não existe, na medida em que o indivíduo, ao utilizar determinada ferramenta, abre mão de parte de seu direito.

Não se quer dizer aqui que a proteção aos dados pessoais não inclui também medidas de exclusão, que possibilitem o usuário remover seus dados pessoais, por exemplo. No entanto, esse *retirar-se* geralmente acarreta também a retirada do usuário de determinada relação contratual: o usuário que deseja que determinado fornecedor de serviço deixe de tratar seus dados pessoais, deve, para isso, encerrar a relação contratual que com ele mantem, em razão da importância do tratamento de dados para o fornecimento do serviço ou para a viabilização do modelo de negócios.

Presumindo-se que a adoção de determinada ferramenta e determinados serviços é um objetivo do indivíduo e cada vez mais uma necessidade na vida moderna, a proteção aos dados pessoais foca sua tutela, sobretudo, no controle: se o tratamento de dados pessoais é hoje um requisito ou interesse fundamental, no campo público ou privado, que tal procedimento, invasivo por natureza, seja conduzido por balizas seguras, que permitam a fiscalização do titular dos dados pessoais e evitem abusos por parte dos interessados.

O terceiro fator diz respeito ao método de tutela. Ao contrário da privacidade em sentido estrito, a proteção de dados pessoais dá maior destaque à autotutela e à tutela administrativa. A primeira se dá, principalmente, pelo estabelecimento de procedimentos a serem adotados pelos próprios usuários para exercício de seus direitos: um *website* deve sempre oferecer uma ferramenta de acesso aos dados tratados naquele serviço, deve possibilitar a remoção daqueles dados (ainda que isso inviabilize parcial ou totalmente a

continuidade da relação contratual), e deve oferecer informações claras sobre suas políticas de privacidade.

Esses poucos exemplos fazem-nos perceber que mais que simples iniciativa da parte para solucionar um litígio de maneira amigável, o indivíduo é armado com diversos poderes para acompanhar o processo de tratamento e utilização de seus dados, direitos esses normalmente garantidos por lei de modo a instrumentalizar os objetivos maiores dessa tutela.

Já a tutela administrativa ganha relevo em razão da necessidade de vias céleres de resolução de controvérsias e de regulamentação. Ela é representada pelas Autoridades de Proteção de Dados, com seus poderes normativos e interpretativos, fiscalizatórios e decisórios. O recurso à via administrativa, com um órgão capacitado e específico para tutelar tais questões, como será visto, é considerado hoje um elemento crucial de um sistema de proteção de dados abrangente e balanceado. A tutela judicial, por sua vez, permanece, com suas vias inibitórias e compensatórias. Como veremos, este é um ponto relevante na comparação entre os modelos de tutela da União Europeia e dos Estados Unidos.

Ainda que estejamos diante de dois institutos bastante diferentes, devemos reconhecer que o direito fundamental do qual emanam esses direitos, os valores protegidos, são os mesmos. Por isso, sustentamos que a privacidade tradicional e a proteção de dados podem ser reunidas sob a sigla de um *direito à privacidade em sentido amplo*, como gênero que comporta duas espécies, distintas mas aparentadas.

1.5. Interdependência, globalismo e *soft law*

Estabelecidas as bases essenciais sobre privacidade e dados pessoais, cabe explorar conceitos atinentes aos campos do Direito Internacional e das Relações Internacionais que serão relevantes para a análise a ser realizada posteriormente. Falamos aqui dos conceitos de interdependência, globalismo e *soft law*.

Antes que se dê mais um passo, é de extrema importância reconhecer que a presente investigação, de caráter jurídico, deve utilizar-se sobretudo do conceito de *soft law* em seu desenvolvimento, conceito jurídico que é. No entanto, os conceitos de interdependência e globalismo, ainda que estranhos a um arcabouço de investigação científica jurídica, serão

relevantes neste trabalho pois nos permitem vislumbrar, de modo auxiliar, um *porquê* para certas tendências identificadas.

A investigação da *razão* dos fatos não é propriamente um objetivo *jurídico* da investigação, mas questão afeiçoada à ciência política e às relações internacionais. A razão que nos leva a buscar esse contexto de causalidade provido por tais conceitos é que tal esforço, esperamos, possa trazer maior *impacto prático* ao presente estudo. Enquanto é possível realizar os objetivos estabelecidos na introdução simplesmente analisando a legislação dos blocos escolhidos e tecendo considerações sobre *como* tal integração de sistemas pode acontecer, no entanto tal condução nos deixaria sem uma compreensão mais ampla pela qual se pode atuar sobre tais resultados ou mesmo sem uma compreensão clara de por que certas vias regulatórias, como a *soft law*, podem trazer maiores benefícios para os esforços de integração e composição entre Estados Unidos e União Europeia no campo da proteção de dados pessoais.

Assim, utilizaremos os conceitos de interdependência e globalismo, ainda que com reservas, para estabelecer as razões que podem explicar certas tendências identificadas na condução do presente estudo, deixando entretanto à investigação jurídica o trabalho de buscar o objetivo principal aqui delineado, que é a compreensão de se é juridicamente possível a aproximação material dos sistemas de proteção de dados pessoais da União Europeia e dos Estados Unidos, com especial contribuição do Direito Internacional. Feitas tais considerações, podemos passar à análise dos conceitos mencionados.

O conceito de interdependência tem sua origem na década de 1970 como uma evolução do que se convencionou chamar, na teoria das Relações Internacionais, de dependência. A ideia por trás desse desenvolvimento foi explicar a razão pela qual os estados agiriam de determinada forma no contexto internacional, como tentaram também as teorias realistas e idealistas antes mesmo do desenvolvimento do conceito de interdependência.

Dentre os autores mais destacados em tal corrente, podemos mencionar Joseph Nye e Robert Keohane, que em suas obras conseguiram não só definir o conceito, mas explorar diversas facetas que tornam a interdependência uma real ferramenta de análise do comportamento dos estados em termos econômicos, militares e sociais.[60]

Para nossos propósitos, é importante entender que a interdependência é um conceito utilizado para explicar as relações de poder no cenário internacional e para identificar as

[60]KEOHANE, Robert O.; NYE, Joseph S. Power and interdependence in the information age, *cit*.

razões que levam determinado país a agir de determinada maneira, seja no âmbito internacional (em suas relações com outros países), seja no âmbito doméstico (em relação a suas políticas econômicas e sociais).

O conceito representa um fator não reconhecido em teorias realistas anteriores que julgavam que o mundo era movido por simples relações de poder militar, demonstrações de força e uma busca por segurança em um ambiente de outra forma anárquico, tendo como objetivo maior a sobrevivência e a dominância do estado em um ambiente de contínua busca pela expansão militarista.[61] A interdependência também excede as chamadas teorias idealistas, para as quais, em forte contraposição ao realismo, as relações internacionais buscam a convivência pacífica e a coibição dos abusos de poder, sendo natural então a criação de organizações internacionais voltadas à colaboração em objetivos setoriais.[62]

Na definição de Keohane e Nye, dependência significa simplesmente um estado de ser determinado ou significativamente afetado por forças ou elementos externos, enquanto a interdependência é justamente a mútua dependência. Assim, interdependência em política internacional significaria situações caracterizadas por efeitos ou influência recíproca entre estados.[63]

Em outros termos, a interdependência é uma característica ou um tipo de relação que geralmente se desenvolve no cenário internacional em que dois estados, blocos ou unidades soberanas estabelecem relações econômicas, sociais e mesmo militares em que são estabelecidos liames de mútua dependência. Um exemplo clássico é desenhado por Nye e Keohane em sua obra *Power and Interdependence* quando são avaliadas cenas do século XX, como a rivalidade entre Estados Unidos e União Soviética, mutuamente dependentes em razão da mútua ameaça de destruição por armas nucleares; e os diferentes níveis de interdependência demonstrados nas crises do petróleo da década de 1970, em que os Estados Unidos se mostrou menos sensível a tais variações de preço que, por exemplo, o Japão, altamente dependente então.[64]

---

[61]MORGENTHAU, Hans J. *Politics among Nations*: the struggle for power and peace. New York: Alfred A. Knopf, 1948.

[62]Sobre o tema, confiram-se os "Fourteen Points" do presidente norte-americano Woodrow Wilson, descritos em seu discurso de 8 de janeiro de 1918 (FOURTEEN Points, (January 8, 1918), declaration by U.S. Pres. Woodrow Wilson during World War I outlining his proposals for a postwar peace settlement. Disponível em: https://www.britannica.com/event/Fourteen-Points), e também ROCHA, Antonio J. *Relações internacionais*: teorias e agendas. Brasília-DF: IBRI, 2002, e CASTRO, Thales. *Teoria das relações internacionais*. Brasília-DF: FUNAG, 2012.

[63]KEOHANE, Robert O.; NYE, Joseph S. *Power and interdependence*. 4. ed. Boston: Longman, 2012. p. 7.

[64]*Id. Ibid.*, p. 9-10.

Dois aspectos importantes da interdependência são sensibilidade e vulnerabilidade. Sensibilidade é basicamente a medida em que determinado país é afetado, antes de qualquer resposta interna, por determinado fator ou alteração externa. Assim, um país que tem sua matriz energética inteiramente dependente da importação de recursos terá maior sensibilidade a uma alteração no preço desses recursos no mercado internacional que um estado que supra ao menos parcialmente sua demanda por tais recursos a partir de sua produção interna.

De outro lado, vulnerabilidade é medida na disponibilidade de outras medidas, caminhos ou recursos alternativos, disponíveis em custos razoáveis a determinado estado, e passíveis de utilização como alternativa à submissão dos efeitos decorrentes dos fatores externos. Assim, uma país que pode recorrer a uma fonte alternativa de energia, estará menos vulnerável às variações do preço do petróleo que outro país que não tenha tais recursos a sua disposição. Disso, decorre que a vulnerabilidade é medida geralmente a partir de uma hipótese de *mudança de políticas:* podendo o estado alterar certas decisões ou políticas internas (por exemplo, sua matriz energética), sua vulnerabilidade corresponderá justamente ao grau de dificuldade de tal alteração e dos efeitos remanescentes dos fatores externos que não puderam ser mitigados com tal mudança de política.

Tais conceitos serão de grande valia para avaliar e compreender as razões de certas medidas recentes tomadas tanto pelos Estados Unidos quanto pela União Europeia na aproximação de seus sistemas de proteção de dados pessoais, por exemplo na forma do Privacy Shield.

Já o globalismo, termo preferido à “globalização” poderia ser considerado a aplicação das relações interdependentes a contextos complexos, envolvendo mais de dois países e, especialmente, considerando não apenas um foco estreito para análise da relação entre esses atores, mas sim na totalidade das relações, sejam elas econômicas, sociais ou militares entre os atores em questão.

Em diversos casos é comum ouvir a expressão “globalização” para descrever esse tipo de processo de expansão dos liames de interdependência complexa entre os estados, mas nesse ponto concordamos com Nye e Keohane quando estes dizem que a expressão leva à presunção de algo que necessariamente está sempre em crescimento. Ocorre que esse aspecto de integração complexa entre agentes internacionais é variável e o fato de ser o conceito relativamente novo não impede que identifiquemos altas e baixas em sua aplicação prática

ao longo das décadas dos séculos XIX e XX. Assim, na linha de tais autores, preferimos a expressão globalismo, que pode indicar tanto maior ou menor "densidade" de tal globalismo: as relações podem ser mais ou menos globais ou globalizadas.

Enquanto se diria interdependente a relação entre dois países em que o primeiro depende do segundo para o fornecimento de derivados do petróleo e o segundo depende do primeiro na obtenção de minério de ferro, o globalismo representa uma análise integral do relacionamento desses dois atores, inclusive no contexto do relacionamento deles com outros países.

Na concepção de Nye e Keohane, o globalismo é um estado de coisas envolvendo redes de interdependência em um contexto multicontinental. São fluxos e influência em capital, bens, informações e pessoas, bem como questões biológicas e ecológicas, que criam essas conexões. Se a interdependência se refere a situações caracterizadas por efeitos recíprocos entre países distintos, o globalismo pode ser considerado um tipo de interdependência, mas com características especiais: primeiramente, ele se refere a uma multitude de conexões, uma rede se se quiser, mas não vínculos simples, bilaterais; em segundo lugar, para que tal rede seja considerada de fato global, devem se considerar distâncias multicontinentais e não meramente regionais.[65]

Assim, o globalismo tem dois requisitos básicos: tratar sempre de uma multiplicidade de relações em diversos domínios e considerar relações de nível global e não apenas local.

Do ponto de vista jurídico, tais conceitos de relações internacionais nos auxiliam a entender que razões levam sistemas jurídicos de diferentes origens a convergir para adotar institutos semelhantes ou, ao menos, compatíveis, mas não *como* tal aproximação ocorre.

Na presente análise, é de suma importância o conceito de *soft law*, que, como será visto, foi e é um importante instrumento no campo da proteção de dados para o desenvolvimento tanto de normas internacionais como de normas nacionais sobre o tema. Na nossa visão, é também feito da *soft law*, mesmo que não isoladamente, a aproximação que tem sido observada entre os diversos modelos de proteção de dados existentes no mundo atual.

---

[65]KEOHANE, Robert O.; NYE, Joseph S. Globalization: what's new? what's not? (and so what?). *Foreign Policy*, n. 118, p. 105, 2000.

Soft law, no conceito consolidado pela doutrina, traduz a ideia normas não vinculantes,[66] mas não se trata de um conceito sem seus próprios requisitos. Já se quis dizer que a *soft law* não é de fato uma norma ou que não seria uma norma jurídica per se, mas apenas uma norma ética. O fato de que seu descumprimento raramente tem uma consequência formal e prática colabora para tal ceticismo quanto a seu valor jurídico.

No entanto, a *soft law*, como enquadrada pela doutrina moderna, apresenta plenamente os requisitos essenciais para a caracterização de uma norma jurídica, fugindo então do conceito antiquado de que a norma não é norma se não preconizar uma sanção por seu descumprimento. Assim, segundo Wagner Menezes, é possível definir a *soft law* como sendo documentos formais e solenes derivados de alguma forma de um foro internacional, possuindo conteúdo variável e não obrigatório, fundados no princípio da boa-fé e que não vinculam seus signatários a obrigações firmes, mas, por seu caráter e relevância no contexto global, refletindo princípios e concepções éticas e ideais, têm capacidade de produzir repercussões no Direito Internacional e no próprio direito interno dos Estados.[67]

Dentre os exemplos clássicos da *soft law*, encontramos resoluções e recomendações das organizações internacionais, pareceres de organizações internacionais, conferências, tratados não ratificados ou tratados-modelo. No entanto, a *soft law* não se limita a isto, visto que sua própria definição abre espaço para que venha a abranger outros tipos de documentos que, mesmo que possuam o status de tratado internacional, por exemplo, podem ser classificados também como *soft law*. É o caso de tratados cujas regras sejam meramente declaratórias ou sem efeito vinculante, tratados que não apresentam de fato obrigações a serem cumpridas, mas apenas metas ou ideais a serem alcançados. Esse tipo de tratado existe não por uma falha, mas sim pois são instrumentos importantes para flexibilização que permitem aos estados, mesmo quando um compromisso absoluto não seja possível, acordar sobre metas que poderão então ser perseguidas das mais variadas formas pelo estado envolvido, tendo então tal tratado o efeito prático de uma *soft law*, apesar de revestir-se formalmente como um tratado ratificado.[68]

---

[66]MENEZES, Wagner. *Ordem global e transnormatividade*. Ijuí: Ed. Unijuí, 2005. p. 147.
[67]*Id. Ibid.*, p. 147.
[6868]MENEZES, Wagner. *Ordem global e transnormatividade*, *cit.*, p. 153.

CAPÍTULO 2. PROTEÇÃO DE DADOS NO SISTEMA DA UNIÃO EUROPEIA

2.1. Considerações iniciais

Estabelecidas as premissas gerais do trabalho, cabe então iniciar o esforço comparativo entre o sistema de proteção de dados da União Europeia e o sistema de proteção de Dados dos Estados Unidos da América. Para tanto, cumpre primeiro explorar e analisar o sistema de proteção de dados da União Europeia.

A análise a ser empreendida nos transporta inicia com o desenvolvimento de premissas específicas sobre o funcionamento da União Europeia, uma vez que um elemento marcante de tal sistema é sua capacidade integrativa. Isso é especialmente importante quando recordamos que a União Europeia estabeleceu regras supranacionais sobre o tema justamente com o interesse de homogeneizar a proteção dos cidadãos europeus, mas também para garantir o livre fluxo de dados entre os Estados-Membros, o que a regulação busca alcançar ao estabelecer um padrão único de proteção.

Estabelecidas tais premissas, passaremos pelo desenvolvimento do direito à privacidade como direito da personalidade e de seu desenvolvimento em um direito autônomo à proteção dos dados pessoais, para finalmente avaliar o desenho normativo vigente e os elementos centrais desse sistema. Desse modo, busca-se contextualizar a análise funcional para entender um caractere central do sistema europeu que se focaliza na própria natureza dos direitos relacionados à proteção de dados pessoais.

2.2. Introdução sobre o sistema legal da União Europeia

Antes que iniciemos o estudo da proteção de dados na União Europeia, é relevante repassar brevemente algumas premissas sobre a União Europeia, seu funcionamento e seu sistema normativo, dado que o bloco talvez represente hoje um dos casos mais avançados de integração regional, o que por sua vez se traduz em grande complexidade em seu funcionamento.

A União Europeia é formada por 27 Estados-Membros e dentre seus principais órgãos encontramos o Conselho Europeu, o Conselho da União Europeia a Comissão Europeia e o Parlamento Europeu.

O Conselho Europeu é formado por um representante de cada um dos 27 Estados-Membros e o Presidente da Comissão Europeia. Suas atribuições gerais incluem a definição das prioridades para o bloco e o direcionamento político da agenda do bloco. Em relação aos demais órgãos, apesar de não haver propriamente submissão, o Conselho Europeu é o órgão máximo em termos políticos.

O Conselho da União Europeia (também conhecido como Conselho de Ministros ou simplesmente o "Conselho"), por seu lado, é o principal órgão de decisão da União Europeia, tanto em questões políticas quanto legislativas, sendo formado por um ministro de cada um dos 27 Estados-Membros (que podem variar, de acordo com o tema da reunião). As decisões dos ministros reunidos no Conselho têm o condão de vincular seus respetivos Estados às decisões do Conselho, de modo que este seja talvez um dos mais importantes órgãos da União. Suas atribuições incluem a coparticipação no processo legislativo juntamente ao Parlamento Europeu: enquanto a Comissão geralmente propõe uma nova normativa e o Parlamento a discute e modifica, é papel do Conselho a aprovação final e adoção da normativa, transformando-a em um regulamento, diretiva ou decisão, por exemplo.

Já o Parlamento Europeu é composto por 705 representantes eleitos, sendo que seu papel corresponde a (i) desenvolvimento legislativo, supervisão de outras instituições, representação democrática e desenvolvimento orçamentário, conforme artigo 14 do Tratado de Lisboa de 2007, que veio a consolidar o Tratado da União Europeia e o Tratado sobre o Funcionamento da União Europeia. Apesar de aparentar ser o principal órgão responsável pela atividade legislativa, na verdade o Parlamento tem muito mais uma função consultiva e deliberativa, atuando de forma a propriamente *aprovar* normativas apenas em certos tipos de procedimento. O Parlamento também, em geral, não propõe nova legislação, podendo apenas instar a Comissão a apresentar uma proposta sobre um tema que lhe pareça relevante.

Por fim, a Comissão Europeia é o órgão executivo da União Europeia e atua, em termos gerais, para implementar as decisões do Parlamento e do Conselho, tornando efetivas as normativas supranacionais, supervisionando sua aplicação e, quando necessário, sua adoção pelos Estados-Membros. A Comissão, em outros aspectos, assemelha-se muito ao ramo executivo de um governo, no sentido de que é a responsável pela execução de políticas,

pela garantia da correta execução dos tratados e do cumprimento pelos Estados-Membros de suas respectivas responsabilidades, bem como pela negociação de tratados internacionais em nome do bloco, cabendo, entretanto, ao Conselho aprova-los de forma definitiva. No campo legislativo, cabe à Comissão o papel de proposição de nova legislação, considerando sempre as orientações políticas e diretivas gerais estabelecidas pelo Conselho Europeu e pelo Parlamento.

Vale mencionar também a Corte de Justiça da União Europeia, um órgão judicial formado pelo Tribunal Geral e pelo Tribunal de Justiça, que atua para fiscalizar e interpretar as normas supranacionais da União Europeia, fiscalizar a implementação de tais normas pelos Estados-Membros e para, em termos gerais, controlar a legalidade dos atos dos demais órgãos da União supranacional.

A União Europeia, de larga história cuja explanação não é objeto deste trabalho, é atualmente regida por diversos instrumentos internacionais, dentre os quais os mais relevantes são o Tratado da União Europeia de 1992 (também conhecido como Tratado de Maastricht), o Tratado sobre o Funcionamento da União Europeia de 2007 (conhecido anteriormente como Tratado de Roma de 1957), tendo ambos sido alterados e consolidados pelo Tratado de Lisboa de 2007, e a Carta de Direitos Fundamentais da União Europeia de 2000.

O Tratado da União Europeia, em resumo, cria as instituições e regras basilares do que se entende hoje por União Europeia, focando na integração entre os Estados-Membros e o estabelecimento de um mercado único europeu, abrangendo a circulação de pessoas, mercadorias, serviços e moeda.

Já a Carta de Direitos Fundamentais da União Europeia, de 2000, funciona como uma Carta de valores fundamentais e estabelece, em termos diretos, os direitos fundamentais que serão basilares para a estruturação de todas as demais instituições, normas e valores defendidos pela União Europeia. A Carta funciona quase como uma matriz principiológica para os demais tratados e também para as normas produzidas no seio do bloco, o que resulta em sua grande importância para este estudo, dada a consolidação do direito à proteção dos dados pessoais em tal documento, como será explorado adiante.

Ainda, o Tratado sobre o Funcionamento da União Europeia, que passou por sua última grande reforma em 2007, é voltado à estruturação detalhada das instituições que compõem a União Europeia, atentando tanto ao seu papel institucional quanto aos detalhes de seu funcionamento interno, seus componentes, suas atribuições, competências e poderes,

dentre outros assuntos. O Tratado sobre o Funcionamento da União Europeia é também de grande interesse para este estudo pois define os tipos normativos supranacionais existentes e suas características essenciais.

O quadro normativo supranacional europeu é composto por normas de diferentes naturezas. Em apertada síntese, regulamentos são normas vinculativas diretamente aplicáveis a todos os países, incluindo-se aí seus cidadãos e pessoas jurídicas, valendo como se direito nacional fosse. Diretivas são normas adotadas pela Comissão e pelo Parlamento Europeu que fixam um objetivo que todos os Estados-Membros devem alcançar, cabendo a cada um decidir os meios exatos para tal, respeitando os preceitos básicos da norma supranacional. Em outras palavras, as Diretivas criam uma obrigação para o Estado-Membro de adotar medidas (leis, por exemplo) para cumprir os objetivos previstos em tais instrumentos, mas não são diretamente aplicáveis aos cidadãos. Decisões são atos vinculativos apenas para partes específicas, sejam elas Estados ou empresas, sendo diretamente aplicáveis para os envolvidos. Recomendações e pareceres são atos não vinculativos e podem ser emitidos por diversas instituições europeias, contendo normalmente a recomendação de se adotar ou evitar certa posição ou comportamento, ou a declaração de uma posição quanto à determinada questão.[69]

A complexidade do sistema normativo só cresce ao descermos um patamar, das normas supranacionais para as normas nacionais de cada Estado-Membro. No tema da proteção de dados pessoais, as normativas nacionais de cada Estado-Membro são razoavelmente uniformes em seus quesitos centrais, uma vez que em sua maioria decorreram da adoção de normas internas a partir do comando da Diretiva nº 95/46/CE, a antiga Diretiva de Proteção de Dados, que foi substituída pelo Regulamento Geral de Proteção de Dados, o GDPR (na sigla inglesa, *General Data Protection Regulation),* como ficou largamente conhecido.[70]

Com a aprovação do Regulamento, as normas nacionais permaneceram, em tese, em vigor naquilo que não fossem conflitantes com o GDPR; as diferenças e especificidades da

---

[69]Os atos jurídicos normativos da União Europeia estão descritos no artigo 288 do Tratado sobre o Funcionamento da União Europeia (TFUE). O TFUE resultou da alteração do Tratado de Roma, de 1957, que estabeleceu a Comunidade Europeia, pelo Tratado de Lisboa assinado em 2007, que reforma os tratados base da União e reorganiza suas instituições.

[70]Regulamento 679/2016. EUROPEAN PARLIAMENT. COUNCIL EUROPEAN. *Regulation (EU) 2016/679 of the European Parliament and of the Council.* 27 April 2016. on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/o.

regulamentação, deixadas ao arbítrio dos Estados-Membros pelo próprio Regulamento, permaneceram em grande parte as mesmas que já separavam os diversos regimes na época da Diretiva, mas agora unificados por um "ramo central" mais espesso que a outrora vigente Diretiva, que deixa ainda mais espaço de escolha aos Estados-Membros.

Não nos aventuraremos às minúcias da regulação nacional neste estudo, dado que nosso objetivo maior diz respeito não a especificidades (e nem isso a comparação proposta exige), mas sim a traços mais gerais e centralizados para buscarmos justamente pontos de conexão e convergência entre União Europeia e Estados Unidos.

2.3. O histórico da Proteção de Dados Pessoais na União Europeia

A proteção dos dados pessoais já não era matéria nova nos Estados-Membros da União Europeia quando da aprovação da primeira diretiva sobre o assunto.[71] Em verdade mais de dez anos antes do início dos debates sobre a possibilidade de regulamentação da matéria em nível comunitário através de uma diretiva, a proteção dos indivíduos em relação ao processamento automático de dados pessoais já era discutida em diversos meios.

Na França, ainda no começo do século XIX, os tribunais ainda relutavam em reconhecer um direito subjetivo à proteção da intimidade, tratando o assunto como situação excepcional. Os tribunais franceses só vieram a falar do direito à privacidade, incidentalmente, em decisão de 1858, no caso Felix c. O'Connell,[72] apesar da existência anterior de regras esparsas que, com a criação do conceito de privacidade, foram incluídas sob esta sigla, como é o caso do segredo de correspondência, decretado na França já em 1790, com leis que aboliam os famigerados *cabinets noirs*.[73]

Foi apenas em 1970, após longo processo de elaboração pela jurisprudência que o legislador modificou o artigo 9º do Código Civil Francês para introduzir um "direito ao

[71]A Diretiva 95/46/CE que traçava as linhas gerais da matéria até 2018.

[72]JURISPRUDENCE française en matière de droit civil. *Revue Trimestrielle de Droit Civil*, Paris, p. 111, jan./mars. 1971.

[73]Escritórios oficiais franceses responsáveis pela fiscalização da correspondência, onde cartas de pessoas ou com conteúdo suspeito eram abertas para verificação. A abolição de tais práticas e a confirmação do sigilo de correspondência veio pela Lei 10 de 24 de agosto de 1790 e Lei 10 de 11 de julho de 1791, na esteira da Revolução Francesa e da reforma de institutos e instituições características dos regimes absolutistas. A esse respeito, confira-se FERNANDES, Milton. *Proteção civil da intimidade*. São Paulo: Saraiva, 1977. p. 17.

respeito de sua vida privada".[74] A partir desse momento, os tribunais passaram a produzir grande quantidade de decisões sobre a proteção da privacidade.[75]

Na Itália, a questão, no entanto, começou a atrair atenção por volta de 1971, com a vinda à tona do chamado "primeiro caso Fiat"[76]. Naquele ano, tornou-se pública a informação de que a Fiat, fabricante de automóveis, vinha se utilizando, desde 1948, de dados pessoais fornecidos pela polícia, pelos militares e pelo serviço secreto italiano – dados esses coletados desde o período fascista – para selecionar seus empregados.[77] Foi este o episódio que marcou o início dos debates sobre privacidade e dados pessoais no cenário legislativo do país, tema impulsionado ainda pela súbita consciência de que outros países vizinhos começavam também a se preocupar com a questão.

A partir de então, a doutrina e a jurisprudência foram responsáveis pela evolução do *diritto alla riservatezza*, que veio abarcar também a proteção dos dados pessoais, entendida como simples extensão da proteção à personalidade e à identidade pessoal.[78] Não obstante os diversos projetos de lei apresentados desde então, o país permaneceu até 1996 sem legislar sobre o assunto, o que causou diversos problemas a empresas italianas no meio tempo, sendo o mais famoso deles o "segundo caso Fiat" que envolvia a transferência de dados de funcionários da filial francesa para a sede na Itália.

---

[74]FERNANDES, Milton. *Proteção civil da intimidade*, *cit.*, p. 25.

[75]"A jurisprudência francesa é abundante em matéria de direitos da personalidade, ao proteger a vida privada, a imagem, o nome, a sepultura, os souvenirs de família, as 'lettres missives', o direito moral de autor e outros bens da personalidade. Sua força se fez sentir, quando em 17 de julho de 1970 foi promulgada a Lei nº 70.643, que modificou o art. 9º do Código Civil, ao reconhecer a proteção da vida privada, nestes termos: '*Chacun a droit au respect de sa vie privée'.* A nota do referido artigo assinala que *les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire teutes mesure, telles que séquestre, saisie et autres, popres à empêcher ou faire cesser un atteinte à l'intimité de la vie privée; ces mesures peuvent, s'il y a urgence, être ordenées en référe."* GOGLIANO, Daisy. *Direitos privados da personalidade*. São Paulo: Quartier Latin, 2013. p. 86.

[76]Não se pode confundir este caso com o famoso "caso Fiat" dos anos 1980, no qual a Fiat italiana foi impedida pela CNIL, autoridade francesa de dados pessoais, de receber dados dos empregados de sua filial francesa pela ausência de legislação sobre proteção de dados pessoais.

[77]DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, *cit.*, p. 249-250.

[78]"A *identità personale* compreende, sucintamente, não apenas a identificação de uma pessoa que é feita pelos registros públicos, porém uma representação pluridimensional de sua identidade (e, consequentemente, de sua personalidade), que compreende também suas atividades, posição profissional, social, cultural, religiosa e ideológica. A trajetória do *diritto alla identità personale* apresentou diversos paralelos com o próprio direito à privacidade, principalmente quando se reconhece nele o poder de disposição sobre informações pessoais, o que fez com que diversos interesses, que em outros países eram tidos como referentes ao direito à privacidade, na Itália fossem tutelados através do direito à identidade pessoal." [Nota de rodapé] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, *cit.*, p. 250.

Conta-se que a primeira lei nacional[79] sobre a matéria foi a lei sueca sobre o controle de bancos de dados, de 1973. Em 1977 foi a vez da promulgação da lei federal alemã sobre o tema, seguindo o exemplo do *Land* de Hesse, a lei denominada *Bundesdatenschutzgesetz.* A ela seguiu-se a lei francesa de 1978, denominada *Informatique et Libertés*, pela qual se instituiu a autoridade de dados pessoais do país, a *CNIL - Commission Nationale de l'Informatique et des Libertés.* Não muito mais tarde países como Dinamarca, Áustria e Noruega promulgaram também leis próprias.[80]

Não obstante o quadro internacional, a criação de regras específicas, estritas e vinculantes sobre o processamento de dados pessoais não decorreu naturalmente de um interesse dos órgãos supranacionais da União Europeia ou de seus Estados-membros. Duas correntes tentam explicar a evolução do trato da matéria no seio da comunidade europeia, cada uma optando por modelos opostos para explicar a sequência de eventos que levou à aprovação da Diretiva 95/46/CE.[81] A análise de Abraham Newman sobre o papel dos agentes transnacionais no caso da referida diretiva demonstra em detalhes a dinâmica.

O primeiro modelo é baseado em uma lógica intergovernamental liberal, segundo o qual o desenvolvimento da matéria no âmbito comunitário se deu pela intervenção dos Estados-membros mais poderosos do grupo em razão de seus interesses econômicos. Tais preferências econômicas seriam agregadas, em nível nacional, e representadas no nível europeu por uma liderança do Poder Executivo, que passaria a influir, de acordo com seu "peso" econômico e político, no direcionamento da política comunitária.

A partir da década de 1970, a França, a Alemanha e o Reino Unido adotaram regras estritas sobre a proteção de dados pessoais, o que não foi o caso de países como Itália e Espanha. Segundo o modelo de análise, as empresas dos países que já haviam adotado regras sobre dados pessoais teriam uma desvantagem em relação a empresas situadas em outros Estados-membros, estas beneficiadas pela ausência de regulação.

---

[79]A primeira lei sobre o assunto não tinha alcance nacional: em 1970 no *Land* de Hesse, na Alemanha, foi promulgada a *Hessisches Datenschutzgesetz*, lei bastante sintética sobre a atividade de centros de processamento de dados geridos pelo Estado e instituições correlatas. A esse respeito, confira-se DONEDA, Danilo. *Da privacidade à proteção de dados pessoais, cit.*, p. 228.

[80]*Id. Ibid.*, p. 228.

[81]Diretiva que atualmente centraliza o trato da matéria na União Europeia. UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial L. 281, 23 de novembro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046.

Consequentemente, esperar-se-ia que empresas de países com alto nível regulatório pressionassem seus governos a buscar, no âmbito comunitário, a adoção de normativas equivalentes ou semelhantes, perseguindo maior competitividade das empresas nacionais.[82] Não foi esse o caso, no entanto.

A criação de regras supranacionais que regulassem a proteção dos dados pessoais e o fluxo transnacional desses dados foi fortemente combatida por associações pan-europeias de empresas, como a União de Confederações Industriais e Patronais da Europa (UNICE),[83] argumentando que isso resultaria na imposição de um grande fardo à indústria. Mesmo empresas de países com altos níveis regulatórios foram contrárias à regulação regional, com especial menção à indústria do Reino Unido e da Alemanha,[84] mesmo na década de 1990, quando até a Comissão Europeia reviu sua posição e passou a preparar propostas para essa regulamentação. Newman relata também que não há qualquer evidência de que Estados-membros que já contavam com alto nível regulatório ou grupos de interesse econômico buscaram influenciar a Comissão para a criação de normas supranacionais[85] nas décadas de 1970 e 1980.

O segundo modelo é baseado na chamada tradição neofuncionalista, segundo a qual "a Comissão Europeia tem a habilidade de expandir suas competências e alargar o escopo das tomadas de decisão supranacional",[86] em uma abordagem cume/base. Segundo tal raciocínio, a Comissão seria capaz de, ao criar grupos de estudos e comissões transnacionais para estudar o assunto, promover a inclusão de determinada matéria na agenda da regulação regional.

Nesse passo, a Comissão ou altos funcionários ligados à Diretoria do Mercado Interno teriam promovido a discussão sobre o assunto e buscado angariar apoio de diversos grupos de interesses transnacionais para pressionar os Estados-membros pela criação de marcos regulatórios.[87]

---

[82]NEWMAN, Abraham L. Building transnational civil liberties: transgovernmental entrepreneurs and the European data privacy directive. *International Organization*, v. 62, n. 1, p. 106, Jan. 2008. doi: https://doi.org/10.1017/S0020818308080041.

[83]Union of Industrial and Employers' Confederations of Europe. Confira-se *European Report*, "UNICE Calls for Changes in Proposal on Personal Data", 1651, 1991, 3, *apud* NEWMAN, Abraham L. *op. cit.*

[84]Confira-se WIRTSCHAFT fürchtet Nachteile durch verschärften Datenschutz. *Computerwoche* (Internet Edition), 21.12.1990. Disponível em: https://www.computerwoche.de/a/wirtschaft-fuerchtet-nachteile-durch-verschaerften-datenschutz,1149120.

[85]NEWMAN, Abraham L. *op. cit.*, p. 111.

[86]*Id. Ibid*., p. 107.

[87]*Id. Ibid*., p. 197-108.

As previsões do segundo modelo também não correspondem ao que efetivamente ocorreu, segundo Newman. Com a aprovação de leis nacionais sobre proteção de dados pessoais na década de 1970, formou-se uma rede de especialistas que passaria a pressionar instituições europeias para a adoção de regulações regionais sobre o tema: esses especialistas temiam que a regulamentação parcial na região pudesse trazer sérios riscos, sobretudo quanto às transferências internacionais de dados.

Empresas interessadas em fugir à aplicação de regras mais estritas poderiam concentrar suas operações de dados em países sem leis nacionais sobre o assunto, contribuindo para a criação de "paraísos de dados pessoais". Esses esforços renderam poucos resultados concretos.

Junto ao Parlamento Europeu esse grupo conseguiu a aprovação de resoluções que clamavam pela necessidade de regras pan-europeias,[88] mas houve pouco interesse por parte da Comissão, sob o argumento de que a regulação supranacional elevaria os custos de operação na Europa e de que regras sobre privacidade seriam afetas ao setor público, excedendo a jurisdição da Comunidade Europeia.[89]

Outro sucesso do grupo teve alcance limitado e é representado pela assinatura da Convenção de Estrasburgo em 1981, formulada no seio do Conselho da Europa. A efetividade da Convenção, como se viu, foi restrita dada a necessidade de implementação nacional e o foco na simples redução de entraves quanto aos fluxos transnacionais de dados.[90]

Com a incapacidade dos dois modelos expostos de explicar o desenrolar dos fatos que levaram à concretização da diretiva sobre proteção de dados pessoais, Newman sustenta que a alteração na posição da Comissão Europeia sobre a possibilidade de regras pan-europeias foi resultado de pressões exercidas pelas Autoridades Nacionais de Proteção de Dados. Normalmente instituídas pelas leis nacionais de proteção de dados para supervisionar e controlar certas atividades do ramo, essas autoridades eram essencialmente órgãos administrativos, relativamente autônomos e independentes, dotados de poderes delegados.

---

[88]Confiram-se as resoluções O.J (C100) 27 de 3 de maio de 1976; O.J. (C140) 147 de 8 de maio de 1979; e O.J. (C87) 39 de 9 de março de 1982.

[89]Confira-se a Recomendação da Comissão 1981 O.J. (L246) 31. EUROPEAN COMMISSION. *81/679/EEC*: Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data. Official Journal L 246, 29/08/1981, P. 0031. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31981H0679.

[90]NEWMAN, Abraham L. *op. cit.*, p. 109-110.

Apesar da grande variação na composição e conjunto de atribuições de país para país, praticamente todas tinham poder para influir em transferências transfronteiriças de dados pessoais, inclusive condicionando ou vedando tais transferências.

Adotando os argumentos já reiterados pelos quadros de especialistas reunidos desde 1970,[91] de que a regulamentação supranacional da questão aumentaria a proteção dos usuários evitando a criação de "paraísos de dados", unificaria essa proteção e facilitaria o fluxo de dados em todo o território da comunidade europeia, as autoridades nacionais de dados existentes à época, em ações coordenadas, passaram a pressionar instituições da comunidade europeia por normas supranacionais sob a ameaça de bloquear o fluxo de dados em grande parte da Europa.[92] O diferencial, nesse caso, foi o poder de vedar certas transferências para países que não possuíssem o mesmo nível de proteção do país de origem. Com a resistência encontrada, os critérios para análise dessa equivalência de proteção, já estabelecidos em leis nacionais, passaram a ser aplicados com mais rigor e resultando, em casos relevantes, no bloqueio de transferências de dados.[93]

Após a repetição de situações semelhantes, o grupo de autoridades conseguiu alterar a balança da tomada de decisões no referente à legislação supranacional sobre dados pessoais,[94] tornando muito mais custoso à comunidade europeia a manutenção de um vácuo regulatório. Isso resultou, no início da década de 1990, na revisão pela Comissão Europeia

---

[91]Em muitos casos, os nomeados para exercer altos cargos nesses órgãos eram especialistas que já participavam das redes de experts.

[92]O Comissário para Proteção de Dados de Hess (Alemanha) à época, Spiros Simitis, afirmou em uma conferência em 1990, resumindo a posição do grupo de autoridades: "If there are no common rules by 1992 amongst the twelve Community members then quite simply five of the countries of the European Community without such laws will have to be treated in exactly the same way as those with no rules for data privacy. Therefore, there will be no personal data transfers to those countries because data commissioners will oppose such transfers." Confira SIMITIS Reports Data Protection Chaos. *Transnational Data and Communications Report*, p. 26, Jun./Jul. 1990.

[93]A respeito, bem escreve Newman, comentando o Caso FIAT (o "segundo caso FIAT", já mencionado): "One of the most visible attempts to raise the issue to the European Community level occured in July 1989, when the national data privacy authority of France threatened to block data transfers between Fiat's corporate offices in France and Italy. Invoking Article 24 of the French law, the French Data Privacy Authority (*Commission Nationale de l'Informatique et des Libertés - CNIL)* argued that Italy did not have adequate regulations. The CNIL blocked the transfer of information about French citizens, forcing Fiat Italy to find a solution to the data impasse." NEWMAN, Abraham L. *op. cit.*, p. 114.

[94]"The recommendation to join the Convention of the Council of Europe did come. Bit it was not enough. Since 1975, the European Parliament had constantly admonished the Commission to commence preparation of a Directive. It was only when the "Swedish incident" (i.e. the interruption of transborder data flow from Sweden to the UK - an earlier case had involved Germany when it still lacked a federal law) repeated itself within the European market that serious work on an instrument started: The French CNIL had intervened in a planned transfer from France to Italy (the "FIAT" case). (…) Finally, in 1990, the Comission came out with its proposal for a directive which still took another five years to be finalized." BURKERT, Herbert. Privacy-data protection: a German/European perspective. *In*: ENGEL, Christoph; KELLER, Kenneth H. (Eds.). *Governance of global networks in the light of differing local values*. Baden-Baden: Nomos Verlagsgesellschaft, 2000. p. 52-53.

de seu posicionamento sobre a possibilidade de regulamentar, tanto no âmbito público quanto privado, a proteção e a livre circulação de dados pessoais através de uma normativa comunitária.[95] O resultado das discussões subsequentes, no âmbito da Comissão, foi a Diretiva 95/46/CE.

A Diretiva 95/46/CE[96] foi a norma em vigor que centralizou os principais conceitos no campo da proteção dos dados pessoais na União Europeia até maio de 2018. Tal diretiva trazia os princípios básicos da tutela dos dados pessoais, tanto na coleta, quanto na manipulação e tratamento de tais dados pelos interessados e por terceiros, direitos básicos dos titulares dos dados tratados, estabelecia padrões para as transferências internacionais de dados e criava ainda um aparato de supervisão que sirva como fiscal e órgão de registro, nas funções que a Diretiva lhe atribui.[97]

Durante os trabalhos de acompanhamento da implementação e aplicação da Diretiva 95/46/CE, o *Primeiro relatório sobre a implementação da directiva relativa à proteção de dados*[98] noticiava que ainda havia certo atraso na transposição da diretiva para os ordenamentos pátrios dos Estados-membros, o que foi resolvido até o próximo relatório, de 2007,[99] em que se constatou a transposição da diretiva por todos os países do grupo.

No meio tempo, foram aprovadas outras diretivas, de caráter complementar, buscando a transposição dos princípios da Diretiva 95/46 para outras áreas de controle antes não abrangidas pelo sistema.

A implementação da Diretiva 95/46/CE se deu, ainda que com alguns atrasos, de forma completa. O acompanhamento desse processo era previsto no artigo 33 da própria diretiva e era atribuição do grupo de trabalho instituído pelo artigo 29 da diretiva - conhecido também como GT 29.[100]

---

[95]NEWMAN, Abraham L. *op. cit.*, p. 113-114.

[96]UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial L. 281, 23 de novembro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046.

[97]MIGUEL ASENSIO, Pedro Alberto de. *op. cit.*, p. 284-286.

[98]Relatório da Comissão COM (2003) 265. COMMISSION OF THE EUROPEAN COMMUNITIES. Report From the Commission. *First report on the implementation of the Data Protection Directive (95/46/EC)*. Brussels, 15.5.2003 COM(2003) 265 final. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF.

[99]COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o acompanhamento do programa de trabalho para uma melhor aplicação da directiva relativa à proteção de dados.* COM(2007) 87 final. Bruxelas, 7 mar. 2007. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52007DC0087.

[100]"Grupo de Trabalho 29", tradução do nome *Working Party 29*, em referência ao artigo que o institui.

No ano de 2003 o Grupo apresentou o primeiro relatório sobre a implementação da Diretiva, baseado não apenas em estudos sobre o processo de transposição da diretiva para os ordenamentos nacionais, mas também utilizando-se de pesquisas sobre a aplicação das normas trazidas pela Diretiva no dia a dia, conduzidas junto a especialistas, indivíduos e agentes do mercado como empresas, associações e grupos econômicos.

No primeiro relatório[101] o Grupo de Trabalho 29 constatou que a implementação da diretiva pelos Estados-Membros estava atrasada, provavelmente em razão da dificuldade de transposição de uma norma que por um lado deixava grande margem ao Estado e por outro exigia respeito a uma infinidade de pormenores.[102]

Foi constatado também que a Diretiva parecia atingir seu objetivo de fornecer um alto nível de proteção de dados pessoais sem criar entraves intransponíveis, de modo que a recomendação final do relatório foi a desnecessidade - e até imprudência - de promover reformas à Diretiva naquele momento.[103] Duas outras observações valiosas foram feitas no relatório e merecem breve menção.

A primeira dizia respeito à aplicação efetiva das regras contidas na diretiva. Segundo o relatório, "dado o caráter ubíquo do tratamento de dados pessoais, é difícil obter informações precisas ou completas sobre a sua conformidade com a lei",[104] sendo tal falta de transparência quanto à legalidade dos tratamentos, aparentemente, resultado de três fenômenos inter-relacionados: *(i)* a insuficiência dos recursos atribuídos às autoridades de controle no que toca à fiscalização e a baixa prioridade atribuída a tal incumbência diante de diversas outras atribuições; *(ii)* certa relutância dos responsáveis pelo tratamento dos dados em alterar suas práticas a fim de cumprir regras que podem parecer complexas e onerosas diante de baixa probabilidade de penalização diante de seu descumprimento; e *(iii)* um nível aparentemente baixo de conhecimento dos usuários sobre seus direitos quanto ao tratamento

---

[101]COMISSÃO EUROPEIA. Relatório da Comissão. *Primeiro Relatório sobre a implementação da Directiva relativa à protecção de dados (95/46/CE)*. COM(2003) 265 final. Bruxelas, 15 maio 2003. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52003DC0265.

[102]"A implementação de uma diretiva deste gênero, ou seja, uma diretiva que deixa uma margem considerável aos Estados-Membros, mas que também os obriga a respeitar uma quantidade significativa de pormenores, e, sem dúvida, uma tarefa complicada. Mas os atrasos graves na implementação da diretiva ocorridos na maioria dos Estados-Membros constituem a primeira e principal lacuna que a Comissão tem o dever de registrar (…)" COMISSÃO EUROPEIA. Relatório da Comissão. *Primeiro Relatório sobre a implementação da Directiva relativa à protecção de dados (95/46/CE)*. COM(2003) 265 final, *cit.*, p. 10.

[103]"A Comissão considera que os resultados da revisão, na generalidade, aconselham a que não se proponha uma alteração da diretiva nesta fase." *Id. Ibid.*, p. 7.

[104]*Id. Ibid.*, p. 12.

de seus dados pessoais. Nesse aspecto, o relatório defendia o acompanhamento atento dessas tendências e a coleta de maiores informações que viessem a confirmar ou negar tais indícios.

Um segundo comentário importante dizia respeito às tecnologias que aumentam a privacidade - tradução direta da expressão *privacy-enhancing technology*. O relatório defendia a promoção e encorajamento de tais tecnologias, que têm como objetivo reduzir a coleta e utilização de dados pessoais ao mínimo necessário e impedir formas ilegais de coleta e tratamento, como medida essencial e complementar à abordagem jurídica da questão.

Os problemas da abordagem tecnológica pareciam ser os mesmos do tratamento de dados: como é possível verificar se determinado produto conta com tal tipo de tecnologia, ou ainda, como garantir que o produto que anuncia tal tecnologia realmente a aplica de modo adequado conforme as leis aplicáveis? Surge aqui, pela primeira vez, a sugestão de um padrão de certificações para produtos em conformidade com as regras europeias de proteção de dados pessoais e privacidade.[105]

O segundo relatório, enviado ao Parlamento Europeu em 2007, demonstrou que o processo de implementação da diretiva no âmbito dos Estados-Membros finalmente havia sido concluído. Verificou-se, entretanto, que em certos casos sua aplicação ou sua transposição deixou a desejar, diante da ausência de certas disposições ou pelas escolhas legislativas feitas no ato de transposição que excediam a margem de manobra deixada aos Estados-Membros pela Diretiva.[106]

No entanto, o relatório continuava a sustentar a adequação fundamental das regras estabelecidas e voltava a desaconselhar a alteração da Diretiva 95/46/CE naquele momento.

Apesar disso, a partir de 2010 começou-se a discutir novamente a necessidade de reformas na proteção dos dados pessoais.

O projeto de reforma teve seu surgimento marcado por uma comunicação da Comissão ao Parlamento Europeu, datada de novembro de 2010 sob o título de "*Uma abordagem global da protecção de dados pessoais na União Europeia*".[107] Nesse novo

---

[105]COMISSÃO EUROPEIA. Relatório da Comissão. *Primeiro Relatório sobre a implementação da Directiva relativa à protecção de dados (95/46/CE)*. COM(2003) 265 final, *cit.*, p. 16.

[106]COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o acompanhamento do programa de trabalho para uma melhor aplicação da directiva relativa à proteção de dados.* COM(2007) 87 final, *cit.*, p. 5-6.

[107]COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões*. *Uma abordagem global da protecção de dados pessoais na União Europeia*. COM(2010) 609 final. Bruxelas, 4 nov. 2010. Disponível em: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_pt.pdf. Acesso em: 24 mar. 2019.

relatório justificava-se a necessidade de novos estudos para a alteração e atualização da Diretiva de proteção de dados, em primeiro lugar, pela evolução tecnológica e pela consequente revolução no modo como os indivíduos interagem e compartilham seus dados pessoais, com especial menção a redes sociais e à chamada *cloud computing*[108] - esta que traz sérios questionamentos pois o armazenamento de dados pessoais em servidores de terceiros retira do usuário grande parte de seu controle sobre seus dados.

Em segundo lugar, a reforma se mostrava necessária pela utilização, em escala cada vez maior, de dados pessoais para finalidades diversas, multiplicando-se também os meios de rastreamento e coleta de dados, com especial menção a métodos sub-reptícios de coleta.

A fim de endereçar tais questões emergentes, o relatório recomendava o estudo de cinco aspectos das leis atuais que podem ser reformados. O primeiro dizia respeito ao fortalecimento de direitos individuais, com *(i)* a garantia de uma proteção mais eficaz, *(ii)* maior transparência por parte dos responsáveis pelo tratamento, *(iii)* maior controle do indivíduo sobre seus dados, *(iv)* a busca pela conscientização dos indivíduos sobre seus direitos sobre seus dados pessoais, *(v)* fortalecimento do instituto do consentimento livre e informado para o tratamento de dados, *(vi)* melhoria na proteção a dados sensíveis, e *(vii)* a garantia de maior eficácia das sanções em caso de descumprimento das regras sobre tratamento de dados.

O segundo aspecto a ser estudado era a criação de um arranjo institucional com maior capacidade para garantir a aplicação das normas sobre proteção de dados pessoais. O relatório considerava as autoridades de proteção de dados parte essencial do sistema de proteção, por serem "guardiões independentes de direitos e liberdades fundamentais relacionados à proteção de dados pessoais, nos quais os indivíduos confiam para garantir a proteção de seus dados e a legalidade de operações de processamento",[109] sendo então aconselhável uma revisão dos poderes e atribuições dessas entidades, de modo a garantir que pudesse cumprir integralmente sua função.

