UNIVERSIDADE D
COIMBRA

Érica Nogueira Soares d'Almeida

DISSEMINAÇÃO NÃO CONSENSUAL DE IMAGENS ÍNTIMAS

UMA ANÁLISE À LUZ DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

VOLUME 1

Dissertação no âmbito do 2.º Ciclo de Estudos em Direito (conducente ao grau de Mestre), na Área de Ciências Jurídico-Políticas/Menção em Direito Internacional Público e Europeu, orientada pela Professora Doutora Ana Mafalda Castanheira Neves de Miranda Barbosa e apresentada à Faculdade de Direito da Universidade de Coimbra.

Outubro de 2020

UNIVERSIDADE D
COIMBRA

Érica Nogueira Soares d'Almeida

DISSEMINAÇÃO NÃO CONSENSUAL DE IMAGENS ÍNTIMAS
UMA ANÁLISE À LUZ DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

NON-CONSENSUAL DISSEMINATION OF INTIMATE IMAGES
AN ANALYSIS IN LIGHT OF THE GENERAL DATA PROTECTION REGULATION

VOLUME 1

Dissertação no âmbito do 2.º Ciclo de Estudos em Direito (conducente ao grau de Mestre), na Área de Ciências Jurídico-Políticas/Menção em Direito Internacional Público e Europeu, orientada pela Professora Doutora Ana Mafalda Castanheira Neves de Miranda Barbosa e apresentada à Faculdade de Direito da Universidade de Coimbra.

Outubro de 2020

RESUMO

O presente trabalho pretende analisar o problema da disseminação não consensual de imagens íntimas (NCII) na perspectiva da proteção de dados pessoais, indagando sobre a possibilidade de aplicação do direito ao apagamento previsto no artigo 17.º do Regulamento (UE) 2016/679 às situações de NCII. Para isso, busca-se, em um primeiro momento, compreender em que medida a NCII afeta o direito à proteção de dados pessoais, analisando a sua relação com os direitos da personalidade, e examinando a NCII à luz da ideia de integridade contextual. Em seguida, passa-se a uma análise da NCII como prática que viola o direito à proteção de dados pessoais no contexto do Regulamento (UE) 2016/679, examinando, primeiramente, a evolução do direito à proteção de dados pessoais nos EUA e na Europa ao longo dos tempos, o papel do consentimento como forma de legitimação do tratamento e seus limites. Posteriormente, examina-se o direito ao apagamento previsto no artigo 17.º, diferenciando-o das várias acepções de direito ao esquecimento. Por fim, tendo em vista que as imagens normalmente são publicadas em redes sociais ou *sites* de compartilhamento de conteúdo pelo usuário, busca-se analisar qual o papel desempenhado pelo usuário da plataforma que compartilha as imagens e pela própria plataforma no caso da NCII, para compreender a que sujeito compete a obrigação de apagamento correlata ao direito previsto no artigo 17.º do RGPD.

Palavras-chave: Proteção de dados pessoais; direito ao apagamento; direito ao esquecimento; disseminação não consensual de imagens íntimas; Regulamento Geral de Proteção de Dados

ABSTRACT

The aim of this work is to analyze the problem of the non-consensual dissemination of intimate images (NCII) from a data protection perspective, investigating the possibility of applying the right to erasure under article 17 of Regulation (EU) 2016/679 to NCII cases. To this end, we will, at first, examine the extent to which the NCII affects the right to the protection of personal data, evaluating its relationship with personality rights, and examining NCII in light of the idea of contextual integrity. Then, we analyze NCII as a practice which violates the right to the protection of personal data in the context of Regulation (EU) 2016/679, examining the evolution of the right to the protection of personal data in the USA and in Europe over time, the role of consent as legal basis for data processing and its limits. Subsequently, we examine the right to erasure provided for in article 17, drawing the distinction between the right to erasure and the various meanings of the right to be forgotten. Finally, considering the fact that the images are usually published on social networks and user-generated content *websites*, we aim to analyze the roles of the platform user who sends the images and the platform itself in the case of NCII, in order to understand who must comply with the erasure obligation foreseen in article 17 of the GDPR.