O terceiro ângulo pelo qual as normas em vigor deveriam ser reavaliadas dizia respeito à necessária dimensão global da proteção de dados pessoais. Nesta sede, sugeriu-se o *(i)* esclarecimento e simplificação de regras para a transferência internacional de dados

---

[108]Computação em nuvem, em tradução livre.

[109]"They are independent guardians of fundamental rights and freedoms with respect to the protection of personal data, upon which individuals rely to ensure the protection of their personal data and the lawfulness of processing operations."

para fora da União Europeia (especialmente os critérios para avaliação da "adequação" do nível de proteção); *(ii)* o estudo de novas soluções para casos de transferências para países que não garantissem um nível de proteção adequado e em que as cláusulas-tipo adotadas pela Comissão não eram suficientes pelo caráter não-contratual da situação; e *(iii)* a promoção, no âmbito internacional, de princípios universais para o tratamento de dados, de modo a elevar o nível geral de proteção de dados pessoais.

O quarto aspecto que merecia atenção era a revisão de regras de proteção de dados pessoais na área de cooperação policial e judicial em questões criminais. A necessidade de novas normas surge pois as regras gerais da Diretiva 95/46/CE não são aplicáveis a tais áreas de atuação do Poder Público, além da insuficiência da atual normativa em vigor, a Decisão-Quadro 2008/977/JAI,[110] que, por exemplo, dizia respeito apenas a transferências transfronteiras de dados pessoais, dentro da União Europeia, para tais finalidades, não abrangendo, portanto, as transferências entre instituições de um mesmo país.

O relatório ainda sugeria novos estudos sobre medidas que visassem otimizar o mercado interno, como a eliminação de divergências entre leis nacionais na transposição da Diretiva 95/46/CE e a redução de ônus administrativos para a aplicação das normas comunitárias por parte dos responsáveis pelo tratamento de dados pessoais.

Em 2012, a Comissão enviou ao Parlamento o comunicado intitulado "Proteção da privacidade num mundo interligado - Um quadro europeu de proteção de dados para o século XXI",[111] acompanhado de propostas para uma nova Diretiva[112] e um Regulamento.[113]

O Regulamento proposto buscava dar vazão à maioria das críticas feitas no relatório de 2010, com especial menção à fragmentação notada na transposição da Diretiva 95/46/CE pelos Estados-Membros. Segundo o relatório que introduzia as propostas, a aprovação de

---

[110]CONSELHO DA UNIÃO EUROPEIA. *Decisão-Quadro 2008/977/JAI*. Decisão-Quadro do Conselho de 27 de novembro de 2008 relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal. Jornal Oficial L 350, 30 de dezembro de 2008. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32008F0977.

[111]COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões*. *Proteção da privacidade num mundo interligado*: um quadro europeu de proteção de dados para o século XXI. COM(2012) 9 final. Bruxelas, 25 jan. 2012. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52012DC0009.

[112]COMISSÃO EUROPEIA. *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados*. COM(2012) 10 final. Bruxelas, 25 jan. 2012. Disponível em: http://eur-lex.europa.eu/procedure/PT/201285.

[113]COMISSÃO EUROPEIA. *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. COM(2012) 11 final. Bruxelas, 25 jan. 2012. Disponível em: http://docplayer.com.br/3497609-Proposta-de-regulamento-do-parlamento-europeu-e-do-conselho.html.

um Regulamento visava, principalmente, eliminar a necessidade de transposição e os casos de aplicação divergente do conteúdo da Diretiva, visto que os regulamentos, por sua natureza, são normas de direito comunitário que são diretamente aplicáveis em todos os Estados-Membros, não exigindo o exercício de transposição.

Aprovado em 2016, o regulamento então proposto passaria a ser conhecido como o *General Data Protection Regulation,* o *GDPR,* normativa que se tornou o principal diploma legal a reger a matéria na União Europeia, que será melhor explorada adiante.

2.4. O direito à proteção dos dados pessoais

O Direito à Proteção dos Dados Pessoais, como é geralmente referenciado na União Europeia, desenvolveu-se especialmente a partir da segunda metade do século XX na região, chegando ao status de talvez um dos principais modelos regulatório na matéria em todo o mundo, havendo em testemunho disto um sem número de países que adotaram legislação de tom semelhante ao do GDPR, incluindo o próprio Brasil. Antes de prosseguir, cabe breve exploração da origem de tal direito e seu caminho até ser confirmado como um direito fundamental na União Europeia, com sua inclusão na Carta dos Direitos Fundamentais da União Europeia.

2.4.1. Origem: o direito à privacidade

O direito à privacidade - em sua concepção moderna, frise-se - é recente e seu surgimento remonta aos fins do século XIX. No entanto, muitos autores sustentam que é possível encontrar regras jurídicas pertinentes ao que hoje se entende como privacidade já em normas muito mais antigas. Como escreve Milton Fernandes,[114] é costume na academia de letras jurídicas a tentativa de sempre situar as origens de determinado instituto jurídico atual no direito romano, tradição essa especialmente cara aos civilistas.

[114]FERNANDES, Milton. *Proteção civil da intimidade, cit.*

E não é outro o caso do direito à privacidade. Traços do direito inicialmente são detectáveis em institutos que visavam a proteção da dignidade do indivíduo no Direito Romano, tendo caráter eminentemente privado de início.

Giovanni Pugliese, por exemplo, busca no século XVI diversas regras espalhadas pelo ordenamento então vigente, que pareceriam sustentar já algum tipo de tutela da privacidade, ainda que admitisse que, por excessivamente esparsas, não poderiam criar um sistema.[115]

Milton R. Konvitz, na mesma linha, aponta o episódio bíblico de Adão e Eva como demonstração mítica de uma natureza moral ligada ao recato.[116] Frequentemente mencionam-se as *kakegorias diké* dos gregos e a *actio iniuriarum* romana, esta última originária de uma atitude de desprezo da personalidade alheia, além de diversos outros textos em que um jurista moderno poderia identificar sementes dos institutos jurídicos atuais.[117]

A inserção da privacidade no grupo de *direitos da personalidade*, como muitos outros direitos sob tal sigla, foi resultado não "da criação" do direito em si, mas do desenvolvimento do próprio conceito de personalidade[118] e do reconhecimento da identidade entre o fundamento do direito à privacidade e dos demais direitos da personalidade - a dignidade da pessoa.

Daniel Becourt, jurista francês de grande renome, apresenta-nos um apanhado da evolução da convivência em sociedade, de grande valia para compreender a razão do surgimento e evolução recente do direito à privacidade. Segundo o autor, em um estado tribal primitivo, uma sociedade pastoril buscou inicialmente proteger a integridade do indivíduo contra a violência física e a apropriação indevida de bens.

Com o advento da agricultura e a sedentarização da sociedade, o lar fixo sucedeu à tenda nômade e tal propriedade passa a ser também protegida. Com o intercâmbio entre povoados surge a necessidade de identificação pessoal, com o aumento da relevância do nome, do estado civil e dos estatutos governantes do indivíduo.

---

[115]PUGLIESE, Giovanni. Il diritto alla riservatezza nel quadro dei diritti della personalità. *In*: STUDI in onore di Alberto Asquini. Padova: CEDAM, 1965. p. 1553-1554.

[116]KONVITZ, Milton R. Privacy and the law: a philosophical prelude. *Law and Contemporary Problems*, Duke University Press, v. 31, n. 2, p. 272-280, 1966. Disponível em: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3108&context=lcp.

[117]CASTRO, Federico de. Los llamados derechos de la personalidad, cuestiones previas a su estudio. In: STUDI Giuridici in Memoria de Filippo Vassali. Torino: Torinese, 1960. p. 403-406.

[118]"(…)muito embora a maioria dos direitos da personalidade se identifique com aqueles consagrados nas declarações de direitos humanos como direitos subjetivos públicos, esses direitos, denominados personalíssimos, inatos, conaturais, individuais, etc., não surgiram com a positivação dos direitos do homem, à época da Revolução Francesa." GOGLIANO, Daisy. *op. cit.*, p. 24.

Com a implementação da escrita, a comunicação deixa de ser apenas oral e possibilita o desenvolvimento de novas formas de comunicação, como a comunicação postal. São estas últimas etapas em que são semeados os direitos da personalidade.[119]

As revoluções americana e francesa do século XVIII, no entanto, não criaram esses direitos, mas elevaram os direitos da personalidade ao *status* de liberdades públicas, marcando-se então um período em que tais direitos seriam vistos quase que exclusivamente por seu caráter público, de defesa do indivíduo contra o Estado.[120]

Os direitos fundamentais do homem - nessa concepção - "surgiram" como uma necessária proteção contra os possíveis abusos por parte do Estado no exercício de seu poder de mando, com base na ideia de um permanente conflito entre o Estado e o indivíduo, típico do liberalismo do século XVIII. Em verdade, o que houve foi uma reunião e recaracterização de direitos, que já eram esboçados desde o Direito Romano, sendo-lhes conferido peso significativo e uma estruturação mais clara e completa.

No entanto, sua evolução na União Europeia ultrapassou em muito o clássico dilema entre Estado e indivíduo, impulsionada, como explica Jacques Velu, pelo surgimento de direitos socioeconômicos e a necessidade de colocar também ao abrigo da lei tais direitos quando relevantes em relações entre particulares,[121] retornando então àquela visão privatista na qual encontramos os embriões dos direitos da personalidade.

Percebe-se aqui que, enquanto no período intermédio os direitos da personalidade eram tratados de modo fragmentário sem que fossem sistematizados ou bem delimitados, como defende Daisy Gogliano, aqueles direitos foram finalmente consolidados com o *humanismo jurídico* e o desenvolvimento do *direito natural* e a mudança de perspectiva por eles trazida.[122]

---

[119]BECOURT, Daniel. *Troisième Colloque International sur la Convention Européenne des Droits de l'Homme,* (Comunicação escrita) Bruxelas, 1970, *apud* FERNANDES, Milton. Os direitos personalíssimos. *Revista Jurídica da Advocacia Geral do Estado de Minas Gerais*, Belo Horizonte, n. 1, p. 12, jul./dez. 2004.

[120]"Basta atentar para o fato de que os direitos do homem, reconhecidos publicamente como direitos subjetivos, dentro da relação indivíduo-Estado, tiveram o seu apogeu com a Revolução Francesa, após longa meditação histórica dos direitos subjetivos privados, aliada à noção de personalidade jurídica. Todos os princípios levados a efeito pela escola de *direito natural* serviram de alicerce e sustentáculo à afirmação dos direitos humanos. GOGLIANO, Daisy. *op. cit.*, p. 25.

[121]VELU, Jacques. *Le droit au respect de la vie privée*: conférences données à la Faculté de droit de Namur. Namur, Belgique: Presses universitaires de Namur, 1974. p. 7.

[122]"Não encontramos no direito intermédio a sistematização de uma teoria de proteção à personalidade. O que vimos foram apenas esboços, breves lineamentos, ainda penumbrosos, no sentido de se buscar maiores garantias contra as violações cometidas contra a pessoa. Todos esses traços não deixam de ter a sua importância, porque, na medida em que a civilização evolui, vemos, passo a passo, crescer e avolumar-se a

O direito à privacidade, no entanto, é de desenvolvimento mais tardio, ainda que encontre nos direitos da personalidade seu fundamento último. Enquanto a maioria dos outros direitos da personalidade parece ter sido bem estruturada e desenvolvida durante os séculos XVII e XVIII, o real significado da privacidade parece ter origem mais recente.

Na Alemanha, o conceito foi mais tarde desenvolvido por Heinrich Hubmann e Heinrich Helkel, em 1953 e 1957, respectivamente, no que se convencionou chamar de Teoria dos Círculos Concêntricos ou Teoria das Esferas.[123] Segundo tal modelo, a privacidade seria composta de três esferas concêntricas que conteriam os diferentes níveis de segredo da vida privada de um indivíduo. A camada externa corresponderia à privacidade, a camada intermediária à intimidade e o núcleo ao segredo.[124]

Na Itália, pontificaram Ravà em 1934 e Adriano de Cupis, pouco depois, em uma série de obras sobre o assunto, devendo-se especial menção a *I Diritti della Personalità* de 1942. Ambos os autores reconheciam a existência de um direito à reserva, garantindo a não intromissão de terceiros em determinada esfera pessoal.[125]

De Cupis, em especial, utiliza a expressão direito ao resguardo, que conceitua "como o modo de ser da pessoa que consiste na exclusão do conhecimento, por parte das outras pessoas, de quanto se refere à própria pessoa". O autor ainda esclarece que o objeto de tutela do direito ao resguardo não se limita ao que deve permanecer completamente inacessível

---

noção de honra, dignidade e liberdade, como embriões em crescimento, que lentamente vão superando as suas próprias barreiras. Foi com a penetração do *humanismo jurídico* que esses direitos passaram a ser vistos, no momento em que novo movimento se abre, com a escola dos pós-glosadores, *i.e.*, os comentadores ou conciliadores, que após a Escola de Bolonha, iniciam uma nova teoria de aplicação do direito, contrapondo-se ao antigo regime estatutário medieval, dentro de um método mais livre e flexível de interpretação e argumentação." GOGLIANO, Daisy. *op. cit.*, p. 57-58.

[123]SILVA, Carlos Bruno Ferreira da. *op. cit.*, p. 38.

[124]Adotamos o viés apresentado por Henkel, pois parece mais razoável que o segredo, aquilo que nunca deixou a mente do indivíduo, deva ser mais protegido que a intimidade, essa entendida como traços pessoais do indivíduo, convicções, crenças e preferências. Sobre tais teorias, veja-se COSTA JR., Paulo José da. *O direito de estar só*: tutela penal da intimidade. São Paulo: Editora Revista dos Tribunais, 1970.

[125]"Já definimos o direito ao resguardo, como o modo de ser da pessoa que consiste na exclusão do conhecimento, por parte das outras pessoas, de quanto se refere à própria pessoa. Pois bem: à pessoa refere-se não só a sua figura física, isto é, o conjunto das suas formas físicas, mas também a sua voz e, além disto, todos os acontecimentos e o desenvolvimento da sua vida." DE CUPIS, Adriano. *op. cit.*, p. 155.
Confira-se também, acerca do direito à imagem, parte do direito ao resguardo na visão de De Cupis: "Todo indivíduo desenvolve parcialmente a sua vida em circunstâncias e em ambientes subtraídos ao exame de terceiros, e esta é a esfera íntima da sua vida privada. Ora, pode suceder que o ordenamento jurídico lhe confira proteção no que respeita a esta particular esfera da vida, considerando ilegítima a reprodução da sua imagem, quando ela reflita as cinrcunstâncias e ambientes referidos. A famosa frase "la vie privée doit être murée" alude precisamente à exigência de salvaguardar da indiscrição e da curiosidade tudo o que a estas especialmente repugne." DE CUPIS, Adriano. *op. cit.*, p. 141.

ao conhecimento alheio, o que define como segredo,[126] mas inclui também aquilo que, embora acessível ao conhecimento de terceiros, não deve ser divulgado indiscretamente, sem critério ou limites.[127]

Assim, com as primeiras tentativas de definição de um direito à privacidade no século XIX, a tutela da intimidade passou por grande evolução durante todo o século XX e hoje encontra-se novamente no limiar de uma ressignificação de seu conteúdo.

2.4.2. Da privacidade à autodeterminação informática

A inclusão da proteção de dados pessoais como parte do direito à privacidade vem do início do século XX, quando, com a transmutação do Estado liberal ao Estado de bem-estar social, o governo passa a coletar informações de seus cidadãos, com a finalidade de aumentar a eficiência da gestão e melhor distribuir seus recursos. Essa atividade era inicialmente conduzida pelo Estado pois envolvia grandes investimentos e uma infraestrutura que mesmo os grandes grupos empresariais ainda não possuíam ou simplesmente optavam por não utilizar, em razão da incerteza quanto à utilidade de tais dados.[128]

Diante dos avanços mais recentes tanto da tecnologia por trás da rede mundial quanto de sua evolução como ferramenta e sua adoção generalizada pela sociedade, surge a preocupação com o controle sobre tais informações. Uma vez que tais informações dizem respeito à vida pessoal do indivíduo, consideram-se derivados da própria privacidade.

Foi nesse sentido que se desenvolveu, já a partir de 1970, uma segunda acepção do direito à intimidade: o direito à privacidade como direito de controle sobre quais aspectos da

---

[126]"O direito do segredo constitui um aspecto particular do direito ao resguardo: Certas manifestações da pessoa destinam-se à conservação e completamente inacessíveis ao conhecimento dos outros, isto é, secretas; não é apenas ilícito o divulgar tais manifestações, mas também o tomar delas conhecimento, e o revelá-las, não importa a quantas pessoas." DE CUPIS, Adriano. *op. cit.*, p. 158.

[127]"Afora estas limitações, o direito ao resguardo existe em toda a sua extensão; e repare-se que tal direito não está circunscrito à esfera daquilo que deve permanecer completamente inacessível ao conhecimento dos outros, isto é, secreto; mas compreende sim o que, embora acessível ao conhecimento alheio, não deve ser indiscretamente difundido. Pense-se, por exemplo, em certos dados do registro civil, como seja a idade de uma senhora ou de uma menina que, apesar de resultarem oficialmente do registro do estado civil, não devem ser indiscretamente divulgados." DE CUPIS, Adriano. *op. cit.*, p. 157-158.

[128]DONEDA, Danilo. *Da privacidade à proteção de dados pessoais, cit.*, p. 12-15.

vida privada do indivíduo e informações a ele relacionados devem ser mantidos em segredo e quais podem ser revelados, total ou parcialmente.[129]

Em uma ótica mais extrema, sustentam Juan Carlos Menéndez Mato e Maria Eugenia Gayo Santa Cecilia que ainda que tradicionalmente o direito à proteção dos dados pessoais seja vinculado ao direito à privacidade, aquele começa a ser reconhecido como direito autônomo, com conteúdo próprio, fundado em princípios específicos e tutelado por mecanismos especiais.[130]

Já Pedro Servera vê o liame entre o direito à privacidade e o direito à proteção dos dados pessoais no mecanismo fundamental sobre o qual ambos os direitos repousam: o consentimento. Tanto no caso dos dados pessoais quanto no caso da privacidade em sentido amplo, cabe ao titular dos direitos decidir quem pode adentrar na sua esfera íntima (seja entrando em sua casa e em sua convivência familiar ou tomando conhecimento de seus dados colocados, por exemplo, em seu perfil de uma rede social).[131]

David Ordóñez Solís compactua com ambos os entendimentos: a proteção dos dados pessoais é ao mesmo tempo fundada na privacidade e direito autônomo por si só. Não se quer aqui excluir o fundamento valorativo do novo direito, mas reconhecer que apesar de tal identidade, a proteção de dados pessoais é garantia que requer mecanismos específicos de tutela.[132]

---

[129]Como bem aponta Marcelo Cardoso Pereira, a ideia foi inicialmente desenvolvida pela jurisprudência norte-americana e vocalizada finalmente por Alan Westin. PEREIRA, Marcelo Cardoso. *op. cit*., p. 128-130.

[130]MENÉNDEZ MATO, Juan Carlo; GAYO SANTA CECILIA, Maria Eugenia. *Derecho e informática*: ética y legislación. Barcelona: Bosch, 2014. p. 281.

[131]Desglosando cada uno de los derechos con los que hemos conformado 'la protección de la vida privada', intimidade, honor, propria imagen y protección de datos personales, puede observar-se que en todos (salvo en el derecho al honor por sus propias peculiaridades) la primera línea de protección de la vida privada la determina el titular de los derechos a través de su derecho a decidir (a través de su consentimiento): es la persona la que decide quién puede entrar en su casa (es la persona la que decide si un tercero le puede seguir en *facebook* o no), es la persona quien decide si una información puede ser conocida por otros (es la persona la que decide qué información va transmitiendo a través de *twitter*) (…).GRIMALT SERVERA, Pedro. La necessária reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflitos y solapamentos com otros derechos y libertades en internet. *In*: VALEROS TORRIJOS, Julián (Org.). *La protección de los datos personales en internet ante la innovación tecnológica*: riesgos, amenazas y respuestas desde la perspectiva jurídica. Cizur Menor, Navarra: Thomson Reuters/Aranzadi, 2013. p. 71-72.

[132]"Y tampoco nadie duda de la singularidad que en el ámbito del derecho a la privacidad representa el derecho a la protección de datos personales, que significa y pretende que nadie almacene ni utilice los dados relativos, por ejemplo, a su raza, a sua salud, a su religión o a su ideología. (…)
La aplicación del derecho a la protección de datos personales deriva, por tanto, del concepto de privacidad, en cuanto delimita el ámbito de la vida privada que en un momento dado se haya desarrollado en la sociedad y, por lo que se refiere a nuestros días, en la sociedad global. (…) En este sentido, las denominadas redes sociales de Internet contribuyen a configurar un nuevo concepto de privacidad pero al mismo tiempo reclaman una delimitación del propio derecho a la protección de los datos personales frente a su

O que se percebe, das mais diversas abordagens ao direito à proteção de dados pessoais, é que apesar de ter sua base primeira no direito à privacidade - seu fundamento axiológico, se assim se quiser - , a proteção de dados hoje já é vista como merecedora de normatização específica, constituindo um direito fundamental por si só. Tal tendência significa, do ponto de vista prático, que a proteção de dados, ainda que ligada à privacidade, deve ser regida por normas próprias, com seus princípios e regras específicos,[133] não sendo possível apenas "remendar" as leis em vigor através da modificação legislativa ou interpretação extensiva (em realidade, *criativa*, dada a ausência de menções claras sobre dados pessoais).

A essa posição, subscrevem-se também Stefano Rodotà[134] e Arnaud Belleil,[135] para quem as questões postas dentro de um novo contexto social devem ser resolvidas dentro desse novo contexto e tendo por base os valores em conflito neste novo cenário, ao invés de buscar em concepções de privacidade baseadas em realidades anteriores a solução para tais problemas. Assim, ainda que se reconheça o liame entre os direitos, a proteção aos dados pessoais deve ser submetida a uma análise atual, inserida nas disputas entre interesses presentes dos diversos atores nas relações que envolvam dados pessoais.

Após o desenvolvimento inicial do conceito de dados pessoais e sua aceitação como elementos a serem tutelados paralelamente à vida privada sob a sigla do "novo direito à

---

almacenamiento, a su tratamiento y a su transmisión a terceros; en realidad, se puede constatar que Internet es un desafío para las categorías jurídicas tradicionales." ORDÓÑEZ SOLÍS, David. *Privacidad y protección judicial de los datos personales.* Barcelona: Bosch, 2011. p. 15-17.

[133]"O tratamento da proteção de dados pessoais de forma autônoma é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos. Os desdobramentos e efeitos do tratamento automatizado de informações pessoais, mais do que justificar mudanças e atualizações pontuais no ordenamento jurídico, formam as bases daquilo que vem sendo tratado, hoje, como um direito fundamental à proteção de dados." DONEDA, Danilo. O direito fundamental à proteção dos dados pessoais, *cit.*, p. 66.

[134]"As novas dimensões da coleta e do tratamento de informações provocaram a multiplicação de apelos à privacidade e, ao mesmo tempo, aumentaram a consciência da impossibilidade de confinar as novas questões que surgem dentro do quadro institucional tradicionalmente identificado por este conceito. Hoje, porém, o problema não é adaptar uma noção nascida em outros tempos e em outras terras a uma situação profundamente modificada, respeitando suas razões e sua lógica de origem. Quem consegue decifrar o debate ora em curso percebe que ele não reflete somente o tema clássico da defesa da esfera privada contra as invasões externas, mas realiza uma importante mudança qualitativa, que nos incita a considerar os problemas da privacidade de preferência no quadro da organização do poder, no âmbito do qual justamente a infra-estrutura da informação representa hoje um dos componentes fundamentais." RODOTÀ, Stefano. *op. cit.*, p. 23-24.

[135]No entanto, isto [o desenvolvimento de tecnologias mais antigas de coleta de dados] em nada enfraquece a tese segundo a qual a rede das redes dá uma nova dimensão às questões da privacidade. As tecnologias e as ferramentas citadas desenvolvem-se e interconectam-se já hoje entre si, em virtude da expansão exponencial da *web*. A Internet marca efetivamente o nascimento de uma nova era em matéria de atentados tecnológicos à vida privada (…). BELLEIL, Arnaud. *op. cit.*, p. 52.

privacidade",[136] a doutrina buscou sistematizar sua proteção, notando inicialmente que dois fatores principais deveriam ser utilizados na aferição de legalidade na coleta de dados. Anderson Schreiber chama a esses fatores de dimensão procedimental e dimensão substancial da privacidade,[137] sendo que aquela abrangeria a legalidade do modo de coleta de dados e esta a finalidade da coleta de dados e seu uso efetivo.[138]

Para que determinado procedimento de coleta e tratamento seja considerado legal, tanto o procedimento de coleta e tratamento quanto o emprego final desses dados devem ser legais e legítimos.

A tais fatores subentende-se uma posição ativa do sujeito, que deve ter o poder, assegurado por lei, de modificar, substituir, incluir ou remover as informações sobre ele constantes de um determinado banco de dados. Stefano Rodotà, no mesmo sentido de Westin[139] e Canotilho,[140] definiu tal posicionamento ativo como um "direito de autodeterminação informática", que não só cria direitos para o sujeito, mas também deveres positivos para os utilizadores dos dados pessoais: o dever de solicitar autorização para coleta de dados, a vinculação entre a autorização concedida e a finalidade informada da coleta de dados, o dever de fornecer ao sujeito acesso ao banco de dados onde tenha seus dados inscritos, entre diversos outros.[141]

Tais deveres, entre outros, já despontavam de maneira insípida em antigas leis alemãs das décadas de 1970 e 1980,[142] mas foram finalmente consolidados na forma de princípios orientadores na Convenção de Estrasburgo de 1981 para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais, sendo os principais em número de cinco: o princípio da publicidade, o princípio da exatidão, o princípio da

---

[136]"O direito à privacidade abrange, hoje, não apenas a proteção à vida íntima do indivíduo, mas também a proteção de seus dados pessoais. Em outras palavras: o direito à privacidade hoje é mais amplo que o simples direito à intimidade. Não se limita ao direito de cada um de ser 'deixado só' ou de impedir a intromissão alheia na sua vida íntima e particular. Transcende essa esfera doméstica para alcançar qualquer ambiente onde circulem dados pessoais do seu titular, aí incluídos suas características físicas, código genético, estado de saúde, crença religiosa e qualquer outra informação pertinente à pessoa. Nesse sentido, a privacidade pode ser definida sinteticamente como o direito ao controle da coleta e da utilização dos próprios dados pessoais" SCHREIBER, Anderson. *op. cit.*, p. 136-137.

[137]Reside aqui a falha da análise de Thomson, que avalia a privacidade informacional apenas pelo viés procedimental, do ponto de vista da coleta de informações por terceiro.

[138]SCHREIBER, Anderson. *op. cit.*, p. 138-140.

[139]WESTIN, Alan. Privacy and Freedom, New York: Atheneum, 1970 *apud* PEREIRA, Marcelo Cardoso. *op. cit.*, p. 128.

[140]CANOTILHO, J.J. Gomes. *Direito constitucional e teoria da Constituição*. 7. ed. Coimbra: Almedina, 2003. p. 515.

[141]SCHREIBER, Anderson. *op. cit.*, p. 137.

[142]DONEDA, Danilo. *Da privacidade à proteção de dados pessoais, cit.*, p. 228.

finalidade, o princípio do livre acesso e o princípio da segurança física e lógica.[143] A Convenção nº 108 do Conselho da Europa, conhecida como Convenção de Estrasburgo de 1981, traz tais princípios, respectivamente, em seus artigos 5º[144], 7º[145] e 8º.[146]

Pelo princípio da publicidade ou transparência entende-se que "a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para seu funcionamento, pela notificação de sua criação a uma autoridade, ou pela divulgação de relatórios periódicos."[147] Em outras palavras, a existência de uma coleta de dados em andamento, mais que simplesmente pedir a autorização do indivíduo para coleta de dados, deve ser publicizada.

O princípio abrange também a necessidade de informar o titular dos dados sobre o tratamento de dados pessoais: o titular deve ter consciência de que, em determinadas circunstâncias (ao aderir a um contrato, ao utilizar um serviço ou produto), serão coletados dados pessoais seus, quais dados serão estes, a que finalidade tal coleta se presta e sob responsabilidade de quem o tratamento se desenvolve. Assim, por exemplo, ao contratar determinado serviço pela Internet o usuário deve ser informado se o *website* do provedor do serviço coletará informações suas enquanto usa o serviço. Esse segundo aspecto de transparência é hoje tido em mais alta conta, dado que a maioria dos sistemas de proteção entendeu como inviável o estabelecimento de um sistema de notificação ou autorização prévia para coleta de dados pessoais.

---

[143]MIGUEL ASENSIO, Pedro Alberto de. *op. cit.*, p. 298-306.

[144]Article 5 - Quality of data
Personal data undergoing automatic processing shall be:
A. Obtained and processed fairly and lawfully;
B. Stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
C. Adequate, relevant and not excessive in relation to the purposes for which they are stored;
D. Accurate and, where necessary, kept up to date;
E. Preserved in a form which permits identification of the data subjects for no longr than is required for the purpose for which those data are stores.

[145]Article 7 - Data security
Appropriate security measures shall be taken for the procetction of personal data store in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

[146]Article 8 - Additional safeguards for the data subject
Any person shall be enabled:
A. To establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
B (...)

[147]DONEDA, Danilo. *Da privacidade à proteção de dados pessoais, cit.*, p. 216.

O princípio da finalidade, também conhecido como princípio da limitação dos propósitos,[148] é um dos mais relevantes nos embates atuais sobre a legalidade do mercado de compra e venda de dados pessoais coletados, notadamente, nas redes sociais e outros serviços de Internet de caráter "gratuito".[149] Tal princípio busca limitar o efeito da autorização dada pelo indivíduo para coleta de seus dados pessoais, impedindo que estes sejam usados de modo que contrarie a vontade inicial do indivíduo.

Assim, por tal princípio, os dados só podem ser coletados, tratados e utilizados para a finalidade apresentada ao usuário e por ele aceita, não sendo possível, por exemplo, que o usuário autorize a exibição de sua imagem de maneira pública em determinada rede social, mas que sua foto, seu nome, e demais informações sejam vendidos a terceiro para serem utilizados em peça publicitária, uma vez que tal uso não foi descrito na proposta inicialmente apresentada ao usuário.[150]

Mais que isso, no entanto, a finalidade declarada do tratamento é utilizada para verificar se os dados coletados são adequados e necessários ou se a coleta é excessiva ou ilegítima.[151] Assim, se o responsável deseja coletar dados para poder personalizar o serviço prestado ao usuário, deve informar a ele para que serão utilizados tais dados, por exemplo. Ao mesmo tempo, o responsável que fornece um serviço de correio eletrônico personalizado não pode coletar dados de saúde do usuário, por serem tais dados incompatíveis com a finalidade do tratamento.

O princípio do livre acesso, por sua vez, garante que o usuário tenha acesso aos seus dados, não importando onde estejam localizados, podendo obter cópias desses registros, corrigir informações e mesmo suprimir aquelas obsoletas. Tal princípio relaciona-se com o instituto brasileiro do *habeas data*, apesar de ter maior amplitude por abranger também os bancos de dados privados. Esse princípio conjuga-se com o princípio da exatidão. Por este assegura-se ao indivíduo que seus dados pessoais inseridos em determinado banco de dados sejam fiéis à realidade, corretamente colhidos, tratados e armazenados. Não

---

[148]PEARCE, Graham; PLATEN, Nicholas. Orchestrating transatlantic approaches to personal data protection: a European perspective. *Fordham International Law Journal*, v. 22, n. 5, p. 2029, 1998. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1641&context=ilj.

[149]As aspas se justificam pelo corrente ditado, em voga na comunidade da Internet, de que "se não se paga por um produto ou serviço, o usuário é o verdadeiro produto".

[150]BENSOUSSAN, Alain. *op. cit*., p. 518.

[151]Derivando aqui para o princípio da qualidade dos dados, que mede a proporcionalidade entre a mitigação da privacidade (dados coletados) e os fins do processamento. A esse respeito confira-se PEARCE, Graham; PLATEN, Nicholas. *op. cit*., p. 2029.

sendo este o caso, assegura-se ao sujeito o direito à correção daqueles dados, pela modificação, inclusão ou remoção.

O princípio do livre acesso é de suma importância para todo o sistema de proteção de dados pessoais, uma vez que é um dos mecanismos essenciais para que o titular dos dados exerça seu controle sobre o tratamento dos dados pessoais e sobre sua legalidade. É por meio dele que o titular pode verificar se todo o processo de tratamento, desde a coleta até sua utilização, atende aos requisitos legais, como a limitação da coleta apenas aos dados necessários, a segurança e confidencialidade desses dados e a adequação dos dados à finalidade do tratamento.[152]

Por fim, o princípio da segurança física e lógica estabelece a responsabilidade do depositário de tais informações pela segurança dos dados contra destruição, alteração e acesso indevido, por vias físicas ou virtuais. A responsabilidade aqui não se resume à indenização em caso de violação, mas exige também a adoção de medidas tecnológicas e organizativas para reduzir os riscos inerentes ao processamento de dados pessoais e à possibilidade de tal processamento acarretar danos aos titulares dos dados.[153]

Assim, por exemplo, se determinada violação maliciosa por terceiros decorre da não implementação pelo responsável pelo tratamento de medidas de segurança técnicas (como a criptografia dos dados) ou organizacionais (permitindo assim que os dados sejam acessados por qualquer pessoa dentro da empresa, por exemplo), o responsável deve ser responsabilizado por não ter adotado tais medidas para mitigar o risco de violações.

2.4.3. A consolidação de um direito fundamental

Além do desenvolvimento legislativo ordinário, é relevante entender o caminho percorrido pelo direito à privacidade e pelo direito à proteção de dados até sua consolidação

---

[152]"Although the right of access to personal data is sometimes considered as an ancillary right as compared with the other ARCO rights, it is important to underline that access constitutes the first but irrevocable step towards the full protection of personal data. In other words, it is the *sine qua* son for the exercise of informational rights." GALETTA, Antonella; HERT, Paul de. *A European perspective on data protection and access rights*. Increasing Resilience in Surveillance Societies (IRISS) Project, 2014. Disponível em: http://irissproject.eu/wp-content/uploads/2014/06/European-level-legal-analysis-Final1.pdf. Acesso em: 25 mar. 2019.

[153]"The security principle. Technical and organizational security measures should be taken that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller must not process data except on instructions from the controller." PEARCE, Graham; PLATEN, Nicholas. *op. cit*., p. 2029.

como um direito fundamental, visto que tal status lhe confere relevância e abre novos questionamentos sobre suas limitações.

Para explicar a consolidação do direito à proteção de dados pessoais na União Europeia como direito fundamental, é necessário avaliar brevemente o histórico do Direito Internacional no desenvolvimento da matéria, em especial convenções que foram de especial influência até a consolidação da Carta de Direitos Fundamentais da UE.

A primeira ocorrência do direito à privacidade no Direito Internacional contemporâneo aparece na Declaração Universal dos Direitos Humanos, de 1948.[154] Nascida como reação natural às atrocidades da Segunda Guerra Mundial, a Declaração contém, em seu artigo 12, a garantia de um direito geral à proteção da intimidade e da vida privada e familiar, além do sigilo de correspondência, protegendo todos os indivíduos contra interferência arbitrária nessas esferas. De maneira conexa, a Declaração garante também a liberdade de opinião e expressão em seu artigo 19, o que em certos aspectos relaciona-se com a proteção do segredo e da intimidade do indivíduo, que deve ter liberdade para ter suas próprias crenças e opiniões sem interferências indevidas. Apesar de aparentar certa contradição, a Declaração reconhece em seu artigo 29 que os direitos nela previstos deverão ser balanceados e que nenhum é absoluto per se.

Duramente afetada pela Segunda Guerra Mundial, o desejo de garantir que tai atrocidades não voltassem a ocorrer permitiu a criação ainda de outro tratado semelhante, este, no entanto, de caráter não meramente declaratório como a Declaração Universal. Assim, em 1950, em Roma, foi assinada a Convenção Europeia sobre Direitos Humanos,[155] que veio a fortalecer o arcabouço de direitos, garantias e liberdades fundamentais primeiro delineado pela Declaração em 1948.

A Convenção é aplicável apenas aos países signatários e aos membros do Conselho da Europa, que devem necessariamente aderir também à Convenção quando de sua entrada no Conselho. Diferentemente da Declaração, como já foi dito, a Convenção criava uma obrigação objetiva para que todos os seus membros estabeleçam e garantam os direitos e liberdades nela previstos em suas respectivas jurisdições, criando assim uma real obrigação de adotar legislação interna compatível com o tratado.

---

[154]NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos*. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos.

[155]CONSELHO DA EUROPA. *Convenção Europeia dos Direitos do Homem*. Disponível em: https://www.echr.coe.int/documents/convention_por.pdf.

Ainda, mais que a simples obrigação estabelecida, a Convenção conta com um sistema de aplicação e fiscalização, consubstanciado na Corte Europeia de Direitos Humanos, estabelecida em Estrasburgo. A Corte, tida constantemente como uma instituição da União Europeia, em verdade tem competência mais ampla e sua função é estabelecida não em razão dos tratados da União Europeia, mas sim com base na Convenção, tendo então a corte um escopo de atuação bastante amplo.

Assim, a Corte Europeia de Direitos Humanos pode julgar casos levados a ela relacionados a violações da Convenção, tendo seus julgamentos efeitos vinculantes aos Estados-Membros da Convenção.

A Convenção Europeia de Direitos Humanos previu em seu artigo 12, ecoando a Declaração Universal, que todo indivíduo deve ter garantido seu direito à intimidade e à vida privada e familiar, além do sigilo de correspondência, exceto quando tal violação seja necessária para finalidades que a justifiquem, como persecução penal, segurança nacional, dentre outros, sempre com garantias para que a intromissão se dê de forma legal e proporcional.

Como se vê, enquanto a privacidade encontrou desde cedo status de direito fundamental, foram ainda muito anos até que o direito à proteção de dados fosse reconhecido do mesmo modo.

Foi só com a Carta de Direitos Fundamentais da União Europeia, de 2000,[156] que o direito à proteção de dados pessoais foi elevado à categoria de garantia fundamental. Constou então do artigo 8º da Carta:

> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
>
> 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessa 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 respetiva retificação.
>
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

O que se deve notar é que a Carta não foi simplista na sua garantia. Ao invés de simplesmente elevar o direito a um grau fundamental para o sistema jurídico, a Carta acabou

[156]PARLAMENTO EUROPEU. CONSELHO DA EUROPA. *Carta de Direitos Fundamentais da União Europeia* (2000/C 364/01). Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf.

por incluir também outros três pontos como essenciais para que o cumprimento do direito fundamental à proteção dos dados seja de fato verificado.

O primeiro aspecto é que para que se considere o direito cumprido, o tratamento de dados pessoais que eventualmente seja efetuado deve ser (i) leal, (ii) para fins específicos, e (iii) fundamentado em uma base legal adequada, seja ela o consentimento ou uma outra.

Por tratamento leal se pode compreender um tratamento que seja de fato adequado, isto é, realizado dentro das expectativas do titular dos dados e de acordo com o que tenha sido a ele informado. Assim, se o titular tem seus dados tratados de modo diferente do que lhe foi informado quando ele inicialmente forneceu os dados, tal direito estaria desde já violado.

A limitação do tratamento a "fins específicos" reverbera o princípio da finalidade, já analisado, pelo qual dados pessoais devem ser coletados e tratados apenas para finalidades específicas, sem que seja possível o simples acúmulo de dados, com a expectativa de que tal conjunto de dados um dia se mostre valioso.

Ainda, quando se diz que o tratamento de dados deve ser baseado no consentimento ou outro fundamento legal aplicável, a Carta explicita, em resumo, que o tratamento de dados pessoais é a exceção, e não a regra. Ao contrário do que se vê em outros países, aqui o tratamento de dados é em regra *proibido, a não ser que haja uma justificativa legal para o tratamento de dados.* Ou seja, na ausência de um fundamento legal, é proibido o tratamento de dados pessoais. Como veremos, esse aspecto será de grande relevância para nossa análise, uma vez que não se trata aqui de uma simples regra procedimental, mas sim de um princípio elevado a garantia fundamental. É dizer que violar tais princípios relacionados ao tratamento de dados, certamente previstos no GDPR, representam não só uma violação do próprio Regulamento, mas também a violação de um direito fundamental garantido pela Carta de Direitos Fundamentais da UE.

Em segundo lugar, o artigo estabelece como condição primária para o cumprimento do direito fundamental a garantia de um direito de acesso ao titular, pareado com um direito de retificação caso os dados estejam incorretos. Apesar de haver outros direitos garantidos no GDPR, os direitos de acesso e retificação foram assim elevados ao patamar de direitos fundamentais pela Carta.

Ainda, em terceiro lugar, segundo a Carta é exigido, para que se considere o texto integralmente cumprido, que os direitos relacionados a dados pessoais sejam fiscalizados por uma autoridade independente. Tal dicção traz imenso impacto, ao estabelecer como elemento fundamental da disciplina a existência das chamadas Autoridades de Proteção de Dados e, ainda mais, de seu caráter independente, o que, como visto, sempre foi um ponto de conflito ao longo da implementação da Diretiva de Proteção de Dados.

2.5. Desenho normativo

O sistema de proteção de dados pessoais da União Europeia (U.E.) é considerado hoje um dos mais avançados e serviu de fonte de inspiração para leis em todo o mundo. Tem-se hoje que não só o modelo europeu é visto como um dos polos da discussão sobre a regulação dos dados pessoais, mas também representa forte fator de influência para o modelo contraposto, vigente principalmente nos Estados Unidos da América.[157]

O caso europeu ainda demanda alguma atenção extraordinária pela complexidade do quadro legislativo em vigor, que deve comportar o Direito comunitário com suas diretivas, regulamentos, orientações e jurisprudência próprios; assim como é integrado também no espectro nacional por leis, decretos e jurisprudência próprios, podendo se constatar importantes variações nos espaços discricionários criados pelo direito comunitário para garantir maior flexibilidade na adoção de suas normas pelos Estados-partes e buscar, consequentemente, maior adesão e efetividade das garantias e regras instituídas.

Considerando o objetivo de nosso estudo, nossa análise se concentrará, neste momento no Regulamento Geral de Proteção de Dados, o GDPR, mas passaremos rapidamente também por outras normativas como a Convenção nº 108 do Conselho da Europa, a Diretiva sobre e-Privacy e o programa conhecido como Privacy Shield.

---

[157]Como coloca Newman: "The United States, which long supported market-based solutions, rejected the legitimacy of the EU's legislation, stoking the first trade conflict of the information age.(...) Against U.S. objections, European rules became the de facto international standard with more than thirty countries following the European approach." NEWMAN, Abraham L. *op. cit.*, p. 104. Confira-se também: CASTETS-RENARD, Céline. *Droit de l'internet*: droit français et européen. 2. éd. Paris: Montchrestien, 2012. p. 26.

2.5.1. A Convenção 108 do Conselho da Europa

Em primeiro lugar, a Convenção nº 108 do Conselho da Europa de 1981, também conhecida como "Convenção para a Proteção de Indivíduos em relação ao Tratamento Automatizado de Dados Pessoais" ou, mais simplesmente, Convenção de Estrasburgo, é a norma internacional de maior relevância para o bloco europeu sobre proteção de dados pessoais. Ao contrário das outras normativas internacionais já mencionadas, a Convenção de Estrasburgo é a primeira do seu gênero a enfrentar diretamente o desafio de estabelecer regras sobre como deve se dar qualquer tipo de tratamento de dados pessoais.

Diferentemente de outros instrumentos internacionais da época, a Convenção já exigia que seus signatários tomassem internamente as medidas necessárias para implementar e aplicar os princípios previstos em seu texto.

O ponto de partida da Convenção foi o reconhecimento de que aqueles que utilizam dados pessoais possuem certas responsabilidades para que tal uso dos dados não cause danos ou afete os indivíduos aos quais os dados dizem respeito de um modo negativo. No entanto, a Convenção já reconhece que a simples proteção dos indivíduos não pode ser o único valor defendido em tal contexto, tomando como valor a ser também impulsionado o livre trânsito dos dados pessoais dentro de certos limites. Isto é, pela primeira vez, é estabelecido um mecanismo de controle sobre transferências internacionais: enquanto o tráfego de dados pessoais entre os países signatários da convenção deve ser incentivado, uma vez que cada um comprometeu-se a promover os mesmos valores sobre proteção de dados em suas respectivas legislações internacionais, por outro lado a transferência de dados para outros países é, em tese, proibida ou minimamente desencorajada.

Em termos substantivos, como já vimos, a Convenção normatizou o princípio da publicidade, o princípio da exatidão, o princípio da finalidade, o princípio do livre acesso e o princípio da segurança física e lógica, já explorados brevemente anteriormente.[158]

Apesar de já em muito superada pela legislação mais atual, a Convenção continua a representar um marco normativo para a proteção de dados, especialmente por sua característica internacional. A Convenção, inclusive, está aberta à adesão de países não membros da União Europeia, contando hoje com 51 países que a ratificaram.

---

[158]MIGUEL ASENSIO, Pedro Alberto de. *op. cit.*, p. 298-306.

A Convenção de Estrasburgo foi reformada em 2018 por um Protocolo de Alteração[159], sendo modernizada e expandida em diversos pontos. Além dos princípios previstos na convenção, é interessante notar que em sua versão atualizada a Convenção também consolida disposições sobre transparência sobre o tratamento (isto é, quais informações devem ser fornecidas ao titular dos dados sobre o tratamento), proibição do tratamento de dados sensíveis (isto é, categorias especiais de dados cujo tratamento em regra é proibido, exceto em casos restritos), direitos assegurados ao titular (entre eles, acesso, retificação, objeção ao tratamento, objeção a decisões automatizadas, entre outros) e disposições sobre a atuação das autoridades de proteção de dados pessoais.

2.5.2. Regulamento Geral de Proteção de Dados

O sistema europeu de proteção de dados pessoais sofreu grande alteração em 2016, quando foi aprovada uma grande reforma gestada desde 2010[160]. A reforma se deu, sobretudo, pela introdução do Regulamento nº 679/2016 do Parlamento e do Conselho, que substituiu a Diretiva nº 95/46/CE e unificou a disciplina da proteção dos dados pessoais, uma vez que é diretamente aplicável como se norma interna fosse. A substituição de uma diretiva por um regulamento vem também atender a uma necessidade de unificação do sistema, já que não é mais necessária a incorporação do texto supranacional por uma lei interna. Tal regulamento ficou conhecido como o Regulamento Geral de Proteção de Dados[161], o *General Data Protection Regulation*, ou, simplesmente, GDPR[162].

---

[159]EUROPEAN COMMISSION. Council of Europe. *128th Session of the Committee of Ministers*. (Elsinore, Denmark, 17-18 May 2018). Ad hoc Committee on Data Protection (CAHDATA) - Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e.

[160]COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões*. *Uma abordagem global da protecção de dados pessoais na União Europeia*. COM(2010) 609 final, cit.

[161]UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção 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 L. 119/1008, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679.

[162]Juntamente ao GDPR foi também aprovada a Diretiva nº 2016/680/CE, que regula o tratamento de dados pessoais no contexto da investigação, repressão e persecução criminais pelas autoridades competentes, mas que não nos interessa diretamente no presente estudo. Confira-se: UNIÃO EUROPEIA. Diretiva (UE) nº 2016/680 do Parlamento Europeu e do Conselho 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

O GDPR é uma normativa de ampla abrangência e que oferece, possivelmente, um dos mais complexos sistemas de proteção no globo na atualidade. Este capítulo tem como proposta sistematizar os principais pontos de comparação entre os sistemas, mas é relevante nesse ponto apresentar breve resumo do que dispõe o GDPR.

O GDPR conta com uma extensa coleção de consideradas que oferecem material valioso para a interpretação das disposições normativas do Regulamento, totalizando 173 considerandas. O texto da normativa em si é dividido em 11 capítulos: (i) disposições gerais, (ii) princípios, (iii) direitos dos titulares de dados, (iv) controladores e operadores, (v) transferências internacionais de dados, (vi) autoridades de supervisão independente, (vii) mecanismos de cooperação e consistência entre autoridades, (viii) remédios, responsabilidade e penalidades, (ix) disposições sobre processamentos específicos, (x) implementação e medidas delegadas aos Estados-Membros e (xi) disposições finais.

Dentre os temas mais relevantes, destacamos (i) os princípios e condicionantes para tratamentos de dados, (ii) os direitos dos titulares, (iii) as responsabilidades dos controladores e operadores, e (iv) as autoridades de proteção de dados.

Em relação aos princípios e condicionantes, é necessário dizer que, além dos princípios aplicáveis ao tratamento de dados que o restringem em determinados aspectos, o GDPR estabelece que para que o tratamento de dados seja lícito, ele deve se basear no consentimento do titular dos dados ou em alguma das outras hipóteses legais para tratamento, que incluem, por exemplo, o tratamento de dados que é necessário para o cumprimento de um contrato ou o tratamento de dados necessário para cumprimento de uma obrigação legal, hipóteses nas quais o consentimento é dispensado.

Mesmo quando o tratamento é baseado no consentimento do titular, o GDPR estabelece critérios e requisitos estritos sobre tal consentimento, exigindo-o livre, informado e inequívoco, por exemplo. O tratamento de dados de categorias especiais (os “dados sensíveis” na dicção nacional), que incluem por exemplo dados sobre saúde e opinião política é submetido a restrições ainda maiores, sendo mais restritas as hipóteses em que é admitido seu tratamento, como também é o caso do tratamento de dados de crianças e adolescentes.

No que toca os direitos dos titulares de dados, o GDPR traz uma lista de direitos que devem ser garantidos, incluindo (i) o direito a receber informação transparente, clara e

circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Jornal Oficial L. 119/89, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0680.

concisa sobre o tratamento de dados; (ii) o direito de acessar os dados tratados; (iii) o direito de retificar os dados tratados quando estes estejam incorretos ou desatualizados; (iv) o direito de eliminação dos dados (também chamado "direito ao esquecimento"[163]); (v) o direito de requisitar a restrição ao tratamento de dados; (vi) o direito a solicitar a portabilidade dos dados tratados para outro provedor de serviços semelhantes; (vii) o direito de objetar a decisões automatizadas baseadas no tratamento de dados pessoais; (viii) o direito de objetar ao tratamento, entre outras variantes garantidas na legislação esparsa.

Em relação às responsabilidades dos controladores e operadores, o GDPR traz uma longa lista de obrigações que incluem desde a indicação de um encarregado por supervisionar os tratamentos de dados (o Encarregado ou *Data Protection Officer*), passa pela adoção de medidas adequadas de segurança, físicas, técnicas e administrativas, para garantia da segurança e confidencialidade dos dados pessoais, e vai até a adoção de práticas responsáveis sobre o tratamento de dados, o que é geralmente interpretado pelo mercado como uma obrigação geral de adotar regras e procedimentos internos para garantir que o tratamento de dados conduzido pela entidade é feito em estrita conformidade com a lei, em um modelo de programa de *compliance* característico de áreas como prevenção à lavagem de dinheiro e anti-corrupção.

Ainda, é relevante notar que o GDPR, repercutindo o disposto na Carta de Direitos Fundamentais de 2000, na Diretiva de Proteção de Dados de 1995 e na Convenção de Estrasburgo de 1981, estabelece com grande detalhe a obrigação de cada Estado-Membro criar, dentro de características bastante específicas, uma autoridade independente de supervisão para fiscalizar o cumprimento do GDPR e de outras normativas relacionadas à proteção de dados. Como já dito, o caráter independente dessas autoridades é especialmente importante, uma vez que as regras do GDPR dizem respeito não apenas ao tratamento de dados pela iniciativa privada, mas também pelos órgãos públicos de cada Estado-Membro.

Tais autoridades, para que possam cumprir sua finalidade, devem possuir poderem amplos para investigar e punir, mas também para intervir em conflitos entre particulares quando deles toma conhecimento (por exemplo, por uma reclamação feita por um particular), assim como intervir em processos judiciais e administrativos dentro das suas competências.

---

[163]Note-se que o direito ao esquecimento europeu não é exatamente equivalente ao direito ao esquecimento brasileiro. Sobre esse tema, confira-se GUIDI, Guilherme Berti de Campos. O Caso Costeja v. Google Spain e o direito ao esquecimento: para além da implementação e rumo ao diálogo global. *In*: MENEZES, Wagner (Org.) *Tribunais internacionais e a implementação procedimental de suas decisões*. Belo Horizonte: Arraes, 2018.

As autoridades, por natureza, possuem também competências consultivas e normativas, podendo estabelecer recomendações ou normativas de menor grau para regulamentar e interpretar pontos específicos da legislação aplicável sobre proteção de dados, oferecendo então maior detalhamento aos princípios e regras gerais contidas no GDPR e outras regras de ampla abrangência.

2.5.3. Diretiva 2002/58/CE e a *e-Privacy Directive*

A Diretiva 2002/58/CE,[164] mais tarde alterada pela Diretiva 2009/136/CE, regula área não suficientemente abordadas pelo GDPR no campo específico das comunicações eletrônicas, ou seja, serviços de comunicação que impliquem na transmissão de sinais através, por exemplo, de redes de telecomunicação ou radiofusão. Essa diretiva declara expressamente que sua finalidade é a especificação e complementação das regras sobre proteção de dados trazidas pelo GDPR.[165]

Para isso, o diploma apresenta algumas regras especialmente relevantes ao setor por peculiaridades dos serviços prestados ao usuário. Aborda também algumas práticas específicas do setor, como o *spam*, determinando por fim que os Estados-Membros da União Europeia devem promulgar leis nacionais que internalizem tais regras.

Para atingir seu objetivo, a Diretiva trabalha em duas frentes, criando obrigações para os Estados por um lado e para os responsáveis pelo tratamento de outro. Aos responsáveis pelo tratamento dos dados pessoais, a Diretiva impõe as obrigações de *(i)* garantir que os dados em processamento só sejam acessados por pessoas autorizadas, inclusive dentro de sua própria organização; *(ii)* proteger os dados de perda, destruição ou alteração acidental, e contra qualquer forma de tratamento ilegal ou não autorizado; *(iii)* garantir a aplicação de uma política de segurança no que diz respeito ao tratamento dos dados pessoais; *(iv)* notificar todos os casos de violação de dados pessoais, internas ou externas, acidentais ou dolosas, à autoridade nacional no prazo de 24 horas; *(v)* eliminar ou tornar anônimos os dados que não

---

[164]UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas. Jornal Oficial L. 201, 31 de julho de 2002. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002L0058.

[165]Artigo 1º, 2: Para os efeitos do nº 1, as disposições da presente diretiva especificam e complementam a Diretiva 95/46/CE. Além disso, estas disposições asseguram a proteção dos legítimos interesses dos assinantes que são pessoas coletivas.

forem mais necessários para efeito de comunicação ou faturamento de serviços prestados, salvo se dado o consentimento do titular para a continuidade do uso dos dados para fins de comercialização; *(vi)* em relação aos dados citados no item anterior, cessar a utilização de dados mantidos exclusivamente para fins de comercialização imediatamente caso o titular retire seu consentimento para tal, o que pode ser feito a qualquer momento.

Aos Estados-Membros, a Diretiva estabelece as obrigações de *(i)* garantir, de modo geral, a confidencialidade das comunicações realizadas através de redes públicas; *(ii)* proibir a instalação de escutas e outras formas de vigilância e interceptação de comunicações e dados em tráfego sem a autorização do titular, exceto quando autorizada por decisão judicial; *(iii)* garantir que só sejam armazenadas informações (pelo provedor do serviço) no dispositivo do titular dos dados ou sejam essas informações acessadas por provedores de serviços de comunicação eletrônica apenas quando o titular for devidamente informado sobre isso e, podendo recusar, dê seu expresso consentimento.

Por fim, apesar de certas regras de derrogação presentes no GDPR quanto à exigência do consentimento do titular dos dados em tratamento, a Diretiva 2002/58/CE estabelece alguns casos específicos em que o consentimento se mantém como requisito para a legalidade do uso dos dados.

Exige-se o consentimento expresso do titular dos dados *(i)* antes de lhe serem enviadas comunicações não solicitadas,[166] por qualquer via de comunicação;[167] *(ii)* antes da inserção de informações, pelo provedor, no equipamento pessoal do usuário do serviço ou antes do acesso dessas informações pelo provedor do serviço (implementação de cookies);[168] e *(iii)* antes da inclusão de dados de contato (telefones, endereços físicos ou e-mail) do titular em listas públicas.

2.5.4. O Tribunal de Justiça da União Europeia

---

[166]"Le *spamming* ou *spam* peut se définir comme une communication commerciale non sollicitée. Il est apparu nécessaire au législateur communautaire de protéger les internautes contre toute violation de leur vie privée par des communications non sollicitées effectuées à des fins de prospection directe, en particulier au moyen d'automates d'appel, de télécopies et de courriers électroniques, y compris les messages courts (SMS)." CASTETS-RENARD, Céline. *op. cit.*, p. 77.

[167]E-mail, SMS, mensagens instantâneas e qualquer outro tipo de mensagem, textual ou multimídia.

[168]"Les '*cookies'* ou témoins de connexion sont de véritables mouchards 'pondus' sur le disque dur de l'internaute par le gestionnaire d'un site. Ces mouchards prennent la forme de petits fichiers qui demeurent après la déconnexion, enregistrent des données sur le type et caractéristiques techniques de l'ordinateur, les logiciels installés et utilisés, les sites et pages consultés. Lors de la connexion suivante, toutes les données du cookie sont rapatriées vers le site 'pondeur' pour être exploitées." CASTETS-RENARD, Céline. *op. cit.*, p. 76.

A União Europeia tem razões de sobra para ser um dos principais fóruns de discussão de questões relacionadas às novas tecnologias.[169] Sendo pioneira, tanto no aspecto supranacional quanto por seus Estados-Membros, na regulação de aspectos que são hoje chave para boa parte da matéria, nominalmente a privacidade e a proteção de dados pessoais,[170] após décadas de experiência prática, encontramos ali um espaço maduro para discussões de largo calibre.

Um ponto talvez ainda mais interessante seja a peculiaridade sobre o modelo de organização regional do bloco, que conta com um nível de integração sem precedentes que permite, em especial, a existência e a atuação de um Tribunal internacional regional, como é o Tribunal de Justiça da União Europeia (TJUE).

O Tribunal de Justiça é órgão da União de atividade adjudicatória e consultiva. Compete a ele decidir sobre diversos assuntos, em especial os pedidos de anulação de atos das instituições da União e sobre a interpretação ou validade das disposições do direito da União, inclusive no que toca a compatibilidade de leis nacionais com as regras supraestatais.[171] Disso decorre que o Tribunal tem um papel primordial na garantia da coesão e coerência do sistema jurídico da União, permitindo alguma uniformidade na aplicação da lei naquele território.[172]

Como seria de se esperar, o papel do Tribunal de Justiça da União Europeia foi decisivo na experiência da Diretiva nº 95/46/CE e continua o sendo com a vigência do GDPR.[173]

Na história recente do Tribunal, alguns casos se destacam por seu protagonismo em questões de grande alcance. A primeira diz respeito à revogação da Diretiva nº

---

[169]GUIDI, Guilherme Berti de Campos. *A proteção dos dados pessoais na internet*: contribuições da experiência europeia ao modelo brasileiro, *cit*.

[170]Sobre as experiências na Alemanha e na França, confira-se DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, *cit*.

[171]CASELLA, Paulo Borba. *União Europeia*: instituições e ordenamento jurídico. São Paulo: LTr, 2002. p. 118-119.

[172]MENEZES, Wagner. *Tribunais internacionais*: jurisdição e competência. São Paulo: Saraiva, 2013. p. 170.

[173]Com a entrada em vigor do Regulamento Geral de Proteção de Dados Pessoais em maio de 2018, a competência do Tribunal foi expandida. Na vigência da Diretiva, a competência do Tribunal lhe permitia conhecer de questões relacionadas a falhas de transposição da Diretiva para o direito interno de cada Estado-Membro ou de conflitos interpretativos da lei local, que seriam então solucionados com base no texto da Diretiva. Isso ocorre porque a Diretiva é norma que atribui aos Estados-Membros a obrigação de adotar leis internas em determinado sentido, não sendo diretamente aplicável, no que se diferencia do Regulamento, que constitui norma supranacional diretamente aplicável aos governos, empresas e indivíduos.

2006/24/CE[174], a segunda à revogação dos acordos conhecido como Safe Harbor e Privacy Shield, entre União Europeia e Estados Unidos.

A Diretiva nº 2006/24/CE dispunha sobre a retenção de dados de conexão pelos provedores de acesso. Os dados de conexão são informações como os nomes dos usuários envolvidos em determinada troca de dados (se disponíveis), seus endereços IP, sua localização, e o tipo de comunicação[175], coletados especificamente para fins de investigação, detecção ou persecução penal de delitos graves. Tal ponto recebia tratamentos diversos nos países membros da União Europeia, trazendo inconsistências na regulamentação regional da matéria, razão pela qual optou-se pela uniformização de tal regramento pela aprovação de uma Diretiva.

Em abril de 2014 o Tribunal de Justiça da União Europeia declarou essa diretiva inválida[176] ao considerar que, enquanto a obrigação de retenção de certos dados de conexão não viola, *per se*, direitos fundamentais da Carta de Direitos, o modo como é determinada a retenção é desproporcional.

No entendimento da Corte, a diretiva violava direitos individuais vez que *(i)* não definia suficientemente a gravidade dos crimes que justificariam o acesso a esses dados; *(ii)* não exigia decisão judicial para permitir o acesso aos dados;[177] *(iii)* não criava obrigações de garantia suficientes para a proteção dos dados retidos; e ,principalmente, *(iv)* não exigia que tais dados fossem armazenados no território da União Europeia, impossibilitando a supervisão das autoridades independentes de dados pessoais competentes.

Em um segundo caso, o Tribunal tomou importante decisão relativa a transferências internacionais de dados pessoais de cidadãos europeus. A Decisão da Comissão 2000/520/EC, datada de 26 de julho de 2000, criava um programa de "porto seguro"[178]

---

[174]UNIÃO EUROPEIA. Directiva 2006/24/CE do Parlamento Europeu e do Conselho de 15 de março de 2006 relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Diretiva 2002/58/CE. Jornal Oficial L. 105, 13 de abril de 2006. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32006L0024&from=FI.

[175]Os dados de conexão, como se percebe, servem apenas como identificadores das partes envolvidas em uma troca de dados, em conformidade com o artigo 5º da Diretiva 2006/24/CE, mas nunca os dados *objetos da comunicação em si*, como bem prevê o parágrafo 2º do mesmo artigo.

[176]UNIÃO EUROPEIA. Corte de Justiça da União Europeia. *Casos conjuntos C-293/12 e C-594/12*. Digital Rights Ireland Ltd. v. Ireland, julgados em 8 de abril de 2014. Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=PT&cid=513860. Acesso em: 09 out. 2014.

[177]A esse respeito, conferir os artigos 4º e 8º.

[178]"Safe Harbour"

juntamente ao Departamento de Comércio dos Estados Unidos da América.[179] Em razão de diversas revelações sobre a devassa de dados pessoais por órgãos governamentais, a reação do Tribunal foi dura.[180]

Os Estados Unidos têm uma abordagem bastante diferente da europeia, sendo notável o aspecto econômico dos dados pessoais naquele país, em que são vistos mais como mercadoria do que como aspectos personalíssimos a serem protegidos.[181] Diante disso, as transferências de dados pessoais para os Estados Unidos poderiam ser proibidas com base no artigo 25 da Diretiva 95/46/CE, que veda transferências tais a países que não possuam um nível de proteção adequado aos dados.

Buscando evitar a interrupção no fluxo de dados entre a União Europeia e aquele país, criou-se um programa de conformidade, aplicável às empresas que desejassem receber dados da União Europeia. O programa funcionava com o cadastramento de empresas norte-americanas junto ao Departamento de Comércio daquele país, devendo tais empresas declarar a adesão ao programa publicamente, adotar e apresentar uma Política de Privacidade adequada às normas da União Europeia e obter uma certificação anualmente junto ao Departamento de Comércio.[182]

Em decisão datada de 6 de outubro de 2015, o Tribunal de Justiça da União Europeia, diante das denúncias feitas pelo ex-agente da Agência de Segurança Nacional norte-americana (*NSA),* Edward Snowden,[183] julgou inválida a Decisão 2000/520/CE. A Corte sustentou que os dados transferidos da União Europeia aos Estados Unidos estariam sujeitos ao acesso e processamento pela *NSA* sem a conformidade necessária com os princípios do "Safe Harbour", sendo tratados para finalidades e em medidas incompatíveis com o estritamente necessário para a proteção da segurança nacional. Isso representaria grave

---

[179]COMISSÃO EUROPEIA. *Decisão 2000/520/CE*. Decisão da Comissão de 26 de julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de "porto seguro" e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América. Jornal Oficial L 215, 25 de agosto de 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32000D0520.

[180]O caso ficou conhecido como o "escândalo PRISM", em que a Agência de Segurança Nacional dos EUA foi implicada por um ex-agente em operações massivas de vigilância. Sobre o assunto, confira-se: GREENWALD, G; MACASKILL, E. NSA Prism program taps in to user data of Apple Google and others. *The Guardian Online*, June 7, 2013. Disponível em: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em: 10 mai. 2017.

[181]"In contrast to other areas of the world such as the United States, where personal information is widely traded like a conventional good, European rules limited the commodification of individual data." NEWMAN, Abraham L. *op. cit.*, p. 104.

[182]Além da Decisão já mencionada, mais detalhes do programa podem ser encontrados no *website* oficial do SAFE Harbour Framework. Disponível em: www.export.gov/safeharbor/index.asp.

[183]GREENWALD, G.; MACASKILL, E. *op. cit*.

violação à intimidade dos titulares de tais dados, o que seria ainda agravado pela inexistência de meios para que tais indivíduos buscassem seus direitos e protegessem sua intimidade e seus dados pessoais contra sua violação ou utilização abusiva.[184]

Na sequência dessa decisão, entabularam-se novas discussões entre Estados Unidos e União Europeia, a fim de criar um novo programa para garantir o intercâmbio de informações. O resultado desses esforços foi a Decisão de Execução 2016/1250/CE[185], que estabeleceu o agora conhecido programa "Privacy Shield", que aprimorou o anterior[186].

No entanto, em processo semelhante ao que levou à derrocada do Safe Harbour, foi instaurado novo processo perante o TJUE para análise do novo Privacy Shield. A demanda, iniciada pelo mesmo ativista que havia questionado a validade do Safe Harbour, ficou conhecida como "o caso Schrems II".[187]

Nesse novo processo, mais que um simples questionamento sobre o programa, questionavam-se também o mecanismo de *cláusulas contratuais padrão.* A título de curta explicação, como já mencionado, o GDPR não permite que o controlador dos dados pessoais (a empresa que realiza o tratamento) transfira dados pessoais para países fora da União que não apresentem um nível adequado de proteção, isto é, que não possuam, em seu sistema

---

[184]"Moreover, the foregoing analysis of Decision 2000/520 is borne out by the Commission's own assessment of the situation resulting from the implementation of that decision. Particularly in points 2 and 3.2 of Communication COM(2013) 846 final and in points 7.1, 7.2 and 8 of Communication (COM(2013) 847 final, the content of which is set out in paragraphs 13 to 16 and paragraphs 22, 23 and 25 of the present judgment respectively, the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased." UNIÃO EUROPEIA. Corte de Justiça da União Europeia. *Caso C-362/14*. Maximillian Schrems v. Data Protection Commissioner, julgado em 6 de outubro de 2015. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=515620. Acesso em: 08 out. 2015.

[185]UNIÃO EUROPEIA. Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. Jornal Oficial L. 207/1, 01 de agosto de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016D1250.

[186]A adesão ao programa Privacy Shield é voluntária, apesar de ser requisito para transferências de dados que envolvam a União Europeia. Uma vez feita a adesão ao programa, no entanto, o atendimento a seus requisitos é obrigatório e exigível pela lei local norte-americana. Para mais informações, confira-se: PRIVACY Shield Frameworks. Disponível em: https://www.privacyshield.gov/.

[187]COURT OF JUSTICE OF THE EUROPEAN UNION (CJEU). *Case C-311/18*. Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. Judgment from the Court of Justice of the European Union (CJEU) relating to the transfer of personal data by a private company from a European Union (EU) Member State to a private company in a third country for commercial purposes. It concerns specifically the legality of standard contractual clauses (SCCs) as a mechanism to transfer personal data outside the EU. The judgment became known as the *Schrems II* judgment. Disponível em: https://www.europeansources.info/record/cjeu-case-c-311-18-data-protection-commissioner-v-facebook-ireland-and-maximillian-schrems/.

jurídico, normas que garantam um nível ao menos semelhante ao garantido pelo direito europeu. Alternativamente, o controlador deve no mínimo demonstrar que, mesmo que o país de destino não apresente garantias legislativas suficientes, que os dados serão protegidos por medidas contratualmente impostas. Assim, a União Europeia possui conjuntos de Cláusulas Contratuais Padronizadas, aprovadas pela Comissão Europeia, que, quando utilizadas pelo controlador para proteger os dados sujeitos a transferência internacional, em tese já estaria tal transferência autorizada e devidamente e automaticamente garantida.

Enquanto o programa Privacy Shield fundamentava-se em um reconhecimento de adequação (a Comissão reconhecia que dados sujeitos ao programa estariam sujeitos a "um nível de proteção adequado", sendo as transferências assim possíveis), em outros casos os controladores geralmente usavam de modo "cego" as cláusulas-padrão, sem uma preocupação real sobre se tais cláusulas seriam de fato suficientes para garantia da segurança do tratamento de dados.

O Tribunal de Justiça da União Europeia, analisando a reclamação sobre tais dois pontos em relação à continuidade dos programas de vigilância estatal nos Estados Unidos, especialmente os baseados no *Foreign Intelligence Surveillance Act (FISA)*, lei norte-americana que estabeleceu os programas de vigilância então tornados públicos por Edward Snowden, considerou inicialmente que o programa Privacy Shield não oferecia proteção adequada no caso de transferências internacionais. Isso porque, em termos gerais, o FISA não oferecia garantias processuais suficientes sobre o exercício básico de direitos (de acesso, por exemplo) quanto aos dados tratados com base no programa de vigilância e que mesmo os remédios judiciais disponíveis contra abusos por tais programas de vigilância eram absolutamente insuficientes.

A decisão considerou também que as cláusulas contratuais padrão aprovadas pela Comissão, apesar de não serem invalidadas, só deveriam ser consideradas como "garantias adequadas" para tais tipos de transferências se fossem de fato adequadas ao tratamento em questão, não sendo mais um "cheque em branco" para transferências internacionais. Na prática, isso retiraria a presunção de legalidade que adviria pelo uso das cláusulas contratuais padrão, estando a transferência internacional sujeita ao escrutínio dos titulares e das autoridades para eventual questionamento quanto a sua legalidade caso as cláusulas utilizadas não fossem plenamente adequadas.

Assim, em suma, apesar de em tese ainda existente, o programa Privacy Shield não pode ser mais utilizado para fundamentar transferências internacionais, por não ser mais considerado "adequado" nos termos do GDPR, enquanto a eficácia das cláusulas contratuais padrão foi flexibilizada, eliminando a presunção de legalidade existente em tal tipo de operação.

2.6. Considerações sobre proteção de dados no sistema europeu

As normativas descritas representam o cerne de onde emana o sistema europeu de proteção de dados pessoais, aí compreendidos também os subsistemas nacionais. O conjunto de normas supranacionais formado por tais diretivas, regulamentos e decisões, por si só, é digno de nota diante de sua própria ambição.

O GDPR, nesse contexto, é talvez o texto central do conjunto, objetivando a tutela no contexto do tratamento de todo e qualquer dado pessoal, seja ele automatizado ou não, na esfera pública ou privada. Obviamente outros diplomas são igualmente relevantes em *valor*, mas considerando o objetivo deste estudo, em grande parte são as disposições do GDPR que estabelecem o parâmetro a ser tido para comparação com o sistema norte-americano.

É de grande relevância para o presente estudo compreender como o conjunto de normas é estruturado de modo a permitir certa segmentação, ao mesmo tempo em que se mantém uma unidade mínima que diz respeito a todos os setores de regulamentação. Nessa estrutura encontramos a Convenção de Estrasburgo de 1981 como a fonte principal dos valores a serem tutelados, posicionada no topo do conjunto e figurando até o presente como fundamento filosófico para todos os outros esforços normativos na matéria. A partir de 2000, a Carta dos Direitos Fundamentais da União Europeia, consolidando a posição de garantia fundamental da proteção dos dados pessoais, passou a figurar também no polo axiológico do tema.

Dito isso, quatro pontos principais merecem nossa atenção para o estabelecimento de pontos comuns para comparação: a abrangência das normativas, as limitações e condicionantes do tratamento de dados em si, os direitos dos titulares de dados e a forma de tutela e as obrigações impostas ao responsável pelo tratamento de dados.

2.6.1. Abrangência

Em termos de abrangência, as regras europeias sobre proteção de dados conseguem abranger um amplo espectro de atividades, tanto de caráter público quanto privado, além de ter seu escopo ampliado pela definição aberta do que se entende por tratamento de dados pessoais.

A princípio o GDPR aplica-se ao tratamento de dados pessoais, seja por meios automatizados ou não, físicos ou digitais. O conceito de tratamento engloba um sem-número de ações, como já visto aqui, sendo considerado tratamento qualquer tipo de uso ou interação com dados pessoais. O conceito de dado pessoal, como também já visto, é amplo e designa toda e qualquer informação relacionada a uma pessoa física identificada ou identificável.

Dentre as exclusões da aplicação do GDPR contidas no artigo 2º constam os tratamentos realizados pelos Estados-Membros para finalidades relacionadas a segurança pública, segurança nacional, persecução penal e fins militares, além daqueles efetuados por uma pessoa física para finalidades exclusivamente pessoais ou domésticas. Essa última exclusão, inclusive, é bastante restrita, sendo que qualquer tipo de uso de dados que fuja do absolutamente comum estaria sujeito ao GDPR, mesmo que se trate de um tratamento realizado por uma pessoa individual.

Em seu escopo territorial, a aplicação do GDPR é também bastante ampla, o que inclusive é capaz de gerar problemas de ordem internacional em razão da sua aplicação extraterritorial em certos casos. Em resumo, estão sujeitos ao GDPR (i) todos os tratamentos ocorridos no território da União ou em local em que sejam aplicáveis as leis da União, (ii) todos os tratamentos realizados no contexto da operação de entidades estabelecidas na União, e (iii) todos os tratamentos realizados por entidades estabelecidas fora da União mas que, de alguma forma, ofereçam bens e serviços a pessoas na União Europeia ou monitorem o comportamento de pessoas localizadas na União Europeia.[188]

Por tais definições, não haveria qualquer limitação à aplicação da legislação a tratamentos sem fins lucrativos ou realizados por pessoas individuais, nem qualquer consideração sobre o tamanho do tratamento ou o faturamento mínimo decorrente de tal operação.

---

[188]Art. 3º.

Note-se também que o critério de aplicação considera no geral pessoas *localizadas* na União Europeia, e não residentes ou mesmo cidadãos. Dessa forma, mesmo uma pessoa que se encontre apenas de passagem por aquele território teria a garantia de que seus dados deverão ser tratados em conformidade com o GDPR.

Ainda, como mencionado acima, é necessário apontar que em teoria o GDPR seria aplicável também *fora* do território da União Europeia, na medida em que uma empresa estabelecida fora daquele território, uma vez que venha a oferecer bens e serviços àquele mercado, viesse a tratar dados também em submissão ao Regulamento. Com isso, fica claro que a preocupação do GDPR é ignorar em parte o aspecto territorial para reconhecer que a lei só seria efetiva caso tivesse como centro o tratamento de dados, e não onde ele ocorre ou onde está localizado o responsável.

2.6.2. Condicionantes do Tratamento de Dados

Um dos aspectos de maior distintividade do sistema europeu é o fato de que o sistema coloca diversas condicionantes e limitações ao tratamento de dados, através da criação de (i) hipóteses legais que autorizam o tratamento (estando o mesmo, em tese, proibido na ausência de uma hipótese legal cabível) e de (ii) princípios e regras sobre a legalidade do tratamento que, mesmo depois que se verifica o tratamento possível, ainda limitam *como* o tratamento deve ser realizado, sua medida, especificações, finalidades e meios.

É dizer que não se trata de um sistema simplista, pelo qual o tratamento é ou não possível com base na incidência de determinada hipótese legal, mas sim que mesmo que o tratamento seja plenamente *possível,* ele ainda pode ser amplamente desleal e, portanto, ilegal.

O primeiro aspecto condicionante diz então respeito às chamadas bases legais de tratamento. A primeira delas, que talvez melhor auxilie em sua compreensão, é o próprio consentimento do titular dos dados. Assim, se o titular dos dados *autoriza* que seus dados sejam coletados e tratados, há em tese uma base legal que permite o tratamento.

Ocorre que a legislação europeia foi sábia em reconhecer que nem sempre o consentimento será uma base legal adequada. Basta considerar, por exemplo, a hipótese em que uma vítima de um acidente chega desacordada a um hospital: o tratamento de dados (a

abertura de um prontuário médico para registrar o tratamento) é necessário para permitir que a vítima tenha o atendimento necessário, mas em tal estado não é ela capaz de autorizar (ao menos não em livre consciência, o tratamento dos seus dados pessoais. No mesmo sentido, imagine-se a dificuldade em obter o consentimento específico de todos os clientes de determinada empresa apenas para que esta possa cumprir com suas obrigações legais relacionadas, por exemplo, a seus registros de vendas de produtos para fins de administração tributária. Não só a questão é se o consentimento é *possível*, mas também se ele é *adequado*, uma vez que não seria razoável limitar a capacidade de uma empresa de cumprir suas obrigações fiscais apenas porque determinado consumidor optou por não autorizar tal tratamento de dados pessoais.

Assim, o GDPR, no que parece uma medida adequada, reconhece também hipóteses legais que autorizam o tratamento de dados que não dependem do próprio consentimento. Assim é o caso dos tratamentos voltados ao cumprimento de obrigação legal, à prestação de serviços de saúde e/ou proteção à vida do titular ou de terceiro, ao exercício regular de direitos (por exemplo em processo judicial, em que não é razoável esperar a autorização da parte contraposta), e para a execução de um contrato.

Uma hipótese, entretanto, que chama a atenção e é relevante para a comparação a ser realizada é a do Interesse Legítimo. Segundo o GDPR, um controlador pode tratar dados pessoais quando possuir um interesse legítimo relevante que não prejudique de modo desproporcional os direitos e garantias fundamentais do titular dos dados. Ao colocar a questão dessa forma, o legislador basicamente exige que se realize um exercício de proporcionalidade entre o interesse do controlador do tratamento e os direitos do titular, de modo que se verifique se há proporcionalidade no tratamento proposto.

A amplitude do legítimo interesse se justifica pela necessidade de flexibilizar o sistema e prever situações que não fossem concebidas pelo legislador ao tempo da elaboração do Regulamento. Obviamente, justamente por tal flexibilidade, o interesse legítimo é uma das bases legais que mais atenção recebe das autoridades, sempre buscando regulamentar seu uso e limitar suas hipóteses de aplicação. Mesmo assim, é interessante notar (até pelo caráter das regulamentações), que o interesse legítimo é uma verdadeira válvula de escape do GDPR, permitindo que a legislação se adeque, sem maior dificuldade, a novos usos e finalidades para o tratamento de dados pessoais, desde que mantida a premissa de que os titulares não sejam injustamente prejudicados por tal tratamento de dados.

Superada a verificação sobre a *possibilidade* do tratamento, devem-se considerar também as limitações e condicionantes à *forma* do tratamento. Nesse aspecto, os princípios de proteção de dados, já explorados anteriormente, são de grande relevância. Os princípios da finalidade, da necessidade e da adequação no geral são responsáveis pelas maiores limitações na forma como os dados são tratados. Pelo primeiro princípio, como já vimos, o dado deve ser tratado para finalidades específicas expressamente informadas ao titular. Igualmente, pelo princípio da necessidade, o dado só pode ser tratado se for de fato necessário para o atingimento da finalidade definida. Ainda, pelo princípio da adequação, o tratamento deve ser realizado estritamente nos moldes em que tenha sido comunicado inicialmente ao titular dos dados.

Como veremos, esses princípios são de suma importância não só para o GDPR, mas são relevantes para nosso esforço comparativo na medida em que podemos encontrar alguns ecos deles nas regulações dos Estados Unidos, como explicitaremos no capítulo 4.

No todo, é dizer então que, uma vez coletado o dado (i) para determinada finalidade, (ii) sendo ele necessário para tal finalidade, só pode o dado ser tratado estritamente de acordo com tais especificações, conforme informadas aos titulares dos dados. Enquanto a explicação pode parecer simples, na prática tal intento é de especial dificuldade prática, uma vez que envolve controlar de forma apurada, *para cada dado pessoal coletado,* qual a finalidade da coleta e a informação efetivamente dada ao titular, para evitar que tal dado seja utilizado para outras finalidades diversas que possam surgir ao longo da operação da empresa.

2.6.3. Direitos do titular e tutela

A garantia dos direitos do titular de dados é um dos eixos centrais da legislação sobre proteção de dados pessoais na União Europeia. Como vimos, mesmo os direitos de acesso e retificação foram prestigiados como direitos fundamentais ao serem incluídos no artigo 8º da Carta de Direitos Fundamentais da União Europeia. Ocorre que este talvez seja um grande diferencial entre o sistema da União Europeia e dos Estados Unidos, pelo que vale prevê incursão no tema.

Os direitos do titular estão garantidos, sobretudo, no artigo 8º da Carta, no artigo 9º da Convenção de Estrasburgo e no capítulo III do GDPR. Considerando este último como o

repositório mais detalhado de tais direitos, que inclusive abrange os direitos garantidos nos outros dois diplomas, focaremos nossa análise no capítulo III do GDPR.

Um primeiro foco dos direitos diz respeito ao direito à informação sobre o tratamento. O GDPR é detalhista quanto a quais informações devem ser comunicadas ao titular, seja em situações em que o tratamento de dados pessoais é realizado diretamente após a coleta direta de dados do próprio titular (com este fornecendo os dados, por exemplo, através de um questionário ou formulário de cadastro), as circunstâncias em que deve se dar tal fornecimento de informação e inclusive as características de tal informação (clara, concisa, completa, etc). O GDPR inclusive diferencia tal circunstância daquela na qual os dados tratados não são obtidos diretamente do titular dos dados, mas sim de terceiro que anteriormente teve contato com o titular. É o caso, por exemplo, de uma empresa que adquire dados de outra, esta sim que teve contato direto com o titular; mesmo que tal coleta seja indireta, a primeira empresa (que não tem contato direto com o titular), deve ainda prover meios para que este se informe sobre o tratamento, o que pode incluir mesmo a publicização ampla de tais informações.

Não só *como* o controlador deve informar, mas também *o que* deve ser objeto da comunicação são pontos abordados pela legislação: o controlador deve informar, em suma: (i) a identidade e contato do responsável pelo tratamento, (ii) o contato do encarregado de proteção de dados, (iii) as finalidades do tratamento e o fundamento jurídico para o tratamento, (iv) os dados efetivamente tratados, (v) os destinatários dos dados pessoais, caso eles sejam compartilhados, (vi) informações sobre a transferência internacional de dados, (vii) o prazo de conservação dos dados pessoais, (viii) os direitos garantidos ao titular dos dados, (ix) se o tratamento de dados e seu compartilhamento resultam em uma obrigação legal ou contratual, e (x) se o titular estará sujeito a decisões automatizadas, incluindo a definição de perfis, baseadas em dados pessoais (bem como as informações relevantes sobre os critérios de tais decisões automatizadas).

Em modo semelhante ao direito à informação, o direito de acesso não só permite o acesso do titular aos dados que são efetivamente tratados, incluindo informações sobre o tratamento em geral, incluindo as informações acima elencadas e também sobre a origem de tais dados, caso não tenham sido diretamente obtidos do titular. O direito de acesso é tido como um dos elementos basilares da chamada *autodeterminação informática*, uma vez que é apenas a partir do acesso efetivo aos dados e às informações sobre o tratamento que o titular pode, de modo informado e ponderado (i) avaliar se o tratamento está sendo conduzido de

forma lícita ou se deseja apresentar ao responsável ou à autoridade de supervisão uma reclamação, e (ii) decidir se deseja exercer algum dos outros direitos garantidos pela legislação.

É garantido, de modo acessório ao direito de acesso, o direito de eliminação e o direito de correção. Pelo direito de correção, o titular tem o direito de atualizar ou corrigir dados sobre si que estejam de fato incorretos ou que sejam inexatos. Pelo direito de eliminação, o titular pode solicitar o apagamento dos dados pessoais em certas circunstâncias. No geral, a eliminação dos dados só será possível quando o tratamento for baseado no consentimento e este for revogado ou quando o dado seja tratado de maneira irregular, seja de modo excessivo ou na falta de uma base legal aplicável ao tratamento, não sendo assim um direito absoluto.

Entre outros direitos garantidos, podemos citar também o direito à restrição ao tratamento dos dados (geralmente aplicável quando há alguma decisão ou definição pendente sobre o tratamento de dados em razão de uma reclamação ou solicitação do titular), o direito à portabilidade de dados (que permite o titular transferir seus dados pessoais a outro prestador de serviços), o direito de oposição ao tratamento (pelo qual o titular pode se opor ao tratamento de seus dados para certas finalidades como e-mail marketing), e o direito de se opor a decisões automatizadas (ou seja, pedir que determinada decisão não seja baseada exclusivamente no tratamento automatizado de dados pessoais).

A multiplicidade de direitos garantidos pela legislação da União Europeia denuncia um fortalecimento da autocomposição para a resolução de conflitos: cabe, inicialmente, ao próprio titular o dever de fiscalizar como seus dados são utilizados e agir para limitar ou eliminar o tratamento de dados irregular, caso note tal necessidade. Trata-se de faceta constantemente reforçada da *autodeterminação informativa,* pela qual busca-se armar o titular dos dados com os instrumentos necessários para tomar as próprias decisões sobre seus dados pessoais.

Na prática, no entanto, este não é um passo obrigatório no caminho para a judicialização de conflitos. Obviamente, é preferível, até para o próprio titular, que certas demandas sejam intentadas primeiramente pela via particular, onde ainda há chance de se resolver determinado conflito. O interessante é que esse mecanismo *exige* que o responsável pelo tratamento se exponha e coloque sua própria justificativa para o tratamento de dados em questão para análise.

Explicando de outra forma, na ausência de tais direitos, o responsável não seria legalmente obrigado a responder uma solicitação do titular. Não sendo obrigado a responde-la, teria maior vantagem caso a demanda fosse diretamente proposta em um foro administrativo ou judicial, no qual poderia mais facilmente administrar sua defesa. Quando tais direitos são garantidos, no entanto, o responsável não só é obrigado a responder dentro de certo prazo, mas tal justificativa passa a vincular as estratégias de defesa a sua disposição: caso o responsável utilize uma determinada justificativa na resposta a uma solicitação de direito do titular, o titular pode utilizar aquela resposta para levar o caso à autoridade de supervisão ou ao próprio judiciário; nesse caso, mesmo que o responsável mude sua tese de defesa, estará vinculado à resposta inicial – mesmo que sua nova tese encontre guarida no judiciário, a resposta incorreta inicial ainda pode ser objeto de reprimenda.

Assim, a garantia de direitos ao titular é importante ferramenta para exigir que os responsáveis pelo tratamento cumpram corretamente suas obrigações no tratamento leal dos dados e respondam corretamente às solicitações, uma vez que uma resposta errada pode gerar diversos prejuízos ao responsável, funcionando isso como uma ferramenta de responsabilidade e prestação de contas.

De outro lado, os direitos do titular são também importante ferramenta para exigir informações e submeter tais informações recebidas ao escrutínio das autoridades. É assim, portanto, que o titular de dados pode obter as informações relacionadas a determinado tratamento de dados irregular para então levar tais informações à autoridade de supervisão ou ao próprio Poder Judiciário. Pode-se então dizer que, apesar do aspecto de autocomposição que os direitos do titular parecem ter como eixo central, eles também são relevantes em um quadro maior sobre a efetividade da tutela de direitos, considerando não apenas os direitos do Capítulo III do GDPR, mas os direitos reflexos de todas as obrigações de tratamento justo e correto decorrentes do Regulamento.

2.6.4. Responsabilidade, *accountability* e segurança

Por fim, mas não menos importante, é necessário ressaltar as obrigações relacionadas a responsabilização dos responsáveis pelo tratamento, prestação de contas (*accountability)* e segurança dos dados.

Em um primeiro aspecto, os responsáveis pelo tratamento, geralmente chamados *agentes de tratamento*, podem ser controladores ou operadores. Em termos simples, o controlador é o responsável geral pelo tratamento, aquela entidade que define as finalidades e os meios do tratamento e que possivelmente recolhe os principais benefícios do tratamento de dados. Já o operador, de modo simplificado, é a entidade que simplesmente trata os dados (ou de qualquer forma intervém no tratamento) apenas sob ordens do controlador.

Tal diferenciação é relevante pois reflete inclusive na divisão das responsabilidades contratuais entre as partes em caso de vazamento de dados, por exemplo. No entanto, o reflexo prático mais interessante diz respeito a como a divisão de responsabilidades leva os controladores a estabelecerem relações contratuais com diversas amarras obrigacionais, de modo a garantir que as ações do operador sejam sempre conforme a lei. Dessa feita, o GDPR inaugurou uma prática de mercado para negociação de robustas cláusulas de proteção de dados que, mesmo que não exigida pela legislação, se tornou boa prática em diversos lugares do mundo, inclusive no Brasil.[189]

Tal impacto é sentido também no chamado princípios de *accountability*. Segundo o GDPR, não só os agentes de tratamento devem cumprir a lei, mas sim realizar esforço positivo para *demonstrar* tal cumprimento. Essa responsabilização pós-fato decorre largamente da mudança de um sistema que flertava com a autorização prévia de tratamentos de dados para um sistema de controle posterior, em que o cumprimento da lei é geralmente fiscalizado após o início do tratamento de dados.

Em termos práticos, a obrigação de *accountability* desenvolveu-se para abranger programas complexos de governança em dados pessoais, no formato de programas de compliance anti-corrupção, por exemplo, que conjugam, por exemplo, o estabelecimento de políticas e regras internas sobre tratamento de dados, a adoção de práticas contratuais responsáveis, o treinamento constante do corpo de colaboradores, e, principalmente, a gestão de riscos proativa em proteção de dados, com a elaboração de relatórios e registros de tratamentos executados antes mesmo do início de um projeto, de forma a registrar (para eventual fiscalização) que "o dever de casa foi feito".

[189]Sobre este assunto, confira-se: ALVES, Carla Segala; GUIDI, Guilherme Berti de Campos. Cláusulas contratuais e dados pessoais: controladores, operadores, cocontroladores e transferências internacionais. *In*: BLUM, R.O.; VAINZOF, R.; MORAES, H.F. *Data protection officer (encarregado)*: teoria e prática de acordo com a LGPD e o GDPR. São Paulo: Thomson Reuters Brasil, 2020.

Por fim, e de forma alguma não menos importante, encontramos as obrigações de segurança dos dados. O GDPR, após décadas de experiência com a Diretiva de Proteção de Dados, adotou o mesmo posicionamento da Diretiva quanto à segurança dos dados pessoais. Seria razoavelmente fácil perder-se em determinações sobre tecnologias variadas que deveriam ser empregadas para garantia do tratamento; o que se notou desde cedo, entretanto, é que a legislação sobre um tema tão mutável quanto proteção de dados deve ser, dentro do possível, tecnologicamente neutra.

Isso porque, em resumo, enquanto o campo fático da proteção de dados (e da tecnologia) tem um ritmo de alteração altíssimo, não é tão simples atualizar leis para que correspondam aos mais novos padrões tecnológicos disponíveis. Assim, o GDPR recorre a uma generalização, complementada por um outro dever cujo cumprimento é avaliado pós-fato: os agentes de tratamento devem adotar as medidas *adequadas,* sejam elas *técnicas, físicas ou administrativas,* para salvaguardar os dados. Não são apresentadas medidas específicas para dizer *o que é adequado,* mas sim critérios que devem ser utilizados pelo agente do tratamento em tal avaliação, que poderá mais tarde ser submetida ao crivo das autoridades.

Assim, as medidas de segurança a serem aplicadas devem necessariamente resguardar a confidencialidade, a integridade, a disponibilidade e a resiliência dos dados (o conjunto básico de valores defendidos pela disciplina de segurança da informação) e considerar ainda (i) as características e os riscos do tratamento, (ii) a tecnologia disponível, e (iii) os custos de aplicação das medidas de segurança.

Tais requisitos flexíveis de segurança serão um fator interessante de comparação, vista sua amplitude e seu fundamento em práticas já estabelecidas do campo de segurança da informação no que se refere à gestão dos riscos de segurança.

CAPÍTULO 3. PROTEÇÃO DE DADOS NO SISTEMA DOS ESTADOS UNIDOS DA AMÉRICA

3.1. Considerações iniciais

Uma vez visitado o sistema da União Europeia cabe então analisar como os Estados Unidos da América lidam com a privacidade e a proteção de dados pessoais. Tal análise deve necessariamente abordar primeiro algumas premissas gerais sobre o sistema legal dos Estados Unidos e o histórico de desenvolvimento do chamado *right to privacy* naquele país, que diverge em parte da narrativa já construída até aqui. Tal esforço será necessário e útil pois é justamente em razão de tal linha de desenvolvimento que o direito norte-americano é tido como lacônico ou incompleto no tema dos dados pessoais, de modo que entender a origem do direito será essencial para avaliar quais as possibilidades de construção para um direito à proteção de dados pessoais.

Em seguida, nos debruçaremos sobre os limites no reconhecimento do direito à privacidade como um direito constitucionalmente protegido e sobre os contornos atuais do *enforcement* naquele país relativo às práticas relacionadas a proteção de dados. Essa via de investigação será de grande interesse para o presente trabalho pois muito do que é dito e feito nos Estados Unidos sobre proteção de dados é antes visto na esfera do *enforcement* do que da diretamente transposto à lei estatutária.

Assim, passaremos em seguida a uma análise sucinta de algumas propostas legislativas mais amplas para então buscar identificar elementos centrais de tal sistema para nosso esforço comparativo.

3.2. Introdução sobre o sistema legal dos Estados Unidos

É necessário estabelecer algumas premissas sobre o funcionamento geral do sistema legal norte-americano, pois tais premissas nos auxiliam a identificar importantes considerações sobre a distribuição de competências e atribuições entre os diversos órgãos públicos dos Estados Unidos, nos auxiliando também a entender as interações entre normas, *common law* e outros institutos daquele sistema.

Os Estados Unidos da América são uma república federativa dotada de um sistema de governo presidencialista. O governo é dividido entre Poderes, sendo eles o Legislativo, o Executivo e o Judiciário, que interagem de maneira a se equilibrar, por meio de um sistema de *checks and balances,* ou de "pesos e contrapesos", de modo que cada Poder funciona não apenas para suas próprias finalidades, mas também para a fiscalização e limitação dos demais poderes.

A Constituição vigente no país foi apresentada inicialmente em 1787 e vige desde 1789, tendo sofrido diversas emendas desde sua aprovação. As emendas de número 1 a 10, conhecidas como *Bill of Rights,* formam o núcleo do que se pode considerar o conjunto de direitos fundamentais protegidos pela Constituição naquele país.

O sistema federativo é de especial nota, dada a autonomia concedida aos estados para dispor sobre temas locais, inclusive pela aprovação de ampla legislação sobre diversos assuntos. Diferentemente, por exemplo, do Brasil, são menores as restrições de competência ou reservas de competência ao poder federal, de modo que em muitos assuntos a legislação mais relevante é aquela aprovada pelo estado. Isso porque a reserva de competências exclusivas ao governo federal disposta no artigo 1º da Constituição é, comparativamente, bem mais suscinta e restrita no que proíbe aos estados e reserva à federação.

Em termos normativos, os Estados Unidos não poderiam ser mais diferentes da União Europeia. O Direito norte-americano tem como suas fontes a Constituição federal e as constituições de cada estado, leis estatutárias aprovadas pelo Poder Legislativo, regras e regulamentos estabelecidos por órgãos administrativos e o *common law* ou direito comum.[190]

A *common law* é uma forma de direito norte-americano caracterizada pelo desenvolvimento incremental através de decisões judiciais perante casos concretos. Cada nova decisão serve como um precedente para as decisões seguintes e as cortes buscam sempre decidir novos casos de forma coerente com os casos anteriores, o que gera para cada decisão o que se geralmente refere por peso de precedente (*precedential weight).* É de se notar que na *common law* mais tradicional são os próprios juízes que desenvolvem, criam, regras a serem observadas, como foi o caso da maior parte das regras sobre contratos, responsabilidade civil e mesmo responsabilidade criminal, sendo que em certo ponto de maturidade tais regras podem ser incluídas em regras estatutárias formais. No entanto, a

[190]SWIRE, Peter P.; KENNEDY-MAYO, DeBrae. *U.S. Private-sector privacy*: law and practice for information privacy professionals. 2. ed. Portsmouth: IAPP, 2018. Cap. 1.

common law emerge também da interpretação e aplicação, pelas cortes, das normas estatutárias existentes, de modo que ao aplicar determinada norma não é suficiente ler o texto da lei, mas também consultar o que dizem os tribunais a tal respeito.[191]

O *direito comum*, também referido como *case law*, *common law* ou normas costumeiras é de especial interesse ao nosso estudo, uma vez que dado o pouco tempo em que os direitos relacionados à proteção de dados pessoais tiveram para se desenvolver, é natural que encontremos ainda no direito comum (não transformado em leis estatutárias) boa parte das regras aplicáveis sobre proteção de dados.

Talvez por tal motivo haja uma impressão generalizada – incorreta – de que os Estados Unidos não só não possuem uma lei central e geral de proteção de dados, mas que também não teriam regras gerais sobre o uso de dados pessoais. Como veremos, apesar da ausência de uma lei estatutária central e geral sobre proteção de dados, os Estados Unidos cultivam práticas bem estabelecidas por outras vias regulatórias, como pela atuação da *Federal Trade Comission* (FTC), para dispor sobre o que é aceitável em termos de proteção de dados. Não objetaremos, nesse momento, o fato de que a ausência de leis estatutárias gerais impede um *enforcement* particular mais amplo, tendo o indivíduo que se resguardar com o *enforcement* de algumas poucas agências federais ou órgãos legais (como o *Attorney General* de cada estado, atuando como principal representante jurídico do estado), que geralmente possuem recursos limitados e alcance limitado na sua tutela de casos individuais.

No entanto, é importante reconhecer que não se trata de um vazio legal que deve necessariamente ser preenchido com institutos importados de outros sistemas (como o Europeu). Assim, pela própria natureza da comparação a ser efetuada, é relevante que não nos rendamos a soluções simplistas de importação legislativa, mas sim avaliemos cada sistema em seu respectivo contexto legal.

---

[191]"*Common law is a form of Anglo-American law that is characterized by incremental development through judicial decisions in a series of concrete cases. The decisions serve as precedent – judges aim to decide cases consistently with previous decisions. In the most traditional form of common law, judges develop the legal rules. Much of Anglo-American tort law, contract law, property law and criminal law emerged through this process. Many parts of these bodies of law were later codified into statutes, especially criminal law, which today in the United States is almost entirely statutory. There is also another form of common law that emerges through the interpretation of constitutions and statutes. Although judges do not create the initial rules, their decisions on the meaning of those rules have precedential effect and become essential to the interpretation of the rules."* SOLOVE, Daniel; HARTZOG, Woodrow. The FTC and the new common law of privacy. *Columbia Law Review*, v. 114, n. 583, p. 619-620, 2014. Disponível em: https://cyberlaw.stanford.edu/files/publication/files/SSRN-id2312913.pdf.

Em termos de fiscalização e aplicação das leis, doravante entendido como o conjunto de estatutos, *case law* e normas costumeiras, tem-se geralmente a esfera civil, a esfera criminal e a administrativa. Ao mesmo tempo, pode-se pensar em ações públicas ou em *private rights of action* para cada uma dessas esferas. No primeiro aspecto, como acontece também em sistemas de *civil law*, uma demanda pode ser iniciada na esfera civil, na esfera criminal ou na esfera administrativa, a depender do tipo de lei que embasa tal ação. Na esfera criminal geralmente se exige a pré-existência de tipos criminais específicos em legislação estatutária especialmente designada a regular tal matéria, podendo a iniciativa ser da vítima, mas geralmente estando também aberta à atuação das autoridades jurídicas, como o *Attorney General* ou o escritório da promotoria.

Na esfera civil, pode-se pensar tanto em ações individuais ou coletivas, geralmente dadas à iniciativa privada do prejudicado ou interessado que possua um *right of action,* ou seja, a previsão legal de que a violação de determinado direito pode ter como remédio um tipo específico de ação judicial ou uma ação judicial geral, como no caso dos *torts,* que representam ações baseadas em responsabilidade extracontratual geral e em que o objetivo é geralmente obter compensação por um dano sofrido.

Como veremos, no campo da privacidade as ações individuais e as *tort claims* são geralmente restritas pelo próprio *common law* por terem aplicação específica (no caso das *torts)* ou por não haver um direito expresso de ação, dado que o direito à privacidade nos Estados Unidos, além de alguns aspectos específicos, é tido como uma construção doutrinária e jurisprudencial, mas não consolidada em lei estatutária geral.

Por fim, o *enforcement* administrativo tem grande valia para nossa análise. Ele geralmente ocorre pela atuação de órgãos federais ou estaduais que, tomando a iniciativa para exigir o cumprimento da lei, interpelam, questionam, cobram ou de outra forma decidem, na esfera administrativa, sobre determinados casos, podendo considerar que uma entidade ou uma empresa, por exemplo, tenha violado determinada normativa e, por tal razão, é cabível a aplicação de penalidades administrativas previstas na lei, sob pena de iniciar-se um litígio cível ou criminal.

Esse tipo de enforcement, como se verá, é extremamente relevante para proteção de dados em razão do papel central que a FTC tem desempenhado nesse cenário, chegando alguns estudiosos inclusive a defender que a atuação da FTC passou a criar um verdadeiro

common law específico para proteção de dados, apesar de não haver quase nenhum caso judicializado.

Definidas as premissas gerais sobre o funcionamento do sistema dos Estados Unidos, podemos passar à análise específica da privacidade e da proteção de dados em tal sistema.