Keywords: Data protection; right to erasure; right to be forgotten; non-consensual dissemination of intimate images; General Data Protection Regulation

LISTA DE SIGLAS E ABREVIATURAS

- AEPD: Agência Espanhola de Proteção de Dados

- BVERFGE: Tribunal Constitucional Federal da Alemanha

-CDFUE: Carta de Direitos Fundamentais da União Europeia

-CEPD: Comitê Europeu para a Proteção de Dados

-Convenção 108: Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal do Conselho da Europa

-EDPB: European Data Protection Board

-GG: Grundgesetz – Lei Fundamental (Constituição da República da Alemanha)

-GT 29: Grupo de Trabalho do Artigo 29.º para a Proteção de Dados Pessoais (Article 29 Data Protection Working Party)

-NCII: Disseminação não consensual de imagens íntimas

-OCDE: Organização para a Cooperação e Desenvolvimento Econômico

-RFID: Identificação por radiofrequência

-RGPD: Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral de Proteção de Dados Pessoais)

-SNS: Social Network Service (Serviço de Rede Social)

-TEDH: Tribunal Europeu dos Direitos do Homem

-T.G.I. de Paris: Tribunal de Grande Instance de Paris

-T.G.I. de la Seine: Tribunal de Grande Instance de la Seine

-TJUE: Tribunal de Justiça da União Europeia

-UE: União Europeia

ÍNDICE

INTRODUÇÃO 8
1. CONSIDERAÇÕES SOBRE O PROBLEMA DA DISSEMINAÇÃO NÃO CONSENSUAL DE IMAGENS ÍNTIMAS 12
1.1 A digitalização, o aumento da capacidade de armazenamento e processamento de dados, a *web 2.0* e a "ascensão da lembrança" 12
1.2 A prática da disseminação não consensual de imagens íntimas 17
1.3. Os riscos associados à disseminação não consensual de imagens íntimas 23
2. O DIREITO À PROTEÇÃO DE DADOS PESSOAIS COMO UM DOS DIREITOS AFETADOS PELA DISSEMINAÇÃO NÃO CONSENSUAL DE IMAGENS ÍNTIMAS 27
2.1 A proteção de dados pessoais e a tutela da personalidade 27
2.2 A Integridade Contextual e a disseminação não consensual de imagens íntimas como uma violação ao direito à proteção de dados pessoais. 44
3. O CONSENTIMENTO E SEUS LIMITES 53
3.1 O direito à proteção de dados pessoais ao longo dos tempos. 53
3.1.1 Observações sobre a evolução do *right to privacy* no contexto Estadunidense 53
3.1.2 O direito à proteção de dados no contexto europeu 61
3.1.2.1 As primeiras gerações de leis em matérias de proteção de dados 61
3.1.2.2 As gerações subsequentes e a Decisão dos Censos de 1983 64
3.1.2.3 Considerações sobre a proteção de dados no contexto europeu 71
3.2 O consentimento como forma de legitimação do tratamento de dados no Regulamento (UE) 2016/679 73
3.3 Os limites do consentimento 80
3.4 A Disseminação de imagens íntimas e o Regulamento (UE) 2016/679: tratamento ilícito de dados sensíveis 87
4 O DIREITO AO APAGAMENTO DE DADOS COMO RESPOSTA À DISSEMINAÇÃO NÃO CONSENSUAL DE IMAGENS ÍNTIMAS: ALGUMAS QUESTÕES 92

4. 1 O Direito ao apagamento dos dados (direito a ser esquecido) no caso da disseminação não consensual de imagens íntimas 92
4.1.1 A perspectiva tradicional do direito ao esquecimento 93
4.1.2 O direito ao esquecimento na Internet e o caso *Google Spain* 97
4.1.3 O Artigo 17.º do Regulamento e o "direito a ser esquecido" 105
4.2 A NCII, o apagamento e o esquecimento 109
4.2.1 O papel do usuário de rede social ou *site* de compartilhamento de imagens e vídeos 112
4.2.2 O papel do provedor do serviço de rede social ou *site* de compartilhamento de imagens ou vídeos 119
4.2.3 Conclusões sobre o responsável pelo tratamento no caso da disseminação não consensual de imagens íntimas 129
CONCLUSÕES 134
REFERÊNCIAS 141
JURISPRUDÊNCIA 168