3.3. O histórico da *privacy* nos Estados Unidos

Don R. Pember, que em sua obra "*Privacy and the Press*" traça um dos primeiros históricos sobre o direito à privacidade, menciona regras específicas no Direito norte-americano, que parecem refletir a questão central da privacidade já nas últimas décadas do século XIX, sem no entanto abordar o núcleo duro do direito.[192]

Também Raymond Lindon, um dos mais destacados escritores dedicados ao tema, sustenta que o direito à privacidade é relativamente recente, tendo sido desenvolvido nos séculos XIX e XX, não sendo portanto necessária uma busca em passado remoto.[193] Assim a primeira menção a tal direito, muitos sustentam,[194] aparece em obra do juiz norte-americano Thomas McIntyre Cooley denominada *The Elements of Torts*, publicada originalmente em 1895. Nesta obra, considerada seminal, o autor descreve em certa passagem um direito a um tipo de "imunidade pessoal", um direito a ser deixado só.

Como dito, credita-se a cunhagem de tal expressão a Cooley, mas dificilmente poder-se-ia dizer que foi esta obra que finalmente reconheceu, de alguma forma, um direito à privacidade. Interpretada de maneira ampla, a expressão nos leva a uma imunidade não só física, como mental, íntima, psicológica. Mas o contexto em que tal passagem se encontra, e a evolução do argumento no texto em si, nos mostra que Cooley referia-se muito mais a uma proteção contra a agressão, física ou psicológica, que uma invasão da intimidade do

---

[192]"As the 'Gay Nineties' opened, the American people still did not have a legally enforceable right of privacy. Courts in both England and the United States had granted individual rights which were on the periphery of privacy, but no court had ever stopped the kind of 'Paul Pry' journalism which was described earlier on the ground that it was an invasion of privacy. Yet, according to the commentators of the era, the nation was ready for the recognition of such a right." PEMBER, Don R. *Privacy and the press*: the law, the mass media and the first amendment. Seattle: University of Washington Press, 1972. p. 18.

[193]LINDON, Raymon. *Une création prétorienne*: les droit de la personnalité. Paris: Dalloz, 1974. p. 6-7.

[194]Cf. PEREIRA, Marcelo Cardoso. *op. cit.*, p. 112; PEMBER, Don R. *op. cit.*, p. 20-25; SCHREIBER, Anderson. *op. cit.*, p. 134-135.

indivíduo,[195] demonstrando, pois, uma abordagem indireta do tema, como foi dito ser comum no sistema da *Common Law*.

Em países da *Common Law*, a privacidade desenvolveu-se inicialmente, em manifestação infinitamente inferior ao seu alcance atual, como decorrência implícita do direito de propriedade e de liberdade.[196] No entanto, foi justamente um autor de um desses países que deu a maior contribuição ao tema, inclusive em seu tratamento no sistema da *Civil Law*.

Parece mais adequado atribuir a primeira elaboração do direito à privacidade a Samuel Warren e Louis Brandeis, autores do famoso artigo "*The right to privacy*"[197] publicado em 1890. Não só mais adequada tal atribuição, mas também mais correta, uma vez que tal artigo não só introduziu a ideia de um direito a não ter sua intimidade exposta, mas foi o que melhor pode elaborar as primeiras bases e contornos desse direito sem ter de recorrer diretamente a direitos anexos aos de propriedade, liberdade pessoal e à responsabilidade civil.[198]

O artigo de Warren e Brandeis representa o ápice da formação do direito na linha traçada por Daniel Becourt, pois a obra não só inaugura o estudo sistemático da privacidade, mas também representa uma alteração de perspectiva, movendo-se o foco da relação entre o Estado e o indivíduo para as relações particulares, movimento acompanhado também pelo tratamento privado dos direitos da personalidade.[199] Percebe-se finalmente que a violação da

---

[195]"Personal immunity - The right to one's person may be said to be a right to complete immunity; to be let alone. An attempt to commit a battery usually involves an insult, a putting in fear, a sudden call upon the energies for prompt and effectual resistance; and the law for theses reasons makes the assult a wrong even though no actual battery takes place. But a mere threat to commit an injury, though sometimes made criminal, as an assault also is, is not an actionable private wrong." COOLEY, Thomas McIntyre. *The elements of torts*. Kindle Edition, 2015. pos. 4060-4067.

[196]FERNANDES, Milton. *Proteção civil da intimidade, cit.*, p. 17.

[197]WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, Dec. 1890. Disponível em: https://www.jstor.org/stable/pdf/1321160.pdf?refreqid=excelsior%3Ac5f30ce85672d3d6b0e51c6350c80d0b.

[198]Em comentário a tal artigo, Danilo Doneda escreve: "No entanto, o artigo é inédito ao propor uma força inédita ao novo *right to privacy*, e também é mais que mero reflexo de uma época, fazendo estender sua influência por algumas de suas características: (i) partia-se de um novo fato social, que eram as mudanças trazidas para a sociedade pelas tecnologias de informação (jornais, fotografias) e a comunicação de massa, fenômeno que se renova e continua moldando a sociedade futura; (ii) o novo "direito à privacidade" era de natureza pessoal, e não se aproveitava da estrutura da tutela da propriedade para proteger aspectos da privacidade; (iii) no que interessa somente aos EUA, o artigo abriu o caminho para o reconhecimento (que porém ainda tardaria décadas) do reitio à privacidade como um direito constitucionalmente garantido." DONEDA, Danilo. *Da privacidade à proteção de dados pessoais, cit.*, p. 138-139.

[199]GOGLIANO, Daisy. *op. cit.*, p. 25.

privacidade por outros indivíduos, além do Estado, pode ser tão ou mais perigosa para a integridade da personalidade do titular desses direitos.

Samuel D. Warren, à época advogado e industrial, foi levado a escrever o famoso artigo por experiências pessoais desagradáveis com a imprensa da época. Casado com a filha do então futuro Secretário de Estado, o Senador Thomas F. Bayard, Warren fazia parte da alta sociedade de Boston e seu lar, frequentemente aberto a eventos sociais, foi alvo de grande interesse para a imprensa sensacionalista,[200] com pouco ou qualquer respeito à privacidade dos envolvidos.

O artigo *The Right to Privacy* pode ser dividido em três seções, sendo que a primeira estabelece a necessidade do reconhecimento legal de um direito de estar só, fundada essa necessidade principalmente nos métodos investigativos do jornalismo da época e nas tecnologias de registro de imagem e voz que então avançavam; a segunda parte em que os autores analisam a possibilidade (frustrada) de adequação de institutos da *common law* e da *equity* para tutelar tal direito; e trazendo a terceira parte uma tentativa de delimitar o proclamado direito.

Demonstrando uma guinada da doutrina do *common law*, a principal contribuição do artigo para o desenvolvimento da matéria é o reconhecimento de que a proteção à intimidade do indivíduo não está ligada à propriedade, mas a sua personalidade. Os autores chegam a tal conclusão ao analisar a tutela de escritos pessoais[201] e os eventuais danos causados por sua publicação.

> "But where the value of the production is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all, it is difficult to regard the right as one of property(…)".[202]
>
> "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."[203]

---

[200]FERNANDES, Milton. *Proteção civil da intimidade, cit.,* p. 21-22.

[201]No mesmo sentido: "Não se deve confundir aqui o direito à privacidade e a proteção da intimidade, protegendo-se portanto os segredos e a vida privada do indivíduo, inclusive quando tais atributos encontram-se postos em um suporte fático (como um diário ou cartas pessoais), com os direitos morais de autor, que pressupõem a esteticidade da obra. Ainda assim, sustentam os autores que aos pensamentos, sentimentos e emoções expressados por meios artísticos ou não é concedida uma proteção abrangente por um direito maior a estar só." FERNANDES, Milton. *Proteção civil da intimidade, cit.,* p. 23.

[202]WARREN, Samuel D.; BRANDEIS, Louis D. *op. cit.,* p. 200.

[203]*Id. Ibid.,* p. 205.

A ideia inicial do direito à privacidade era resguardar a vida privada do indivíduo da invasão de terceiros, em um sentido claramente negativo, característico das liberdades públicas, em razão do estabelecimento de um dever de abstenção.

Com as primeiras investigações, alguns autores buscaram definir exatamente qual seria essa proteção, entre eles Judith Jarvis Thomson. A autora, após avaliar diversos casos comuns onde se poderia dizer que houve uma violação de privacidade, posiciona-se para defender que não se proíbe que terceiros tenham conhecimento de fatos sobre determinada pessoa, mas sim que este terceiro *busque tomar conhecimento* de tais fatos, o que representaria sim uma violação à privacidade.[204]

O exemplo utilizado para ilustrar o ponto é o de um casal que briga em sua própria casa: se o casal briga com as janelas abertas, de modo que qualquer passante possa ouvir, esses terceiros não violam a privacidade se simplesmente tomam conhecimento da briga enquanto passam; por outro lado, se alguém *busca* tomar conhecimento da mesma briga, dessa vez conduzida a janelas fechadas e à voz baixa, tem-se uma violação.[205]

Não parece razoável contradizer tal posicionamento, uma vez que não se pode simplesmente obrigar os passantes que ouviram tal briga, por exemplo, a esquecer o que ouviram. O que é necessário aqui é uma adequação. Enquanto Thomson analisa uma situação contida - o que deve se esperar diante do momento histórico do artigo - , não considera a etapa subsequente de utilização ou aproveitamento da informação. Como analisar a questão se em ambas as situações o terceiro que toma conhecimento do fato decide divulgá-lo? Não é por outra razão que a proteção de dados pessoais é sempre analisada em um contexto de *trocas de informações*.[206]

Ocorre que a liberalidade dos autores no reconhecimento de um direito à privacidade nem sempre encontrou respaldo no avanço do tema nas cortes. O reconhecimento amplo de um direito à privacidade, em verdade, só foi ocorrer em 1965, segundo Henkin,[207] com a conclusão do caso *Griswold v. Connecticut* da Suprema Corte.

---

[204]THOMSON, Judith Jarvis. The right to privacy. *Philosophy and Public Affairs*, Princeton University Press, v. 4, n. 4, p. 307, 1975.

[205]*Id. Ibid.*, p. 296.

[206]"Em uma sociedade caracterizada pelo constante intercâmbio de informações, o direito à privacidade deve se propor a algo mais que àquela finalidade inicial, restrita à proteção da vida íntima. Deve abranger também o direito da pessoa humana de manter o controle sobre os seus dados pessoais. Mais sutil, mas não menos perigosa que a intromissão na intimidade doméstica de uma pessoa, é a sua exposição ao olhar alheio por meio de dados fornecidos ou coletados de forma aparentemente inofensiva, no preenchimento de um cadastro de hotel ou no acesso a um *site* qualquer da Internet." SCHREIBER, Anderson. *op. cit.*, p. 136-137.

[207]HENKIN, Louis. Privacy and autonomy. *Columbia Law Review*, v. 74, n. 8, p. 1410, Dec. 1974.

No caso, a Suprema Corte invalidou uma lei do estado de Connecticut que proibia o uso de contraceptivos por pessoas casadas, sob o argumento de que tal provisão violaria um direito constitucional de "privacidade marital", que por sua vez seria parte ou aspecto de um direito mais amplo à privacidade. A argumentação para definição de um direito constitucional geral à privacidade, entretanto, não é de fácil apreensão.

Em termos simples, a expressão *privacidade* não é mencionada em nenhum momento na Constituição dos Estados Unidos. Algumas expressões de tal direito são, em realidade, protegidas pelas diversas emendas. A Quarta Emenda, por exemplo, prevê um direito de o indivíduo garantir a segurança de sua própria pessoa, sua residência, seus bens e escritos contra buscas e apreensões governamentais que não sejam propriamente justificadas, isto é, que não se baseiem em um mandado judicial ou em "causa provável". Já a Terceira Emenda, raramente invocada, garante ao proprietário de uma casa que o Governo não pode aquartelar soldados em sua residência, em tempos de paz, sem sua autorização expressa, o que parece proteger tanto um direito de propriedade quanto um direito à inviolabilidade da residência privada.

A Quinta Emenda garante a qualquer acusado ou testemunha que não seja compelida a testemunhar contra si mesma, se autoincriminando em um testemunho perante uma corte de justiça. Apesar de altamente afeita à justiça e ao devido processo legal, essa disposição parece garantir alguma forma de privacidade quanto aos fatos da vida de uma pessoa, especialmente quando tais fatos lhes sejam prejudiciais.

Ainda, as próprias liberdades gerais, incluindo a liberdade de manifestação, a liberdade de crença, a liberdade de publicação, todas estas possuem um aspecto negativo que se refere à liberdade de não se manifestar, a liberdade de não informar outros sobre sua crença, a liberdade de não publicar.

Como se vê, pela lógica convencional, o legislador elegeu certas circunstâncias em que se poderia ver reconhecido um direito à privacidade com proteção constitucional; entretanto, tendo o legislador deixado de mencionar expressamente um direito maior à privacidade (ou outro termo que lhe fosse equivalente), parece razoavelmente claro que seu objetivo era justamente restringir o reconhecimento constitucional a tal direito apenas àquelas situações expressamente mencionadas.

Não obstante, o julgamento da Suprema Corte em *Griswold v. Connecticut* de certa forma reverteu tal lógica ao proclamar, mesmo com diversos casos de divergência entre os juízes da Corte, que existiria um direito geral à privacidade formado pelas diversas menções

constitucionais a tal direito em situações específicas, juntamente a uma consideração sobre a "sombra" que tais direitos individuais lançariam.[208]

Como bem colocado por Henkin, um dos benefícios (ou desvantagens, a depender do lado em que se encontra) do direito baseado em precedentes é que o desenvolvimento dos precedentes acaba por relevar certas dificuldades interpretativas.[209] Uma vez colocado o primeiro precedente, torna-se relativamente desnecessário revisitar toda a linha argumentativa do precedente original, dada a *precedential force* que tal precedente carrega, permitindo-se assim um desenvolvimento geralmente orientado à coesão. Obviamente que precedentes contrários podem vir a surgir para disputar um argumento anterior, mas não é essa a regra.

No caso da privacidade, provavelmente se notou que mesmo que a argumentação do caso *Griswold v. Connecticut* não fosse perfeita em termos lógicos, a alternativa seria buscar o reconhecimento de que os Estados Unidos não possuem um direito geral à privacidade, o que poria a descoberto diversos outros precedentes e, em especial, não traria qualquer bem à sociedade em geral. Talvez por tal razão o precedente em *Griswold v. Connecticut* tenha sido tão relevante, marcando o início da consolidação jurisprudencial do direito geral à privacidade.

A esse caso, seguiu-se também na Suprema Corte *Stanley v. Georgia*, em 1969. No caso, a Corte decidiu que o estado da Georgia não poderia condenar Stanley por simplesmente possuir, em sua casa, um filme obsceno. A justificativa da Corte se baseou em um direito fundamental a receber informações e ideias, mas também no direito geral de se ver livre de intromissões indesejadas pelo Estado em sua privacidade. Note-se que por direito à privacidade, nessa circunstância, a Corte entendeu não apenas o direito a não se tomar conhecimento de tal fato, mas também um direito a adotar determinada conduta (possuir um filme obsceno).

O desenvolvimento do direito à privacidade pela jurisprudência norte-americana, nesses moldes, se deu de forma incremental, mas foi em 1973 que um caso da Suprema Corte

---

[208]O entendimento da Suprema Corte pode ser resumido da seguinte forma, nas palavras de Henkin: "since the Constitution, in various 'specifics' of the Bill of Rights and in their penumbra, protects rights which partake of privacy, it protects other aspects of privacy as well, indeed it recognizes a general, complete right of privacy. And since the right emanates from specific fundamental rights, it too is 'fundamental,' its infringement is suspect and calls for strict scrutiny, and it can be justified only by a high level of public good." HENKIN, Louis. *op. cit.*, p. 1421.

[209]*Id. Ibid.*, p. 1410.

trouxe à mesa não só um direito geral de privacidade, mas também sua exigibilidade contra não só o governo federal, mas também contra os estados.

Em *Roe v. Wade*, em 1973, a Suprema Corte invalidou uma lei do estado do Texas que proibia o aborto exceto para salvar a vida da mãe. Tal decisão se baseou no fato de que tal proibição teria violado o direito à privacidade da mãe ao, sem uma justificativa plausível e sem um *devido processo legal*, privar a mãe de um aspecto importante de sua liberdade pessoal, com base na 14ª Emenda.

A título de esclarecimento, o devido processo legal mencionado na decisão é um conceito constitucional norte-americano que não se relaciona apenas a processos judiciais, mas a uma *forma de se conduzir* do Estado. Basicamente, uma liberdade fundamental não pode ser negada, diminuída ou restringida de qualquer forma sem o *devido processo legal*, o que pode estar implícito em um julgamento justo ou na atividade razoável e justificada do Poder Executivo ou mesmo pela elaboração de uma lei. O que desclassifica o devido processo legal, entretanto, é o fato de o Estado não realizar o devido balanceamento entre o bem público defendido pela limitação da liberdade individual e a própria liberdade garantida pela Constituição.[210]

O que deve se entender então da decisão de *Roe v. Wade*? Em verdade, o que se reconhece como um direito à privacidade é na verdade um componente de um direito maior à liberdade, *à autonomia*.

Em todos os casos narrados e em diversos outros em que se reconheceu um direito geral à privacidade, é interessante notar que o direito reconhecido não é acompanhado apenas da liberdade contra algum tipo de intromissão ou à proteção da informação em si, mas sim um direito à própria conduta questionada, essa sim livre de qualquer forma de intromissão exceto se presentes condições que justifiquem tal interferência externa.

A privacidade nos Estados Unidos, dessa forma, reveste-se também de um aspecto maior de proteção à própria liberdade e à autonomia. Autonomia, sim, pois é dentro de tal "espaço" de decisão que não só o indivíduo deve se ver livre do conhecimento de tais fatos por parte de terceiros, mas também deve ser livre para agir conforme sua própria intuição, ditando seu comportamento apenas conforme seu próprio arbítrio. É só quando o indivíduo se vê livre do escrutínio público ou de terceiros é que sua conduta pode ser de fato livre.

---

[210]HENKIN, Louis. *op. cit*., p. 1411 e ss.

No reconhecimento de tal espaço de decisão do indivíduo, o direito à privacidade mostra-se menos relacionado à propriedade do que inicialmente se pode imaginar, e igualmente mais relacionado à própria individualidade do cidadão, sua própria *personalidade* se assim se quiser. Não obstante, tal desenho ainda reforça a ideia de que a privacidade não é importante para a proteção contra o conhecimento alheio de fatos da vida íntima de uma pessoa (ou ao menos não apenas para isso), mas sim que a privacidade é um direito *diferente,* relacionado não apenas ao *conhecimento sobre um ato,* mas à liberdade de agir em si, uma vez que o sujeito não será plenamente livre para agir se não puder manter afastados terceiros do âmago de tal decisão.

Em outras palavras, a privacidade se torna uma proteção acessória à liberdade, mas que pouca relevância tem por si só: não fosse o impacto que o conhecimento público de tal ato teria na conduta de determinado indivíduo, pela lógica até aqui exposta nos casos analisados parece que faria pouco sentido, para o sistema norte-americano, privilegiar ou reconhecer estatura constitucional ao direito à privacidade. E isso parece se refletir no desenvolvimento da proteção de dados naquele país.

3.4. Privacidade e responsabilidade civil: *torts*

O salto da privacidade à proteção de dados pessoais, de certa forma, nunca ocorreu nos Estados Unidos. Por isso queremos dizer que a distinção que já fizemos entre a privacidade em sentido estrito e a proteção de dados não se desenvolveu de forma objetiva, diante da ausência de leis ou jurisprudência específica sobre proteção de dados, mas também pela divisão razoavelmente *dura* feita entre os dois domínios pelas cortes, dada a construção jurisprudencial do direito à privacidade.

O que de fato ocorreu, como ilustrado no item anterior, foi o desenvolvimento do conceito de privacidade até que se reconhecesse um direito mais ou menos autônomo, mas ainda mais ligado à privacidade tradicional que à preocupação com os dados pessoais. Um exemplo bastante claro disso foi o desenvolvimento de tipos específicos de responsabilidade civil extracontratual, os chamados *torts* na tradição norte-americana.

Em realidade, no histórico do *common law* norte americano são poucos os casos que chegaram a abordar o âmago duro do direito à privacidade fora dos quatro principais casos de responsabilidade civil extrajudicial: invasão ao espaço íntimo, apropriação de nome e

aparência física de outrem, divulgação pública de fatos privados e exposição pública sobre falsa luz.[211] O famoso artigo de William L. Prosser, "*Privacy",* explora os contornos de tais *torts.*[212]

Um primeiro *tort* diz respeito à invasão à reclusão do indivíduo em seus assuntos pessoais. Esse tipo de responsabilidade nasce quando há uma intrusão indevida na vida privada de um indivíduo, podendo tal intrusão ser ou não resultado de alguma forma de fraude ou invasão de propriedade. Como bem nota Prosser, esse tipo de ação inicialmente geraria alguma dúvida sobre seu cabimento ou o cabimento de uma ação por invasão de propriedade privada (*trespassing)*. No entanto, o desenvolvimento jurisprudencial veio a abranger sob tal sigla mais que apenas a invasão física de espaços privados, mas também a captação indevida de sons ou informações, como pelo uso de microfones, grampos telefônicos, e mesmo o simples ato de entreouvir informações privadas alheias. Em certo ponto, os tribunais chegaram até mesmo a reconhecer o direito à indenização contra uma pessoa que teria olhado pela janela de uma residência e contra outra que teria telefonado insistentemente a seu devedor para cobrar uma dívida.

Para configuração de tal responsabilidade, em resumo, exige-se algum tipo de ato invasivo, mesmo que tal invasão não seja física. Como colocado por Thomson, não basta que determinado fato seja, por exemplo entreouvido quando duas pessoas discutem em público, ou que determinado fato se torne de conhecimento de terceiro por mero acidente; é necessário que o terceiro que tome conhecimento do fato privado de fato tenha a intenção ou assuma o risco de invadir a privacidade do indivíduo em questão. Dessa forma, é necessário algum tipo de conduta, omissiva ou comissiva, daquele que busca se imiscuir na vida privada alheia.

Em um segundo aspecto, para que se configure o *tort* a coisa ou assunto que é invadido deve de fato ser privado, o que exclui, por exemplo, fatos incluídos em registros públicos e outras informações de cunho público, como a conduta de um indivíduo em locais públicos, a aparência geral da sua residência, e outros fatos notórios, como o fato de ser casado ou de se relacionar com seus vizinhos de maneira amistosa.

O objeto defendido em tais ações parece ser de fato primariamente uma inviolabilidade mental ou psicológica, de modo que a indenização decorre de um dano moral

---

[211]SOLOVE, Daniel; HARTZOG, Woodrow. *op. cit*.

[212]PROSSER, William L. Privacy. *California Law Review*, v. 48, n. 3, p. 383, Aug. 1960. Disponível em: https://lawcat.berkeley.edu/record/1109651.

mais que apenas material.[213] Tal colocação inclusive é interessante do ponto de vista comparativo, dada a tradição das cortes norte-americanas a buscar remediar danos morais apenas quando estes são de extremo relevo.

Um segundo *tort* diz respeito à divulgação pública de fatos privados, geralmente embaraçosos ou negativos, sobre a vida privada do indivíduo. Curiosamente, o artigo seminal de Warren e Brandeis ocupa-se primariamente deste tipo de invasão à privacidade, dado o contexto dos fatos que levaram os autores a tal publicação.

O *tort* relacionado à divulgação pública de fatos privados geralmente diz respeito a divulgação de informações que não são de conhecimento público e que geralmente podem causar algum tipo de embaraço ou dano por sua divulgação pública, quando a informação deveria permanecer conhecida apenas por um número restrito de pessoas. Para ilustrar sua aplicação, Prosser cita o caso de 1931 na California, *Melvin v. Reid.*[214]

Na ocasião, Darley, uma mulher que trabalhou em sua juventude como prostituta, teria sido anteriormente julgada (e inocentada) em um caso de homicídio doloso. Passados tais acontecimentos, Darley mudou de profissão, se casou e no todo alterou grande parte da sua vida pessoal, abandonando os fatos narrados e sua vida pregressa, quando foi produzido um filme sobre sua história – não apenas sobre o julgamento, mas sobre sua vida em geral e sua ocupação à época – , inclusive utilizando seu nome, que veio a revelar a seus parentes e amigos tais fatos da vida privada de Darley. Tal ocorrência, naturalmente, gerou grande prejuízo a Darley, resultando na ação judicial que exigia compensação por tal divulgação.

Considerando tal caso, notamos que são alguns os requisitos para esse tipo de *tort.* Primeiramente, a divulgação dos fatos privados deve ser pública, com amplo alcance, e não uma divulgação direcionada ou de alguma forma limitada. Assim, por exemplo, os tribunais americanos não julgaram uma violação de privacidade que o credor divulgasse ao empregador do devedor a existência da dívida, ou outras situações em que a divulgação é feita a um pequeno grupo de pessoas.

Em segundo lugar, os fatos divulgados devem ser de fato privados. Uma primeira consequência disto é que a divulgação de fatos efetivamente públicos, como aqueles constantes de registros públicos, ou acontecimentos que tenham relevância para a liberdade de informação, não será considerada uma violação. Não obstante, o fato de a informação

---

[213]PROSSER, William L. *op. cit.*, p. 390-392.
[214]*Id. Ibid.*, p. 393-395.

constar de registro público, por si só, apesar de extremamente importante para a análise sobre ter ocorrido ou não uma violação de privacidade, não é absoluta.

No próprio caso *Melvin v. Reid* parte das informações divulgadas constavam de fato de um registro público e, sendo da própria natureza do sistema legal norte-americano, a liberdade de imprensa deve encontrar apenas restrições absolutamente necessárias, especialmente quando se trata de registros públicos. Nesse caso, entretanto, a corte não se restringiu a avaliar a revelação do conteúdo de registros públicos sobre o julgamento de Darley, mas também de outros fatos acessórios que, por si só, representaram uma violação.

Ainda em outro aspecto de tal limitação do *tort* de divulgação, informações sobre como o indivíduo se porta em público ou fatos públicos sobre ele, como sua ocupação, seu endereço, os negócios que conduz publicamente, não estarão cobertos por tal *tort*. Tal segundo requisito nos traz um questionamento importante do ponto de vista da *publicidade da informação*: o simples fato de uma pessoa estar em um ambiente público permite que sua imagem seja registrada em uma fotografia, por exemplo? E se tal fotografia por utilizada comercialmente?

As respostas a tais questionamentos são encontradas nos outros *torts*, especialmente no que diz respeito a apropriação de nome e imagem. Para o *tort* de divulgação, o simples registro fotográfico não é, de fato, uma violação, mas tal ato pode ser punível se tal imagem é utilizada indevidamente para a propaganda de determinado produto (pelo *tort* de apropriação de imagem e nome) ou se tal imagem é utilizada para associar a imagem do indivíduo a circunstâncias falsas ou que denigram sua imagem, como usar tal imagem para ilustrar um artigo sobre dependência química a drogas ilícitas (pelo *tort* de exposição sob falsa luz).

Ainda sobre o *tort* da divulgação, em oposição ao cenário de captura de imagens ou descrições em ambiente público, o *tort* é plenamente aplicável caso a captura da imagem ou da informação se dê em ambiente privado, de modo sub-reptício ou à revelia do indivíduo retratado, uma vez que em tal cenário presume-se que a imagem é capaz de revelar informações que não estão geralmente disponíveis ao público.

Como um terceiro requisito, o *tort* de divulgação exige que os fatos revelados ao público sejam de alguma forma ofensivos, embaraçosos ou de outra forma que sua divulgação pudesse, por justificativa razoável, ser obstada pelo indivíduo em razão de sua natureza íntima. Esse requisito decorre do fato de que todo indivíduo, de alguma forma, tem

parte de sua vida exposta ao olhar público, não sendo então razoável exigir que aquelas informações comumente apreendidas pela simples convivência em sociedade tivessem que ser mantidas como segredo absoluto. Nessas hipóteses, não há propriamente dano, pois é esperada a exposição pública do indivíduo, de modo que são elas excluídas do dever de indenizar.

Uma terceira hipótese de responsabilidade concerne à publicidade ou divulgação que coloca o indivíduo sob uma falsa luz ou de forma a denegrir sua imagem. Uma das formas mais comuns em que tal violação aparece diz respeito à falsa atribuição de opiniões, frases, escritos ou produções em geral a determinada pessoa. Esse tipo de violação aproxima-se muito dos institutos de calúnia e difamação, quando há uma falsa atribuição a determinada pessoa de um ato ou fala – a grande diferença, criticada pelo próprio Prosser, é que não há nesse caso as limitações que existiriam em casos envolvendo difamação (como a exceção de verdade). Independentemente disso, esse tipo de *tort* é geralmente aplicável não só por falsa atribuição, mas de modo mais amplo quando uma determinada forma de divulgação pode levar o público a uma assunção errônea sobre o indivíduo.

A título de exemplo, no *tort* anterior discutimos a ausência de violação de privacidade quando há um simples ato de tirar uma foto de uma pessoa em local público – imaginemos a foto de um jovem adulto parado do lado de fora de um bar, fumando um cigarro, ato que não seria ilícito na maioria dos casos. A pessoa retratada não foi consultada nem de qualquer forma possui um contrato com o fotógrafo, nem tem o fotógrafo conhecimento sobre qualquer aspecto da vida daquela pessoa.

Caso tal foto, no entanto, seja utilizada para ilustrar um artigo sobre um assunto não relacionado ao indivíduo, que pode ser tanto algo razoavelmente inócuo como um artigo sobre “a vida difícil de jovens desempregados” quanto algo problemático como “a falta de perspectiva no mercado de trabalho dos dependentes químicos”, pode-se alegar a violação de um direito à privacidade por meio do *tort* de exposição sob falsa luz, uma vez que a imagem é utilizada para associar determinada pessoa a um fato que não condiz com sua realidade: o indivíduo retratado não é dependente químico tampouco desempregado, sendo que tal exposição prejudica sua reputação e o associa indevidamente a tais alegações.

Como se nota, a *falsa luz* não precisa necessariamente ser difamatória, apesar de frequentemente o ser, mas deve ser passível de objeção por parte do indivíduo, considerando o objetivamente razoável. Inicialmente tal restrição parece conduzir à conclusão de que o

objeto de proteção do *tort* seria primariamente a reputação do indivíduo, o que parece correto. Entretanto, é necessário atentar para o fato de que não só aquelas atribuições estritamente difamatórias podem ser "razoavelmente obstadas", mas também aquelas que exibem o indivíduo de forma contrária à qual este deseja, justificada assim a objeção no interesse do indivíduo de não ser retratado erroneamente perante a sociedade, mesmo que o atributo erroneamente associado a ele não seja propriamente ilegal. Isso nos leva a observar que tal *tort* possui um caractere adicional à simples proteção da reputação, chegando a proteger também a *correção* da informação veiculada sobre o indivíduo.

Ainda, em uma quarta hipótese, se reconhece a obrigação de indenizar àquele que se apropria indevidamente, para seu próprio benefício, da imagem, aparência e/ou nome de outra pessoa. Este *tort* relaciona-se diretamente com a exploração indevida da identidade do indivíduo e, se analisado comparativamente ao direito brasileiro, poderia assemelhar-se à proteção do direito à imagem e do direito ao nome. Tais conceitos no desenvolvimento da *common law* norte-americana foram incluídos sob a alcunha do direito geral à privacidade, por dizerem respeito ao espaço de autonomia e liberdade do indivíduo e, como é comum, tais direitos da personalidade são geralmente reunidos como aspectos de uma única liberdade geral, em suas diversas manifestações.

Um primeiro exemplo trazido por Prosser diz respeito exatamente a *Pollard v. Photographic Co.* de 1888, em que um fotógrafo que teria tirado a foto do reclamante para posteriormente a vender a terceiro, sem seu consentimento. Em iterações mais modernas, o *tort* de apropriação é largamente utilizado em casos envolvendo publicidade ou outras formas de manifestação pública em que determinada empresa ou entidade busca utilizar-se da imagem e nome do indivíduo para promover causas, produtos ou serviços como se fosse tal indivíduo um apoiador ou de outra forma endossante.

Retomando o exemplo dado no *tort* sobre falsa luz, imaginemos que o indivíduo fotografado tivesse sua imagem associada não a um artigo ou outra manifestação que lhe fosse prejudicial, mas sim utilizada para propagandear uma marca de cigarros. Tal aproveitamento *comercial* da imagem sem a autorização do indivíduo gera, por este *tort*, um dever de indenizar em razão de uma violação de privacidade.

Um primeiro requisito, pois, desta modalidade de responsabilidade civil é o *aproveitamento pelo violador*, seja tal aproveitamento teoricamente lícito (inserção em uma propaganda), quanto ilícito, como no caso do roubo de identidade para cometimento de

fraude, obtenção de crédito, cometimento de outros crimes, entre outros. O benefício pode ser direto ou indireto, mas precisa necessariamente beneficiar o próprio apropriador, o que pode ser objeto de crítica, uma vez que em tese permitiria a apropriação para casos não comerciais ou casos em que o apropriador o faz sem um benefício próprio, mas em benefício de terceiro.

Um segundo requisito diz respeito ao que é efetivamente apropriado. Não basta que o nome de um indivíduo seja simplesmente reproduzido em um livro, um anúncio ou outra forma de publicação, uma vez que ninguém pode reclamar exclusividade sobre um nome específico, podendo um nome designar mais de uma pessoa sem que isso represente algum tipo de ilícito. O relevante é que a apropriação de fato diga respeito a uma pessoa específica, o que pode incluir seu nome, mas pode incluir meramente sua imagem ou mesmo caracteres da sua personalidade que sejam suficientemente distintivos. Assim, por exemplo, mesmo que não se utilize o nome de John Smith, caso ele seja o CEO de uma grande corporação e tenha certos hábitos e manias que são então retratadas em um livro, com menção específica à empresa e ao cargo de John, a violação prescinde da utilização do nome, desde que seja razoavelmente conectada à personalidade do indivíduo.

Quando ausentes tais hipóteses e ausentes danos a serem remediados, os casos sobre privacidade geralmente revolvem em torno de relações público-privadas, como no caso *Roe v. Wade,* em que o direito à privacidade, de uma mulher tomar decisões de forma privada sobre seu próprio corpo, foi utilizado para permitir a livre escolha de tal mulher sobre a prática do aborto.[215]

Tal cenário, no entanto, não significou o simples abandono de qualquer ideia de que dados pessoais possuam algum tipo de valor. Como bem ilustrado pelos próprios casos de responsabilidade extracontratual, mesmo quando se busca defender a privacidade é possível que a proteção dos dados pessoais seja uma consequência relacionada.

Tomemos como exemplo o cenário de apropriação de nome e aparência de outrem. Como visto, o interesse em tal situação é coibir o uso indevido e o roubo de identidade, que uma pessoa se passe por outra em benefício próprio assumindo a responsabilidade desse outro. Nesse caso, apesar de não se tratar do principal objetivo do *tort,* há de fato uma preocupação em impedir a utilização indevida do nome da vítima e de sua aparência física,

[215]HENKIN, Louis. *op. cit*., p. 1422-1423.

o que pode ser feito, por exemplo, pela falsificação de documentos ou pelo uso de dados pessoais em cenários de comunicação e interação digital.

A mesma preocupação com o uso do nome e da imagem pode ser encontrado no *tort* sobre falsa luz, enquanto o *tort* sobre divulgação de fatos privados trata diretamente de dados pessoais, uma vez que a concretização de tais informações são dados pessoais que podem ser utilizados e comunicados pelo infrator.

3.5. *Fair Information Privacy Principles* e normas estatutárias

Os Estados Unidos não possuem uma lei geral de proteção de dados pessoais no âmbito federal. Em lugar de tratar a disciplina da coleta e do uso dos dados pessoais de uma maneira uniforme, optou-se por dar um tratamento setorial à matéria. Desse modo, o país possui leis federais que disciplinam a proteção e o uso de dados pessoais de crianças e adolescentes, os dados médicos ou de saúde, os dados financeiros, os dados pessoais inseridos no contexto das comunicações eletrônicas, entre outros setores específicos, mas não há uma lei central que defina princípios e regras comuns, ou que estabeleça direitos unificados aos cidadãos. Alguns estados também possuem legislação específica sobre privacidade e proteção de dados, devendo-se destacar o exemplo da Califórnia, que é uma das referências naquele país no tema[216].

O que se nota de tal sistema é que os Estados Unidos escolheram regrar apenas aquelas situações envolvendo dados pessoais que representem maior risco e, portanto, maior necessidade de regulação, focando-se a regulação em *tipos específicos de dados pessoais* e no seu uso *por entidades específicas*. É assim, por exemplo, que os dados cadastrais tratados por praticamente todos os tipos de empresas em relação a seus próprios colaboradores não merecem maior atenção das leis estatutárias, mas o mesmo não se pode dizer dos dados de crédito e informações bancárias, protegidas que estão pelo *Fair Credit Reporting Act* (FCRA) de 1970[217] *Gramm-Leach-Bliley Act* (GLBA) de 1999.[218]

---

[216]SOTTO, Lisa J.; SIMPSON, Aaron P. United States. *In*: JAY, Rosemary P. (Ed.). *Data Protection & Privacy:* in 31 jurisdictions worldwide. 3. ed. London: Law Business Research, 2015. p. 208-209. Disponível em: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2011/04/DDP2015_United_States.pdf.

[217]UNITED STATES CODE. 15 U.S. *Code § 1681 - Congressional findings and statement of purpose*. Disponível em: https://www.law.cornell.edu/uscode/text/15/1681.

[218]UNITED STATES CODE. 15 U.S. *Code § 6801 - Protection of nonpublic personal information*. Disponível em: https://www.law.cornell.edu/uscode/text/15/6801.

Uma das primeiras manifestações de relevância sobre o uso de dados pessoais vem na forma de um relatório do *U.S. Department of Health, Education and Welfare,* datado de 1973 e intitulado *Records, Computers and the Rights of Citizens.*[219] Esse relatório, na história norte-americana, é a primeira manifestação governamental sobre regras ou princípios básicos a regrarem o tema dos dados pessoais. Parte dos mesmos princípios seria mais tarde incorporada pelas Guidelines da OCDE sobre proteção de dados,[220] assim como pela própria *Federal Trade Commission (FTC)* em 1998.[221]

Podemos sumarizar os princípios que ficariam conhecidos como *Fair Information Privacy Principles* (FIPPs) ou *Fair Information Practices* (FIPs), em suas diversas manifestações, em 10 princípios, subdivididos em quatro áreas: direitos dos titulares de dados, controles e limitações sobre os dados, ciclo de vida dos dados pessoais e gerenciamento de dados.[222]

Na área de direitos dos titulares, encontramos três princípios básicos dos FIPPs: *notice, choice and consent,* e *data subject access.*

Pelo princípio de *notice,* que poderia ser traduzido como aviso, transparência ou declaração, as organizações que coletem e utilizem dados pessoais devem dar aos titulares dos dados pessoais transparência sobre como seus dados são coletados e tratados, incluindo as finalidades do tratamento e do compartilhamento dos dados, geralmente na forma de um aviso ou declaração de privacidade de ampla divulgação. O que o princípio busca proteger aproxima-se em larga escala do que já vislumbramos sobre o princípio da transparência no modelo europeu, ou seja, uma obrigação geral de que o titular dos dados tenha conhecimento, ou ao menos possa tomar conhecimento, dos detalhes sobre a coleta e uso de seus dados pessoais por uma determinada entidade. Tal conhecimento é essencial pois é ele que possibilita o exercício dos demais direitos básicos garantidos ao titular, quais sejam, escolha e acesso.

Pelo princípio de *choice and consent,* que pode ser traduzido por escolha e consentimento, é assegurado ao titular de dados, diante das informações fornecidas por uma

---

[219]RECORDS, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. U.S. Department of Health, Education & Welfare. July 1973. Disponível em: https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

[220]Como veremos no Capítulo 4.

[221]UNITED STATES. Federal Trade Commission - FTC. *Privacy online*: a Report to Congress. June 1998. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[222]SWIRE, Peter P.; KENNEDY-MAYO, DeBrae. *op. cit*.

entidade sobre como esta coleta e usa seus dados pessoais, fazer escolhas significativas, onde possível, sobre se e como seus dados serão utilizados e compartilhados. Na maioria das iterações do princípio fica claro, entretanto, que o conceito de escolha nem sempre será apropriado ao tratamento, visto quem em certas situações não pode haver de fato uma escolha do titular sobre o tratamento de dados em si, mas sim apenas sobre a situação mais ampla de vinculação entre ele e tal entidade. Por tal cenário fazemos referência àqueles casos em que o tratamento de dados, diante de outras circunstâncias, não pode ser negado sem a geração de consequências negativas para a entidade ou para o titular, como quando o controlador dos dados os utiliza para cumprir com uma obrigação legal, ou quando o tratamento de dados é necessário para cumprir com um contrato celebrado entre o controlador e o titular dos dados.

Assim, um aspecto importante do princípio é que as escolhas sobre o tratamento de dados só sejam de fato oferecidas ao titular quando há uma escolha a ser feita, e não no caso de uma simples aparência de escolha que leve o titular a entender, erroneamente, por exemplo, que pode recusar determinado tratamento de dados quando o tratamento em realidade é necessário e ocorrerá independentemente de tal consentimento do titular. Ademais, tal escolha deve ser de fato relevante, isto é, deve representar uma alteração que de fato cause impacto em como os dados são tratados, e não meras escolhas procedimentais que não afetam realmente os direitos do titular ou que não permitam de fato que o titular, por tal escolha, resguarde seus dados pessoais contra um uso que não aprove. Esse exemplo encontra suporte em situações em que o controlador pode vir a oferecer escolhas que tenham pequeno ou nenhum impacto no tratamento de dados e que na verdade não permitam ao titular realmente optar por consentir ou não com o tratamento de determinados dados, apenas para simular a existência de algum tipo de escolha.

Ainda nessa área, o princípio de *data subject access,* que pode ser traduzido por um direito de acesso a ser concedido ao titular dos dados, complementa o direito geral à obtenção de informações por meio do apropriado *notice.* Se a obrigação geral de transparência sobre o tratamento de dados dá ao titular de dados acessos às informações sobre o tratamento em geral, é pelo direito específico de acessar os dados sobre si que estão sendo efetivamente tratados que o titular completa as premissas necessárias para que possa atuar em relação aos seus dados, seja reclamando pelo descumprimento de uma promessa de privacidade, seja para corrigir tais dados ou exigir sua transferência a outro prestador de serviço, quando tal direito é aplicável.

Na área de controles e limitações sobre uso de dados, encontramos os princípios *information security* e *information quality*.

Por *information security*, ou segurança da informação, dos dados pessoais, entende-se o dever de uma organização de adotar medidas físicas, administrativas e técnicas de segurança adequadas ao porte da operação para proteger os dados pessoais em tratamento contra o uso, divulgação ou acesso indevidos. Esse princípio reflete definições que já há muito tempo orientam o ramo de proteção de dados em diversos sistemas diferentes. Parece, pois, que se estabelece um consenso de que o controlador que se dispõe a tratar dados pessoais deve sempre, qualquer que seja sua jurisdição, garantir minimamente que tais dados estejam seguros contra usos indevidos ou ilegais.

Tal aspecto de segurança desponta talvez como uma consequência de uma regra mais ampla de que produtos e serviços geralmente oferecidos ao mercado devem contar com o nível razoável de segurança que deles se espera. Mesmo que tal princípio pareça excepcionalmente afeto ao direito consumerista, em verdade parece ele decorrente antes de uma regra geral de que um produto ou serviço, qualquer que seja seu mercado, tem entre suas qualidades essenciais não só o produto ou serviço em si, mas também as *condições* em que é prestado ou fornecido, como expressão básica de boa-fé contratual e da legítima tutela das expectativas das partes quanto a determinado contrato ou promessa.

Ainda nesta área encontramos também o princípio da *information quality* ou qualidade dos dados. Com fundamento mediato semelhante ao do *tort* sobre exposição sob falsa luz, é de se reconhecer que o tratamento de dados deve, sempre que possível, ser realizado com dados corretos e exatos, evitando-se assim falsear a verdade ou as consequências do tratamento em razão de dados desatualizados. Por essa razão, os FIPPs reconhecem como essencial quanto aos controles sobre os dados o estabelecimento de regras, processos e outras salvaguardas que permitam ao controlador manter os dados atualizados e corretos. Segundo Prosser, os *privacy torts, o* de falsa luz inclusive, quando de sua consolidação, tiveram efeito semelhante sobre a mídia em geral,[223] incentivada a buscar sempre maior exatidão em seu reporte de notícias e fatos do cotidiano, de modo evitar algum tipo de responsabilização por exposição sob falsa luz, o que se aproxima dos propósitos deste princípio (apesar de não haver o reconhecimento de um *tort* específico para uma violação do princípio de *information quality* per se).

[223]PROSSER, William L. *op. cit.*

Na área de ciclo de vida dos dados pessoais, encontramos três princípios a serem seguidos: *collection, use and retention,* e *disclosure.*

Por *collection* deve-se entender que dados pessoais só podem ser coletados para as finalidades definidas na declaração de privacidade. Essa afirmação simples esconde potencialmente um significado maior, uma vez que limitar a coleta pode significar (i) coletar apenas os dados identificados na declaração de privacidade ou (ii) coletar apenas os dados necessários conforme os propósitos descritos na declaração de privacidade. No nosso entender, a principal limitação diz respeito aos dados pessoais indicados na própria declaração de privacidade (i), mas pode-se subentender também a segunda limitação, especialmente se a declaração de privacidade não for exaustiva ao elencar quais tipos de dados serão coletados. Na ausência de tal identificação exaustiva dos tipos de dados a serem tratados, se ainda assim é aplicável a limitação da coleta, tal limitação não teria outro critério a utilizar para definir o que pode ser coletado que não a própria necessidade, isto é, uma relação de razoável adequação entre o que se coleta e o propósito de tal coleta.

Esse raciocínio se repete no princípio que limita o uso e a retenção de dados pessoais (*use and retention):* esses dados só podem ser usados para as finalidades descritas na declaração de privacidade, sempre com base no consentimento implícito ou explícito do titular. Adicionalmente, seguindo também essa lógica, se o dado só pode ser coletado para finalidades definidas e só pode ser utilizado em conformidade com tais finalidades, uma vez cumpridas tais finalidades passaria o dado a ser então desnecessário, pelo que sua retenção não mais se justificaria.

Ainda, por *disclosure* o compartilhamento desses dados com terceiros deve ser também se dar apenas em conformidade com as finalidades descritas na declaração de privacidade e com o consentimento explícito ou implícito do titular. É interessante que tanto no uso quanto no compartilhamento de dados há geralmente a menção a um consentimento explícito ou implícito. Por consentimento explícito parece mais adequado pensar nas hipóteses de consentimento que se aproximam dos requisitos da União Europeia, em que o consentimento deve ser uma ação afirmativa e passível de prova. Já o consentimento implícito, por seu lado, pode abranger uma variedade de circunstâncias, podendo vir a incluir mesmo hipóteses de simples ciência e concordância tácita com as finalidades do tratamento quando este é absolutamente necessário, não sendo assim possível, em realidade, a discordância do titular, pelo que se presume seu consentimento ao permanecer em determinada relação ou dar continuidade a determinada transação. Seria o caso, no exemplo,

do indivíduo que contrata um serviço e, recebendo sua declaração de privacidade e ficando ciente de que o tratamento de dados é necessário para a prestação do serviço contratado, daria seu consentimento implícito ao realizar a contratação do serviço em si para o tratamento de dados pessoais.

Por fim, na área de gerenciamento de dados, podemos sumarizar os princípios geralmente endossados em dois aspectos: *management and administration* e *monitoring and enforcement*. Esses aspectos geralmente envolvem a criação de programas de governança em que sejam estabelecidos processos, políticas internas e regras para tornar efetivas as promessas feitas nas declarações de privacidade, garantindo que tais promessas sejam cumpridas e que tal conformidade seja objetivamente documentada, de modo a ativamente comprovar seu cumprimento, endereçando ainda reclamações e demandas que surjam eventualmente por parte das autoridades e dos próprios titulares. Tais aspectos, como se verá, são bastante reforçados na "jurisprudência" da FTC, dada sua vocação para exigir das empresas o estabelecimento de práticas continuadas com a finalidade de coibir condutas identificadas como lesivas ou abusivas.

Apesar da eloquência desses princípios, poucos deles foram efetivamente incorporados à legislação estatutária dos Estados Unidos, visto que tal legislação continua sumariamente setorial e bastante restrita quando consideramos sua real abrangência em relação aos dados efetivamente protegidos e as circunstâncias de seu tratamento. Não obstante, é possível identificar alguns de seus traços nas disposições efetivamente existentes no direito estatutário, mesmo que geralmente restritos a determinado setor, determinado uso dos dados ou determinado tipo de dado pessoa. Assim, é necessário explorar também brevemente as leis estatutárias em vigor naquele país.

No âmbito de direito estatutário federal, destaca-se inicialmente o *Privacy Act* de 1974.[224] Apesar de sua aparentar larga aplicação em razão de seu nome, o *Privacy Act* em verdade dispõe sobre princípios gerais para uso justo de dados pessoais, incluindo sua coleta, manutenção, uso e disseminação, mas apenas no contexto das agências federais. Dentre os princípios trazidos pelo *Privacy Act* já identificamos alguns princípios inicialmente refletidos dos *Fair Information Privacy Principles*, dentre eles o direito dos titulares de dados de acessar seus registros mantidos por tais agências federais.

[224]UNITED STATES. *Privacy Act, 88 Stat. 1896*. Public Law, Washington D.C., 31 Dec. 1974. Disponível em: https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf.

A lei aborda regras sobre a revelação de dados pessoais a outras agências ou terceiros, geralmente mediante o consentimento do titular ou diante de alguma circunstância de interesse público - no exercício da administração pública ou em atividades particulares com fins estatísticos, históricos, negocial, entre outros; garante direitos de acesso; limitações quanto à finalidade, quantidade e qualidade dos dados tratados; diretrizes para garantir a segurança, sigilo e a transparência dos tratamentos; diretrizes sobre as políticas internas de segurança e tratamento de dados; a obrigatoriedade de registro dos bancos de dados federais submetidos ao *Privacy Act*, entre tantos outros assuntos menores.

Outra lei interessante no âmbito federal é o *Electronic Communications Privacy Act* de 1986[225], constituído do *Wiretap Act*, o *Stored Communications Act* e o *Pen Register Act.* O *Wiretap Act* proíbe a interceptação, uso ou revelação de qualquer tipo de comunicação telefônica, oral ou eletrônica, aplicando-se tanto ao setor privado quanto ao público (salvo as exceções em caso de investigação criminal, por exemplo). Note-se que a referência aqui é a comunicação *em fluxo*, o que se extrai do próprio termo *interceptação*. Os dados referentes a comunicações armazenadas, que já foram recebidas ou enviadas e não se encontram mais em fluxo, são protegidos, por sua vez, pelo *Stored Communications Act*, que diz respeito aos dados de comunicação e de cadastro (como nome, endereço, etc) armazenados por provedores de serviço. O *Pen Register Act* regula a utilização pelo governo (e a proibição ao público em geral) dos *pen registers* e outros dispositivos de rastreamento de chamadas. Esses dispositivos servem para identificar os terminais em uma determinada comunicação (geralmente telefônica), mas não tem capacidade para interceptar ou acessar o conteúdo da comunicação em si.

Ainda no âmbito federal, há o COPPA, acrônimo para *Children's Online Privacy Protection Act*[226], lei de 1998 que cria salvaguardas para a interação de crianças com menos de 13 (treze) anos com a Internet em geral e no que diz respeito a sua privacidade. A Lei traz um mecanismo interessante de *safe harbor*, diferente do projeto internacional entre Estados Unidos e União Europeia. Por tal mecanismo, associações setoriais de empresas podem submeter à FTC códigos de autorregulação que serão então avaliados e eventualmente

---

[225]UNITED STATES. *Electronic Communications Privacy Act, 18 U.S.C. §2510 e ss*. Public Law, Washington D.C., 21 Oct. 1986. Disponível em: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#:~:text=in%20Section%202516.-,18%20U.S.C.,billing%20records%2C%20or%20IP%20addresses.

[226]UNITED STATES. *Children's Online Privacy Protection Act, 15 U.S.C. §6501-6506*. Public Law, Washington D.C., 21 Oct. 1998. Disponível em: https://www.ftc.gov/enforcement/statutes/childrens-online-privacy-protection-act.

homologados, tornando-se vinculantes para as empresas associadas. O diferencial aqui diz respeito ao fato de que tais códigos geralmente preveem mecanismos de resolução de disputas entre as empresas associadas e seus consumidores e/ou mecanismos internos de disciplina das empresas envolvidas em possíveis violações de privacidade. Com tais provisões, uma vez aprovado o código, empresas em violação do COPPA estariam primeiro sujeitas aos procedimentos disciplinares setoriais, e só depois, em certos casos, poderiam ser submetidas à investigação da FTC.

No setor financeiro, pode-se citar o *Fair Credit Reporting Act* (FCRA) de 1970[227] e o Gramm-Leach-Bliley Act (GLBA) de 1999.[228] O FCRA regula, em resumo, as agências de proteção ao crédito, empresas que utilizam os relatórios elaborados por tais agências e as empresas que fornecem dados às agências para a elaboração de tais relatórios. No geral, o FCRA traz regras sobre o uso de relatórios de crédito (*credit reports)* para fins de verificação de antecedentes por potenciais empregadores, o que inclui a exigência do consentimento do titular dos dados e limitações sobre o uso dos relatórios; as obrigações dos credores de fornecerem informações sobre créditos em aberto, inclusive em relação à exatidão e correição de tais informações, que devem ser exatas e atualizadas; obrigações de transparência e acesso à informação por parte das agências de proteção ao crédito; obrigações sobre processos e garantias de que a informação tratada de fato está correta e atualizada, de modo que cabe às agências de proteção ao crédito manter vigilância constante sobre tais aspectos; e obrigações de emitir avisos aos titulares de dados em certas situações em que seus dados pessoais são consultados.

Já o GLBA, em sua *Privacy Rule*, exige que instituições financeiras forneçam uma declaração de privacidade a seus clientes no momento do início da relação e anualmente, que deve explicar quais dados são coletados, como são utilizados, quais dados são compartilhados e como como eles são geralmente protegidos pela instituição. Qualquer alteração em tais circunstâncias do tratamento deve ser refletida na declaração de privacidade e os titulares devem ser notificados de tais alterações. Além da obrigação de transparência, o GLBA concede aos titulares de dados um direito de objetar ao compartilhamento de dados

---

[227]UNITED STATES. Federal Trade Commission - FTC. *Fair Credit Reporting Act. 15 U.S.C § 1681*. Revised September 2018. Disponível em: https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf.

[228]UNITED STATES. Federal Trade Commission - FTC. *Gramm-Leach-Bliley Act*. Disponível em: https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf.

com terceiros, exceto no contexto do FCRA, direito esse renovado a cada atualização da declaração de privacidade.

O GLBA conta também com uma *Safeguards Rule* que basicamente exige que as instituições financeiras desenvolvam um plano formal de segurança da informação que descreva como a empresa previne riscos e de outras formas garante a segurança das informações pessoais *não-públicas* tratadas no contexto da sua operação. Como requisitos mínimos, a instituição deve dedicar ao menos um empregado para gestão do programa de segurança da informação; empregar análises periódicas de risco para cada departamento que trate dados pessoais; desenvolver, manter e monitorar o programa continuamente; e realizar as mudanças necessárias, de tempos em tempos, para garantir a segurança dos dados pessoais coletados, armazenados e utilizados pela instituição.

No setor da saúde, vige o *Health Insurance Portability and Accountability Act* de 1996, mais conhecido por *HIPAA*, que contém regras federais setoriais de privacidade e proteção de dados médicos[229]. Tal lei traz disposições a respeito de padrões de segurança, física e técnica de dados relacionados à saúde em formato eletrônicos; a obrigação de notificar os titulares dos dados, e muitas vezes a Secretaria de Saúde[230] e a mídia local[231] no caso de vazamento ou violações de dados pessoais; as condições básicas para o tratamento justo e legal dos dados pessoais e as situações em que o consentimento do titular é ou não necessário; direitos básicos de acesso aos dados e informação sobre o tratamento e as cabíveis medidas de segurança e sigilo; além de diretrizes específicas sobre a responsabilidade da "entidade abrangida" pela lei por seus funcionários, incluindo-se aí treinamentos, questões de política interna de privacidade e disciplina.

O sistema estadunidense não possui uma Autoridade de Proteção de Dados nos moldes europeus, um órgão técnico, independente e dedicado unicamente à matéria da privacidade e da proteção de dados pessoais. Em seu lugar, certos órgãos já existentes e não exclusivos do governo atuam como agências reguladoras, sendo responsáveis pelo *enforcement* das leis vigentes. Esses são separados por setores econômicos de modo que sua atuação não é necessariamente homogênea, como também não o são necessariamente suas posições em relação às controvérsias que possam surgir sobre este ou aquele conceito. Assim,

---

[229]UNITED STATES. *Health Insurance Portability and Accountability Act, 110 Stat. 1936*. Public Law, Washington D.C., 21 Aug. 1996. Disponível em: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

[230]U.S. Department of Health and Human Services.

[231]Quando o número de indivíduos afetados superar 500 (quinhentos) em um mesmo estado.

a *Federal Trade Commission* é responsável, por exemplo, por fiscalizar a aplicação do COPPA e das regras relativas à proteção do consumidor, segundo seu próprio estatuto[232], que podem incluir abusos na coleta e utilização de dados dos consumidores. Já o *Department of Health and Human Services* é responsável pela supervisão do cumprimento do HIPAA. No setor financeiro, temos o *Consumer Financial Protection Bureau*.

Tais agências geralmente têm competências fiscalizatórias, sancionatórias e normativas, podendo complementar as regras setoriais de que cuidam, mas o Poder Judiciário ainda exerce um importante papel no sistema de tutela. Mesmo tais agências e escritórios precisam recorrer ao Judiciário para executar suas decisões ou buscar o cumprimento de certas obrigações, o que demonstra a posição central do processo judicial no sistema. Não bastasse tal, na ausência de leis mais amplas de proteção de dados, os princípios e regras gerais necessários para um modelo mais completo de tutela geralmente têm que ser deduzidos de precedentes judiciais, reafirmando sua importância.

O que se tem observado, no entanto, é a ascensão da FTC como o órgão de fiscalização de questões relacionadas a proteção de dados pessoais por excelência. Tal afirmação decorre de um exame amplo realizado por Daniel Solove e Woodrow Hartzog.[233] Como sustentam os autores, apesar de o *enforcement* realizado pela FTC raramente resultar em algum tipo de litígio judicial, o corpo de acordos feitos entre o órgão e empresas que teriam violado regras sobre "atos desonestos e injustos de comércio" constitui um verdadeiro corpo de regras de *common law*, apesar de não haver propriamente precedentes judiciais a instruí-lo.

Em resumo, a FTC possui competência para fiscalizar (i) atos que violem a livre concorrência e (ii) atos e práticas comerciais desonestas ou abusivas, sendo tal competência (em especial o item (ii)) na Seção 5 do *Federal Trade Commission Act* (FTCA). A partir de tal competência, a FTC consegue expandir sua competência para fiscalizar práticas comerciais relacionadas a dados pessoais, servindo em grande parte como uma autoridade de proteção de dados. Para entender tal afirmação, entretanto, devemos dar um passo atrás e entender qual o escopo de atuação da FTC, como ela geralmente se conduz em questões

---

[232]UNITED STATES. Federal Trade Commission – FTC. *Federal Trade Commission Act*. Incorporating U.S. SAFE WEB Act amendments of 2006 (Unofficial version). [15 U.S.C. §41-58. Public Law, Washington D.C., 1914]. Disponível em: https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf.

[233]SOLOVE, Daniel; HARTZOG, Woodrow. *op. cit*.

relacionadas a proteção de dados e qual o seu modo geral de agir, o que abordaremos no próximo item.

Ainda na esfera legislativa, encontramos também fortes contribuições dos próprios estados que, como dito anteriormente, possuem larga autonomia para criar regras sobre proteção de dados aplicáveis a seus respectivos territórios e/ou cidadãos.

Em alguns aspectos, tal liberdade pode ser limitada no sentido de que o estado não pode promulgar leis sobre assuntos sobre o qual já existe uma lei federal, como é o caso do COPPA, que preclui todas as leis estaduais sobre o mesmo assunto. Em outros casos, entretanto, mesmo que já haja uma lei federal sobre determinado tema, os estados podem aprovar leis próprias que constroem e tornam mais estritos determinados requisitos, impondo um conjunto adicional de obrigações a determinadas entidades, como é o caso do HIPAA: os estados podem criar requisitos adicionais por meio de leis próprias, mesmo que já haja um diploma federal em vigor.

Assim, na esfera estadual encontramos quatro grandes áreas de interseção entre a legislação estadual e proteção de dados pessoais: (i) a aprovação de leis setoriais complementares, (ii) a aprovação de leis sobre vazamentos de dados pessoais e outros tópicos individuais, (iii) leis de proteção ao comércio e à concorrência que podem ser utilizadas para fiscalizar práticas sobre dados pessoais, e (iv) leis gerais de proteção de dados que buscam tratar a matéria de forma ampla.

No primeiro ponto, como já mencionado acima, encontramos leis que são complementares a leis federais já existentes, acrescentando apenas requisitos ou obrigações adicionais. Geralmente o conflito entre leis federais e estaduais pode ser resolvido de três formas mais comuns: em um primeiro caso determinada lei federal pode permitir que os estados aprovem legislação própria sobre determinado assunto, valendo então tal lei estadual sobre a lei federal, sendo que esta servirá apenas como regulamentação subsidiária, isto é, aplicável na ausência de disposição diferente do próprio estado. Em um segundo caso, a lei federal pode superar a legislação estadual, simplesmente proibindo que o estado adote regras diferentes para regulamentar determinada matéria, sendo a lei federal o total das regras aplicáveis àquele caso. Em terceiro, a lei federal pode prever que o estado não pode aprovar legislação *contrária* à lei federal, que representa uma garantia mínima, mas que o estado pode criar legislação adicional que constrói e complementa sobre tal patamar mínimo.

Assim, é possível encontrar lei estaduais que complementem leis federais sobre temas relacionados a proteção de dados. Um exemplo típico seria o da lei estadual que é mais rigorosa que as regras do HIPAA no referente à notificação de certos diagnósticos, como HIV, exigindo maior rigor na proteção de tais dados em razão da sua sensibilidade.

No segundo ponto, todos os estados norte-americanos atualmente contam com alguma forma de lei estadual que obrigue empresas a notificar as autoridades (e às vezes os próprios titulares) quando venham a sofrer algum tipo de violação ou vazamento de dados pessoais.

Tais normas, apesar de simples em sua natureza e de pouco se aproximarem de quadros mais completos de proteção de dados, são de grande relevância para o sistema norte-americano, uma vez que permitem às autoridades (geralmente no *Attorney General* do estado em questão, que corresponde à mais alta autoridade legal naquela unidade federativa) iniciar procedimentos civis ou criminais para responsabilização da empresa em questão, caso identifiquem algum tipo de negligência ou má-conduta como causa do incidente. Dado que o conhecimento sobre tais vazamentos demandaria investigações aprofundadas, tais leis trazem tais questões à lume justamente para permitir a fiscalização pelas autoridades competentes, ao estabelecer uma obrigação de notificação de tais incidentes.

No terceiro ponto, temos um importante instrumento que pode ser utilizado também pelas autoridades estaduais (geralmente o *Attorney General*) para fiscalização de práticas desonestas e abusivas relacionadas a proteção de dados. Dada a vocação *federal* da FTC e do FTCA, muitos estados acabaram incorporando regras semelhantes à Seção 5 do FTCA para combater tais tipos de atos danosos, o que representa também um importante instrumento de fiscalização, como veremos a seguir.

Por fim, é relevante notar como alguns estados norte-americanos têm buscado se adiantar em relação à legislação federal e propor normas abrangentes sobre proteção de dados pessoais. Apesar de seu escopo amplo, essas normas ainda não têm o condão de alterar o modelo norte-americano daquele voltado à regulamentação setorial e à autorregulação, mas tais normas começam a consolidar práticas tidas como já bem aceitas pelo mercado e inclusive geralmente promovidas como desenvolvimentos naturais dos princípios já constantes na legislação esparsa e nas diversas recomendações e conjuntos de princípios enunciados por diversos órgãos da administração federal, como é o caso dos *Fair Information Practice Principles.*

Dentre estas, podemos apontar como exemplo o *California Consumer Privacy Act* de 2018 (CCPA)[234] como uma das primeiras e mais abrangentes leis estaduais a tratar sobre o tema da proteção de dados pessoais. Essa lei, apesar de bastante revolucionária no panorama norte-americano, ainda traz certas restrições geralmente não presentes em leis gerais de proteção de dados.

Inicialmente é de se destacar que tal lei é aplicável a *empresas* (excluídas, portanto, instituições sem fins lucrativos) que conduzem negócios na Califórnia, o que não equivale necessariamente a ter sua sede na California, mas pode de fato incluir qualquer tipo de oferecimento de produtos ou serviços a pessoas localizadas na California. Esse tipo de limitação é comum nos Estados Unidos, uma vez que se reputa que o maior risco e o *fardo da regulação* deve recair sobretudo sobre negócios que almejem lucros. Não obstante, diversos tipos de entidades podem se organizar como entidades sem fins lucrativos mas utilizar dados pessoais para finalidades quase comerciais: os dados pessoais são tratados como ativos e utilizados em formas comerciais, apesar de a entidade não se estruturar de forma a distribuir lucros a seus sócios e acionistas. Ademais, mesmo usos não comerciais dos dados (como usos para pesquisa científica) podem trazer riscos aos titulares dos dados e, em muitos casos, são justamente responsáveis pelos maiores riscos em razão da inovação nos métodos como buscam tratar dados pessoais.

Em segundo lugar, a lei protege apenas as informações pessoais de pessoas que sejam residentes na California e, de alguma forma, estejam no estado não apenas de passagem ou em residência provisória. Tal limitação é coerente com o fato de se tratar aqui de uma lei estadual, de modo que o próprio legislador enfrentaria obstáculos para promulgar uma lei com efeitos extraterritoriais.

Um ponto importante do CCPA é que o conceito de informações pessoais (*personal information* ou *personally identified information)* abrange não apenas dados cadastrais ou dados de identificação, mas todos os dados que digam respeito a uma pessoa que esteja abrangida pela lei, o que inclui indivíduos ou domicílios. Esse parece um avanço em relação à maioria das leis sobre proteção de dados nos Estados Unidos, que geralmente possuem limitações sobre quais dados serão protegidos, de modo que a lei se aplique apenas àqueles

[234]CALIFORNIA STATE LEGISLATURE. *SB-1121 California Consumer Privacy Act of 2018*. Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

dados que representem maior sensibilidade, como dados de identificação, dados bancários e financeiros e dados de saúde.

Em relação às obrigações impostas às empresas submetidas ao CCPA, a lei traz disposições, especificamente, sobre o fornecimento de uma declaração de privacidade com requisitos mínimos sobre quais informações devem ser fornecidas aos titulares dos dados pessoais, incluindo necessariamente informações sobre compartilhamento de dados; oferecimento de pelo menos dois canais para comunicação entre a empresa e o titular para comunicação sobre requisições dos titulares de dados em relação aos direitos previstos no CCPA; a existência de um processo de verificação de identidade do consumidor para que esse possa exercer os direitos previsto no CCPA; o fornecimento gratuito de informações sobre o tratamento e os dados tratados em si em até 45 dias, em um formato que permita ao titular transferir tais dados a um provedor concorrente (direito à portabilidade dos dados); a obrigação de oferecer ao titular, de modo simples e acessível, uma forma de *opt-out* para que este escolha não permitir a venda de seus dados pessoais a terceiros, sendo tal opção observada e respeitada pela empresa; uma obrigação geral de não discriminar ou de outra forma prejudicar titulares que venham a exercer seus direitos; e a obrigação de treinar seus empregados sobre o atendimento aos direitos garantidos aos titulares pelo CCPA.

Por fim, é de se notar que o *enforcement* de tal lei se dará de duas maneiras: pelo *State Attonery General*, que pode tanto buscar o cumprimento específico da lei quanto aplicar penalidades de até USD 7.500,00 por violação; e pelo próprio titular dos dados, ao qual é concedido um direito privado de ação. Como já mencionamos, a garantia de um *private right to action* concede um importante recurso aos titulares, uma vez que judicialmente estão geralmente limitados aos *privacy torts* que, como vimos, são também limitados e raramente conseguem abranger questões envolvendo diretamente dados pessoais.

Dentre as disposições mais interessantes, é necessário ressaltar que as regras sobre fornecimento de informação e acesso aos dados ressoam muito do que sempre foi dito sobre *notice and choice* e *access*, enquanto outras regras, como aquelas sobre o direito ao apagamento dos dados e a optar por não permitir a venda de dados pessoais a terceiros, representam grandes avanços na legislação estatutária norte-americana.

3.6. Proteção de dados e autorregulação

Como então é possível dizer que hoje os Estados Unidos possuem algum tipo de regulamentação central sobre proteção de dados? A resposta a tal pergunta reside em um sistema largamente setorial, em que leis são aprovadas para proteger *dados específicos* e para evitar abusos ou violações *em cenários específicos de tratamento*, confiando as demais situações, dados, cenários à autorregulação. As normativas específicas setoriais foram estudadas acima, mas cabe também explorar em maior detalhe o cenário da autorregulação.

A título de esclarecimento, é necessário compreender que autorregulação pode se referir a um sem-número de situações diferentes, uma vez que a autorregulação pode tocar três domínio específicos da normatização: criar a lei, fiscalizar a lei e decidir a lei. Desses domínios, é possível que a autorregulação e a atividade estatal encontrem variados arranjos, podendo, por exemplo, a autorregulação atuar apenas na fase criativa, enquanto o Estado atua nas demais fases. É o que acontece, em alguns países como a Itália,[235] em que associações podem criar códigos de conduta sobre proteção de dados que, uma vez aprovados pela autoridade nacional de proteção de dados, serão fiscalizados por esta, podendo ainda eventuais conflitos decorrentes de tais regras serem resolvidos junto àquela autoridade ou junto ao judiciário.

Em outras situações, é possível que todo o processo seja regido pela autorregulação, pelo qual a criação, fiscalização e adjudicação são todas conduzidas no seio da associação, sem interferência externa.

Dito isso, é importante notar que a autorregulação não precisa necessariamente ser conduzida por grupos empresariais ou associações setoriais, e é em tal fato que se baseia largamente a experiência norte-americana com proteção de dados pessoais.

Como narram Solove e Hartzog, no início da década de 1990, com o crescimento da Internet comercial, parte das principais páginas *web* começou a adotar as chamadas *privacy notices*, declarações públicas sobre como aquela página e aquela empresa específica coletavam, usavam e compartilhavam dados pessoais de seus usuários. Tais declarações de privacidade (por vezes também chamadas de políticas de privacidade ou avisos de privacidade atualmente), não decorriam de uma obrigação legal, mas simplesmente de uma

[235]Ver GUIDI, Guilherme Berti de Campos. *A proteção dos dados pessoais na internet*: contribuições da experiência europeia ao modelo brasileiro, *cit*.

prática que surgiu na época e se popularizou, possivelmente para incentivar a adoção dos serviços web ao tentar mitigar o receio de grande parte da população sobre a segurança de tais serviços em momento tão inicial da rede mundial de computadores.[236]

É verdade que algumas leis setoriais já exigiam algum tipo de aviso ou declaração sobre privacidade, sobre como os dados pessoais dos indivíduos seriam tratados em determinados contextos, como é o caso da lei sobre privacidade infantil online, o COPPA de 1998, o GLBA de 1999, que dizia respeito às instituições financeiras, e o próprio HIPAA de 1996. No entanto, a prática foi adotada inclusive por empresas não sujeitas a tal legislação, provavelmente com o interesse de passarem a seus usuários e consumidores uma imagem de confiabilidade e transparência.

Com o crescimento de tal prática, em poucos anos seriam poucos os websites dentre os maiores do mercado que não possuíssem uma tal declaração de privacidade. O que não ficou claro à época era que tais declarações passariam a ser entendidas, cada vez mais, como *promessas* feitas pela empresa sobre como ela trataria os dados pessoais.

Note-se, no entanto, que não se fala aqui de um contrato propriamente, uma vez que, pela tradição da *common law*, um contrato demandaria uma oferta e uma aceitação, além de um compromisso específico, uma troca de bens ou dinheiro. Assim ainda há alguns exemplos de tentativas de aplicar a declaração de privacidade como um contrato, tentando se exigir seu cumprimento judicialmente, mas na ausência de danos específicos e em muitos casos sendo a declaração não considerada suficientemente firme como uma *oferta*, são poucas as situações em que o judiciário efetivamente trata a matéria com base na Lei dos Contratos (considerando-se esta o corpo comum de normas sobre questões contratuais em sistemas de *common law*).[237]

Não obstante, parece razoavelmente aceito, especialmente quando avaliado o histórico recente de atuação da FTC, que as declarações de privacidade voluntariamente publicadas por uma empresa (ou exigidas pela legislação) constituem, em realidade, uma *promessa* de privacidade: ao publicar determinado texto que descreve como uma organização tratará dados pessoais, quais dados serão tratados e para quais finalidades, assim como por quais vias e de que formas tais dados serão protegidos, a organização vincula-se a tal promessa, devendo, a partir de tal momento, honrar tais promessas, sob pena de incorrer em

[236]SOLOVE, Daniel; HARTZOG, Woodrow. *op. cit*., p. 593-594.
[237]*Id. Ibid.*

comportamentos considerados incompatíveis com o FTCA e com a legislação estadual a ele semelhante que proíbem, em conjunto e de forma ampla, condutas consideradas enganosas ou abusivas que venham a prejudicar a concorrência, o comércio ou o consumidor, em geral.

A quebra de tais promessas, como veremos, dificilmente tem impacto direto na esfera de direitos do próprio titular, tanto é que não é reconhecido a este um "direito privado de ação" do qual possa se valer para buscar a justa compensação pela violação do FTCA. No entanto, o modelo norte-americano apoia-se largamente em tal tipo de promessa e mecanismo autorregulatório para a regulamentação de questões envolvendo dados pessoais, o que, enquanto do ponto de vista individual pode resultar em certo aparente descaso, do ponto de vista coletivo, sistemático representa uma maior cautela na regulamentação de temas essencialmente afeitos à inovação tecnológica e à liberdade econômica.

3.7. A FTC e os Consent Decrees

Como já colocado, a FTC tem tido atuação destacada na regulação da proteção de dados nos Estados Unidos. Apesar de existir desde 1914, foi apenas em 1995 que a FTC passou a se envolver no tema, incentivando inicialmente a autorregulação no tema sob a justificativa de que a regulação estatal poderia prejudicar o desenvolvimento de um ramo nascente da economia, especialmente com o recente surgimento e popularização de tecnologias digitais e da Internet.

Ao invés de o Estado criar leis, o FTC incentivava as empresas a criarem suas próprias regras sobre como elas tratariam os dados pessoais de seus clientes e se propunha a, uma vez publicizadas tais regras pelas próprias empresas, atuar como *enforcer*, cobrando das empresas o cumprimento de tais promessas.

O principal fundamento da atuação da FTC em tal campo é a própria Seção 5 do FTCA, que proíbe "atos enganosos e abusivos no ou afetando o comércio". Um primeiro aspecto de nota é que a atuação da FTC deve necessariamente abranger apenas entidades atuando no comércio, excluindo-se então a fiscalização de entidades sem fins lucrativos. O segundo ponto diz respeito à conceituação do que seriam "atos enganosos" (*deceptive acts)* e "atos abusivos" (*unfair acts)*. Como é comum na tradição norte-americana, a definição do que seriam tais atos é geralmente definida pelo caso concreto e não em abstrato, uma vez que seria provavelmente um esforço fútil a definição antecipada de tais conceitos quando a

prática, naturalmente, exigiria análise individualizada de situações complexas para correta definição do que seria enganoso e do que seria abusivo. Não obstante, ao longo da "jurisprudência" da FTC podemos notar alguns padrões sobre tais tipos de atos, padrões estes que discutiremos adiante neste item.

Antes que discutamos como tais definições afetam o campo da proteção de dados, é necessário entender o *processo* de fiscalização adotado pela FTC. Como dito, a FTC é um órgão administrativo federal, tendo a capacidade de fiscalizar e processar empresas que violem o FTCA. Ocorre que, na maioria dos casos, os casos de fiscalização da FTC não chegam a ser propostos perante o Judiciário, sendo antes resolvidos diretamente entre a FTC e a empresa em falta pelo procedimento dos *Consent Decrees.*

Os *consente decrees,* em muitos aspectos, assemelham-se a instrumentos como o Termo de Ajuste de Conduta ou mesmo o Acordo de Leniência na legislação brasileira. A FTC mantém um monitoramento constante por práticas que possam consistir em violação ao FTCA, dependendo largamente, entretanto, de reclamações de consumidores e denúncias feitas por canais de comunicação. Uma vez identificada determinada violação, por tal procedimento a FTC publica inicialmente um parecer sobre como a empresa em questão teria violado o FTCA, incluindo a identificação de práticas específicas que resultariam em tal violação e em que sentido tais práticas são consideradas abusivas ou enganosas. Juntamente a tal documento, a FTC publicaria também os termos gerais de uma proposta de ajustamento de conduta, ou seja, como a FTC considera que a empresa deveria agir para (i) corrigir e compensar os atos violadores e (ii) corrigir sua conduta dali em diante para não violar o FTCA. A isso geralmente se seguem negociações entre a FTC e a empresa, podendo a empresa escolher por aceitar o acordo ou aguardar a judicialização da questão. Não aceito o acordo (o *consent decree),* a FTC pode acionar o Judiciário para comprovar a violação do FTCA e assim exigir da empresa em questão a compensação adequada, inclusive em relação ao ajuste de suas condutas consideradas ilegais.

O acordo proposto, geralmente designado *consent decree,* prescinde do reconhecimento de culpa pela empresa, mas antes representa um compromisso sobre atos e condutas a serem adotados pela empresa para (i) compensação dos danos eventualmente causados e (ii) correção da sua conduta atual, o que pode incluir alterações na política de privacidade, implementação de medidas e processos internos para proteção dos dados pessoais, alterações em como a empresa opera com dados pessoais, criação de programas de conformidade e governança, entre diversas outras medidas que serão acompanhadas pela

FTC pelos próximos anos. Caso o acordo não seja integralmente cumprido, geralmente ele mesmo já prevê sanções que podem então ser cobradas judicialmente em face do descumprimento, comprovada então a culpa da empresa na violação do FTCA.

Merece esclarecimento o fato de que os *consent decrees* não possuem peso de precedentes (*precedential weight).* Na tradição do *common law*, as decisões emanadas dos tribunais possuem peso de precedente uma vez que os tribunais buscam sempre julgar novas demandas de forma coerente com posicionamentos anteriores da corte. É assim que o caráter de precedente de uma decisão vincula decisões futuras, afetando não só as partes de um determinado processo mas também as partes de processos futuros sobre aquele mesmo tema. Os "precedentes" da FTC em seus *consent decrees* não possuem tal peso e a FTC, em tese, não está obrigada a ser consistente em seus posicionamentos, não havendo uma obrigação de observar o posicionamento em casos anteriores para a definição dos termos de um *consent decree.*

Não obstante, defendem Solove e Hartzog que, dada a tendência da FTC de ser de fato coerente em seus posicionamentos, pode-se olhar para o conjunto de casos em que a FTC fez acordos com empresas em violação do FTCA como um verdadeiro corpo de precedentes que se reforça com cada nova decisão, construindo teorias sobre o que seriam condutas violadoras e quais seriam as condutas adequadas em situações razoavelmente similares. Assim, neste trabalho podemos nos referir a tal corpo de decisões e acordos como "o *common law* da FTC", ficando a nota de que, apesar de tal denominação, não há de fato o reconhecimento formal (pelas cortes, por exemplo) de que tal conjunto de acordos e casos constitui de fato um conjunto de "precedentes", no sentido técnico da palavra.

Dito isto, podemos explorar dois aspectos principais do *common law* da FTC, quais sejam (i) as teorias sobre atos enganosos e abusivos e (ii) as proposições corretivas constantes dos diversos *consent decrees* da FTC, muito bem explorados por Solove e Hartzog em seu artigo "*FTC and Privacy Common Law".*[238]

Dentre as condutas geralmente consideradas enganosas, encontramos: (i) promessas de privacidade descumpridas, (ii) condutas enganosas em geral, (iii) declarações de privacidade insuficientes e (iv) promessas de segurança de dados descumpridas.

Já dentre as condutas consideradas abusivas, encontramos: (v) mudanças retroativas do tratamento, (vi) coleta de dados com incentivos enganosos, (vii) uso impróprio de dados

[238]SOLOVE, Daniel; HARTZOG, Woodrow. *op. cit*.

pessoais, (viii) design abusivo e configurações padrões abusivas de software, e (ix) práticas abusivas em segurança da informação.

Em relação às condutas, é de se notar que nem sempre há uma separação absoluta entre o que é considerado *enganoso* e o que é considerado *abusivo,* mas essas teorias de violação podem na verdade se sobrepor, sem nenhum prejuízo à argumentação de cada tipo de violação, visto que seja a conduta enganosa ou abusiva, estará sempre sob o cobertor do FTCA, sendo passível das punições e medidas adequadas.

Para remediar tais violações, já é costumeiro que a FTC utilize uma variedade de medidas, geralmente combinadas, para compensar a conduta passada e corrigir a conduta futura. Dentre esses remédios, encontramos (i) a proibição de determinadas condutas consideradas enganosas ou abusivas; (ii) notificação ao consumidor sobre a violação, remediação de danos e prevenção e mitigação de riscos; (iii) aplicação de multas e outras penalidades pecuniárias; (iv) apagamento dos dados que tenham sido coletados com algum tipo de vício ou cujo tratamento represente algum tipo de conduta considerada enganosa ou abusiva; (v) realizar alterações em políticas de privacidade para adequar a operação da empresa com dados pessoais aos padrões considerados aceitáveis pela FTC; (vi) estabelecimento de programas compreensivos de compliance em proteção de dados, de execução contínua, que buscam garantir que as práticas envolvendo dados pessoais de determinada empresa estejam em conformidade com o exigido pela lei e pela FTC; (vii) estabelecimento de rotinas de auditoria externa em segurança e privacidade, de modo que um profissional independente verifique se os termos do acordo entre a empresa e o FTC estão sendo cumpridos; (viii) submissão de relatórios periódicos de conformidade pela empresa à FTC, de modo a demonstrar o cumprimento do *consent decree* e da legislação aplicável; e (ix) a obrigação de notificar a FTC sobre mudanças materiais na operação da empresa que possam de alguma forma afetar a conformidade desta com o *consent decree.*

Como se percebe, a prática da FTC aproxima muito, na prática, o esperado de empresas nos Estados Unidos do esperado de empresas localizadas na Europa no tocante aos requisitos para tratamento de dados pessoais, muito mais que a própria legislação estatutária norte-americana.

Obviamente, desníveis existem ainda assim e dentre eles talvez esteja, como um dos pontos principais, o fato de o FTC não ter atualmente capacidade e recursos para executar sua fiscalização de modo abrangente, de modo que todas as denúncias recebidas sejam de

fato investigadas, por exemplo, considerando que a comissão tem diversas outras atribuições relacionadas à proteção do consumidor e da livre concorrência em geral. A título de exemplo, a FTC em seu relatório sobre as atividades de 2019 no campo de *Privacy and Security*, em um ano extremamente produtivo comparativamente com anos anteriores, 44 casos envolvendo violações (i) ao *Section 5* do FCTA, (ii) legislação estatutária (como COPPA) e (iii) ao então ainda vigente Privacy Shield. Considerando-se que não há um direito privado de ação neste caso, esse é o total de situações em que os padrões de compliance em proteção de dados da FTC foram de fato exigidos ao longo de 2019, o que parece bastante reduzido considerando o provável número total de casos de violação do FCTA, quanto mais de situações em que dados pessoais são tratados de forma incorreta ou desleal.

3.8. Propostas para leis abrangentes sobre proteção de dados

Nos últimos anos tem-se observado uma crescente iniciativa para dotar os Estados Unidos de uma lei geral de proteção de dados, de forma a concretizar em norma estatutária o que nas últimas décadas foi desenvolvido pelo *common law*. Tais iniciativas, no entanto, encontraram forte resistência política e ideológica, de modo que acabaram, geralmente, esquecidas, sem nunca serem aprovadas.

Tais projetos, apesar de muito celebrados por seus defensores, nem sempre apresentaram o quadro suficientemente amplo que geralmente se exige de uma lei geral de proteção de dados, em alguns casos focando, como outras regras setoriais, em cenários específicos e obrigações pontuais, como aquelas relacionadas a roubo de identidade e vazamentos de dados pessoais.

Considerando o objetivo do presente estudo, que deve necessariamente desconsiderar o aspecto político, não jurídico, para averiguar se a aproximação entre os sistemas dos Estados Unidos e da União Europeia é juridicamente possível (mesmo que politicamente não seja desejável), cabe breve exploração sobre o que tais projetos de lei, que em tese poderiam auxiliar em tal objetivo de aproximação, de fato trariam à mesa caso fossem aprovados. Essa avaliação, ainda que suscinta, nos permitirá avaliar se o caminho juridicamente desejável ainda seria a imposição de uma lei geral de proteção de dados abrangente nos Estados Unidos, ou se outras soluções, mais restritas, seriam suficientes.

São três os projetos que chamam nossa atenção nesse debate: o projeto do *Consumer Privacy Protection Act* de 2015,[239] o projeto do *Privacy Bill of Rights Act* de 2019[240] e o projeto do *Data Protection Act* de 2020.[241]

O primeiro projeto, do *Consumer Privacy Protection Act* de 2015, pode ser dividido entre três partes principais: (i) regras sobre punições para a ocultação de violações de segurança; (ii) regras sobre a criação de programas de governança em privacidade e segurança da informação, determinando quais os requisitos mínimos de tais tipos de programas; e (iii) regras sobre a obrigatoriedade de notificações sobre vazamentos de dados.

Os itens (i) e (iii) parecem se complementar na busca pelo estabelecimento de regras federais abrangentes sobre a obrigação de notificar vazamentos de dados pessoais às autoridades competentes. Tais disposições somariam às já existentes leis estaduais sobre o assunto, mas desta feita buscando estabelecer padrões mínimos sobre tais notificações, a serem observados também pelos estados. Para as entidades cobertas por tal lei, a nova lei federal seria aplicável em prejuízo a outras leis federais e às leis estaduais em vigor, mas apenas em relação a tal matéria.

O item (ii) é de especial interesse pois traz diversas regras que aproximariam de maneira considerável o modelo dos Estados Unidos do modelo europeu. Entre essas regras, destacamos (i) uma obrigação geral de adotar medidas de segurança adequadas, que inclusive indica os critérios para que a análise de tal "adequação" seja feita, de maneira semelhante ao disposto na legislação europeia; (ii) regras sobre a avaliação e gestão de riscos relacionados à privacidade, inclusive na gestão de terceiros e prestadores de serviço com quem os dados possam ser compartilhados, práticas fundamentais incluída entre recomendações técnicas para a criação de programas de privacidade;[242] e (iii) um mandamento geral de minimização de dados, pelo qual as empresas sujeitas à lei devem buscar sempre utilizar o mínimo possível de dados pessoais cobertos pela lei, mantendo esses dados apenas pelo período necessário

---

[239]US Congress, Senado, S. 1158 de 30 de abril de 2015. UNITED STATES. Senate. *S.1158 - Consumer Privacy Protection Act of 2015*. Disponível em: https://www.congress.gov/114/bills/s1158/BILLS-114s1158is.pdf.

[240]US Congress, Senado, S. 1214 de 11 de abril de 2019. UNITED STATES. Senate. *S.1214 - Privacy Bill of Rights Act*. Disponível em: https://www.congress.gov/bill/116th-congress/senate-bill/1214.

[241]US Congress, Senado, S. 3300 de 13 de fevereiro de 2020. UNITED STATES. Senate. S.*3300 - Data Protection Act of 2020*. Disponível em: https://www.congress.gov/bill/116th-congress/senate-bill/3300/text.

[242]A título de exemplo, verifique-se a norma técnica ISO/IEC 27.701. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. INTERNATIONAL ELECTROTECHNICAL COMMISSION - IEC. *ISO/IEC 27701:2019*. Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en.

para cumprimento das finalidades do negócio, o que reflete largamente os princípios já estudados da finalidade e da necessidade do modelo europeu.

Em uma primeira crítica ao projeto, devemos apontar a ausência de uma definição ampla de dados protegidos pela lei, de forma que apenas alguns tipos de dados estariam sujeitos a ela como dados de saúde, dados financeiros, dados biométricos, dados de localização e dados de identificação sensível (ex.: número do seguro social). Mais uma vez, a legislação estatutária busca apenas regular o uso dos dados que apresentam maior risco em sua utilização. Apesar de se poder argumentar que a iniciativa deve ser louvada por reunir tantos tipos diferentes de dados pessoais, a proteção concedida pela lei contaria ainda com diversos espaços de vazio legislativo, em que as empresas poderiam vicejar em práticas abusivas, sem que isso lhes rendesse maior preocupação ou desabono.

Adicionalmente, a lei só seria aplicável a empresas (excluídas, pois, entidades sem fins lucrativos) e apenas àquelas que se engajam em comércio interestadual, de modo que a lei não é aplicável a pequenos comércios e negócios que atuem apenas em um estado da federação. Apesar de continuar primando apenas pela regulação dos cenários de maior risco, parece temerário excluir uma parcela tão grande de entidades que claramente utilizam dados pessoais (e podem, claramente, violar as práticas aceitas ao fazê-lo), deixando assim o cidadão descoberto.

Já o segundo projeto, do *Privacy Bill of Rights Act* de 2019 corrige alguns problemas do anterior: em primeiro lugar, o conceito de dados pessoais agora abrange a totalidade das informações relacionadas a uma pessoa, e não apenas algumas categorias de dados; em segundo lugar, o projeto abrange qualquer pessoa que faça uso de dados pessoais, sem limitações quanto ao seu caráter ou localização.

O projeto de lei conteria disposições sobre direito à informações ou uma obrigação de transparência; um “direito ao controle”, que poderia ser traduzido como um direito de escolha e consentimento; direitos de acesso, correção, apagamento e portabilidade que seria geralmente aplicáveis mas que poderiam ser restritos em alguns casos; uma proibição de reidentificação ou desanonimização de dados pessoais; a proibição de ofertas que condicionam sua aceitação a um aceite global sobre o tratamento de dados pessoais, sem que o titular tenha escolhas efetivas a fazer; a proibição do fornecimento de incentivos financeiros à autorização ou ao fornecimento de dados pessoais pelo titular; a proibição de compartilhamento de dados com terceiros exceto quando a empresa controladora obtivesse

as garantias necessárias sobre a segurança de tais informações desse terceiro; disposições sobre limitação do uso dos dados coletados; obrigações gerais sobre minimização do uso de dados pessoais e dos dados pessoais utilizados em si; a obrigação de indicação de um encarregado ou responsável, dentro da empresa, que fiscalize internamente a empresa quanto ao cumprimento da legislação aplicável; medidas adequadas de segurança a serem aplicadas para proteção dos dados; além de conceder a todos os titulares um *private right of action*, além da possibilidade de fiscalização pela FTC (na esfera federal) e pelo *Attorney General* de cada estado (na esfera estadual).

Talvez a principal crítica a este projeto diga respeito à efetividade das regras nele dispostas: apesar de em diversos casos o projeto criar regras específicas para conduzir a conduta de empresas e outras entidades que venham a tratar dados pessoais, sendo tais regras prontamente aplicáveis, em diversos outros o projeto meramente delega à FTC a aprovação de regulamentos sobre tais temas, sendo que as regras trazidas pelo projeto na verdade são apenas requisitos mínimos para a regulamentação a ser emitida pela FTC. Esse é o caso, por exemplo, dos direitos garantidos ao titular, as obrigações sobre limitação do uso de dados e minimização e outras disposições sobre segurança e responsabilidade. Apesar de tal solução aparentar buscar termos razoáveis e *coesos* com a prática atual da FTC e a *common law* por ela desenvolvida, é verdade que tal projeto desaponta por ficar aquém do que dele se espera ao projetar regras tão amplas sobre esse domínio.

O terceiro projeto, do *Data Protection Act* de 2020 talvez seja o mais limitado dos três projetos, mas talvez o mais inovador: o projeto tem como seu principal propósito a criação de uma *Data Protection Agency* que teria como finalidade fiscalizar e proteger a privacidade dos cidadãos, prover orientação quanto a questões relacionadas ao tratamento de dados pessoais e promover a implementação dos FIPPs tanto no setor público quanto privado. É verdade que o projeto não traz muitas regras materiais sobre proteção de dados, mas considerando o *status* da matéria como um todo nos Estados Unidos, este talvez seja um dos projetos mais interessantes.

Dentre seus méritos podemos apontar a adoção de definições amplas sobre dados pessoais (envolvendo todo e qualquer tipo de dado relacionado a uma pessoa ou dispositivo) e sobre entidades cobertas (cobrindo não só empresas), o caráter independente da agência, suas capacidades de emitir regulamentações e de receber e resolver reclamações de consumidores, além de sua capacidade geral de fiscalizar e exigir o cumprimento das leis já existentes sobre privacidade e de outras que venham a ser criadas sobre privacidade e

proteção de dados, ocupando uma posição muito semelhante no panorama jurídico à das Autoridades de Proteção de Dados, comuns em modelos derivados daquele da União Europeia.

3.9. Considerações sobre proteção de dados no sistema norte-americano

O modelo regulatório dos Estados Unidos é único na medida que apresenta uma abordagem bastante heterodoxa no que toca às limitações à proteção de dados. Há de fato o reconhecimento de que os dados pessoais têm alguma ligação com a privacidade do indivíduo e com o controle que esse exerce sobre sua vida particular[243], mas a extensão dessa proteção é no geral incerta. Tem-se um "direito à tutela": o titular tem direito a ter considerado o peso de sua privacidade na avaliação do caso concreto, mas o alcance real da privacidade depende desse sopesamento feito pelos tribunais e em casos envolvendo práticas desleais de mercado. Tal "direito à tutela", por consequência, dificilmente é autoaplicável ou diretamente exigível pelo titular dos dados daquele que os coleta e os trata.

Ao mesmo tempo, as leis estatutárias, estaduais e federais, são limitadas quanto ao que buscam regulamentar, primando pela proteção do titular dos dados apenas em relação aos dados mais sensíveis e às situações de maior risco, sem reconhecer, entretanto, que outras tantas situações e circunstâncias cotidianas, reputadas irrelevantes, podem representar, no agregado, o mesmo nível de risco ao titular que um vazamento de dados da maior magnitude.

3.9.1. Setorização, consentimento e autorregulação

Um primeiro aspecto relevante do modelo norte-americano a ser colocado à prova da comparação diz respeito ao seu aspecto setorial. No total, as leis dos Estados Unidos buscam sempre abordar cenários específicos do uso de *certos tipos de dados* por *certos tipos de pessoas ou empresas.* Assim funciona a regulação setorial, em que, por exemplo, as instituições financeiras estão sujeitas a regras específicas sobre a coleta e uso de certos tipos

[243]WESTIN, Alan. Privacy and Freedom, New York: Atheneum, 1970 *apud* PEREIRA, Marcelo Cardoso. *op. cit.*, p. 128.

de dados pessoais, como dados bancários e dados relacionados à proteção do crédito, sobre o adimplemento de obrigações e sobre a falha em pagar o que se deve.

Essas mesmas instituições, entretanto, não estarão sujeitas às mesmas regras em relação aos dados pessoais de seus empregados ou mesmo aos dados de saúde de seus clientes, utilizados para alguma finalidade incomum no ramo bancário mas que poderia conceder algum tipo de benefício àquela empresa. Ao mesmo tempo empresas do ramo de saúde que devem cumprir o HIPAA estão vinculadas a ele apenas em relação aos dados de saúde e outros dados relacionados à prestação dos serviços, não havendo disposições específicas sobre informações sensíveis como aquelas relacionadas a crença religiosa ou orientação sexual.

Em suma, é dizer que, apesar de o modelo setorial se basear na premissa de que a regulação deve recair sobre os setores cujo uso de dados representam maior risco, essa abordagem deixa de considerar a relevância de outras circunstâncias e situações que podem também causar igual dano, apesar de serem menos comuns ou não esperadas. É dizer, portanto, que o modelo setorial regula em normas estatutárias aqueles cenários de risco extremo, deixando aos tribunais e aos órgãos de fiscalização a coibição de condutas consideradas abusivas, por exemplo, com base na Seção 5 do FCTA e de leis estaduais equivalentes, ficando o *enforcement* de tais situações reputadas menos graves restrito a tais vias.

Em um segundo aspecto relevante, a norma de direito mais próxima do indivíduo é, pois, o contrato ou a política de privacidade que rege sua relação com a empresa que coleta e utiliza seus dados pessoais. Talvez por conta da alta estima em que tem a liberdade, o legislador parece deixar às partes estabelecer o que é razoável e possível. O instituto central do modelo norte-americano pode ser apontado, pois, como o *consentimento,* diretamente expressado pelo binômio *notice and choice*. As condições e características desse consentimento variam de acordo com o setor de mercado e com a corte competente ou órgão fiscalizador, mas é bastante claro que o consentimento possui, no contexto norte-americano, valor muito maior que aquele atribuído a ele nos demais modelos regulatórios.

Isso porque não se trata aqui de um *consentimento informado*, livre ou expresso, *resultado da consideração do indivíduo sobre o que se pretende com seus dados* e o sopesamento entre benefícios e malefícios. O consentimento, na tradição norte-americana, parece ter maior ligação com a liberdade do titular e com *espaços de autonomia* do que com o estabelecimento de uma relação entre o usuário e o responsável pelo tratamento, dando-se

ao contrato o tom de uma transação comercial, ao invés de uma licença temporária de direitos sobre os dados em questão[244].

O contrato, a política ou declaração de privacidade, no entanto, não serve sempre como substituto à garantia de certos direitos abrangentes, principalmente em situações em que uma das partes é uma grande empresa e a outra um indivíduo que deseja usufruir de um serviço seu – ao qual não terá acesso caso não aceite o contrato padrão provedor do serviço. Em muitos momentos, o usuário é forçado a aceitar termos impostos pelo provedor, não importa quão injustos, sem que lhe assista um direito privado de ação para buscar compensação por tal injustiça.

Esse desequilíbrio, resultado da disparidade de força das partes, gera situações abusivas que, apesar de em tese poderem ser tuteladas por leis gerais sobre práticas abusivas de mercado (como o FCTA), dependem diretamente da atuação de órgãos fiscalizadores que possuem não só recursos limitados (tratando de 20, 30 casos por ano, como se extrai de seus relatórios anuais), como também têm sua atividade limitada a disposições legais genéricas que nem sempre permitem o enquadramento de determinada prática como abusiva, apesar de não representar um uso legítimo dos dados pessoais dos titulares em questão. Assim, pela ausência de legislação específica e pela massificação dos negócios digitais[245], resta ao titular o recurso a ações judiciais, individuais ou coletivas, como única solução, ações essas que, diga-se de passagem, são geralmente ineficientes para tutela individual, uma vez que exigem a demonstração de algum tipo de dano material, raro em casos envolvendo dados pessoais, salvo os que envolvam algum tipo de fraude ou roubo de identidade.

A judicialização de conflitos, ampliada pela ausência de uma norma geral ou mesmo de um órgão regulador específico, tem diversas consequências, tanto para a efetividade dos direitos garantidos quanto para a condução dos negócios em si.

Por um lado, temos que determinada situação considerada lesiva aos interesses de uma das partes é colocada sob exame de uma autoridade judicial que, ainda que não seja especialista no assunto em tela, tem por delegação o poder estatal para dar solução definitiva

---

[244]"In contrast to other areas of the world such as the United States, where personal information is widely traded like a conventional good, European rules limited the commodification of individual data." NEWMAN, Abraham L. *op. cit.*, p. 104.

[245]Confira-se, por exemplo: BARRETT, Brian. Spotify clears up its controversial Privacy Policy. *Wired Online*, 21 ago. 2015. Disponível em: https://www.wired.com/2015/08/spotify-clears-up-its-privacy-policy/. Acesso em: 19 jan. 2017. PAUL, Ian. Instagram updates privacy policy, inspiring backlash. *PC World*, 18 dez. 2012. Disponível em: http://www.pcworld.com/article/2021285/instagram-updates-privacy-policy-inspiring-backlash.html. Acesso em: 19 jan. 2017.

ao litígio, garantindo a observância da lei tanto no curso do procedimento quanto na execução do provimento. Por outro, consigna-se a solução de um litígio técnico, e que exige rápida resposta, a uma entidade que não possui o conhecimento técnico muitas vezes necessário e cujo prazo mínimo para atingir um primeiro provimento definitivo é grande demais, a ponto de ser totalmente ineficaz do ponto de vista fático.

Afirmamos isso pois a maioria dos dados pessoais em circulação advém e tem como seu contexto a Internet e outros sistemas informatizados, geralmente conectados em rede, e o tempo entre as transações, ações de tratamento, comunicação de dados, é infinitamente menor ao usual, dentro do qual uma solução judicial seria viável.

Em um segundo aspecto, tem-se, no foco da análise, uma consequência mais ampla relacionada ao comportamento das partes desde a concepção de um modelo de negócio até seu efetivo fornecimento. Relegar ao judiciário ou a órgãos federais de pequeno alcance a garantia de direitos, sem criar outros mecanismos que os garantam ou busquem incentivar a adoção de certas práticas de bom tom no tratamento da privacidade dos indivíduos, instila no empreendedor e nas empresas em geral a ideia de que a garantia da privacidade de seus clientes ou futuros clientes é apenas um fator na análise de rentabilidade e viabilidade de um modelo de negócios, e não um valor que deve ser preservado.

Do ponto de vista geral, essa abordagem privilegia a livre iniciativa e a inovação, permitindo que usos novos e não regulados da informação sejam descobertos e utilizados para gerar valor aos consumidores. Sob a ótica da proteção de dados pessoais, no entanto, trata-se de um modelo ineficaz de regulação, que recorre apenas a um viés regulatório jurídico, ao invés de avaliar a conduta regulada em termos econômicos, sociais e de "arquitetura", como queria Lessig.[246] Vale, nesse ponto, questionar se a via adotada pelos juristas estadunidenses é a única e mais efetiva alternativa para realizar os dois propósitos aparentemente contraditórios: privacidade e livre iniciativa[247].

---

[246]LESSIG, Lawrence. *Code version 2.0*. Kindle Edition, 2011. pos. 1536-1545.