INTRODUÇÃO

O presente trabalho tem como tema de pesquisa a disseminação não consensual de imagens íntimas sob a ótica do direito à proteção de dados pessoais, tendo em conta, mais especificamente, o quadro do Regulamento (UE) 2016/679. A disseminação não consensual de imagens íntimas (NCII) consiste no compartilhamento de imagens sexualmente explícitas ou íntimas sem o consentimento da pessoa retratada (BEYENS e LIEVENS, 2016, p. 32; HENRY e POWELL, 2016, p. 399). Sua prática tem sido potencializada nos últimos anos devido à evolução das tecnologias da informação, que facilitam o compartilhamento de imagens e vídeos. Apesar de estudos sobre a frequência da NCII ainda serem escassos, a prática tem sido estudada e discutida principalmente no âmbito do Direito Penal (CITRON e FRANKS, 2014; HENRY e POWELL, 2016; RYAN, 2018) e da Criminologia (BATES, 2017), e se mantém relevante nos tempos atuais: dados da *Revenge Porn Helpline*, no Reino Unido, por exemplo, sugerem que os casos de NCII aumentaram durante o período de quarentena pelo COVID-19 (CRIDDLE, 2020).

A NCII já foi objeto de uma pergunta parlamentar à Comissão Europeia em 2015, indagando sobre possíveis propostas da Comissão sobre o tema, e questionando se o direito ao esquecimento desenvolvido na União Europeia poderia ser uma solução. Na resposta, a Comissão reconheceu que a prática afeta diretamente o direito ao respeito pela vida privada e familiar, previsto no artigo 7.º da CDFUE. Mencionou o direito ao apagamento de dados presente na Diretiva, bem como a decisão do Tribunal de Justiça da União Europeia no caso *Google Spain*, que reconheceu o direito de remoção de links de motores de busca em certas condições como possíveis respostas ao problema. Também afirmou que o "direito a ser esquecido", referido na proposta de reforma da legislação em matéria de proteção de dados, se constrói a partir desses direitos (EUROPEAN COMMISSION, 2015). Uma pergunta semelhante foi formulada em 2017, mencionando a NCII dentro do contexto de práticas violentas na Internet. A Comissão também mencionou, em resposta, a possibilidade de requerer a remoção de dados a motores de busca e *websites*, conforme disposto na legislação da UE (EUROPEAN COMMISSION, 2017).

O "*right to be forgotten*" foi mencionado também por David Ryan, que usou o termo para se referir ao direito ao apagamento, previsto no artigo 17.º do Regulamento (UE) 2016/679, em seu artigo (2018). Ryan afirma que, no caso de disseminação não

consensual de imagens íntimas, o "direito ao esquecimento" tem um aspecto positivo, que é seu efeito transnacional, graças à sua aplicação regional (2018, p. 1067). Ainda há pouca literatura sobre a aplicação do Regulamento Geral de Proteção de Dados Pessoais da União Europeia à disseminação não consensual de imagens íntimas. Ao mesmo tempo, algumas disposições do Regulamento carecem de esclarecimentos, como é o caso, por exemplo, de alguns aspectos do direito previsto no artigo 17.º.[1]

O problema da NCII é relevante não apenas pela sua atualidade, mas pelo impacto que causa nas pessoas envolvidas: a revolução dos sistemas de informação possibilitou uma rede de compartilhamento intenso de informações pessoais, combinada com o aumento da capacidade de armazenamento e organização. Mayer-Schönberger identifica, nesse contexto, o problema da "ascensão da lembrança", referindo-se ao fato de que, com a grande capacidade de conservação e extração de informação, qualquer acontecimento registrado na Internet será potencialmente lembrado eternamente. Trata-se de um problema com o qual a proteção de dados pessoais passa a lidar. O "*right to be forgotten*" é, nesse sentido, apontado pela mídia comum como possível remédio.[2]

A legislação europeia de proteção de dados pessoais tem sido normalmente aplicada a situações que envolvem bancos de dados, como, por exemplo, hospitais e entidades empregadoras. No contexto da Internet, também é facilmente aplicada a casos como empresas que tratam dados recolhidos diretamente dos usuários. A NCII, contudo, apresenta uma situação mais desafiadora do ponto de vista da aplicação da legislação em matéria de proteção de dados pessoais: informação de terceiros, publicada por pessoas singulares em plataformas como redes sociais. Trata-se de uma situação para a qual a legislação em matéria de proteção de dados pessoais não foi tradicionalmente pensada.