[247]De uma parte: "A ideia de consentimento do afetado, cujo estágio temporal é necessariamente após a noção de *informação* anteriormente tratada, é tão central ao modelo europeu de proteção de dados, que um dos maiores e mais antigos estudiosos espanhóis sobre o tema afirmou em uma de suas obras que esse 'es la piedra angular a partir del cual se construye el sistema de protección de datos personales'" SILVA, Carlos Bruno Ferreira da. *op. cit.*, p. 187. De outra parte, confira-se: "De una parte, argumentamos que, en cuanto expediente legitimador y forma de protección del titular de los datos, el consentimiento es un mecanismo inadecuado: la concepción "individualista" que subyace a este enfoque protector no sirve en un mundo de computación ubicua donde las prácticas de obtención y análisis masivo de datos son inevitables y banalizan la idea del tratamiento "consentido". De otra parte, sostenemos que el discurso oficial del control individual de la información personal ligado a esa idea – al que parece aferrarse aún la futura normativa europea – ha

3.9.2. Padrões de boas práticas ou lei?

Por fim, neste estudo é necessário confessar que o cenário encontrado do *enforcement* pela FTC em muito trouxe luz a um campo que se presumia vazio. Ao analisar os recentes *consent decrees* da FTC fica claro que muito do que se propala em outras jurisdições e em leis gerais de proteção de dados sobre todas as condicionantes e limitações aplicáveis ao tratamento de dados pessoais já é reconhecido pela *common law* da FTC. Seja no tocante aos direitos garantidos aos titulares, às práticas consideradas abusivas, ao uso de dados que desconsidera preceitos básicos como transparência e necessidade, a *common law* da FTC se equipara razoavelmente em diversos pontos ao modelo europeu, por exemplo.

A crítica, no entanto, perdura enquanto a prática se restringe a um número reduzido de casos e enquanto o *enforcement* de tais padrões de conduta não estiver franqueado ao próprio titular de dados, interessado primeiro. Os padrões da FTC, como já dito, podem ser elogiáveis, mas enquanto o titular dos dados não puder provocar a atuação de um órgão, seja ele administrativo ou judicial, e obter uma resolução, o sistema permanece limitado, agindo de modo corretivo apenas quando o problema (o dano) é muito grande, mas nem de longe abordando o grande *número* de problemas menores.

Nesse aspecto, a proteção dos dados "não tão importantes" fica relegada à autorregulação e à confiança de que, deixado só, o agente econômico busque uma solução intermediária e razoável e não apenas o que lhe traz maior benefício. Obviamente diversos fatores podem ser argumentados para temperar a busca por lucro das empresas, dizendo-se então que é parte do próprio objetivo da empresa que seus consumidores confiem nela e em seus produtos e serviços, e por tal razão devem estes, ao menos no que é razoável, prezar pela privacidade do consumidor. E mesmo pode-se argumentar que mesmo que a FTC não atinja diretamente todas as empresas em violação, os *consent decrees* servem como orientação às empresas sobre como elas *deveriam* atuar, mas como reconhecem até os

---

acabado convertido en una suerte de letanía que a duras penas se refleja en la práctica y que predica de la legislación de protección de datos un poder para conformar la realidad social que no tiene." OLIVER-LALANA, Angel Daniel; MUÑOZ SORO, José Félix. El mito del consentimiento y el fracaso del modelo individualista de protección de datos. *In:* VALERO TORRIJOS, Julián. (Org). *La protección de los datos personales en internet ante la innovación tecnológica*. Navarra: Aranzadi, 2013. p. 153-196. A respeito dessa discussão, confira-se também: BENNETT, Colin J. *Regulating privacy*: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992. p. 193-219.

defensores da FTC, o peso de suas decisões não é vinculativo e, apesar de boas práticas, pouco caráter têm como lei de fato.

A linha que separa o que uma empresa *diz* para ganhar a confiança de um consumidor e o que ela *faz* efetivamente quando já tem os dados em mãos nem sempre é tão fina. Isso que o digam as conclusões da FTC nos diversos casos analisados ano a ano em que as mais básicas práticas de lealdade, o mais simples princípio de cumprir aquilo que se promete ou de não se engajar em atividades claramente enganosas para obter dados (como se passar por outra pessoa ou instituição), parecem continuar um terreno cinzento e nebuloso para a maioria das empresas que os violam diuturnamente.

Os padrões adotados pela FTC de fato inspiram alguma esperança de que os Estados Unidos venham a garantir um nível adequado de proteção de dados pessoais, facilitando assim o intercâmbio econômico e cultural entre si e diversos outros países que já aderiram a medidas equivalentes ao modelo europeu, como o próprio Brasil. Ainda assim, enquanto não houver maior garantia de efetividade, tanto individual quanto coletiva, administrativa e propriamente judicial (como a garantia de um *private right of action* amplo), é difícil esperar uma maior aproximação entre os sistemas comparados neste trabalho. Mesmo que os cenários políticos para aprovação de uma lei geral de proteção de dados nos Estados Unidos não estejam necessariamente alinhados à realidade, o que parece ser possível afirmar é que predisposição técnica já existe, faltando apenas alguma vontade específica de tornar lei geral o que já é praticado, ainda que em menor escala, pela FTC.

CAPÍTULO 4. PRIVACIDADE E PROTEÇÃO DE DADOS NO CONTEXTO COMPARADO E NO DIREITO INTERNACIONAL

4.1. Considerações iniciais

Tendo visitado os sistemas de proteção de dados da União Europeia e dos Estados Unidos da América, resta agora considerar ambos em uma luz geral e abrangente para primeiro compreender os contornos gerais que tornam tais regimes tão diferentes, mas também em comparação detalhada, de forma a delinear funções específicas exercidas pelos diversos institutos que formam cada sistema. A macro comparação nos permite identificar grandes fundamentos de cada sistema, enquanto a micro comparação nos permite perceber semelhanças funcionais que poderiam nos escapar em outra hipótese.

Como afirmado no início do trabalho, nosso objetivo maior é responder se o direito internacional é capaz, juridicamente, de compor os sistemas da União Europeia e dos Estados Unidos de modo a torná-los compatíveis. Antes de verificar se o Direito Internacional tem tal capacidade, no entanto, é necessário verificar se os sistemas são de fato passíveis de composição considerando os fundamentos da tutela dos dados pessoais, verificando-se assim a existência do que chamamos de "espaços de convergência". Identificados estes, passamos então à análise da proteção de dados no Direito Internacional, traçando sua atuação até o presente momento e como este influenciou o desenvolvimento da matéria nas duas jurisdições, avaliando então possíveis previsões para sua atuação futura.

Por fim, avaliaremos as potenciais consequências da confirmação da hipótese analisada neste trabalho, considerando tanto a relação entre a União Europeia e os Estados Unidos, mas especialmente o impacto de tal conclusão para o intercâmbio internacional de dados pessoais considerando o sistema de transferências internacionais estabelecido pela União Europeia e copiado por diversos países, inclusive considerando os potenciais impactos de tal composição de sistemas para o Brasil.

4.2. Sistemas de proteção

Ao redor do mundo, a proteção de dados pessoais assume formas variadas, diferindo não apenas nas obrigações específicas, mas também nas estratégias regulatórias por trás de tal projeto normativo. É relevante traçar, neste momento, contornos de tais sistemas com a finalidade de, ao final do presente estudo, poder enfatizar o papel do Direito Internacional no preenchimento dos espaços vazios entre esses modelos e o fortalecimento dos pontos em comum.

O contorno inicial desses modelos foi traçado por nós em trabalho anterior, de maneira inicial, em uma comparação promovida entre os sistemas regulatórios do Uruguai, dos Estados Unidos e da União Europeia.[248]

O primeiro modelo passível de definição é aquele da União Europeia, geralmente denominado *abrangente*[249] por contar com legislação central sobre o tema de proteção de dados que é então expandida por diversas outras regulações menores para abarcar, de forma tendente à completude, todo e qualquer tratamento de dados pessoais possível. No entanto, escolhemos denominar tal modelo de *eclético* em nossa exposição, uma vez que a denominação *abrangente* geralmente considera apenas a dimensão da *legislação* para tal categorização, ignorando outras dimensões regulatórias como o mercado, a tecnologia e as próprias práticas sociais.

Assim, escolhemos denominar o sistema da União Europeia de *eclético* não apenas pois ele possui uma lei geral para proteção de dados, o GDPR, centralizada, abrangente, ampla, mas sim porque o sistema de proteção é composto por camadas legislativas, por regulamentações que se direcionam aos mecanismos de mercado, por uma atuação robusta das Autoridades de Proteção de Dados em seus esforços regulatórios e educativos, além de sua atuação fiscalizatória, e mesmo pelos incentivos dados para a própria adaptação da tecnologia pelas empresas conforme ela é desenvolvida. Para melhor ilustração, cabe alguma elaboração sobre cada elemento do modelo eclético, para que sua diferenciação de outros modelos fique suficientemente clara.

---

[248]GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. *In*: BRANCO, Sérgio; DE TEFFÉ, Chiara (Orgs.) *Privacidade em perspectivas*. Rio de Janeiro: Lumen Juris, 2018.
[249]SWIRE, Peter P.; KENNEDY-MAYO, DeBrae. *op. cit*. p. 19-20.

Podemos dividir tal exposição em 4 aspectos: legislação em proteção de dados, incentivos ao mercado, iniciativas de educação e orientação, e tecnologia. No aspecto da legislação em proteção de dados, a tradicional descrição *abrangente* descreve razoavelmente bem o modelo da União Europeia, pois ilustra um sistema em que vige uma lei central, geral, para proteção de dados pessoais que regula a matéria nas mais diversas situações, sendo verdadeira regra geral (em oposição a regras específicas, setoriais). Tal regra geral, de caráter supranacional no caso, é complementada, em primeiro nível por outras regras da própria União Europeia sobre o assunto, como é o caso da Diretiva e-Privacy (que regula alguns aspectos do tratamento de dados em comunicações eletrônicas), do Regulamento 45/2001 (que regula o tratamento de dados por instituições da União Europeia) e de outras Diretivas, Decisões e Pareceres que estabelecem regras sobre pontos específicos.

Em um outro nível, essas regras são complementadas pelas próprias leis nacionais de cada Estado-Membro: ainda que desde a entrada em vigor do GDPR as leis nacionais não possam mais contradizer a norma supranacional frontalmente, estas continuam a vigorar no que diz respeito a regras complementares e outras decisões que o próprio Regulamento deixa a cada Estado-Membro. Por fim, mas não menos importante, no cenário legislativo encontramos também regulamentações administrativas emitidas pelas próprias Autoridades de Proteção de Dados, que dizem respeito a questões técnicas e aspectos muito mais detalhados e que demandam um tipo mais flexível de regulamentação legal, para que possam ser atualizadas a um passo mais rápido, de modo a acompanhar a evolução fática da tecnologia e dos tratamentos de dados pessoais.

No aspecto dos incentivos ao mercado, encontramos o recurso à autorregulação e aos regimes de certificação. Como provisionado pelo próprio GDPR, as empresas envolvidas em tratamento de dados podem, reunindo-se com outras empresas de seu setor, aprovar códigos de conduta que estabeleçam regras e padrões complementares ao disposto no Regulamento. Tais códigos podem ser submetidos à aprovação da Autoridade de Proteção de Dados responsável para então serem considerados padrões aceitos de conduta, de modo que se uma empresa cumpre com tal código, considera-se que ela está em conformidade com o GDPR, dando-se então liberdade a cada setor para desenhar em detalhe o que deveria significar "estar conforme" para aquele setor específico.

Adicionalmente, de um modo mais amplo, o GDPR permite o estabelecimento de programas de certificação que, quando previamente aprovados pelas autoridades competentes, podem representar alguma garantia, ao mercado em geral, de que uma empresa

certificada está de fato em conformidade com o disposto no GDPR. Esse tipo de certificação almeja justamente incentivar o mercado a buscar a conformidade com a possibilidade de ter suas medidas de conformidade avaliadas por um terceiro independente antes de que seu sistema de proteção de privacidade seja "colocado a prova". Isso porque, geralmente, o sistema europeu implementa o controle pós-fato, isto é, não há algum tipo de aprovação prévia de que uma empresa está em conformidade: a empresa deve adotar as medidas que acha adequadas, com base nas orientações das autoridades de proteção de dados, mas a avaliação de estarem ou não tais medidas corretas só ocorre em caso de fiscalização ou no caso de um incidente em que uma autoridade venha a avaliar, para aquele caso, se a empresa está adequada ao GDPR. Assim, na ausência de algum tipo de autorização ou verificação prévia, o responsável pelo tratamento geralmente só terá uma resposta definitiva da autoridade de proteção de dados se esta considerou a empresa conforme ou não em caso de fiscalização, situação na qual não haverá tempo hábil para eventuais correções necessárias antes de algum tipo de autuação. Justamente por tal fato, o regime de certificações prévias é de grande interesse para a maioria das empresas, interessadas em ter alguma validação prévia sobre seus sistemas de *compliance* por um terceiro independente e por uma metodologia aprovada pelas próprias autoridades responsáveis pela fiscalização.

Esse tipo de mecanismo tem grande valia em esforços regulatórios, uma vez que busca incentivar o mercado à adoção de determinadas condutas não simplesmente por mandar a lei, mas por oferecer o regulador à entidade regulada algum tipo de vantagem ou benefício pelo cumprimento da lei. Os esquemas de certificação e autorregulação geralmente têm esse benefício configurado nas próprias vantagens quanto à imagem da empresa participante: ao se certificar como empresa cumpridora das regras aplicáveis sobre proteção de dados, pode a empresa usar tal certificação também como vantagem competitiva, mostrando a seus consumidores e parceiros que está em conformidade e que tal fato valoriza não só sua operação, mas também seus produtos e serviços, demonstrando a maior confiabilidade destes.

Assim, espera-se que os esquemas de autorregulação e certificação sejam buscados não só para verificar o cumprimento da lei, mas para serem utilizados como fator potencializador da concorrência, o que representa uma indução de comportamentos desejados pela oferta de benefícios econômicos, fator de regulação de extrema importância, especialmente em cenários regulatórios complexos em que a mudança de comportamento exigida pela legislação inclui grandes alterações no modo de funcionamento das empresas,

alterações estas que podem inclusive resultar em prejuízos econômicos ou maiores gastos com esforços contínuos de conformidade.

Em relação às iniciativas de educação e informação, encontramos as próprias Autoridades de Proteção de Dados no centro de uma rede em expansão de informações e orientações, fornecidas tanto aos próprios agentes econômicos quanto ao público em geral, para promover a conscientização sobre o tema da proteção de dados pessoais. Como se nota de diversas pesquisas nesse campo,[250] a sociedade da União Europeia, comparativamente ao resto do mundo, apresenta altos níveis de preocupação com temas relacionados à proteção de dados pessoais e à privacidade.

O fator cultural é um dos fatores mais elusivos na maioria dos sistemas: diversos países vieram nos últimos anos a aprovar leis de proteção de dados apenas para perceber que a alteração de comportamento nesse campo é algo que demora a se consolidar, justamente pela falta de conscientização, tanto das entidades e empresas que tratam dados pessoais quanto dos próprios titulares de dados pessoais.

Nesse aspecto uma atuação forte de atores institucionais para educação é essencial, e as autoridades de proteção de dados conseguiram preencher esse papel justamente por seu conhecimento técnico sobre o assunto, mas também por contar com a atenção geral do mercado: as iniciativas educacionais, apesar de não terem caráter fiscalizatório ou regulatório, tomadas como um componente do entendimento da autoridade quanto a determinados assuntos, acaba assumindo lugar importante na composição das posições que serão adotadas pela autoridade em processos de fiscalização e autuação, de modo que mesmo que voltadas aos consumidores, é comum que os próprios agentes de tratamento prestem atenção a tais iniciativas e materiais pois eles podem indicar caminhos que a autoridade pretende seguir na interpretação de certos pontos do GDPR.

Ainda, no aspecto tecnológico, é relevante citar o que se convencionou chamar de *privacy by design and by defaut*, ou seja, privacidade por desenho e por padrão. O conceito, ainda que colocado geralmente na esfera jurídica, tem imenso impacto prático no desenvolvimento da própria tecnologia, o que acaba por abranger mais esse domínio regulatório para buscar influenciar condutas.

---

[250]IAPP-EY Annual Privacy Governance Report 2019. Disponível em: https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/.

Pelo conceito de *privacy by design*[251] quer-se dizer que todo e qualquer projeto, produto ou serviço que seja criado ou desenvolvido deve incluir questões, preocupações com privacidade e proteção de dados desde sua concepção, de modo que tais valores sejam considerados e protegidos durante toda a cadeia de criação do projeto, produto ou serviço. Na prática, isso significa que todo o desenvolvimento de novas tecnologias, especialmente quando tais tecnologias tenham alto envolvimento com o tratamento de dados pessoais, deve sempre considerar tais questões. "Considerar a privacidade", em termos práticos, pode significar otimizar um projeto ou software para que colete o mínimo de dados possíveis, configurar determinada solução técnica para que, sempre que possível, opere sem a utilização de dados pessoais identificados, ou mesmo criar modos de operação que permitam ao titular dos dados pessoais fazer escolhas significativas sobre o tratamento destes. Fato é que tal determinação do GDPR fez surgir toda uma nova gama de preocupações no desenvolvimento de atividades comerciais, que se viram obrigadas a criar cargos e processos no fluxo de desenvolvimento para supervisionar este e garantir que as devidas proteções aos dados pessoais sejam implementadas, consideradas, planejadas juntamente ao desenvolvimento do projeto em si.

O conceito de *Privacy by default* é tido como um dos aspectos do *Privacy by design* e significa, de modo simples, que sempre que houver uma escolha a ser dada ao titular dos dados pessoais sobre como seus dados serão tratados, na ausência de uma manifestação positiva do titular o controlador deve sempre presumir que tal escolha sempre se dá pela opção que melhor preserve a privacidade do titular. Isso se ilustra com as configurações de um aplicativo móvel, por exemplo, que podem permitir ou não o compartilhamento de dados pessoais do titular com terceiros parceiros do controlador para fins econômicos (como terceiros que querem enviar e-mail marketing para esse usuário sobre seus produtos). Enquanto o titular não escolher especificamente ativar tal compartilhamento, deve-se presumir que a escolha do titular é pelo não compartilhamento, de modo que tal funcionalidade deve estar desativada por padrão, sendo ativada apenas se o titular assim quiser.

A implementação prática dos princípios de *Privacy by design e Privacy by default* são bons exemplos de como o sistema regulatório da União Europeia busca influenciar o próprio desenvolvimento tecnológico, mas não são apenas eles os responsáveis por isso,

---

[251]CAVOUKIAN, Ann; TAYLOR, Scott; ABRAMS, Martin E. *Privacy by design*: essential for organizational accountability and strong business practices. *IDIS*, n. 3, p. 409-410, 2010. Disponível em: https://link.springer.com/content/pdf/10.1007/s12394-010-0053-z.pdf. doi https://doi.org/10.1007/s12394-010-0053-z.

tendo as Autoridades de Proteção de Dados também forte influência sobre esse ponto. É assim, por exemplo, que uma autoridade de proteção de dados pode, por exemplo, emitir regulamentações específicas sobre o que ela considera serem processos adequados para anonimização de dados pessoais, de modo que dados pessoais se tornem anônimos (ou seja, não mais identifiquem um titular), estando a partir de então fora do âmbito de aplicação do GDPR. Ocorre que ao definir tais processos adequados, a autoridade geralmente terá que lidar diretamente com soluções técnicas que envolvem o manuseio de dados e informações eletrônicas, avaliando então o que cada solução técnica efetivamente *faz* com os dados para torna-los anônimos a ponto de poder avaliar se tal procedimento é efetivo. Ao definir isso, a autoridade de proteção de dados interfere diretamente no desenvolvimento tecnológico, pois indiretamente estabelece critérios sobre o que pode ser considerado, no exemplo, um processo adequado de anonimização, de modo que as soluções de anonimização disponíveis no mercado deverão se adaptar a tais critérios e especificações para poderem de fato atender a seus clientes com produtos que de fato oferecem *anonimização dentro dos conformes legais.* Por sua vez, isso afeta indiretamente também a tecnologia que os próprios agentes de tratamento buscam no mercado e adotam, assim moldando o mercado de tecnologia com uma preocupação adicional com privacidade e proteção de dados.

Esse agrupamento de medidas regulatórias demonstra claramente o caráter *eclético* do sistema de proteção de dados da União Europeia, uma vez que este escolhe abordar, ao mesmo tempo e com intensidades razoavelmente equivalentes diversas vias de regulação possíveis, como a regulação legal, mercadológica, sócio-cultural e tecnológica. Note-se, entretanto, que denominar este modelo de *eclético* não significa que outros modelos regulatórios não se apoiem igualmente em uma variedade de abordagens regulatórias. Não, o que se quer reconhecer é que em outros modelos há geralmente um foco ou focos do esforço regulatório que criam uma tendência maior a se privilegiar determinada abordagem regulatória, mas no modelo europeu o que chama a atenção é como o esforço regulatório se divide de forma equilibrada entre as diversas vias de regulação, confiando igualmente na regulação legal como se confia na regulação tecnológica, por exemplo.

A principal crítica ao modelo eclético talvez seja justamente o que outros modelos conseguem melhor abordar ao buscar soluções menos restritivas: o peso regulatório infligido sobre os agentes econômicos. É fato que do ponto de vista do titular de dados, o modelo eclético se mostre bastante protetivo ao cercar o agente econômico por todas as vias possíveis para que este adote certo comportamento. No entanto, a abrangência do modelo não precisa

necessariamente significar que a extensão das obrigações do agente econômico seja igualmente vultosa. Nesse aspecto, não discutimos que empresas de grande porte ou que realizam o emprego de grandes volumes e variedades de dados devem ser vinculadas a altos padrões de conformidade, inclusive no que diz respeito aos esforços de prestação de contas de tal conformidade. Para o pequeno e médio empresário, entretanto, a quantidade de obrigações prevista na legislação, combinada com outros aspectos da regulamentação como a intervenção no aspecto tecnológico, pode criar um cenário em que o fardo de estar adequado à lei, mesmo que não inviabilize o negócio, cria resistências da parte do agente econômico a estar de fato conforme.

A preocupação que buscamos expressar aqui é algo que se vê recentemente mesmo no Brasil em relação a sua própria Lei Geral de Proteção de Dados. O agente econômico, pressionado pela legislação, pelo mercado e pelos seus próprios consumidores a se apresentar "conforme", mas não tendo os recursos ou mesmo a disponibilidade necessária para estar materialmente conforme com a lei, acaba optando por uma "conformidade de papel", como se convencionou chamar: o agente econômico pode se munir de todos os documentos, contratos, cláusulas, políticas internas e externas para demonstrar que está em conformidade, mas na prática tais políticas internas não são seguidas, as cláusulas, mesmo assinadas, não são exigidas e os demais documentos são mantidos como mera formalidade, sem que isso altere materialmente o procedimento daquele agente econômico. Apesar de não ser objeto deste estudo avaliar a eficácia e a efetividade de leis sobre proteção de dados, tal tipo de preocupação é, ou de veria ser, de fato relevante para a definição de estratégias regulatórias, o que, em nossa opinião, representa uma clara falha do modelo eclético de proteção de dados.

Por outro lado, temos o que denominaremos como *modelo liberal.* Este inspira-se no dos Estados Unidos, onde há grande recurso à autorregulação e onde o Estado busca interferir ao criar normas apenas em áreas consideradas sensíveis, como saúde, finanças e menores de idade. Nesse modelo, apesar de haver alguma tendência à judicialização, o principal foco é a liberdade de contratação e a possibilidade de o mercado definir, em sua interação com os consumidores, os comportamentos aceitáveis.

O modelo liberal tem como foco três principais aspectos: o grande valor dado à autorregulação e o incentivo à adoção de padrões responsáveis de mercado, a normatização setorial, e a atuação pontual de órgãos administrativos.

No primeiro aspecto é de se destacar que a ausência de leis gerais de proteção de dados não é simples omissão, mas sim estratégia regulatória. Para o modelo liberal, o tratamento de dados pessoais, como tantos outros aspectos da inovação tecnológica, deve ter sua expansão e seu desenvolvimento pautados pelas necessidades do mercado e não pela batuta do regulador. É dizer, sim, que em determinado aspecto da atividade econômica sabe melhor o próprio agente econômico como se portar do que um regulador externo, de modo que se deixa a tal agente econômico a definição de como *deveria* se portar. A solução pode parecer extrema de certos pontos de vista, mas tal escolha nada mais é que uma avaliação valorativa sobre os custos e os benefícios da regulação estatal. Obviamente, não se trata de dizer que a regulação é originariamente algo *negativo* e que não possua benefícios; tampouco se trata de defender que o agente econômico deve ser absolutamente livre de amarras na definição de sua própria conduta e que o ponto de vista do agente econômico será de fato totalmente justo em relação aos interesses envolvidos, sendo suficiente confiar na *consciência* do agente econômico para não adotar comportamentos abusivos. Entretanto, não se trata tampouco de defender que a regulação é sempre necessária e que sem ela os agentes econômicos perseguirão apenas seus próprios interesses sem qualquer consideração para com os direitos básicos dos consumidores.

Em verdade, a linha adotada pelo modelo liberal busca antes um sopesamento entre o desenvolvimento econômico, o valor da regulação específica sobre proteção de dados e o peso que a regulação geral sobre práticas abusivas e enganosas imprime na conduta geral dos agentes econômicos. Isso deduzimos da observação da resistência de tal modelo a adotar leis mais abrangentes e impor obrigações mais detalhadas aos agentes econômicos e de sua – aparentemente contraditória – preocupação com o desenvolvimento de padrões de comportamento abrangentes por vias indiretas, como pelo desenvolvimento da *common law* da FTC.

Em uma visão inicial, parece que o fato de o modelo liberal recorrer largamente à autorregulação e evitar em grande medida a adoção de leis gerais sobre proteção de dados seria incompatível com a imposição de padrões gerais de comportamento dos agentes econômicos no tema da proteção de dados pela via indireta da atuação da FTC, pois esses padrões definidos pela FTC, na prática, funcionam justamente como regras gerais sobre proteção de dados, ainda que não estabelecidas em leis estatutárias. Por que razão então esse modelo se prenderia à autorregulação, se reconhecidas as vantagens de ter regras gerais como as estabelecidas pela FTC?

Como já mencionado, sustentamos que o elemento fundamental de tal equação é justamente o desenvolvimento econômico, na visão do regulador no modelo liberal: o que se quer evitar não são os padrões de comportamento, mas sim a estagnação. Quando o modelo liberal abraça a atuação da FTC mas rejeita as tentativas de aprovação de legislação abrangente o que se quer mostrar é que algum padrão de conduta é possível, mas não há um padrão simples, único ou estático o suficiente que mereça ou sequer possa ser fixado em lei estatutária, pois não só tais padrões de conduta são e devem permanecer volúveis, de acordo com as oscilações do mercado, mas também porque tal definição estatutária poderia ter efeitos deletérios sobre o desenvolvimento tecnológico. Assim, não é verdade que se abandona totalmente a limitação dos comportamentos dos agentes de mercado, mas na análise valorativa concreta é preferível que o comportamento tenha balizas gerais (regras gerais sobre condutas abusivas ou enganosas) e mesmo que certos padrões de conduta sejam aplicados em casos concretos, do que que tal comportamento seja totalmente regulado ao custo do engessamento do desenvolvimento econômico. Em palavras curtas, aceita-se quem o mercado tenha algum espaço para definir como agir, mesmo que isso implique em algumas condutas abusivas ou, ao menos, no limite do que se considera abusivo, em troca de maior espaço para o desenvolvimento econômico e dos próprios padrões de conduta.

O que se percebe entretanto é uma mudança cultural progressiva no que a própria sociedade considera aceitável em termos de privacidade e proteção de dados, razão pela qual mais que nunca as discussões sobre leis gerais de proteção de dados vicejam mesmo no seio do modelo liberal, como vimos no capítulo anterior. As razões dessa mudança e a aproximação entre os modelos liberal e eclético avaliaremos em maior detalhe abaixo.

Em um segundo aspecto, a posição do modelo liberal em relação à legislação estatutária sobre proteção de dados não é uma escolha simplista pela ausência total de regulação. O que se nota do modelo é a escolha significativa feita quanto a *quais dados* e quais *usos* desses dados de fato merecem regulação específica e quais merecem estar submetidos à regra geral da autorregulação. Assim, o legislador parece fazer escolhas absolutamente seletivas e exatas para de fato criar regulação estatal.

Dentre os conjuntos de dados que merecem maior atenção, encontramos os dados de saúde, dados bancários e financeiros, dados de crianças, dados sobre crédito, dados de identificação governamental, dados de cartão de crédito, entre outros grupos a que se reconhece um alto potencial de dano em caso de mau uso. Dentre os usos mais relevantes, encontramos a concessão de crédito, o atendimento em saúde, o uso de dados de crianças em

geral, o fornecimento de serviços bancários, a gestão de dados de identificação governamental (como número de seguridade social), entre outros. Ao combinar conjuntos específicos de dados e usos específicos de dados o legislador busca encontrar as situações que representem o maior risco ao titular dos dados.

Essa regulação setorial, apesar de apresentar omissões notáveis – como no caso de uso de dados de saúde para finalidades não ligadas ao atendimento médico – pode moldar grande parte de seus respectivos setores, uma vez que a fiscalização de um número reduzido de entidades e situações se prova mais simples que a fiscalização de cumprimento de uma lei geral de proteção de dados, por exemplo. Foi assim, por exemplo, que as regras do COPPA passaram a não só ser de grande relevância para o mercado norte-americano mas também ao mercado mundial na definição da linha etária de corte para acesso a serviços online, dada a força de sua aplicação.

Em um terceiro aspecto, o modelo liberal, em razão de sua escolha por uma forma "fraca" de regular comportamentos gerais ao recorrer apenas aos limites gerais aplicáveis a comportamentos abusivos ou enganosos, acaba por depender fortemente da atuação de entidades e órgãos administrativos para garantir tal patamar mínimo de fiscalização e controle. Seria possível incluir aqui também o próprio Poder Judiciário como uma antepara aos atos abusivos que não tenham relevância ou impacto suficiente para serem investigados e tratados pelas autoridades administrativas, mas, como se viu no capítulo anterior, a ausência de um *private right of action* quanto às práticas enganosas e abusivas é geralmente um óbice à maior judicialização na esfera federal, podendo entretanto variar conforme as leis estaduais nesta esfera reduzida.

A atuação da FTC é o exemplo mais relevante de tal tipo de entidade, pelo que se reconhece que a repetição de casos semelhantes perante a FTC e considerando o conteúdo razoavelmente coerente dos seus *consent decrees* têm sido capazes de criar uma *common law* da FTC para a privacidade e para a proteção de dados pessoais. Tal *common law* não tem peso de precedente, como visto, mas concorre para afetar de modo prévio e preventivo o comportamento dos agentes econômicos, uma vez que tal conjunto de *consent decrees* parece indicar ao mercado em geral não só quais práticas são consideradas abusivas e enganosas, mas também quais são os padrões de comportamento esperados pela FTC dos agentes de tratamento em geral.

Obviamente, tal recurso a um órgão centralizado com pouco alcance prático não é livre de críticas. Apesar do número respeitável de casos de *consent decrees* a cada ano, a atuação da FTC ainda fica muito aquém do que um país de dimensões continentais como os Estados Unidos precisa para regulamentar determinado tipo de atividade econômica. A ausência de obrigatoriedade expressa ou vinculação dos "precedentes" criados pela FTC também podem ser objeto de crítica pois deixam tais posicionamentos vulneráveis à mudança de orientação política, trocas na liderança, entre outros fatores de ocasião que poderiam prejudicar a construção da *common law* da FTC.

A ausência de mecanismos abrangentes de *enforcement* talvez seja uma das principais críticas ao modelo liberal, uma vez que o caráter autorregulatório exige maior flexibilidade quanto à definição de padrões de comportamento mas a ausência de leis estatutárias específicas também reduz a eficácia do Estado como ente fiscalizador, limitando as bases pelas quais é possível exigir de um agente econômico certo comportamento, punindo-o caso falhe em adotar a postura adequada. Não é por outras razões que nos projetos de lei avaliados uma grande preocupação foi munir a sociedade de outras armas para combater o uso indevido de dados pessoais, seja pela criação de um órgão dedicado a tais tipos de demandas, como uma autoridade de proteção de dados, seja pela concessão de direitos individuais protegidos por *private rights of action*, permitindo assim aos indivíduos ao menos assumirem o controle sobre as demandas e reclamações que eventual possam ter quanto ao uso de seus dados, levando-as à avaliação do Poder Judiciário.

Essa divisão entre modelo liberal e modelo eclético necessariamente não é fixa e nem sequer exata. Em verdade, é justamente parte do objeto de estudo do presente trabalho a verificação sobre a viabilidade jurídica (mas não necessariamente política) de uma aproximação gradual dos modelos regulatórios em proteção de dados pelo Direito Internacional. Qualquer que seja a resposta a tal pergunta, não fica tampouco descartada a ideia de que os modelos regulatórios existentes podem exercer mutuamente influência uns sobre os outros, gerando mudanças paulatinas que, mesmo na ausência de regras cogentes de Direito Internacional, são capazes de aproximar ou mesmo igualar certos institutos cujas origens são quase que opostas em certas ocasiões.

Não obstante, os modelos identificados nos auxiliam a traçar as linhas gerais da estratégia regulatória de determinado país para a proteção de dados pessoais, refletindo não só as origens dos direitos de privacidade e proteção de dados, mas também a própria cultura

jurídica de determinada sociedade e as soluções práticas e ferramentas fornecidas pelo Direito para fornecer certas garantias fundamentais e apaziguar conflitos.

4.3. Análise comparativa

Feita a análise geral sobre os modelos regulatórios, cabe comparar estes em relação às disposições substantivas sobre proteção de dados que trazem em seu bojo. A título de esclarecimento, neste primeiro momento da análise desconsideraremos o fato de que certos padrões de comportamento, especialmente no modelo liberal, não são instituídos em lei mas de forma mais ou menos coesa pela *common law* da FTC, uma vez que nosso interesse, neste momento, é avaliar o que cada modelo regulatório considera como comportamentos gerais adequados, mesmo que no campo da efetividade de tal regulação haja ainda consideráveis vazios entre os dois modelos.

Além da comparação detalhada a ser realizada, cabe avaliar também os pontos de aproximação e de divergência entre os modelos, de modo a mapear quais os principais pontos sobre os quais o Direito Internacional teria que atuar para poder de fato promover a composição dos sistemas.

4.3.1. Comparação detalhada

O primeiro passo após a análise individual dos modelos regulatórios é realizar uma comparação detalhada, ponto a ponto, entre os dois modelos, de modo a demonstrar de forma completa como tais sistemas podem ser comparados, em que pontos se aproximam e em quais divergem. Em um quadro geral, encontramos:

ANÁLISE COMPARATIVA		
SISTEMAS DE PROTEÇÃO		
TEMA	**UNIÃO EUROPEIA**	**ESTADOS UNIDOS**
Reconhecimento do Direito à Privacidade e à Proteção de Dados	Direito à Privacidade reconhecido legalmente Direito à Proteção de Dados reconhecido legalmente	Direito à Privacidade reconhecido pelos tribunais, limitado por certos aspectos (responsabilidade) mas ampliado em outros (autonomia e liberdade) Direito à Proteção de Dados reconhecido apenas indiretamente pela legislação setorial e pela *common law* da FTC.
Modelo regulatório	Eclético (abrangente)	Liberal (setorial)
Principal fonte de regulação	Estado / União	Autorregulação
Principal ator para aplicação de regras	Autoridades de Proteção de Dados	Federal Trade Comission, Attorney General

Cabe também a comparação sobre a natureza do direito à privacidade e à proteção de dados em geral entre os dois sistemas, visto que pelo até aqui narrado as principais diferenças entre os modelos nascem justamente de tal divergência:

ANÁLISE COMPARATIVA		
NATUREZA		
TEMA	**UNIÃO EUROPEIA**	**ESTADOS UNIDOS**
Direito Fundamental	Direito à proteção de dados pessoais reconhecido como direito fundamental pela Carta de Direitos Fundamentais da U.E. Direito fundamental que inclui (i) princípio da finalidade, (ii) direito de acesso, (iii) direito de retificação e (iv) a fiscalização por uma autoridade independente.	Reconhecimento judicial reiterado de um direito à privacidade de estatura constitucional, mas em estatuto limitado a algumas garantias específicas. Não há reconhecimento da proteção de dados como um direito fundamental.

Natureza do direito	Seguindo a tradição do *civil law*, o direito à proteção dos dados pessoais é considerado um direito da personalidade associado ao direito à privacidade. A proteção de dados pessoais decorre diretamente da inviolabilidade da personalidade e da vida privada do indivíduo. A proteção de dados é, ao mesmo tempo, liberdade pública e direito privado.	Seguindo a tradição do *common law*, o direito à proteção de dados pessoais, apesar de não formalmente reconhecido como direito independente, encontra seu fundamento na inviolabilidade pessoal do indivíduo, especialmente no que diz respeito a sua liberdade e autonomia. A proteção de dados pode ser colocada como um direito acessório, uma decorrência das próprias garantias básicas de liberdade e inviolabilidade física, mental e patrimonial individuais. A proteção de dados, juntamente à privacidade, é essencialmente uma liberdade pública a que os tribunais e os estatutos setoriais reconheceram como um direito privado em casos específicos.

De um ponto de vista objetivo, é necessário também comparar a abrangência de tais sistemas, considerando os dados tratados, os agentes de tratamento e suas atividades respectivas, assim como o próprio território abrangido:

ANÁLISE COMPARATIVA		
ABRANGÊNCIA		
TEMA	**UNIÃO EUROPEIA**	**ESTADOS UNIDOS**
Escopo e aplicação	**Dados pessoais** Toda e qualquer informação que diga respeito a uma pessoa física identificada ou identificável. Geralmente pode dizer respeito a clientes, empregados, prestadores de serviço, sócios e outras pessoas físicas envolvidas na operação. Inclui categorias especiais de dados (dados sensíveis) que, por seu potencial danoso, requerem maior nível de responsabilidade e segurança.	**Personally Identifiable Information (PII)** A legislação estatutária geralmente diz respeito apenas a tipos específicos de dados pessoais (dados de saúde, dados bancários e financeiros, identificação governamental). A prática do FTC abrange todos os tipos de dados pessoais. Dados são sempre relacionados a uma pessoa identificada. Geralmente envolve apenas clientes e consumidores de entidades empresariais (*for profit*). Não há, a princípio, categorias especiais de dados pessoais.

	Atividades cobertas Aplica-se a todo e qualquer tipo de uso de dados pessoais, por qualquer que seja a entidade (empresa, entidade sem fins lucrativos, ou pessoa individual), com exceção das atividades estritamente domésticas.	**Setores cobertos** A legislação estatutária geralmente diz respeito a setores específicos da economia (como hospitais, laboratório, bancos, bureaus de crédito), enquanto a prática da FTC diz respeito a qualquer entidade com fins lucrativos. Regras geralmente não se aplicam a pessoas individuais ou a entidades sem fins lucrativos.
	Setores público e privado Regras se aplicam tanto ao setor público quanto ao setor privado.	**Regras para o setor privado** Regras se aplicam principalmente ao setor público, com exceção de algumas poucas regras direcionadas exclusivamente ao setor público (Privacy Act, ECPA, entre outros).
	Efeitos extraterritoriais Regras almejam qualquer entidade que ofereça bens ou serviços da União Europeia ou que monitore o comportamento de pessoas ali localizadas, independentemente de onde esteja localizado o controlador do tratamento.	**Jurisdição Federal e Estadual** Regras se aplicam ao território estadual ou no âmbito federal, de acordo com a sua natureza. Efeitos geralmente restritos ao território nacional.

Adentrando as regras sobre a prática do tratamento de dados em si, devemos avaliar as hipóteses de tratamento. Como apontado anteriormente, enquanto o sistema europeu apresenta hipóteses claras e fixas que permitem o tratamento e condicionantes expressas, o modelo norte-americano tem conclusões aproximadas em legislação esparsa e na prática da FTC, ainda que existam diferenças essenciais em sua aplicação:

ANÁLISE COMPARATIVA		
HIPÓTESES DE TRATAMENTO		
TEMA	**UNIÃO EUROPEIA**	**ESTADOS UNIDOS**
Princípios	**Princípio da Finalidade** Os dados pessoais só podem ser tratados para finalidades definidas e específicas, conforme tenham sido informadas ao titular dos dados.	**Finalidade e expectativa** Segundo a prática do FTC, tratar dados em desconformidade com as finalidades informadas ao titular seria uma conduta enganosa e abusiva.
	Princípio da Necessidade Apenas os dados pessoais que sejam efetivamente necessários para o atingimento da finalidade do tratamento devem ser tratados.	**Coleta excessiva** Ausência de um princípio ou regra equivalente, apesar de a prática do FTC ter, em casos raros, sustentado a abusividade da coleta excessiva de dados.

	Princípio da Prestação de Contas (Accountability) Obrigação geral de demonstração ativa do cumprimento das obrigações legais sobre proteção de dados.	Prestação de contas em caso de fiscalização Apesar de não haver uma regra geral que determine a prestação de contas ativa, na prática da FTC é comum se exigir que as empresas que sejam fiscalizadas demonstrem o cumprimento das demais medidas de conformidade determinadas pelo órgão.
	Princípio da Transparência O titular deve ser informado e ter acesso a informação clara, completa e concisa sobre o tratamento, tanto de forma prévia ao tratamento quanto de forma contínua.	**Avisos de Privacidade** Diversas leis setoriais como HIPAA, COPPA e GLBA exigem a divulgação de avisos de privacidade que informem o consumidor sobre como seus dados serão tratados. A prática da FTC considera "prática enganosa" o ato de não disponibilizar um aviso de privacidade quando são tratados dados pessoais ou de disponibilizar informação insuficiente.
	Segurança dos Dados Os agentes de tratamento devem adotar todas as medidas de segurança adequadas, técnicas e administrativas, para proteção dos dados pessoais, considerando as circunstâncias do tratamento, o porte do agente, a tecnologia disponível, entre outros critérios.	**Segurança dos Dados** Diversas leis setoriais exigem que seja garantida a segurança dos dados tratados, enquanto algumas, como o HIPAA, trazem regras específicas sobre padrões de segurança mínimos. Na prática da FTC, qualquer tratamento de dados deve garantir padrões mínimos de segurança, avaliados conforme o caso concreto, de modo a fornecer ao consumidor a segurança que se espera de determinado produto ou serviço e para cumprimento das promessas de segurança feitas pelo agente no aviso de privacidade.
Bases legais	**Consentimento** É possível tratar dados pessoais quando o titular dos dados assim autorizar, dando seu consentimento de forma livre, informada e inequívoca, para finalidades específicas. O consentimento deve ser materialmente válido para autorizar o tratamento de dados pessoais, mas não sendo a base legal adequada para todo e qualquer tratamento.	***"Notice and Choice"*** O tratamento de dados em si não precisa, necessariamente, ser autorizado de forma expressa, bastando outros comportamentos que indiquem a concordância do titular com as condições expressas no Aviso de Privacidade (como a contratação de um serviço). Quando possível, no entanto, é recomendável (ainda que não mandatório) fornecer ao titular escolhas significativas sobre o tratamento de dados quando for possível. Não há padrão especificado em lei estatutária sobre quais situações demandam o fornecimento de tal tipo de escolha Algumas leis setoriais, como o COPPA, exigem consentimento expresso (dos pais, no caso) para permitir o tratamento de dados pessoais.

	Execução de contrato É possível tratar dados pessoais quando esse tratamento é necessário para execução de um contrato celebrado com o titular dos dados ou para execução de medidas preliminares à contratação, independentemente da autorização do titular.	**Tratamento de Dados Necessário** Apesar de não haver disposição expressa nesse sentido, uma vez que exige-se dar escolhas ao titular de dados pessoais quando possível (quando o tratamento de dados não seja necessário a ponto de dispensar o consentimento), daí extrai-se também que o tratamento de dados em geral será possível quando for "necessário", o que pode incluir o tratamento necessário para executar um contrato ou cumprir uma obrigação legal, de modo que a proteção de dados não seja óbice ao exercício de uma faculdade ou direito geralmente garantido pela lei, como o desenvolvimento de atividade econômica lícita.
	Obrigação legal É possível tratar dados pessoais quando o tratamento é necessário para o cumprimento de obrigações legais do controlador do tratamento, independentemente da autorização do titular.	
	Exercício regular de direitos É possível tratar dados pessoais quando o tratamento é necessário para o exercício regular de um direito do controlador do tratamento, em âmbito judicial ou administrativo, independentemente da autorização do titular.	
	Legítimo interesse É possível tratar dados pessoais quando o tratamento é necessário para perseguir um interesse legítimo do controlador do tratamento, desde que tal interesse não seja superado pela proteção de direitos e garantias fundamentais do titular. O legítimo interesse é uma hipótese geral de tratamento que busca abranger situações variadas em que seria razoável o tratamento de dados, mas a lei e as autoridades de proteção de dados estabeleceram critérios restritivos sobre tais critérios de razoabilidade, geralmente fundados na expectativa do titular dos dados.	
Fim do Tratamento	**Finalidade definida** O tratamento de dados pessoais deve ter uma finalidade definida que, uma vez atingida, demanda o fim do tratamento de dados pessoais.	**Ausência de regras sobre fim do tratamento** Não há regras, estatutárias ou na prática da FTC, que abordem diretamente o fim do tratamento. Enquanto a existência de uma finalidade para o tratamento é um requisito exigido pela FTC, poderia ser sustentado que na ausência de tal finalidade também não é possível o tratamento,

	Continuidade O tratamento de determinados dados pessoais só pode continuar enquanto houver uma finalidade para tal tratamento e enquanto houver uma base legal aplicável.	mas não há precedente que confirme tal entendimento.

É justamente em relação aos direitos garantidos aos titulares e à forma como é dada tutela a tais direitos em que os modelos possivelmente mais se distanciam, uma vez que enquanto o modelo eclético prevê hipóteses gerais de defesa de direito, no âmbito administrativo e judicial, no modelo liberal as formas de proteção judicial são restritas, enquanto no âmbito administrativo a atuação da FTC, apesar de avançada nas obrigações que vem a reconhecer, tem ainda alcance reduzido.

ANÁLISE COMPARATIVA		
DIREITOS DO TITULAR E TUTELA		
TEMA	**UNIÃO EUROPEIA**	**ESTADOS UNIDOS**
Direitos dos Titulares	**Direito de Acesso** É garantido ao titular o direito de acessar os dados pessoais que são tratados. O direito de acesso é tratado inclusive como direito fundamental.	**Direito de acesso** É garantido ao titular um direito de acessar os dados pessoais tratados por algumas leis setoriais. Na prática da FTC, tal direito deve necessariamente ser concedido, como reflexo dos FIPPs. O direito é garantido também em algumas leis estaduais sobre o tema.
	Direito de Correção É garantido ao titular o direito de corrigir os dados pessoais que estejam desatualizados ou incorretos.	**Ausência de garantia expressa** Não há garantia expressa de um direito à correção dos dados, ainda que tal direito seja considerado como necessário pela FTC, como reflexo dos FIPPs.
	Direito de Eliminação Dentro de certas circunstâncias, é garantido ao titular o direito de solicitar ao controlador o encerramento do tratamento com a eliminação dos dados tratados.	**Direito de eliminação garantido apenas em leis setoriais e leis estaduais** O direito do titular a exigir o encerramento do tratamento e a eliminação dos dados não é tido como um direito geralmente garantido, apesar de haver menção a ele em algumas leis setoriais e leis estaduais como o CCPA.
	Outros Direitos São garantidos ao titular dos dados outros direitos, como o direito de portabilidade, direito de bloqueio, direito de oposição ao tratamento, direito de obter informações adicionais, entre outros.	**Direitos esparsos** A legislação estadual pode prever direitos diversos, entre os quais se destaca o direito a impedir a venda de dados pessoais, previsto no CCPA e em outras leis estaduais.

Proteção administrativa	**Autoridades de Proteção de Dados** O sistema de proteção de dados é fiscalizado especialmente por autoridades de proteção de dados, órgãos governamentais independentes que fiscalizam o cumprimento da lei, arbitram disputas, investigam, aplicam sanções e criam regulamentações específicas para complementar as leis vigentes.	**Órgãos setoriais e a atuação ampla da FTC** Em relação à legislação federal setorial, cada uma delas define uma autoridade específica existente ou diversas para fiscalizar o cumprimento das obrigações constantes de tais leis. No entanto, no contexto do tratamento de dados pessoais em geral, o principal órgão a atuar no campo da proteção de dados pessoais é a FTC, dada sua capacidade de fiscalizar atos *enganosos* e *abusivos* em geral, o que o órgão utiliza para punir empresas que adotem práticas questionáveis em proteção de dados, conforme um *common law* cuidadosamente construído. O alcance de sua atuação, entretanto, é limitado, em razão da limitação de seus recursos e do imenso mercado a ser disciplinado, além de suas outras atribuições na defesa do consumidor e da concorrência.
	Poderes de Investigação As autoridades de proteção de dados são dotadas de poderes de investigação e fiscalização, tanto por iniciativa da própria autoridade quanto por provocação de terceiro, podendo exigir a apresentação de informações e documentos por parte dos responsáveis pelo tratamento.	**Poderes de Investigação** No geral, como parte de seu papel fiscalizatório, a FTC e demais órgãos responsáveis pela fiscalização de leis setoriais possuem poderes de investigação, geralmente garantidos por seus atos de criação.
	Determinação de adoção de medidas Uma vez identificada uma violação ou risco de violação à legislação de proteção de dados, as autoridades de proteção de dados podem determinar administrativamente a adoção de medidas corretivas pelos agentes de tratamento, como atender determinada solicitação de um titular, alterar algum aspecto do tratamento de dados ou mesmo fornecer informações e documentos adicionais para comprovação do cumprimento das leis aplicáveis.	**Autoridades setoriais e a FTC** As autoridades setoriais tem, no geral, poderes para determinar a adoção de medidas. Tais determinações, entretanto, são limitadas ao permitido pelos respectivos atos de criação de cada órgão. Em relação à atuação da FTC, este não tem propriamente o poder de demandar, sozinha, que a empresa adote determinado comportamento, sendo que quando não há um acordo para ajuste de conduta (*consent decree*) firmado entre a empresa e a FTC, esta precisa recorrer ao Judiciário para que este reconheça as violações apontadas e determine a adoção das medidas adequadas para saná-las.
	Sanções Uma vez identificada uma violação da legislação em vigor, podem as autoridades de proteção de dados aplicar sanções administrativas, que podem incluir advertências, alterações na operação, suspensão da operação e mesmo multas pecuniárias.	**Ausência de sanções específicas** Além das ações determinadas por meio de um *consent decree* e de eventuais multas por descumprimento deste, não há propriamente sanções a serem aplicadas pela FTC de modo unilateral.

	Multas Em relação às multas e sanções pecuniárias, estas podem chegar a EUR 20MM ou 4% da receita global anual do grupo econômico, o que for maior.	**Multas da FTC** A FTC pode exigir o pagamento de multas como parte de um *consent decree* e pode inclusive pleitear a aplicação de multas pelo não cumprimento dos *consent decrees*, mas não há realmente um equivalente às sanções administrativas determinadas unilateralmente do modelo europeu.
	Regulamentação As autoridades de proteção de dados têm o poder de aprovar regulamentação adicional que venha a interpretar e complementar as leis em vigor.	**Magnuson-Moss Rulemaking** A FTC pode emitir regulamentações sem a iniciativa do Congresso a partir de suas prerrogativas introduzidas pelo *Magnuson-Moss Warranty Act* de 1975. No entanto, em razão de tal processo ser extremamente burocrático, até o momento não se tem notícia de que a FTC tenha utilizado tais poderes regulatórios para criar normas específicas sobre proteção de dados pessoais.
Proteção judicial	**Possibilidade de recurso ao Poder Judiciário** Independentemente do recurso aos órgãos administrativos, os titulares podem sempre recorrer ao judiciário em caso de violação da legislação vigente sobre proteção de dados.	**Opções limitadas perante o Judiciário** Os titulares de dados, para recorrer ao Poder Judiciário, devem utilizar-se geralmente de um dos quatro *torts* por violação de privacidade: intrusão à privacidade, divulgação de fatos privados, apropriação de imagem e exposição sob falsa luz. Fora de tais hipóteses de responsabilidade civil, raramente os tribunais reconhecem uma obrigação de indenizar por uma invasão genérica à privacidade. Os titulares podem utilizar-se de leis setoriais e leis estaduais para fundamentar uma ação judicial unicamente quando estes preveem um direito privado de ação, o que nem sempre é aplicável. No tocante aos padrões de comportamento abusivos e enganosos fiscalizados pela FTC, geralmente a lei federal e as leis estaduais sobre o tema preveem apenas a iniciativa da própria FTC ou dos *Attorneys General* de cada estado, não sendo geralmente possível iniciar uma ação judicial, individual ou coletiva, de cunho privado, para exigir o cumprimento dos padrões de comportamento geralmente exigidos pela FTC.
	Ações individuais ou coletivas Os titulares podem exercer seus direitos perante o Judiciário de forma individual ou coletiva.	
	Intervenção e atuação consultiva da DPA As autoridades de proteção de dados, além de poderem acionar o Poder Judiciário por sua própria iniciativa em caso de não conformidade de um agente de tratamento a suas determinações, pode também atuar de forma consultiva em qualquer ação judicial em que seja solicitada.	

Por fim, cabe avaliar brevemente as obrigações impostas a cada um dos agentes de tratamento durante o efetivo tratamento dos dados, especialmente as obrigações gerais de segurança, obrigações de prestação de contas e como se dá sua responsabilização por violações.

ANÁLISE COMPARATIVA		
OBRIGAÇÕES DO RESPONSÁVEL PELO TRATAMENTO		
TEMA	**UNIÃO EUROPEIA**	**ESTADOS UNIDOS**
Responsabilidade	**Responsabilidade civil** A responsabilidade civil dos agentes de tratamento é bem definida na legislação aplicável, sendo que o controlador será responsável pela legalidade e legitimidade em geral do tratamento, enquanto o operador é responsável exclusivamente por cumprir com as determinações do controlador e adotar medidas de segurança adequadas.	**Responsabilidade limitada perante o consumidor** As hipóteses de responsabilização de um agente de tratamento perante o titular dos dados, na forma de uma ação judicial, são geralmente limitadas aos *torts* sobre privacidade, que incluem violação de privacidade, apropriação de imagem, divulgação de fatos privados e exposição sob falsa luz. A responsabilidade dos agentes de tratamento por atos que possam ser considerados *abusivos* ou *enganosos* é fiscalizada pela FTC, que pode utilizar-se de *consent decrees* ou de ações judiciais para punir os infratores.
	Agentes de tratamento: controlador/operador Há uma divisão clara entre os tipos de agentes de tratamento, que podem ser controladores ou operadores. O controlador é o agente que determina os meios e as finalidades do tratamento, sendo assim o grande interessado no tratamento de dados pessoais, enquanto o operador atua como mero prestador de serviço, operando apenas conforme as orientações e ordens do controlador do tratamento.	**Tratamento casuístico** Não há distinção, a priori, entre os efetivos responsáveis pelo tratamento e seus prestadores de serviço, sendo a responsabilização definida caso-a-caso de acordo com o peso da responsabilidade de cada parte no caso concreto.
Accountability	**Documentação e inventário de tratamento** Há exigência expressa de manutenção de documentação sobre os tratamentos conduzidos pelo agente de tratamento (usualmente chamado Inventário de Tratamento de Dados), além da documentação sobre outros aspectos relevantes da operação, como decisões de engenharia, decisões sobre quais medidas de segurança adotar, entre outras decisões que demonstrem a correta conduta do agente de tratamento no cumprimento de sua obrigação de prevenir qualquer dano ou violação legal decorrente do tratamento de dados.	**Documentação em Programas de Privacidade** Não há obrigação expressa em lei sobre a adoção de procedimentos de documentação de processamentos e/ou de processos decisórios ou alterações nos tratamentos de dados, apesar de tal prática ser geralmente integrante dos Programas de Privacidade e Segurança adotados largamente pelo mercado como forma de garantir conformidade.

	Relatório de Impacto A legislação exige a condução de relatórios de impacto a proteção de dados (*Data Protection Impact Assessments*) com a finalidade de gerir riscos em certas situações específicas. Em algumas hipóteses (quando houver risco significativo aos titulares de dados), tais relatórios devem ser submetidos à autoridade de proteção de dados para providências, aprovação ou reprovação.	**Reportes à FTC** Não há obrigação legal de reportar aos órgãos fiscalizatórios a existência de processos que impliquem riscos aos titulares dos dados. No entanto, em um cenário de fiscalização ativa em que uma empresa é autuada pela FTC, é comum que as medidas de correção incluam, por período limitado, uma obrigação de reportar à FTC eventuais mudanças nos processamentos de dados conduzidos pela empresa em questão.
	Gestão de riscos Além dos cenários em que são exigidos relatórios de impacto, apesar de não expressamente exigido por lei, é geralmente esperado dos agentes de tratamento que façam a gestão ativa dos riscos de privacidade relacionados ou decorrentes da sua operação, de modo a minimizar eventuais riscos ou prejuízos aos titulares dos dados.	**Gestão de riscos como prática de mercado** Não há obrigação expressa em lei sobre a adoção de procedimentos de gestão de risco, apesar de tal prática ser geralmente integrante dos Programas de Privacidade e Segurança adotados largamente pelo mercado como forma de garantir conformidade.
	Programa de governança Os programas de governança em proteção de dados são a forma como a maioria do mercado escolhe para cumprir de forma contínua suas obrigações sobre proteção de dados, apesar de não haver obrigatoriedade expressa em lei.	**Programas de Privacidade e Segurança** As leis setoriais e estaduais geralmente deixam a critério das respectivas empresas como estas cumprirão suas obrigações. Na prática da FTC, no entanto, é comum que o órgão reconheça a obrigatoriedade de adoção de um Programa de Privacidade ou de um Programa de Segurança como medidas adequadas para garantir a segurança dos dados tratados e evitar abusos.
Segurança	**Obrigações gerais de segurança** Os agentes de tratamento têm uma obrigação geral de adotar medidas de segurança adequadas ao tratamento que conduzem.	**Expectativa de segurança** Todo e qualquer tratamento, de modo a ser considerado justo e não enganoso, deve considerar patamares mínimos de segurança dos dados pessoais tratados.

	Critérios para medidas de segurança Os critérios para se definir que determinado conjunto de medidas é "adequado" são definidos pela lei, incluindo as condições do tratamento e suas finalidades, a tecnologia disponível e o custo de sua implementação.	**Regras setoriais específicas sobre segurança** Alguns setores específicos, como os serviços de saúde e os serviços financeiros e bancários, possuem regras específicas de segurança que exigem que o tratamento de dados se dê de forma segura, com grau variado de detalhamento, sendo a regra de segurança do HIPAA geralmente tida como uma das mais abrangentes e detalhadas na atualidade.
	Notificação de incidentes As leis vigentes estabelecem obrigações gerais de notificação à autoridade de proteção de dados quando o incidente puder representar um risco aos direitos e garantias fundamentais dos titulares dos dados.	**Leis estaduais sobre incidentes** Todos os estados dos Estados Unidos atualmente possuem algum tipo de lei que regula a obrigação de notificar às autoridades competentes (geralmente o *Attorney General* do Estado) a ocorrência de incidentes de violação de dados. Em alguns estados, essa obrigação é limitada apenas a incidentes que envolvem certos tipos de dados (como dados de saúde e financeiros e dados de seguridade social) ou possuem ainda outras limitantes conforme o estado.

4.3.2. Convergências, divergências e globalismo

Até este momento, descrevemos os modelos de proteção de dados sob análise, mas é necessário avaliar *por que* e *como* esses modelos podem ser de fato aproximados pelo direito internacional. O primeiro passo para tanto

Assim, considerando as obrigações materiais relacionadas à proteção de dados entre os diferentes modelos, os pontos comuns, relevantes para a estratégia regulatória, aos dois modelos regulatórios são quatro: (i) a relevância do consentimento; (ii) a obrigação de transparência; (iii) os direitos de acesso, retificação e eliminação de dados; e (iv) as obrigações de segurança e sigilo dos dados pessoais.

Nos dois modelos, o consentimento é tido em alta conta, sendo utilizado como condição para a coleta e para o tratamento de dados. Sem exceção, vê-se o consentimento como fator legitimante da utilização dos dados pessoais, talvez como consequência da ideia de que, seja por uma ótica de direitos da personalidade seja por uma ótica econômica, a vontade do indivíduo é necessária para tornar sua disposição um ato justificado.

Pela ótica econômica, o consentimento é a via pela qual, geralmente, o titular dos dados cede seus dados a fim de obter um benefício (como é o caso de plataformas como Google e Facebook) e aprova os termos pelos quais seus dados serão tratados, com clara remissão à liberdade contratual. Pela ótica dos direitos da personalidade, o interesse do indivíduo em um determinado benefício que lhe permita desenvolver sua própria personalidade é o fator legitimante da disposição de um direito que, normalmente, seria indisponível[252].

O consentimento se manifesta no modelo eclético como uma base legal de tratamento, ou seja, uma hipótese em que a lei autoriza sejam tratados dados pessoais. Apesar de não ser a única base legal, o consentimento é tido possivelmente como a principal delas, de modo a se privilegiar a livre escolha do indivíduo sobre o que é feito com seus dados pessoais como um aspecto importante da autodeterminação informativa.

É também pela grande relevância dada ao consentimento e, provavelmente, pelas largas possibilidades de abuso pelos agentes de tratamento de tal base legal que a legislação estabelece requisitos estritos para sua aplicação legítima. Em outras palavras, o consentimento, para o modelo eclético, deve ser dado de forma efetivamente livre, após o recebimento pelo titular das informações adequadas para que sua decisão seja de fato uma decisão informada, e seja tal consentimento dado para finalidades claras e específicas, sem que se possa recorrer a autorizações genéricas que não definam como e para que os dados pessoais serão utilizados.

Já no modelo liberal, como já foi dito, a *escolha* do titular dos dados pessoais é fator essencial dos FIPPs, sendo o consentimento do titular dos dados exigido também em legislações específicas quanto a certos tipos de tratamento. No entanto, no modelo liberal o consentimento acaba por se tornar quase uma ficção jurídica: na maioria dos casos, aceita-se o consentimento implícito do titular (como no caso dos tratamentos baseados em uma oportunidade de recusar o tratamento, mas com a presunção de aceitação – o mecanismo

[252]Há alguma discussão na literatura sobre a (in)disponibilidade da privacidade, principalmente quando enquadrada como direito da personalidade. No Brasil, especificamente, esse seria um direito indisponível, segundo o texto frio da lei. Obviamente, a interpretação evoluiu para acomodar a grande disparidade entre o que parece ser uma proibição absoluta e a prática comum. Confira-se: "Em uma série de situações não previstas em lei, mas socialmente admitidas, as pessoas desejam e aceitam limitar, pontualmente, o exercício de algum atributo da própria personalidade. O escritor que concede uma entrevista, revelando ao público detalhes da sua vida particular, deixa de exercer, naquela situação específica, seu direito à privacidade. Tal limitação, derivada da vontade do titular, não deve a toda evidência ser reprimida pela ordem jurídica, porque a vontade individual aí não se opõe, mas se dirige à realização da dignidade humana daquele indivíduo." SCHREIBER, Anderson. *op. cit.*, p. 27.

conhecido como *opt-out*), e em outras o consentimento a um determinado contrato ou política de privacidade é tido como simples elemento para vincular o agente econômico a determinadas promessas ou obrigações assumidas perante o titular, sem que se exija um maior grau de liberdade ou informação para que o consentimento seja de fato válido.

Além disso, o consentimento, apesar de ser utilizado, de certa forma, como uma base legal a legitimar o tratamento de dados, em diversas circunstâncias o consentimento, melhor traduzido como *escolha,* é utilizado como uma faculdade do titular de decidir sobre certos aspectos do tratamento, mesmo que não sobre autorizar ou não o tratamento em geral. Assim, apesar de aproximados nesse aspecto, o consentimento se manifesta de diferentes formas nos dois modelos, como ficará mais claro adiante.

O segundo ponto em comum diz respeito à obrigação de transparência dos responsáveis pelo tratamento de dados pessoais ou a um direito reflexo a obter informações sobre o tratamento. Apesar de haver diferenças nos dois modelos, ambos preveem a necessidade de se fornecer ao titular dos dados algumas informações básicas antes do início do tratamento de dados.

Mesmo nos Estados Unidos, onde não há uma norma específica para proteção de dados, a maioria das normas setoriais e também as normas de proteção ao consumidor[253] trazem obrigações sobre as informações que serão repassadas ao titular dos dados, logo no primeiro contato, as chamadas *privacy notices.* Nas normas setoriais, tal obrigação de informação é relativamente clara e objetiva, mas há certa discussão sobre a obrigatoriedade de tal fornecimento de informação no cenário geral, submetido aos padrões estabelecidos pela FTC.

Isso porque a FTC, historicamente, utiliza-se justamente das *privacy notices* como base de promessas feitas por uma empresa a seus consumidores contra a qual compara as práticas efetivas da empresa para um primeiro teste sobre serem suas práticas, no mínimo, de acordo com as informações fornecidas ao consumidor ou se a *privacy notice* de fato é enganosa. O problema aparente ocorreria justamente quando a empresa *não divulga* um

[253]Como *Gramm-Leach-Bliley Act* (1999) UNITED STATES. Federal Trade Commission - FTC. *Gramm-Leach-Bliley Act* (1999) Disponível em: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf, *Fair Credit Reporting Act* (1970) UNITED STATES. Federal Trade Commission - FTC. *Fair Credit Reporting Act* (1970). Revised September 2018. Disponível em: https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf, e *Fair and Accurate Credit Transactions Act* (2003) UNITED STATES. Federal Trade Commission - FTC. *Fair and Accurate Credit Transactions Act of 2003*. Disponível em: https://www.congress.gov/108/plaws/publ159/PLAW-108publ159.pdf.

privacy notice, pois a FTC, em tese, não teria uma base pela qual avaliar se uma afirmação é abusiva ou enganosa pois não há propriamente uma afirmação (um *privacy notice*). Apesar disso, alguns casos recentes[254] demonstram que apesar de a FTC desenvolveu o entendimento de que a ausência de informação pode sim ser considerada uma conduta enganosa, uma vez que coletar dados e/ou fornecer "escolhas" ao titular dos dados sem prover informações a ele exige que o titular dos dados escolha fornecer ou não seus dados, contratar ou não determinado serviço, sem que tenha todas as informações relevantes para decidir, induzindo-o a erro.

No modelo eclético, essa obrigação de fornecer informação pode se manifestar de algumas formas diferentes. O direito à informação é geralmente consubstanciado em uma obrigação de fornecer informação *antes* do início do tratamento de dados pessoais. Não há propriamente um formato específico em que tal informação deva ser passada, mas esse tipo de modelo geralmente adota algumas qualificantes para a informação, que geralmente deve ser clara, acessível e concisa. Mesmo que não haja um formato prescrito, a prática comum veio a adotar o formato dos avisos ou declarações de privacidade, à semelhança do modelo liberal, provavelmente inclusive em razão deste, dada a centralidade do mercado norte-americano no desenvolvimento do mercado da internet na década de 1990.

Não obstante, o modelo eclético vai além da simples obrigação de fornecer informações. Além de fornecer algum tipo de aviso de privacidade, esse aviso de privacidade geralmente deve possuir informações mínimas sobre o tratamento de modo a garantir um certo padrão no fornecimento dessas informações. É assim, por exemplo, que o GDPR exige que o aviso ou declaração de privacidade contenha dados sobre a identidade do controlador e seus canais de contato (inclusive o contato do seu encarregado de proteção de dados), os propósitos do tratamento, quais dados serão coletados e tratados, as bases legais utilizadas para o tratamento de dados, os destinatários dos dados (caso estes sejam compartilhados com terceiros) e o fato de estarem ou não tais dados sujeitos a transferências internacionais, além de informações sobre os direitos garantidos ao titular dos dados e a forma de exercê-los (se por um canal específico ou mediante algum tipo específico de solicitação, por exemplo).

Mais que isso, o princípio da transparência e os direitos do titular exigem também que o controlador forneça informações adicionais ou complementares sobre o tratamento quando assim solicitado pelo titular dos dados, de modo que a obrigação de transparência

[254]Confira-se SOLOVE, Daniel; HARTZOG, Woodrow. *op. cit.*, p. 634-636.

não se exaure pela simples apresentação de um aviso de privacidade, devendo ser cumprida continuamente para fornecer ao titular informações sempre completas.

Em terceiro lugar, os dois modelos avaliados garantem alguns direitos básicos ao titular dos dados, entre eles o de acesso aos dados em tratamento e o de retificação ou eliminação, a depender do ato cabível.

Em relação ao modelo eclético, o direito de acesso é de suma importância para sua estratégia regulatória, uma vez que parte significativa da tutela reside na fiscalização pelo próprio titular dos dados. O direito de acesso consiste, talvez, no instrumento mais relevante de tais sistemas, pois permite o exercício dos demais direitos como de retificação, oposição, eliminação e contestação de decisões automatizadas – um assunto que adquire cada vez mais importância com os avanços em contratos eletrônicos e inteligência artificial. No sistema europeu, especificamente, os direitos de acesso e retificação são inclusive expressamente reconhecidos como direitos fundamentais, parte de um direito à proteção de dados mais amplo, dada sua importância para o modelo regulatório adotado.

Na prática os direitos de acesso, retificação e eliminação representam uma forma direta de controle do titular dos dados, mas também uma forma de controle sobre a legalidade do tratamento e sobre a conformidade da operação de determinado controlador de dados às normativas aplicáveis, uma vez que a resposta incorreta a uma tal solicitação permite ao titular produzir prova suficiente para levar o caso a uma autoridade de proteção de dados para que esta avalie se tal resposta foi adequada e, caso não o seja, se o controlador de fato está em conformidade com as leis aplicáveis.

No modelo liberal, tais direitos foram primeiro sugeridos nas diversas iterações dos FIPPs, começando a ser efetivamente garantidos por leis estaduais, leis federais setoriais e pelo desenvolvimento do *common law* da FTC. Apesar de seus contornos não serem homogêneos nesses diferentes regimes, sua garantia é também ponto central de alguns projetos de lei que almejam dotar os Estados Unidos de uma lei geral de proteção de dados, demonstrando a preocupação do legislador com tais aspectos da proteção de dados.

De forma indireta, é também através do exercício de tais direitos que o titular de dados pode buscar a satisfação de seus direitos ou ao menos uma resposta escrita do controlador do tratamento para buscar as autoridades competentes para realizar uma eventual denúncia. Naturalmente, pelas próprias limitações operacionais da FTC e das autoridades estaduais, nem toda denúncia terá necessariamente efeitos práticos, mas a previsão de

criação de uma autoridade nacional de proteção de dados em alguns projetos de lei também indica a preocupação do regulador em estabelecer um órgão capaz de lidar com tais denúncias de forma sistemática e constante.

O último ponto comum digno de nota diz respeito à segurança e ao sigilo dos dados pessoais, e demais obrigações de cuidado relacionadas ao tratamento de dados pessoais. Como notado em nossa análise, os dois modelos estudados exigem, em alguma medida, tanto medidas técnicas quanto físicas e administrativas ou organizativas para resguardar os dados pessoais.

No modelo eclético, as obrigações de segurança e conformidade resultam em obrigações abrangentes – e muitas vezes pouco definidas – de adoção de *medidas adequadas*. A indefinição de tal termo é reduzida pelos critérios estabelecidos para que se avalie na prática o que seria *adequado*, uma vez que se considere, por exemplo, a disponibilidade de determinada medida ou tecnologia, seu custo de implementação, e as próprias características do tratamento de dados pessoais (por exemplo, se são tratados apenas dados comuns ou se são tratados dados sensíveis ou de categorias especiais, na dicção do GDPR).

Assim, não há uma receita específica para o que seriam consideradas medidas adequadas, devendo cada operação adotar um conjunto personalizado de medidas com base em sua realidade operacional e os riscos nela envolvidos. Desse modo, o que busca na realidade a legislação é estabelecer um sistema efetivo de *gestão de riscos:* não se obriga determinado controlador a garantir em absoluto a inviolabilidade dos dados, mas sim que os riscos inerentes à sua operação sejam devidamente tratados, sem que isso signifique a adoção de medidas de extremo cuidado que não sejam absolutamente exigidas pelo nível de risco da operação.

Ainda, em termos mais simples, o que busca a legislação não é a simples implementação de algumas medidas técnicas como criptografia e autenticação, mas sim geralmente a criação de um programa de gestão de riscos que avalie os riscos existentes e prescreva (e adote) medidas para endereçar esses riscos, sejam elas técnicas (como criptografia, autenticação e outras tecnologias de detecção ou prevenção de invasões ou vazamentos) ou administrativas (como estabelecer regras internas sobre segurança da informação, estabelecer quais empregados podem acessar determinados tipos de dados, ou ter procedimentos específicos para situações como vazamentos de dados). Esse objetivo é

geralmente reconhecido pela prática de proteção de dados, ainda que não esteja expresso na legislação aplicável.

Já no caso do modelo liberal, esse objetivo é um pouco mais claro, mesmo que não seja definido pela legislação e sim pela *common law* da FTC. O órgão já reconheceu como necessária a prática de estabelecer programas de segurança e privacidade para correta proteção dos dados pessoais, que podem incluir avaliações de risco, treinamento de empregados e divisão de responsabilidades pela segurança do tratamento, de modo a cumprir as promessas de segurança geralmente presentes em avisos ou declarações de privacidade.[255]

Devemos no entanto não apenas apontar as semelhanças e pontos de convergência, mas também os aspectos nos quais os dois sistemas de proteção de dados se afastam e diferem. As principais divergências entre os sistemas da União Europeia e dos Estados Unidos são demonstradas em quatro áreas, nominalmente (i) a natureza e a origem do direito, (ii) as limitações quanto à possibilidade de tratar dados em si, (iii) os direitos garantidos ao titular e a forma de sua tutela, e (iv) a forma e a eficácia da fiscalização no cumprimento das leis sobre proteção de dados.

Quanto ao primeiro ponto, parece bastante claro que as diferentes origens do direito à privacidade e do direito à proteção de dados constituem uma divergência fundamental que dificulta em muito uma aproximação total entre os sistemas de proteção de dados. Defendemos, entretanto, que essa divergência pode ser contornada, uma vez que a simples diferença na origem do direito não impediu que a *common law* da FTC e a prática comum na União Europeia viessem a adotar mecanismos muito semelhantes para o cumprimento da legislação vigente sobre proteção de dados pessoais.

A diferença na natureza dos direitos acabar por ter efeitos profundos em como tais direitos são construídos pela doutrina e pela jurisprudência, dificultando em muito sua aproximação do ponto de vista teórico, dado que o direito internacional, em muitos aspectos, seria incapaz de alterar, em uma abordagem impositiva, como determinada cultura jurídica entende determinado instituto jurídico e confere a ele valor. Essa dimensão teórica, no entanto, não é absoluta, uma vez que não impede que materialmente haja equivalência entre os efeitos práticos de suas disposições. Isto é, mesmo que a natureza dos direitos seja divergente na origem, o efeito prático de tais direitos e seu desenvolvimento efetivo pode gerar para os agentes de tratamento obrigações razoavelmente equivalentes. Considerando

[255]SOLOVE, Daniel; HARTZOG, Woodrow. *op. cit*., p. 617-618.

que nosso objetivo é encontrar compatibilidade (espaço para convergência) e equivalência prática, e não similitude absoluta, a divergência quanto à natureza do direito não deve ser um óbice absoluto ao nosso objetivo.

Em um segundo ponto, temos as limitações quanto à possibilidade de tratar dados pessoais em si, que diferem nos dois sistemas provavelmente em razão da própria natureza dos direitos de privacidade e proteção de dados. Como já visto, enquanto na União Europeia encontramos hipóteses específicas que autorizam o tratamento de dados pessoais, como o consentimento, a execução de um contrato ou o exercício regular de um direito, nos Estados Unidos não há uma regra expressa que exija uma "razão juridicamente aceita" para permitir o tratamento de dados pessoais. Apesar de o consentimento ser tido como uma prática geralmente recomendada, ele ainda é dispensável quando se considere que o tratamento é "necessário". Pode-se estabelecer um paralelo entre o "necessário" e as hipóteses de dispensa do consentimento da União Europeia: em resumo, essas hipóteses tentam ilustrar as principais situações em que o tratamento é de fato "necessário" e independe (ou não é possível recorrer ao) do consentimento do titular dos dados. Assim, a categoria de tratamento "necessário" do sistema norte-americano equivaleria, de modo genérico, às hipóteses fechadas da União Europeia, ainda que haja uma diferença considerável entre ter hipóteses especificadas dentro do que é considerado "necessário" e permitir o tratamento que simplesmente se considerar "necessário", sem nenhum critério para fazer tal avaliação.

O grande problema aqui parece ser que mesmo que indiretamente se obtenha a noção de que o tratamento de dados é possível quando seja "necessário" ou "justificado", não há regra expressa que dite tal norma, sendo ela uma indução dos diversos casos práticos julgados pela FTC e não uma regra posta. Como consequência disso, no direito norte-americano não há critérios postos para determinar quando se pode dizer que um tratamento é de fato "necessário" ou "justificado", ficando tal análise relegada ao controle casuístico pós-fato, o que gera considerável insegurança jurídica.

Em um terceiro ponto, encontramos a garantia de direitos e a forma de sua tutela. Podemos discutir aqui os direitos efetivamente garantidos, que são muito mais extensos na União Europeia do que nos Estados Unidos, incluindo direitos acessórios como o direito de oposição e o direito de portabilidade, mas nosso real interesse nesse ponto é entender as diferenças fundamentais em como um titular de dados pode defender seus dados e seus direitos em cada jurisdição.

Na União Europeia, como já vimos, os direitos garantidos pela legislação podem ser reclamados pelo indivíduo perante as autoridades de proteção de dados, em via administrativa, ou diretamente perante o Poder Judiciário. Assim, qualquer descumprimento da legislação aplicável pode ser objeto de uma ação judicial individual ou coletiva, desde que atinja aquele indivíduo ou coletividade de alguma forma. Em relação à atuação das autoridades de proteção de dados, estas geralmente atuam individualmente sobre cada reclamação, que tem o peso propriamente um procedimento administrativo individual. Em outras palavras, a autoridade deve atuar sobre cada pedido individualmente, não sendo esses meras denúncias sobre as quais a autoridade pode escolher atuar ou não.

Tal panorama difere em grande medida da realidade encontrada nos Estados Unidos: apesar de garantidos certos direitos na legislação esparsa e reconhecidos direitos básicos pela prática da FTC, a violação de tais direitos geralmente pode ser objeto de denúncias aos órgãos de controle, mas é prerrogativa destes atuar ou não sobre tais denúncias, podendo a FTC, por exemplo, conduzir investigação preliminar sobre determinada denúncia e decidir que não é viável iniciar um processo completo de investigação que culminaria na proposta de um *consent decree* para a empresa infratora. Do mesmo modo, os titulares só podem acessar o Poder Judiciário, especificamente, quando tiverem um *private right of action,* que deve ser previsto expressamente na legislação para que possa o titular reclamar pela violação das leis aplicáveis. Caso contrário, a iniciativa para judicializar a questão permanece exclusiva dos órgãos de controle e fiscalização, tendo o titular de dados a sua disposição apenas os *torts* genéricos de privacidade para buscar algum tipo de compensação pelos danos sofridos.

Tal ponto de divergência é talvez um dos principais e mais difíceis de se contornar, uma vez que depende diretamente da legislação local. Não obstante, é papel do Direito Internacional buscar a composição de tais *gaps* para aproximar os dois sistemas, como veremos adiante.

Ainda, em um último principal ponto de divergência, temos a forma como é feita a fiscalização do cumprimento das leis de proteção de dados pessoais, questão naturalmente entrelaçada com a própria forma de tutela dos dados pessoais.

Como já colocamos, no sistema de proteção da União Europeia, a fiscalização é realizada primariamente por órgãos administrativos independentes chamados autoridades de proteção de dados, em termo genérico. Tais entidades possuem amplos poderes de

investigação e fiscalização, podendo exigir a apresentação de informações e documentos e conduzir inquéritos para investigar alegações de conduta contrária as leis aplicáveis. Além disso, tais entidades possuem poderes sancionatórios que podem resultar na aplicação de advertências ou restrições à operação do infrator em relação ao processamento de dados, determinação de adoção de medidas específicas ou alterações no processamento, ou mesmo na aplicação de altas multas em razão das violações constatadas.

Tais entidades atuam com base em iniciativa própria mas também por solicitação do titular, que pode sempre registrar uma reclamação perante a autoridade competente para que esta atue inicialmente como mediadora do conflito com o agente de tratamento em questão. Em sua própria iniciativa, pode a autoridade iniciar procedimentos de investigação e sancionamento, além de atuar consultivamente, perante tribunais e outros órgãos públicos, e de emitir regulamentações às regras colocadas na legislação aplicável, buscando detalhar tais normativas.

A abrangência da atuação das autoridades de proteção de dados é ampla, visto que é exigido que sejam dotados de recursos suficientes a sua própria autonomia e independência de outros órgãos e poderes, além de dedicar-se inteiramente ao tema da proteção de dados pessoais.

No sistema norte-americano, por outro lado, encontramos órgãos que recebem competência pontual para fiscalizar a aplicação de certas leis, como é o caso do Consumer Financial Protection Bureau em relação ao FCRA e do *Office for Civil Rights* do *U.S. Department of Health and Human Services* em relação ao HIPAA, além da competência mais abrangente da FTC quanto ao FTCA e alguns outros diplomas legais como o COPPA.

Tais competências fiscalizatórias são conferidas a entidades que não são propriamente independentes mas sim que possuem outras atribuições e competências, estando por vezes ligadas a outros ramos do governo. Essas agências e órgãos, em sua maioria, em razão disso, não possuem especialização na matéria, tendo sua atuação restrita pelos recursos dedicados especificamente a tal ramo de suas atribuições. Esse aspecto de sua atuação é especialmente notável no caso da FTC, considerando a imensa responsabilidade de zelar não apenas por questões de proteção de dados pessoais, como também por todos os outros assuntos relacionados a atos de comércio abusivos e enganosos, proteção do consumidor e proteção da livre concorrência. Apenas a título comparativo, por mais que se possam tecer críticas à estratégia administrativa do governo brasileiro, enquanto os Estados

Unidos contam com a FTC para esses três temas, temos três órgãos diferentes para cuidar deles no Brasil: o Conselho Administrativo de Defesa Econômica (CADE) a Secretaria Nacional do Consumidor (SENACON) e a Autoridade Nacional de Proteção de Dados (ANPD).

Um aspecto adicional que intensifica a significância de tal divergência advém do fato de que enquanto na União Europeia pode o titular recorrer diretamente ao Poder Judiciário caso assim deseje ou caso a resposta da autoridade de proteção de dados não seja efetiva, no caso dos Estados Unidos tal via não é franqueada a qualquer um, mas apenas a titulares que possuam, inscrito em uma lei setorial específica, um *private right of action*, ficando então a maioria dos titulares sujeitos à seletividade da FTC quanto às denúncias que escolhe de fato investigar e iniciar o procedimento para celebração de um *consent decree*.

Analisando os pontos de convergência e as origens do direito à privacidade, nota-se que a convergência dos sistemas em alguns pontos não parece exatamente um desenvolvimento natural, considerando a linha de argumentação para a fundamentação de tais direitos, especialmente nos Estados Unidos. Nesse ponto, argumentamos que alguma influência de um modelo a outro existiu e existe, apesar das distâncias transcontinentais, o que explicamos justamente pela concretização do defendido por Nye e Keohene no tema do globalismo.[256]

Os autores defendem justamente que há relações entre Estados que se baseiam em uma rede de interdependências, criando o que se convencionou chamar de globalismo. Por tais relações, é possível que o globalismo atue em diversas esferas, como as esferas econômica, social e cultural e mesmo tecnológica.[257] Tal análise, inerente às relações internacionais, ainda que separada da análise jurídica conduzida neste trabalho, nos auxilia a entender *por que* tal aproximação é sentida.

Ora, é fato que nas últimas duas décadas, com o crescimento desenfreado da Internet, os laços econômicos e sociais entre Estados Unidos e União Europeia em muito se estreitaram: no aspecto econômico, enquanto é certo que os Estados Unidos são um polo de inovação tecnológica, sendo sede de grandes empresas de tecnologia, essas mesmas empresas vêm no mercado europeu um mercado qualificado, dado o poder aquisitivo de sua

[256]KEOHANE, Robert O.; NYE, Joseph S. Power and interdependence in the information age, *cit.*, p. 81-85.
[257]KEOHANE, Robert O.; NYE, Joseph S. Globalization: what's new? what's not? (and so what?), *cit.*, p. 106-107

população; enquanto a própria Europa é um centro de exportação de tecnologia e cultura, resultando em largo intercâmbio entre as duas sociedades.

Em razão dessas múltiplas relações de mútua influência, a preocupação da sociedade em geral e sua consciência sobre temas como vigilância e privacidade têm despontado, impulsionados especialmente por escândalos de espionagem e vigilância estatal velada, como aqueles denunciados por Snowden. No entanto, apesar de se poder argumentar que os protestos gerados por tais escândalos[258] foram tanto causa como consequência da aproximação ideológica no campo da privacidade entre os dois mercados, o simples fato de que Estados Unidos e União Europeia são polos tecnológicos e econômicos, na teoria de Nye e Keohene, já seria suficiente para gerar efeitos nos dois mercados.

Nos últimos anos, no entanto, essa influência, especialmente da União Europeia para os Estados Unidos, foi mais sentida e discutida pelos operadores do direito, com a publicação de inúmeros artigos e textos de opinião defendendo a adoção pelos Estados Unidos de uma lei geral de proteção de dados,[259] buscando aproximá-los do modelo eclético. Inclusive, os desenvolvimentos narrados ao longo deste trabalho, especialmente quanto à *common law* da FTC e os projetos de lei dos Estados Unidos que implementariam direitos individuais, obrigações para os controladores dos dados ou mesmo criariam uma autoridade de proteção de dados dedicada, podem ser tidos como consequências da aproximação paulatina dos dois modelos.

A simples interação econômica e social, entretanto, não nos parece uma explicação satisfatória para por que tais modelos teriam se aproximado nos últimos anos, uma vez que teria sido necessário alguma forma de manifestação jurídica para iniciar tais processos. Avaliando a linha do tempo da evolução dos dois modelos e sobrepondo-a ao desenvolvimento do Direito Internacional no tema da proteção de dados pessoais nos mostra que possivelmente nenhum tipo de aproximação teria se concretizado não fossem os esforços e os desenvolvimentos do Direito Internacional. Antes de adentrar tal campo, entretanto,

---

[258]THOUSANDS gather in Washington for anti-NSA 'Stop Watching Us' rally. *Support the Guardian.* Disponível em: https://www.theguardian.com/world/2013/oct/26/nsa-rally-stop-watching-washington-snowden.

[259]Como exemplo, confira-se BRYANT, Jennifer. *2021 'best chance' for US privacy legislation*. Disponível em: https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation/ e AMERICA, Your Privacy Settings Are All Wrong. Using an opt-in approach will help curb the excesses of Big Tech. *The New York Times*, Mar. 06, 2021. Disponível em: https://www.nytimes.com/2021/03/06/opinion/data-tech-privacy-opt-in.html e MCCABE, David. Congress and Trump Agreed They Want a National Privacy Law. It Is Nowhere in Sight. *The New York Times*, Oct. 1, 2019. Disponível em: https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html.

cabe considerar quais exatamente são os espaços a serem preenchidos, ou seja, se e onde existem espaços para convergência entre os sistemas.

4.4. Compatibilidade: espaços para convergência

Ao analisar os sistemas de proteção de dados da União Europeia e dos Estados Unidos em detalhe, podemos concluir que apesar de haver pontos de divergência, há também espaço para convergência. Quando consideramos dois sistemas a serem compostos e conciliados pelo Direito Internacional, devemos primeiro avaliar se tal composição é possível, pelo que propomos a ideia de "compatibilidade de sistemas".

Defendemos a ideia de que dois sistemas serão compatíveis e podem ser compostos, aproximados, conciliados pelo Direito Internacional não apenas quando haja pontos de convergência entre eles, mas principalmente quando haja *espaço* para convergência. Em outras palavras, os sistemas analisados devem apresentar não só semelhanças, mas condições favoráveis para que mudanças pequenas e/ou progressivas permitam a aproximação funcional de institutos jurídicos, sem que isso seja obstado por características próprias e fundamentais de um dos sistemas estudados.

Tal ideia poderia passar a impressão de que tais espaços para convergência seriam identificados apenas em aspectos secundários dos institutos jurídicos, aqueles cuja mudança pouco significaria para o sistema estabelecido em si, mas como percebemos pela comparação dos sistemas dos Estados Unidos e da União Europeia quando avaliamos suas regras para proteção de dados, tais espaços para convergência podem ser encontrados mesmo em aspectos inicialmente tidos como fundamentais de um determinado sistema.

A ideia de compatibilidade também não traz necessariamente em si uma ideia de equidade entre os sistemas, não havendo a necessidade de que os dois se encontrem no meio do caminho. É sempre possível que, a depender das relações políticas, sociais e econômicas entre os dois sistemas analisados, haja uma tendência a que a solução final de composição privilegie uma ou outra posição. Não obstante, é necessário sempre um esforço mútuo com compromissos bilaterais, ainda que nem sempre equivalentes.

Quando analisamos os sistemas de proteção de dados da União Europeia e dos Estados Unidos notamos quatro domínios em que parece haver espaço para convergência:

(i) hipóteses gerais para autorização do tratamento e princípios gerais para limitação da coleta e uso de dados, (ii) garantia de direitos básicos aos titulares, (iii) garantia de transparência sobre o tratamento, e (iv) garantia de meios efetivos de resolução de disputas.

Quanto ao primeiro ponto, já vimos que nos dois sistemas há alguma predisposição para recorrer ao menos ao consentimento como base legal geral para autorizar o tratamento de dados pessoais: como coloca o princípio da *escolha,* cabe ao titular dos dados escolher, sempre que possível, se e como se dará o tratamento dos seus dados pessoais. É verdade, entretanto, que as tendências libertárias do sistema norte-americano geralmente buscariam um cenário em que o tratamento de dados não é a priori limitado de acordo com hipóteses autorizativas pré-definidas, mas sim que a limitação seja a exceção e não regra. Não obstante, o sistema norte-americano reconhece também os conceitos da limitação da coleta e a prática da FTC já definiu em certos casos que a coleta não pode ser abusiva.

Mesmo que não caiba aqui o estabelecimento de hipóteses limitadas sobre situações em que o tratamento é permitido, é possível sim considerar ao menos um teste de legitimidade para o tratamento para definir se este é feito dentro do parâmetro da *necessidade* e que tal necessidade só dispense o consentimento quando este não seja propriamente *adequado.* Assim, o que se propõe em realidade é estabelecer uma regra de conduta que emula os efeitos limitantes do rol de bases legais do sistema da União Europeia, mas que em verdade deixa o estabelecimento de qual tratamento é legítimo ou não para um sopesamento caso-a-caso.

De um outro ponto de vista, o estabelecimento de um rol taxativo de hipóteses autorizativas nada mais é que a aplicação de um determinado raciocínio jurídico de quais elementos valorativos tornam um tratamento lícito, legítimo, ou não. Se a liberdade do modelo norte-americano exige espaço para a inovação, cabe liberar certas amarras de forma contida: não haveria um rol taxativo de bases legais de tratamento, mas o tratamento só seria possível quando atendesse certos critérios, quando fosse aprovado por um determinado teste lógico, o mesmo teste lógico utilizado pelo legislador europeu quando estabeleceu o seu rol taxativo. A sistemática de avaliação e proteção de valores assim permaneceria a mesma, mas se atribuiria nova responsabilidade ao controlador, qual seja, ser capaz não de apontar para uma lista e indicar sobre qual base legal se apoia, mas de justificar, por tal teste lógico, o tratamento de dados conduzido.

O teste lógico proposto seria composto de três fases. Em primeiro lugar, as finalidades do tratamento de dados devem ser lícitas (não vedadas por lei) e legítimas tanto em relação ao controlador dos dados (condizentes com as atividades e objetivos centrais de determinada entidade, como seu objeto social e com interesses que sejam compatíveis com sua atuação), quanto em relação ao titular dos dados (finalidades minimamente compatíveis com a expectativa de privacidade desse titular). Este primeiro teste é eliminatório e uma negativa em tal fase do teste representaria uma proibição absoluta ao tratamento de dados em questão. Tal proposta é compatível tanto com o sistema europeu quanto com a prática da FTC nos Estados Unidos, em que é possível considerar determinado tratamento ilegítimo por ser ilegal.

Em segundo lugar, o tratamento deve ser necessário para atingir tal finalidade lícita. Caso o tratamento proposto se utilize de dados excessivos ou seja possível adotar um processo que não envolva o tratamento de dados pessoais, deve-se dar preferência a tal via. Tal proposta é também suportada pelos dois sistemas, pois, pelo lado da União Europeia, reflete o princípio da necessidade e minimização de dados, enquanto pelo lado dos Estados Unidos toca o tema do design abusivo e das configurações padrões ilegítimas; adicionalmente, não encontramos no sistema norte-americano razão de cunho *jurídico* que impeça necessariamente tal proposta. Este teste teria também um caráter eliminatório, caso o tratamento de dados não seja necessário, fica ele igualmente proibido.

Em terceiro lugar, o teste proposto teria que verificar se solicitar o consentimento do titular dos dados é medida *adequada*. Como regra geral no sistema europeu a escolha de uma base legal para fundamentar um tratamento de dados não decorre de uma simples escolha, mas sim de avaliar a real compatibilidade do mecanismo de tal base legal ao caso concreto. Assim, por exemplo, quando um tratamento de dados é *necessário* para executar um contrato (sem o tratamento de dados o contrato não pode ser cumprido), é inadequado utilizar o consentimento como base legal, uma vez que, por exemplo, tal consentimento não seria realmente livre (pois sua recusa causaria a rescisão do contrato) e não seria possível de fato garantir o direito à revogação do consentimento sem outras consequências negativas. Assim, propõe-se o teste para verificar se o consentimento é adequado, ou seja, se pode ser obtido em condições corretas (informado e livre, minimamente).

Esta última etapa do teste, no entanto, seria qualificatória. Se o tratamento já se mostrou possível por (i) ter uma finalidade legítima e (ii) ser necessário para tal finalidade, se o consentimento não for adequado (rememore-se o exemplo do contrato a ser executado),

o tratamento fica autorizado com a dispensa do consentimento do titular por ser efetivamente *necessário.* Se, por outro lado, o consentimento é considerado adequado, ou seja, pode ser coletado de forma adequada e, especialmente, quando a expectativa do titular dos dados encontra-se mais *distante* das finalidades do tratamento, o tratamento de dados, para que seja considerado correto, deve colher o consentimento dos titulares dos dados, obrigatoriamente.

O teste proposto reúne elementos gerais da aplicação de bases legais a tratamentos de dados na experiência europeia, elementos do teste de viabilidade da base legal do legítimo interesse no GDPR e uma preferência declarada à oferta de *escolhas* ao titular dos dados, em conformidade com os princípios largamente adotados de *notice and choice* dos FIPPs, seguidos tanto pela União Europeia como pelos Estados Unidos, de forma mais expressa na prática da FTC, possibilitando a aproximação dos dois sistemas em um ponto extremamente complexo e politicamente resistido.

Um segundo domínio em que identificamos a compatibilidade dos sistemas diz respeito à garantia de direitos básicos aos titulares de dados. Como visto, parte dos direitos adotados na União Europeia já são hoje garantidos nos Estados Unidos por vias transversas, especialmente pela legislação estadual e pela prática da FTC. Não se propõe, naturalmente, uma simples transposição de direitos de um sistema a outro, mas sim o reconhecimento de que os direitos de acesso, correção e eliminação podem ser sustentados em ambos sistemas de proteção sem maiores óbices. Sendo eles, especialmente o direito de acesso, essenciais à concessão ao titular de maior controle sobre seus dados e mesmo mecanismo que permite o exercício de outros direitos, cabe considerar que a alteração legislativa no sistema norte-americano para incluir tais direitos na legislação federal não estaria tão longe da realidade.

Um terceiro domínio que merece atenção é o da transparência do tratamento. Como já visto, a União Europeia adota extensa regulamentação sobre quais informações devem ser fornecidas ao titular dos dados sobre o tratamento de dados, enquanto os Estados Unidos se veem às portas do reconhecimento de uma obrigação geral de transparência com a prática reiterada da FTC em tal sentido, além da adoção das FIPPs por tal sistema. Ainda que não se crie um direito extensivo como no caso da União Europeia, também não seria uma aposta insólita a criação, na legislação federal ou pela regulamentação (*Magnuson-Moss rulemaking*) da FTC, de uma obrigação geral de dar *alguma informação* sobre o tratamento, mesmo que seja limitada a quais dados são tratados e o que é feito deles, como já exige a prática da FTC.

Por fim, um dos temas mais espinhosos na aproximação dos sistemas da União Europeia e dos Estados Unidos seja a solução de disputas. Como visto, enquanto na União Europeia o sistema de tutela é bastante extensivo, compreendendo medidas administrativas e judiciais colocadas à disposição do titular, no caso norte-americano os titulares encontram dificuldades para defender seus direitos. O grande problema é que simplesmente estabelecer um *private right of action* não resolve propriamente a questão, uma vez que o right of action diria respeito primariamente à lei em que se insere; na ausência de positivação de todas as "regras" de conduta exigidas pela FTC em uma lei geral de proteção de dados, por exemplo, uma lei que atribuísse um *private right of action* ao titular em relação às regras da FTC provavelmente teria pouca substância, uma vez que os *consent decrees não têm peso de precedente.*

Dessa forma, ainda que haja perspectivas para uma tal solução definitiva e abrangente, com a aprovação de uma lei geral com direitos essenciais e um *private right of action*, mesmo que sejam perspectivas longínquas, devemos buscar a solução para o problema em outros mecanismos. Nesse aspecto chamamos atenção para o mecanismo adotado pelos agora reduzidos em importância *Safe Harbor* e *Privacy Shield*. Ciente de que os titulares de dados teriam dificuldade de exercer seus direitos perante os tribunais norte-americanos, quando negociou tal acordo a União Europeia buscou outra forma de garantir meios minimamente independentes e justos de solução de controvérsias, o que foi feito pelo recurso aos mecanismos privados de solução de controvérsias. Esses mecanismos, que variam da mediação à arbitragem, deveriam ser garantidos pelos próprios controladores de dados a partir da contratação de um terceiro independente que poderia decidir as disputas entre as partes e mesmo determinar ações a serem tomadas por uma ou outra parte em relação a uma eventual violação de direitos.

Tal mecanismo dispensaria a formalidade associada ao *private right of action* e também dispensaria eventuais discussões (geralmente longas e complexas) sobre o estabelecimento de uma autoridade de proteção de dados, que obviamente seria o cenário ideal, bastando a inserção de tal obrigação de provimento de meios alternativos de resolução de disputas, a ser cumprida pelos próprios controladores de dados, para fornecer maior autonomia aos próprios titulares preservando ainda os contornos do atual sistema de proteção de dados norte-americano.

As propostas aqui reunidas, na nossa avaliação, não encontram óbices jurídicos a sua implementação, senão políticos. Visto que o objetivo deste trabalho é justamente avaliar se as objeções geralmente levantadas seriam de fato jurídicas ou se seriam meramente políticas, encaminhamos tais esforços a uma conclusão de que os sistemas de proteção de dados dos Estados Unidos e da União Europeia são de fato *compatíveis*, sendo *possível sua composição*, restando a ver se o tal composição pode advir do Direito Internacional, isto é, se o Direito Internacional é *capaz* de promover tal composição.

4.5. Direito internacional: *soft-law* e composição progressiva

No campo internacional, as primeiras iniciativas a tratarem sobre a criação de regras internacionais para regular o tratamento de dados pessoais foram do Conselho da Europa e da Organização para Cooperação e Desenvolvimento Econômico - OCDE que buscavam um marco para a difusão de normas sobre a proteção de dados pessoais. O Conselho estabeleceu em 1971 um comitê especial para o estudo da matéria, que aprovou duas resoluções sobre problemas identificados concernentes à privacidade em 1973, iniciando-se em seguida os trabalhos para a criação de uma convenção sobre o tema.

A OCDE, que iniciou seus estudos sobre a proteção de dados em meados da década de 1970, no entanto, produziu o primeiro documento internacional sobre a matéria, com a colaboração de países da Europa, dos Estados Unidos e alguns países asiáticos, documento conhecido como *OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data.*[260]

As *Guidelines* ou Diretrizes da OCDE incluem (i) disposições sobre princípios gerais, incluindo princípios de limitação da coleta, qualidade dos dados, finalidade, limitação de uso, segurança, autodeterminação, e prestação de contas; (ii) regras específicas sobre prestação de contas, com referência expressa a Programas de Privacidade na forma de um programa de gestão e conformidade contínuos; (iii) princípios gerais sobre transferências internacionais de dados e responsabilidade do controlador, independentemente da

[260]"Diretrizes sobre a proteção da privacidade e os fluxos transfronteiras de dados pessoais", em tradução livre. ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT - OECD. *Guidelines governing the protection of privacy and transborder flows of personal data*. 23 September 1980. C(80) 58 final. Disponível em: http://www.refworld.org/docid/3dde56854.html.

localização dos dados; (iv) implementação nacional das Diretrizes; e (v) cooperação internacional e interoperabilidade.

Esse documento, apesar de ser o primeiro a sistematizar os princípios até hoje aplicados e sustentados por normativas e leis nacionais, não tinha caráter vinculativo, mas sim de recomendação aos países integrantes da Organização por ocasião da regulamentação da matéria em seus ordenamentos pátrios.[261] Foi assim que a soft-law foi o primeiro veículo jurídico para a criação de normas internacionais sobre Proteção de Dados Pessoais.

A influências das Guidelines da OCDE é de nota uma vez que, mesmo após aprovados diversos outros instrumentos sobre proteção de dados pessoais, os princípios primeiro positivados pela OCDE continuam atuais e são inclusive a base para a formação dos chamados *Fair Information Privacy Principles*, os FIPPs. Como já se notou, parte dos FIPPs foram primeiro expressados no relatório do *U.S. Department of Health, Education and Welfare* de 1973, para então serem desenvolvidos em sua formatação mais completa em 1980. A relevância e o impacto de tal *soft law* para o quadro internacional de proteção de dados continuaria a ser sentida ainda por muitas décadas, dado que a adesão de um Estado à OCDE demanda necessariamente a observância de tais padrões de proteção de dados, entre outras diretivas da organização.

A proteção dos dados pessoais foi finalmente incluída no quadro legislativo internacional como *hard law* pela Convenção de Estrasburgo de 1981,[262] resultado final dos trabalhos do Conselho Europeu. Essa convenção já reconhecia a proteção dos dados pessoais como um aspecto fundamental da garantia da privacidade, como se extrai de seu artigo primeiro,[263] e foi pioneira ao criar conceitos que seriam utilizados de modo relativamente uniforme em todos os diplomas legais subsequentes, como o próprio conceito de dados pessoais.[264]

Nomeada *Convenção para proteção dos indivíduos em relação ao processamento automatizado de dados pessoais*, a Convenção estabelece princípios básicos para a proteção

---

[261]BURKERT, Herbert. Privacy-data protection: a German/European perspective, *cit*., p. 51-52.

[262]COUNCIL OF EUROPE. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg, 28.I.1981. Disponível em: https://rm.coe.int/1680078b37.

[263]The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (”data protection”).

[264]Article 2 - Definitions
For the purposes of this convention:
a. “Personal data” means any information relating to an identified or identifiable individual (”data subject”);
(…)

dos dados pessoais, como *(i)* a adequação, legalidade e o caráter justo da coleta de dados em relação às finalidades a que se presta;[265] *(ii)* a exatidão e possibilidade de correção dos dados armazenados;[266] *(iii)* a necessidade de processamento seguro que impeça a destruição ou acesso indevido desses dados por terceiros;[267] e (*iv*) a possibilidade de o titular dos dados tomar conhecimento da existência de registro que contenha seus dados.[268]

Ela também contém disposições que visam facilitar transferências de dados pessoais ou arquivos que os contenham entre Estados-partes, não podendo estes proibir ou submeter à autorização especial tais transferências. Esta proibição não se aplica, no entanto, caso existam no país de origem disposições específicas de proteção a certas categorias de dados e o outro Estado-parte não possua regulamentação que ofereça equivalente proteção, ou caso o destinatário final da transferência seja um Estado não contratante que utiliza um Estado-parte apenas como intermediário[269] para fugir à aplicação da lei do país de origem da transferência.

---

[265]Article 5 - Quality of data
data undergoing automatic processing shall be:
a. Obtained and processed fairly and lawfully;
b. Stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
c. Adequate, relevant and not excessive in relation to the purposes for which they are stored; (…)

[266]Article 5, d.: [Personal data shall be] accurate and, where necessary, kept up to date; (…)
Article 8 - Additional safeguards for the data subject
Any person shall be enabled: (…)
c. To obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention; (…)

[267]Article 7 - Data security
Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

[268]Article 8 - Additional safeguards for the data subject
Any person shall be enabled:
a. To establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
b. To obtain at reasonable intervals and without excessive delay or expense confirmation of wheter personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; (…)

[269]Article 12 - Transborder flows of personal ata and domestic law (…)
2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.
3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
a. Insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
b. When the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

O alcance da Convenção de Estrasburgo foi considerado bastante limitado. A Convenção não era autoaplicável, exigindo que seus princípios básicos fossem integrados pela legislação nacional de cada signatário. A título de exemplo, sua aplicação restou inexistente em um número de signatários que não chegaram a aprovar leis que internalizassem os princípios da Convenção, como foi o caso da Espanha.[270]

Ao mesmo tempo, seu conteúdo é limitado em termos de proteções efetivas aos dados pessoais, sendo perceptível que o foco principal da Convenção era a eliminação de entraves para a livre circulação de dados pessoais entre os Estados-membros, atendendo a temores já presentes na época criados pela adoção, por alguns países, de leis sobre proteção de dados que permitiam a restrição de tais transferências sob certas condições adversas.[271] Não obstante, esse tratado serviu como ponto de partida para novas leis sobre o assunto e hoje é considerada a base de tais esforços regulatórios na União Europeia.[272] Ainda assim, sustentamos que sua relevância foi muito maior do que a simples criação de regras sobre viabilização de transferências internacionais, uma vez que a Convenção foi a primeira norma de tal tipo a positivar os princípios que começavam a ser reconhecidos por legislação local na Europa, em *soft law* internacional, como as diretrizes da OCDE, e em *soft law* nacional, como o relatório mencionado dos Estados Unidos.

Uma vez que o Conselho da Europa centralizou seu argumento para a aprovação da Convenção de Estrasburgo no direito fundamental contido no artigo 8º da Convenção Europeia para os Direitos do Homem de 1950, com a subsequente proliferação de normas sobre o assunto, embasadas sobretudo naquela Convenção e nas *Guidelines* da OCDE – como foi o caso da Diretiva 95/46/CE – parece natural que a Carta dos Direitos Fundamentais da União Europeia, do ano de 2000, trouxesse em seu artigo 8º, intitulado "Proteção dos Dados Pessoais", a expressão final de tal garantia como um direito fundamental,[273] encerrando qualquer possível debate sobre tal caráter.

---

[270]A primeira lei espanhola sobre a matéria foi promulgada em 1999, resultado da transposição de Diretivas sobre o assunto para o direito interno.

[271]NEWMAN, Abraham L. *op. cit.*, p. 110.

[272]"É possível considerar a Convenção de Strasbourg como o ponto de referência inicial do modelo europeu de proteção de dados pessoais, mesmo porque ela é fruto de reflexões sobre os rumos da matéria no espaço europeu." DONEDA, Danilo. *Da privacidade à proteção de dados pessoais, cit.*, p. 235.

[273]Artigo 8º - Proteção de dados pessoais

1. Todas as pessoas têm direito à proteção dos dados de caráter 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.

O desenvolvimento internacional da proteção de dados, a esse ponto, supostamente teria *esfriado* e reduzido sua marcha, uma vez que poder-se-ia dizer que os Estados em si teriam tomado a questão em suas próprias mãos, com a aprovação de leis nacionais na União Europeia e com o reconhecimento paulatino, nos Estados Unidos, de um direito geral à privacidade pelas cortes e de um direito reduzido à proteção de dados pela legislação setorial aprovada nas últimas décadas daquele século. Ocorre que tal impressão é enganosa, pois o Direito Internacional continuou a ocupar um papel de relevância na proteção de dados pessoais, especialmente no tocante à relação entre União Europeia e Estados Unidos.

A primeira evidência de tal fato advém das contínuas discussões no âmbito da OCDE e do Conselho da Europa que levariam, anos mais tarde, na atualização tanto das *Guidelines* da OCDE quanto da Convenção nº 108.

As diretrizes da OCDE foram atualizadas em 2013, trazendo grande inovação ao prever expressamente a necessidade de adoção de Programas de Privacidade, ao contrário do que acontecia até então com a legislação nacional e regional europeia. A inovação vem do fato de que tais programas, apesar de serem geralmente considerados como a forma mais adequada pelo mercado e pelos profissionais do setor para o cumprimento integrado de todas as obrigações relacionadas a proteção de dados de forma contínua e coerente, não encontravam exigência ou previsão expressa na legislação vigente. Mesmo com a aprovação do GDPR, tal regra não é vista como uma exigência legal expressa, mas sim como medida de boa prática.

Já a Convenção de Estrasburgo teve aprovado um Protocolo de Alteração em 2018 que foram reforçadas regras sobre a transparência do tratamento de dados, sobre o tratamento de dados sensíveis e de categorias especiais, confirmados e expandidos os direitos garantidos ao titular dos dados e ampliadas as disposições sobre as autoridades de proteção de dados pessoais.

Nos dois casos, o que se nota é a necessidade percebida pelo Estados em questão de que tais normativas internacionais permanecessem atuais e atualizadas, mas mais que isso, que tais instrumentos fossem utilizados como ferramentas para incentivar a adoção de novos e atualizados padrões normativos, seja no campo da União Europeia, seja no campo dos membros da OCDE, sempre com vistas a guiar os Estados no desenvolvimento de sua legislação interna.

A segunda evidência de tal aceleração se deu justamente pelas relações de troca de dados estabelecidas entre Estados Unidos e União Europeia. Como já se explorou anteriormente, dado que a União Europeia não poderia considerar os Estados Unidos "adequado" nos termos das normas que regem as transferências internacionais de dados, não seria possível transferir dados da União Europeia para pessoas ou empresas localizadas nos Estados Unidos, conforme regras expressadas tanto na Diretiva de 1995 quanto no GDPR. A solução, no caso, foi dada justamente pelo Direito Internacional: pela cooperação entre União Europeia e Estados Unidos, desenvolveu-se o programa chamado Safe Harbor, que funcionou até 2015 para prover garantias adicionais para dados que viessem da União Europeia para os Estados Unidos.

Quando tal acordo foi derrubado por uma decisão do Tribunal de Justiça da União Europeia em 2015, foi papel novamente dos Estados envolvidos atuar na criação de um novo programa, esperançosamente livre dos vícios que levaram à derrocada do primeiro regime especial, com a criação do então chamado Privacy Shield. Julgado novamente inválido pelo Tribunal de Justiça da União Europeia em 2020, após novas denúncias de vigilância estatal por parte dos Estados Unidos, atualmente as transferências internacionais entre os dois blocos sustentam-se sobre as precárias bases das cláusulas de proteção de dados padrão, que podem ser julgadas insuficientes em um exame caso-a-caso.

O fluxo de dados pessoais entre Estados Unidos e União Europeia é de grande relevância, não só para os países envolvidos, mas também para uma grande quantidade de pessoas que depende de serviços prestados por empresas americanas e europeias que precisam de tal intercâmbio para poder manter suas operações. Os Estados Unidos entendem também que o mercado europeu é relevante para suas empresas, de modo que encerrar tal intercâmbio de dados não é viável do ponto de vista econômico.

Em uma demonstração clara de como o modelo eclético exerce forte influência sobre outros sistemas de proteção de dados, a União Europeia, em tais acordos, exigiu das empresas norte-americanas o cumprimento de regras básicas sobre proteção de dados pessoais para que os dados dos titulares localizados na União Europeia tivessem tratamento minimamente adequado em relação ao nível de proteção que teriam se fossem tratados na própria União Europeia. Assim, para se habilitar no programa, era exigido das empresas norte-americanas a adesão voluntária a um programa pelo qual tais agentes de tratamento se comprometeriam a cumprir regras específicas, incluindo (i) a obrigação de fornecer meios acessíveis de resolução de disputas; (ii) garantir direitos básicos sobre transparência do

tratamento; (iii) implementar limitações quanto à coleta e uso de dados, especialmente em relação a suas finalidades; (iv) além de exigir o mesmo nível de conformidade para terceiros para quem tais dados eventualmente fosse transferidos.

Independentemente da derrocada de tais programas, é interessante notar como foi justamente o Direito Internacional que proveu por largos anos as bases para a aproximação entre os dois sistemas, buscando um regime de proteção de dados que não chegava ao nível de complexidade do sistema da União Europeia, mas exigia níveis razoáveis de proteção ao "preencher" certos espaços vazios no sistema norte-americano de proteção de dados de modo a aproximá-lo de um mínimo comum.

Tal fato nos traz outras duas conclusões significativas. Em primeiro lugar, os padrões adotados pela União Europeia e pelos Estados Unidos nos dois programas de transferências se aproximam em muito dos princípios gerais trazidos nos FIPPs, tais como consolidados pelas *Guidelines* da OCDE quanto na Convenção de Estrasburgo. Isso nos indica que o padrão de "adequação" buscado pela União Europeia, em geral, aproxima-se muito dos padrões de boas práticas existentes há anos na forma proposta por esses instrumentos internacionais. Em segundo lugar, é possível notar um certo efeito dominó decorrente do modo como o modelo eclético implementado pela União Europeia influencia e molda outros modelos regulatórios.

Mesmo que os programas tenham sido anulados em razão da existência de programas extensivos de vigilância nos Estados Unidos – algo que diz mais respeito à fixação de tal país com a vigilância em massa com vistas à segurança interna e internacional – tais programas, combinados com uma evolução lenta, constante e consistente das regras internacionais sobre proteção de dados pessoais para formar princípios gerais que são hoje reconhecidos pelos dois sistemas são uma prova inegável de que *o Direito Internacional é capaz de compatibilizar os dois sistemas de proteção de dados.* Isto é, o Direito Internacional foi capaz de influenciar ambos os modelos para que estes se aproximassem e paulatinamente se influenciassem mutuamente, sendo então capaz de, pela continuidade de tais esforços de composição, continuar aproximando os sistemas de proteção de dados dos Estados Unidos e da União Europeia até que cheguem a bases comuns que lhes permitam coexistir de forma compatível.

4.6. Efeitos da composição de sistemas para o Brasil e o mundo

Finalmente, as conclusões acima esposadas trazem duas consequências, mas com algum grau de incerteza sobre se seriam elas positivas ou negativas.

O primeiro resultado da composição de sistemas para o Brasil e para o mundo diz respeito à predisposição de sistemas semelhantes ao sistema europeu de apresentarem também um certo nível de compatibilidade com o sistema norte-americano, o que tem grandes consequências para as transferências internacionais de dados. Para retomar o assunto, devemos dar um passo atrás.

Como vimos, a União Europeia adota um mecanismo de transferências internacionais de dados pessoais em que dados de pessoas localizadas em seu território só podem ser transferidos para pessoas ou empresas localizadas em países terceiros em certas hipóteses. Além de cenários envolvendo cláusulas contratuais robustas, códigos de conduta e regras corporativas globais, o principal gatilho para tais transferências é que haja uma *adequacy decision*, um ato da União Europeia que reconheça o sistema de proteção de dados do país de destino como *adequado.*

Dentre os critérios para tal avaliação de adequação, encontramos os listados no artigo 45 do GDPR, que incluem a garantia de direitos fundamentais, a existência de autoridades de supervisão em proteção de dados, e os compromissos internacionais de tal país em relação a proteção de dados e direitos humanos. Não obstante, tal avaliação por natureza baseia-se antes de tudo em uma comparação do sistema terceiro com o sistema da própria União Europeia, pois mesmo que se apontem os critérios relevantes, é necessário estabelecer uma base comparativa para verificar se certo nível de proteção é alcançado ou não, sendo que o padrão não poderia ser outro que não a própria proteção dada pelas leis da União Europeia. Isso parece natural, dado que a avaliação geralmente diz respeito a submeter o dado pessoal ao regime corrente, isto é, o regime aplicável onde o titular de dados se encontra (a União Europeia) ou permitir que seja submetido a um regime diferente (para onde se quer enviar o dado).

A composição do sistema da União Europeia com o sistema dos Estados Unidos, nesse aspecto, poderia auxiliar no reconhecimento deste último como um sistema *adequado* de proteção, permitindo-se assim o livre trânsito de dados pessoais entre tais jurisdições, uma vez que os espaços de convergência identificados cobrem, em grande parte, justamente os critérios analisados para decisão sobre a adequação de um país terceiro.

Ocorre que na esteira dos escândalos denunciados por Snowden e com a reforma legislativa na União Europeia que levaria à aprovação do GDPR, o ressurgimento do tema da proteção de dados levou a uma corrida em diversos lugares no mundo para a aprovação de leis gerais de proteção de dados,[274] sendo que muitas delas acabaram adotando muito do que se primeiro estabeleceu na União Europeia. Nesse aspecto, a nossa própria Lei Geral de Proteção de Dados[275] em muitos aspectos repete o disposto no GDPR. Muitos países que fizeram tal "importação" legislativa inclusive adotaram mecanismos semelhantes para regramento das transferências internacionais.

Diante disso, a primeira consequência sentida pela potencial composição dos sistemas da União Europeia e dos Estados Unidos é o potencial para o reconhecimento dos Estados Unidos como destino *adequado* para dados pessoais, o que, se ocorrer na União Europeia, é possível que ocorra em diversas outras jurisdições que adotam sistema semelhante, critérios semelhantes para avaliação e têm como fiel da análise justamente um sistema muito próximo do europeu.

Em um aspecto positivo, tal movimento representaria uma redução das barreiras aos fluxos internacionais de informação, o que provavelmente resultaria em um aumento nas interações globais, não só em nível econômico, mas também social e cultural, e a um *espessamento* do globalismo. Em um aspecto negativo, entretanto, que nos leva ao segundo ponto relevante, é que tal movimento demonstraria certo servilismo incômodo em relação à União Europeia, atitude esta que tem outras consequências não só no campo da proteção de dados quanto no campo da regulação da tecnologia e do desenvolvimento tecnológico em geral.

A segunda consequência da compatibilização diz respeito a um modelo que busca não só influenciar, mas forçar outros sistemas de proteção de dados a se submeterem a alguns fundamentos específicos que sejam considerados adequados por um bloco-potência, caso contrário as empresas de tal país não terão acesso ao mercado de dados pessoais da União Europeia.

---

[274]UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT - UNCTAD. *Data Protection and Privacy Legislation Worldwide*. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide e BRYANT, Jennifer. *3 years in, GDPR highlights privacy in global landscape*. Disponível em: https://iapp.org/news/a/three-years-in-gdpr-highlights-privacy-in-global-landscape/?mkt_tok=MTM4LUVaTS0wNDIAAAF9UCgN7kihLR2TnlvYH9qiQDTlnr_d9-c6innF-LjkCdiJD0U5ZuB_3JQdlcOsm07HDwzRJNH5Yy1VwA4BSQCYCWHPMILxxInSdIFtBbZBBfRI.

[275]BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Em resumo, como uma criança que acaba com o jogo quando seu time perde por ser a “dona da bola”, a União Europeia também cria uma queda de braço com qualquer outro modelo que se afaste do padrão do que consideraria “adequado”, em que o bloco é capaz de exercer pressão de um modo muito simples: “se o sistema de proteção de dados do seu estado (o “jogo”) não for adequado segundo os meus padrões (“como eu quero”), você não poderá receber os dados de pessoas que estejam no meu território (“a bola”)”.

A crítica aqui não advém de uma avaliação valorativa das próprias regras da União Europeia sobre proteção de dados ou se tais regras são corretas ou se trazem benefícios. De fato as regras sobre proteção de dados da União Europeia no geral baseiam-se em direitos fundamentais bem construídos e em fundamentos muito bem estabelecidos. Não se quer aqui criticar o equilíbrio encontrado na legislação europeia para compatibilizar a proteção do titular de dados com as oportunidades adequadas para o desenvolvimento econômico e tecnológico, apesar do fato de que nenhum sistema está realmente isento de ser criticado. O que não se pode aceitar, por outro lado, é a presunção de que o sistema de proteção de dados da União Europeia seja totalmente *bom*, que ele seja o único correto, que ele seja o único *adequado.*

A discussão nesse ponto quase transborda para um debate ético, mas reenquadrando a questão em termos jurídicos, a presunção de que o modelo europeu é *correto (*e por isso deve ser replicado no resto do mundo, voluntariamente ou por pura pressão para poder acessar o mercado europeu) leva a uma replicação de normas sem qualquer senso crítico e de um modo que pode ameaçar a própria inovação no campo da proteção de dados, dado que sistemas inovadores de proteção ou sistemas que se fiem em um equilíbrio de interesses ligeiramente diferente do adotado pelo modelo europeu possivelmente serão simplesmente abandonados em benefício de algo que seja palatável para a União Europeia. A pluralidade social, cultural e jurídica não pode e não deve ser abandonada, mas sim cultivada em medidas saudáveis.

Assim, em conclusão, tal movimento de composição deve ser observado de perto de modo que a aproximação entre os sistemas da União Europeia e dos Estados Unidos não seja uma de caráter unilateral, mas sim que preserve a pluralidade de sistemas jurídicos existentes, para que o remédio não seja mais amargo que a própria doença.

CONCLUSÃO

A pesquisa e o trabalho de análise realizados nos permitem concordar que os dois sistemas estudados partem de premissas bastante diferentes quanto à proteção da privacidade e dos dados pessoais dos indivíduos. Pelo desenvolvimento histórico da privacidade nos dois sistemas, por exemplo, é compreensível que o sistema norte-americano seja, de fato, muito mais preocupado com a flexibilidade e com a permissão para que os entes econômicos atuem dentro de seu campo de liberdade em um regime de autorregulação, enquanto a União Europeia, desde o começo, enfatizou sua escolha por uma abordagem abrangente e *eclética*, criando normativas específicas e de grande impacto para o mercado como um todo.

As diferenças geralmente apontadas entre os sistemas se confirmam, por exemplo, quando se nota o alcance restrito das leis federais norte-americanas que abordam o tema de proteção de dados apenas de forma setorial, em comparação com a abrangência maior, em relação aos setores, titulares protegidos e dados pessoais abrangidos, das leis nacionais e supranacionais da União Europeia. Tais diferenças, entretanto, não se mostraram, na nossa avaliação, impeditivas de uma maior aproximação entre os sistemas analisados.

Após estabelecidas as premissas do estudo, analisou se em detalhe o modelo da União Europeia para proteção de dados pessoais. Nesse ponto, notamos que os principais elementos que marcam os contornos do sistema são o nível de abrangência das regras sobre proteção de dados, afetando qualquer tipo de dado de uma ampla gama de tipos de titulares de dados; a existência de fortes condicionantes ao tratamento de dados, que incluem um rol taxativo de hipóteses autorizativas do tratamento de dados e ainda princípios sobre finalidade e necessidade que devem ser observados ao longo de todo o tratamento; a forma como o sistema utiliza direitos concedidos ao titular dos dados para ampliar seu controle sobre seus dados, ao mesmo tempo em que oferece canais administrativos e judiciais para resolução de conflitos; e o estabelecimento de requisitos rigorosos de segurança, responsabilidade e prestação de contas, exigindo-se do agente de tratamento não só a observância da lei mas um esforço ativo para demonstrar tal conformidade.

Na sequência, foi avaliado o sistema de proteção de dados dos Estados Unidos da América. Na análise do sistema de proteção norte-americano identificamos como seus principais traços o recurso à legislação setorial, tanto em relação aos agentes de tratamento abrangidos quanto em relação aos dados objeto de tal legislação em si, havendo uma grande

variação em quais tipos de dados são efetivamente protegidos; a limitação das alternativas dadas aos titulares para exigirem a proteção de seus dados, uma vez que restritos a leis setoriais e, no caso de operações envolvendo dados que não se enquadrem em tais normas específicas, a necessidade de confiar tal *enforcement* a autoridades públicas que têm como objetivo a fiscalização geral do mercado e não a defesa individual de titulares; o recurso amplo à autorregulação; e a criação paulatina de padrões de conduta que em muito se aproximam dos padrões da União Europeia por meio da jurisprudência da FTC, apesar de tal fonte de regulação não possuir formas efetivas e abrangentes de tutela aos titulares dos dados.

Em um último capítulo, foi nossa tarefa colocar tais sistemas de proteção de dados lado a lado, identificando pontos de convergência e divergência, ao que concluímos que os dois sistemas, apesar de apresentarem diversas divergências, algumas inclusive fundamentais, tais divergências não impediram a criação de institutos funcionalmente similares, que diferem basicamente apenas no seu grau de aplicabilidade e nas suas formas de tutela. Tais observações puderam confirmar que muito de tal aproximação já consolidada decorreu da atuação do próprio Direito Internacional, por meio de instrumentos de *hard law*, sem dúvida, mas especialmente em razão da *soft law* produzida pela comunidade internacional no tema da proteção de dados pessoais. Nossas conclusões então vieram a apontar a existência de *compatibilidade* entre os dois sistemas, visto que há espaços para convergência e tal convergência parece juridicamente possível diante da experiência anterior do Direito Internacional na aproximação dos dois sistemas e nesses temas específicos.

Diante disso, podemos elaborar breves respostas às questões formuladas no início deste trabalho. Em uma primeira questão, de modo abrangente, o desenvolvimento deste trabalho pode delinear os contornos dos sistemas de proteção de dados de cada um dos países analisados, vindo a nomear dois *modelos regulatórios* diferentes: o *modelo eclético*, marcado pela diversidade de fontes de regulação, no qual o sistema da União Europeia se insere; e o *modelo liberal*, definido largamente pelo recurso à autorregulação e à abordagem baseada em risco na criação de legislação estatutária, no qual se enquadra o sistema dos Estados Unidos da América.

Em uma segunda questão, podemos, ainda que com certa surpresa, responder que existem de fato espaços para convergência entre os sistemas da União Europeia e dos Estados Unidos, o que viemos a chamar de *compatibilidade*. Por tal termo não se quer definir o estado atual da integração entre dois sistemas, mas sim medir o potencial para que tais sistemas venham a ser paulatinamente integrados e compatibilizados.

Por fim, devemos responder às últimas duas perguntas formuladas no início deste trabalho de forma afirmativa. Em primeiro lugar, o Direito Internacional não só é capaz de aproximar os sistemas de proteção de dados da União Europeia e dos Estados Unidos, como isso na verdade se comprova pelo fato de que muito do que ambos os sistemas têm de similar foi consequência da atuação do próprio Direito Internacional ao moldar os Fair Information Privacy Principles ou FIPPs, cujas repercussões são vistas claramente tanto na legislação europeia quanto no desenvolvimento da jurisprudência da FTC. A forma como tal atuação se deu e pode ainda se dar pode envolver uma grande variedade de formatos, desde acordos bilaterais, como no caso do Privacy Shield, quanto acordos de maior abrangência como a Convenção de Estrasburgo, mas o que se notou ter maior impacto prático e constante no desenvolvimento e na aproximação dos dois sistemas foi justamente pela criação da chamada *soft-law*.

As conclusões do presente trabalho trazem ao mesmo tempo esperança e preocupação. A aproximação de dois blocos tão importantes em um tema cada vez mais relevante na prática comercial traz de fato algum alento, pois permite considerar que o modelo restritivo de transferências internacionais de dados adotado pela União Europeia e que por muito tempo causou engasgos nas relações entre Estados Unidos e União Europeia, modelo esse replicado em diversos países com a corrida pela aprovação de legislação sobre proteção de dados nos anos 2000 e 2010, pode finalmente considerar adequado, em um futuro próximo, o sistema dos Estados Unidos da América, permitindo finalmente maior tranquilidade no fluxo de dados entre tais países e entre este e outros países que tenham adotado o mesmo modelo da União Europeia.

Por outro lado, a aproximação desejada deve sempre preservar a diversidade de modelos jurídicos e a liberdade de cada país regular certo tema de acordo com suas próprias necessidades e entendimentos. Tal preocupação decorre do fato de que, tendo sido replicado em diversos outros países, o modelo de transferências internacionais da União Europeia cria uma tendência de uniformidade e homogeneização, uma vez que o adequado é sempre, em alguma medida, o similar ou equivalente. A aproximação deve ser feita com cuidado para que a regulação sobre proteção de dados não fique estagnada, sempre refém dos padrões de adequação da União Europeia, dos padrões de proteção de dados daquele bloco, permitindo-se que novos entendimentos e que o próprio Direito tenha espaço para evoluir.

Apesar de tais alertas, as conclusões do presente trabalho nos trazem algum alento, especialmente sobre proteção de dados, mas também sobre a cooperação internacional em geral. Nossas faculdades e a prática diária do Direito parecem nos indicar que os operadores do Direito vivem em países absolutamente divididos uns dos outros, especialmente quando se compara a tradição do *common law* com a do *civil law*. Mais que demonstrar que não há realmente impeditivos jurídicos à aproximação de dois desses países, aparentemente tão diferentes, em um tema tão específico quanto proteção de dados pessoais, nossa esperança é ter podido demonstrar que o Direito Internacional é sim, e possivelmente sempre será, uma alternativa viável e desejável para solução de problemas reais, concretos, sejam eles grandes como a troca internacional de dados entre dois blocos, sejam eles pequenos como a garantia de direitos a um único indivíduo na proteção de seus dados pessoais.

REFERÊNCIAS

ALPHABET Announces fourth quarter and fiscal year 2020 results. *Mountain View*, Feb. 2, 2021. Disponível em: https://abc.xyz/investor/static/pdf/2020Q4_alphabet_earnings_release.pdf. Acesso em: 01 abr. 2021.

ALVES, Carla Segala; GUIDI, Guilherme Berti de Campos. Cláusulas contratuais e dados pessoais: controladores, operadores, cocontroladores e transferências internacionais. *In*: BLUM, R.O.; VAINZOF, R.; MORAES, H.F. *Data protection officer (encarregado)*: teoria e prática de acordo com a LGPD e o GDPR. São Paulo: Thomson Reuters Brasil, 2020.

AMERICA, Your Privacy Settings Are All Wrong. Using an opt-in approach will help curb the excesses of Big Tech. *The New York Times*, Mar. 06, 2021. Disponível em: https://www.nytimes.com/2021/03/06/opinion/data-tech-privacy-opt-in.html.

ANGWIN, Julia. Protecting your digital privacy is not as hard as you might think. *Consumer Reports*, 20 Sept. 2016. Disponível em: http://www.consumerreports.org/privacy/protecting-your-digital-privacy-is-not-as-hard-as-you-might-think/. Acesso em: 19 jan. 2019.

BARRETT, Brian. Spotify clears up its controversial Privacy Policy. *Wired Online*, 21 ago. 2015. Disponível em: https://www.wired.com/2015/08/spotify-clears-up-its-privacy-policy/. Acesso em: 19 jan. 2017.

BELLEIL, Arnaud. *@-Privacidade*: o mercado dos dados pessoais, proteção da vida privada na internet. Lisboa: Instituto Piaget, 2002.

BENNETT, Colin J. *Regulating privacy*: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992. p. 193-219.

BENSOUSSAN, Alain. *Informatique, télécoms, internet*: réglementation, contrats, fiscalité, assurance, santé, fraude, communications électroniques. 5. ed. Levallois: Editions Francis Lefebvre, 2013.

BRYANT, Jennifer. *2021 'best chance' for US privacy legislation*. Disponível em: https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation/.

BRYANT, Jennifer. *3 years in, GDPR highlights privacy in global landscape*. Disponível em: https://iapp.org/news/a/three-years-in-gdpr-highlights-privacy-in-global-landscape/?mkt_tok=MTM4LUVaTS0wNDIAAAF9UCgN7kihLR2TnlvYH9qiQDTlnr_d9-c6innF-LjkCdiJD0U5ZuB_3JQdlcOsm07HDwzRJNH5Yy1VwA4BSQCYCWHPMILxxInSdIFtBbZBBfRI.

BURKERT, Herbert. Privacy-data protection: a German/European perspective. *In*: ENGEL, Christoph; KELLER, Kenneth H. (Eds.). *Governance of global networks in the light of differing local values*. Baden-Baden: Nomos Verlagsgesellschaft, 2000.

CANOTILHO, J.J. Gomes. *Direito constitucional e teoria da Constituição*. 7. ed. Coimbra: Almedina, 2003.

CASELLA, Paulo Borba. *União Europeia*: instituições e ordenamento jurídico. São Paulo: LTr, 2002.

CASTETS-RENARD, Céline. *Droit de l'internet*: droit français et européen. 2. éd. Paris: Montchrestien, 2012.

CASTRO, Federico de. Los llamados derechos de la personalidad, cuestiones previas a su estudio. In: STUDI Giuridici in Memoria de Filippo Vassali. Torino: Torinese, 1960.

CASTRO, Thales. *Teoria das relações internacionais*. Brasília-DF: FUNAG, 2012.

CAVOUKIAN, Ann; TAYLOR, Scott; ABRAMS, Martin E. *Privacy by design*: essential for organizational accountability and strong business practices. *IDIS*, n. 3, p. 405-413, 2010. Disponível em: https://link.springer.com/content/pdf/10.1007/s12394-010-0053-z.pdf. doi: https://doi.org/10.1007/s12394-010-0053-z.

CERQUEIRA, João da Gama. *Tratado da propriedade industrial*. 3. ed. Rio de Janeiro: Lumen Juris, 2012. v. 2, t. 2.

CISCO Systems Inc. The Zettabyte era: trends and analysis. *Cisco Annual Internet Report*, May 2015. Disponível em: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.pdf. Acesso em: 03 fev. 2019.

COOLEY, Thomas McIntyre. *The elements of torts*. Kindle Edition, 2015.

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

DAVID, René. *Os grandes sistemas do direito contemporâneo*. 2. ed. Lisboa: Meridiano, 1978.

DE CUPIS, Adriano. *Os direitos da personalidade*. Campinas: Romana, 2004.

DINIZ, Maria Helena. *Dicionário jurídico*. 3. ed. São Paulo: Saraiva, 2008. t. 2, t. 3.

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

DONEDA, Danilo. O direito fundamental à proteção dos dados pessoais. *In*: MARTINS, Guilherme Magalhães (Org.). *Direito privado e internet*. São Paulo: Atlas, 2014.

FERNANDES, Milton. Os direitos personalíssimos. *Revista Jurídica da Advocacia Geral do Estado de Minas Gerais*, Belo Horizonte, n. 1, jul./dez. 2004.

FERNANDES, Milton. *Proteção civil da intimidade*. São Paulo: Saraiva, 1977.

FOURTEEN Points, (January 8, 1918), declaration by U.S. Pres. Woodrow Wilson during World War I outlining his proposals for a postwar peace settlement. Disponível em: https://www.britannica.com/event/Fourteen-Points.

GALETTA, Antonella; HERT, Paul de. *A European perspective on data protection and access rights*. Increasing Resilience in Surveillance Societies (IRISS) Project, 2014. Disponível em: http://irissproject.eu/wp-content/uploads/2014/06/European-level-legal-analysis-Final1.pdf. Acesso em: 25 mar. 2019.

GOGLIANO, Daisy. *Direitos privados da personalidade*. São Paulo: Quartier Latin, 2013.

GOOGLE Trends. Disponível em: https://trends.google.com/. Acesso em: 02 abr. 2021.

GREENWALD, G; MACASKILL, E. NSA Prism program taps in to user data of Apple Google and others. *The Guardian Online*, June 7, 2013. Disponível em: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em: 10 mai. 2017.

GRIMALT SERVERA, Pedro. La necessária reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflitos y solapamentos com otros derechos y libertades en internet. *In*: VALEROS TORRIJOS, Julián (Org.). *La protección de los datos personales en internet ante la innovación tecnológica*: riesgos, amenazas y respuestas desde la perspectiva jurídica. Cizur Menor, Navarra: Thomson Reuters/Aranzadi, 2013.

GUIDI, Guilherme Berti de Campos. O Caso Costeja v. Google Spain e o direito ao esquecimento: para além da implementação e rumo ao diálogo global. *In*: MENEZES, Wagner (Org.) *Tribunais internacionais e a implementação procedimental de suas decisões*. Belo Horizonte: Arraes, 2018.

GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. *In*: BRANCO, Sérgio; DE TEFFÉ, Chiara (Orgs.) *Privacidade em perspectivas*. Rio de Janeiro: Lumen Juris, 2018.

GUIDI, Guilherme Berti de Campos. *A proteção dos dados pessoais na internet*: contribuições da experiência europeia ao modelo brasileiro. 2016. Dissertação (Mestrado) – Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de São Paulo, São Paulo, 2016.

HENKIN, Louis. Privacy and autonomy. *Columbia Law Review*, v. 74, n. 8, p. 1410-1433, Dec. 1974.

INTERNATIONAL TELECOMMUNICATION UNION. *Measuring digital development*: facts and figures 2020. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Pages/ff2020interactive.aspx. Acesso em: 03 abr. 2021.

JURISPRUDENCE française en matière de droit civil. *Revue Trimestrielle de Droit Civil*, Paris, jan./mars. 1971.

KEOHANE, Robert O.; NYE, Joseph S. Globalization: what's new? what's not? (and so what?). *Foreign Policy*, n. 118, p. 104-119, 2000.

KEOHANE, Robert O.; NYE, Joseph S. Power and interdependence in the information age. *Foreign Affairs*, v. 77, n. 5, p. 81-94, Sep./Oct. 1998.

KEOHANE, Robert O.; NYE, Joseph S. *Power and interdependence*. 4. ed. Boston: Longman, 2012.

KONVITZ, Milton R. Privacy and the law: a philosophical prelude. *Law and Contemporary Problems*, Duke University Press, v. 31, n. 2, p. 272-280, 1966. Disponível em: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3108&context=lcp.

LESSIG, Lawrence. *Code version 2.0*. Kindle Edition, 2011.

LINDON, Raymon. *Une création prétorienne*: les droit de la personnalité. Paris: Dalloz, 1974.

LINZER, Peter. From the Gutenberg bible to net neutrality - how technology makes law and why english majors need to understand it. *McGeorge Law Review*, v. 39, n. 1, 2008. Disponível em: https://faculty.mcgeorge.edu/documents/Publications/_03b_Linzer_MasterMLR39.pdf.

MARR, Bernard. 5 signs you are a big data hoarder. *Data Informed*, Aug. 12, 2015. Disponível em: http://data-informed.com/5-signs-you-are-a-big-data-hoarder/. Acesso em: 08 fev. 2019.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data*: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Rio de Janeiro: Elsevier, 2013.

MCCABE, David. Congress and Trump Agreed They Want a National Privacy Law. It Is Nowhere in Sight. *The New York Times*, Oct. 1, 2019. Disponível em: https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html.

MENÉNDEZ MATO, Juan Carlo; GAYO SANTA CECILIA, Maria Eugenia. *Derecho e informática*: ética y legislación. Barcelona: Bosch, 2014.

MENEZES, Wagner. *Ordem global e transnormatividade*. Ijuí: Ed. Unijuí, 2005.

MENEZES, Wagner. *Tribunais internacionais*: jurisdição e competência. São Paulo: Saraiva, 2013.

MIGUEL ASENSIO, Pedro Alberto de. *Derecho privado de internet*. 4. ed. Madrid: Civitas, 2011.

MORGENTHAU, Hans J. *Politics among Nations*: the struggle for power and peace. New York: Alfred A. Knopf, 1948.

NEWMAN, Abraham L. Building transnational civil liberties: transgovernmental entrepreneurs and the European data privacy directive. *International Organization*, v. 62, n. 1, p. 103-130, Jan. 2008. doi: https://doi.org/10.1017/S0020818308080041.

OLIVER-LALANA, Angel Daniel; MUÑOZ SORO, José Félix. El mito del consentimiento y el fracaso del modelo individualista de protección de datos. *In:* VALERO TORRIJOS, Julián (Org). *La protección de los datos personales en internet ante la innovación tecnológica*. Navarra: Aranzadi, 2013. p. 153-196.

ORDÓÑEZ SOLÍS, David. *Privacidad y protección judicial de los datos personales.* Barcelona: Bosch, 2011.

PAUL, Ian. Instagram updates privacy policy, inspiring backlash. *PC World*, 18 dez. 2012. Disponível em: http://www.pcworld.com/article/2021285/instagram-updates-privacy-policy-inspiring-backlash.html. Acesso em: 19 jan. 2017.

PEARCE, Graham; PLATEN, Nicholas. Orchestrating transatlantic approaches to personal data protection: a European perspective. *Fordham International Law Journal*, v. 22, n. 5, p. 2024-2051, 1998. Disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1641&context=ilj.

PEDUZZI, Pedro. MJ finaliza nova versão de anteprojeto sobre proteção de dados na internet. *Agência Brasil EBC*, 19 out. 2015. Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2015-10/mj-finaliza-nova-versao-de-anteprojeto-sobre-protecao-de-dados-na-internet. Acesso em: 19 jan. 2019.

PEMBER, Don R. *Privacy and the press*: the law, the mass media and the first amendment. Seattle: University of Washington Press, 1972.

PEREIRA, Caio Mario da Silva. *Instituições de direito civil*. 22. ed. Rio de Janeiro: Forense, 2008. v. 1.

PEREIRA, Marcelo Cardoso. *Direito à intimidade na internet*. 1. ed. 6. impr. Curitiba: Juruá, 2011.

PRAMUK, Jacob. FCC votes to classify internet as a public utility. *CNBC Online*, Feb. 26, 2015. Disponível em: http://www.cnbc.com/2015/02/26/fcc-votes-to-classify-the-internet-as-a-public-utility.html. Acesso em: 05 abr. 2019.

PRIVACY Shield Frameworks. Disponível em: https://www.privacyshield.gov/.

PROSSER, William L. Privacy. *California Law Review*, v. 48, n. 3, p. 383-423, Aug. 1960. Disponível em: https://lawcat.berkeley.edu/record/1109651.

PUGLIESE, Giovanni. Il diritto alla riservatezza nel quadro dei diritti della personalità. *In*: STUDI in onore di Alberto Asquini. Padova: CEDAM, 1965.

ROCHA, Antonio J. *Relações internacionais*: teorias e agendas. Brasília-DF: IBRI, 2002.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Org., sel. e apres. de Maria Celina *Bodin* de Moraes. Rio de Janeiro: Renovar, 2008.

RONCOLATO, Murilo. Por que debater a Lei de Proteção de Dados Pessoais? *O Estado de S. Paulo Online*, 28 jan. 2015. Disponível em: http://link.estadao.com.br/noticias/geral,porque-debater-a-lei-de-protecao-de-dados-pessoais,10000029762. Acesso em: 19 jan. 2019.

SCHMARZO, Bill. *Big data*: understanding how big data powers big business. Indianapolis: Wiley, 2013.

SCHREIBER, Anderson. *Direitos da personalidade*. 2. ed. São Paulo: Atlas, 2013.

SERASA EXPERIAN. Disponível em: https://www.serasaexperian.com.br/solucoes/mosaic/. Acesso em: 03 abr. 2021.

SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional*: teoria e prática na Alemanha, Espanha e Brasil. Belo Horizonte: Arraes, 2014.

SIMITIS Reports Data Protection Chaos. *Transnational Data and Communications Report*, Jun./Jul. 1990.

SOLOVE, Daniel; HARTZOG, Woodrow. The FTC and the new common law of privacy. *Columbia Law Review*, v. 114, n. 583, p. 583-676, 2014. Disponível em: https://cyberlaw.stanford.edu/files/publication/files/SSRN-id2312913.pdf.

SOTTO, Lisa J.; SIMPSON, Aaron P. United States. *In*: JAY, Rosemary P. (Ed.). *Data Protection & Privacy:* in 31 jurisdictions worldwide. 3. ed. London: Law Business Research, 2015. p. 208-214. Disponível em: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2011/04/DDP2015_United_States.pdf.

SWIRE, Peter P.; KENNEDY-MAYO, DeBrae. *U.S. Private-sector privacy*: law and practice for information privacy professionals. 2. ed. Portsmouth: IAPP, 2018.

THOMSON, Judith Jarvis. The right to privacy. *Philosophy and Public Affairs*, Princeton University Press, v. 4, n. 4, p. 295-314, 1975.

THOUSANDS gather in Washington for anti-NSA 'Stop Watching Us' rally. *Support the Guardian.* Disponível em: https://www.theguardian.com/world/2013/oct/26/nsa-rally-stop-watching-washington-snowden.

VELU, Jacques. *Le droit au respect de la vie privée*: conférences données à la Faculté de droit de Namur. Namur, Belgique: Presses universitaires de Namur, 1974.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, Dec. 1890. Disponível em: https://www.jstor.org/stable/pdf/1321160.pdf?refreqid=excelsior%3Ac5f30ce85672d3d6b0e51c6350c80d0b.

WIRTSCHAFT fürchtet Nachteile durch verschärften Datenschutz. *Computerwoche* (Internet Edition), 21.12.1990. Disponível em: https://www.computerwoche.de/a/wirtschaft-fuerchtet-nachteile-durch-verschaerften-datenschutz,1149120.

Documentos nacionais e internacionais

BRASIL. *Decreto nº 10.046 de 9 de outubro de 2019*. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Diário Oficial da União, Brasília, DF, 10 de outubro de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm.

BRASIL. *Lei nº 12.414 de 9 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de possas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial da União, Brasília, DF, 10 de junho de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.

BRASIL. *Lei nº 12.529 de 30 de novembro de 2011*. Estrutura o Sistema Brasileiro de Defesa da Concorrência (...). Diário Oficial da União, Brasília, DF, 01 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12529.htm.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. *Lei nº 9.279 de 14 de maio de 1996*. Regula direitos e obrigações relativos à propriedade industrial. Diário Oficial da União, Brasília, DF, 15 de maio de 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm.

BRASIL. *Lei nº 9.610 de 19 de fevereiro de 1998*. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Diário Oficial da União, Brasília, DF, 20 de fevereiro de 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9610.htm.

BUNDESREPUBLIK DEUTSCHLAND. *Bundesdatenschutzgesetz. Bundesgesetzblatt I (BGBI)*, 27 Jan. 1977.

CALIFORNIA STATE LEGISLATURE. *SB-1121 California Consumer Privacy Act of 2018*. Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o acompanhamento do programa de trabalho para uma melhor aplicação da directiva relativa à proteção de dados.* COM(2007) 87 final. Bruxelas, 7 mar. 2007. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52007DC0087.

COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões*. *Uma abordagem global da protecção de dados pessoais na União Europeia*. COM(2010) 609 final. Bruxelas, 4 nov. 2010. Disponível em: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_pt.pdf. Acesso em: 24 mar. 2019.

COMISSÃO EUROPEIA. *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões*. *Proteção da privacidade num mundo interligado*: um quadro europeu de proteção de dados para o século XXI. COM(2012) 9 final. Bruxelas, 25 jan. 2012. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52012DC0009.

COMISSÃO EUROPEIA. *Decisão 2000/520/CE*. Decisão da Comissão de 26 de julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de "porto seguro" e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América. Jornal Oficial L 215, 25 de agosto de 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32000D0520.

COMISSÃO EUROPEIA. *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados*. COM(2012) 10 final. Bruxelas, 25 jan. 2012. Disponível em: http://eur-lex.europa.eu/procedure/PT/201285.

COMISSÃO EUROPEIA. *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. COM(2012) 11 final. Bruxelas, 25 jan. 2012. Disponível em: http://docplayer.com.br/3497609-Proposta-de-regulamento-do-parlamento-europeu-e-do-conselho.html.

COMISSÃO EUROPEIA. Relatório da Comissão. *Primeiro Relatório sobre a implementação da Directiva relativa à protecção de dados (95/46/CE)*. COM(2003) 265 final. Bruxelas, 15 maio 2003. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52003DC0265.

COMMISSION OF THE EUROPEAN COMMUNITIES. Report From the Commission. *First report on the implementation of the Data Protection Directive (95/46/EC)*. Brussels, 15.5.2003 COM(2003) 265 final. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF.

CONSELHO DA EUROPA. *Convenção Europeia dos Direitos do Homem*. Disponível em: https://www.echr.coe.int/documents/convention_por.pdf.

CONSELHO DA UNIÃO EUROPEIA. *Decisão-Quadro 2008/977/JAI*. Decisão-Quadro do Conselho de 27 de novembro de 2008 relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal. Jornal Oficial L 350, 30 de dezembro de 2008. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32008F0977.

COUNCIL OF EUROPE. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg, 28.I.1981. Disponível em: https://rm.coe.int/1680078b37.

COURT OF JUSTICE OF THE EUROPEAN UNION (CJEU). *Case C-311/18*. Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. Judgment from the Court of Justice of the European Union (CJEU) relating to the transfer of personal data by a private company from a European Union (EU) Member State to a private company in a third country for commercial purposes. It concerns specifically the legality of standard contractual clauses (SCCs) as a mechanism to transfer personal data outside the EU. The judgment became known as the *Schrems II* judgment. Disponível em: https://www.europeansources.info/record/cjeu-case-c-311-18-data-protection-commissioner-v-facebook-ireland-and-maximillian-schrems/.

EUROPEAN COMMISSION. *81/679/EEC*: Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data. Official Journal L 246, 29/08/1981, P. 0031. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31981H0679.

EUROPEAN COMMISSION. Council of Europe. *128th Session of the Committee of Ministers*. (Elsinore, Denmark, 17-18 May 2018). Ad hoc Committee on Data Protection (CAHDATA) - Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Disponível em: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e.

EUROPEAN PARLIAMENT. COUNCIL EUROPEAN. *Regulation (EU) 2016/679 of the European Parliament and of the Council*. 27 April 2016. on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

IAPP-EY Annual Privacy Governance Report 2019. Disponível em: https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION - ISO. INTERNATIONAL ELECTROTECHNICAL COMMISSION - IEC. *ISO/IEC 27701:2019*. Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en.

NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos*. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos.

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT - OECD. *Guidelines governing the protection of privacy and transborder flows of personal data*. 23 September 1980. C(80) 58 final. Disponível em: http://www.refworld.org/docid/3dde56854.html.

PARLAMENTO EUROPEU. CONSELHO DA EUROPA. *Carta de Direitos Fundamentais da União Europeia* (2000/C 364/01). Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf.

RECORDS, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. U.S. Department of Health, Education & Welfare. July 1973. Disponível em: https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

RÉPUBLIQUE FRANCAISE. Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés. *Journal Officiel de la République Française*, 7 janv. 1978. Disponível em: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/.

SAFE Harbour Framework. Disponível em: www.export.gov/safeharbor/index.asp.

UNIÃO EUROPEIA. Corte de Justiça da União Europeia. *Caso C-362/14*. Maximillian Schrems v. Data Protection Commissioner, julgado em 6 de outubro de 2015. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=515620. Acesso em: 08 out. 2015.

UNIÃO EUROPEIA. Corte de Justiça da União Europeia. *Casos conjuntos C-293/12 e C-594/12*. Digital Rights Ireland Ltd. v. Ireland, julgados em 8 de abril de 2014. Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=PT&cid=513860. Acesso em: 09 out. 2014.

UNIÃO EUROPEIA. Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. Jornal Oficial L. 207/1, 01 de agosto de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016D1250.

UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas. Jornal Oficial L. 201, 31 de julho de 2002. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002L0058.

UNIÃO EUROPEIA. Directiva 2006/24/CE do Parlamento Europeu e do Conselho de 15 de março de 2006 relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Diretiva 2002/58/CE. Jornal Oficial L. 105, 13 de abril de 2006. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32006L0024&from=FI.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial L. 281, 23 de novembro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046.

UNIÃO EUROPEIA. Diretiva (UE) nº 2016/680 do Parlamento Europeu e do Conselho 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 L. 119/89, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0680.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção 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 L. 119/1008, 04 de maio de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT - UNCTAD. *Data Protection and Privacy Legislation Worldwide*. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

UNITED STATES CODE. 15 U.S. *Code § 1681 - Congressional findings and statement of purpose*. Disponível em: https://www.law.cornell.edu/uscode/text/15/1681.

UNITED STATES CODE. 15 U.S. *Code § 6801 - Protection of nonpublic personal information*. Disponível em: https://www.law.cornell.edu/uscode/text/15/6801.

UNITED STATES. *Children's Online Privacy Protection Act, 15 U.S.C. §6501-6506*. Public Law, Washington D.C., 21 Oct. 1998. Disponível em: https://www.ftc.gov/enforcement/statutes/childrens-online-privacy-protection-act.

UNITED STATES. Electronic Communications Privacy Act, 18 U.S.C. §2510-2523. Public Law, Washington D.C., 21 Oct. 1986. Disponível em: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#:~:text=in%20Section%202516.-,18%20U.S.C.,billing%20records%2C%20or%20IP%20addresses.

UNITED STATES. Federal Trade Commission - FTC. *Fair and Accurate Credit Transactions Act of 2003*. Disponível em: https://www.congress.gov/108/plaws/publ159/PLAW-108publ159.pdf.

UNITED STATES. Federal Trade Commission - FTC. *Fair Credit Reporting Act* (1970). Revised September 2018. Disponível em: https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf.

UNITED STATES. Federal Trade Commission - FTC. *Fair Credit Reporting Act. 15 U.S.C § 1681*. Revised September 2018. Disponível em: https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf.

UNITED STATES. Federal Trade Commission – FTC. *Federal Trade Commission Act*. Incorporating U.S. SAFE WEB Act amendments of 2006 (Unofficial version). [15 U.S.C. §41-58. Public Law, Washington D.C., 1914]. Disponível em: https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf.

UNITED STATES. Federal Trade Commission - FTC. *Gramm-Leach-Bliley Act* (1999) Disponível em: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

UNITED STATES. Federal Trade Commission - FTC. *Gramm-Leach-Bliley Act*. Disponível em: https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf.

UNITED STATES. Federal Trade Commission - FTC. *Privacy online*:a Report to Congress. June 1998. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

UNITED STATES. *Health Insurance Portability and Accountability Act, 110 Stat. 1936*. Public Law, Washington D.C., 21 Aug. 1996. Disponível em: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

UNITED STATES. *Privacy Act, 88 Stat. 1896*. Public Law, Washington D.C., 31 Dec. 1974. Disponível em: https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf.

UNITED STATES. Senate. *S.1158 - Consumer Privacy Protection Act of 2015*. Disponível em: https://www.congress.gov/114/bills/s1158/BILLS-114s1158is.pdf.

UNITED STATES. Senate. *S.1214 - Privacy Bill of Rights Act*. Disponível em: https://www.congress.gov/bill/116th-congress/senate-bill/1214.

UNITED STATES. Senate. S.*3300 - Data Protection Act of 2020*. Disponível em: https://www.congress.gov/bill/116th-congress/senate-bill/3300/text.