Nesse sentido, a presente dissertação busca responder à seguinte pergunta: o direito ao apagamento de dados pessoais ("direito a ser esquecido") previsto no artigo 17.º do RGPD pode ser aplicado ao caso de disseminação não consensual de imagens íntimas? Para responder a essa pergunta, teremos de indagar: 1) em que medida a disseminação não

[1] Observa-se, por exemplo, que alguns autores como Ryan (2018) e Keller (2018) tendem a utilizar o termo "direito ao esquecimento" para se referir ao artigo 17.º do RGPD, adotando, assim, "direito ao esquecimento" e "direito ao apagamento" como sinônimos, o que, como se verá adiante, não corresponde a uma utilização precisa dos termos. Tal abordagem pode ter sido induzida, contudo, pela própria redação do artigo, que justapõe os dois termos, colocando o termo "direito a ser esquecido" entre parênteses ao lado do título "Direito ao apagamento dos dados".

[2] O "*direito ao esquecimento*" delineado no caso *Google Spain* chegou a ser celebrado como remédio ideal para as vítimas de NCII (EDWARDS, 2014).

consensual de imagens íntimas afeta o direito à proteção de dados pessoais, 2) se o apagamento de dados previsto no artigo 17.º do RGPD, aplicado em caso de disseminação não consensual de imagens íntimas, decorre da configuração do direito ao esquecimento, e 3) a que sujeito compete a obrigação de apagamento correlata ao direito previsto no artigo 17.º do RGPD, tendo em vista que a prática de NCII normalmente depende de dois atores: a pessoa singular que publica o conteúdo, e a plataforma na qual o conteúdo é disseminado.

A presente dissertação divide-se em quatro capítulos. O primeiro capítulo dedicar-se-á à descrição da prática da disseminação não consensual de imagens íntimas, retratando aspectos relevantes que serão tidos em consideração na sua análise posterior, do ponto de vista da proteção de dados pessoais. Assim, examinar-se-á o contexto em que a prática está inserida (tópico 1.1), seus principais aspectos (tópico 1.2) e os efeitos para a pessoa retratada nas imagens (tópico 1.4). No segundo capítulo, proceder-se-á à análise da NCII sob a ótica da proteção de dados, buscando compreender em que medida afeta o direito à proteção de dados pessoais. Nesse sentido, o tópico 2.1 examinará a relação entre a disseminação não consensual de imagens íntimas e os direitos da personalidade que estão ligados à proteção de dados pessoais. O tópico 2.2, por sua vez, buscará construir a NCII como uma violação ao direito à proteção de dados pessoais, tendo como ponto de partida a ideia de integridade contextual de Nissenbaum (2004, 2010) trazida para a proteção de dados pessoais, como sugere Bioni (2019).

O terceiro capítulo abordará mais especificamente a NCII à luz do Regulamento (UE) 2016/679, considerando o papel do consentimento como forma de legitimação do tratamento de dados pessoais. Em um primeiro momento, examinar-se-á o direito à proteção de dados ao longo dos tempos, observando sua construção no direito estadunidense (tópico 3.1.1) e a sua evolução no contexto europeu, abordando a construção geracional de Viktor Mayer-Schönberger (tópico 3.1.2). Em seguida, examinar-se-á o consentimento como forma de legitimação do tratamento de dados pessoais (tópico 3.2), bem como seus limites (tópico 3.3), decorrentes de problemas cognitivos e estruturais. Finalmente, no ponto 3.4, abordar-se-á a NCII como um tratamento ilícito de dados por violação ao disposto no artigo 9.º, número 1, do Regulamento, que proíbe o tratamento de categorias especiais de dados, nas quais se inserem dados sobre a vida sexual de uma pessoa.

O quarto capítulo será dedicado ao direito ao apagamento de dados pessoais no contexto do NCII. Considerando que o NCII afeta não só o direito à privacidade e outros direitos da personalidade, mas também o direito à proteção de dados pessoais, e tendo em vista que a disseminação não consensual de imagens íntimas pode configurar um tratamento ilícito de dados pessoais, configura-se uma hipótese de aplicação do direito previsto no artigo 17.º do Regulamento. Assim, o tópico 4.1 analisará a relação entre o direito ao apagamento e o direito ao esquecimento, a fim de examinar uma possível configuração do direito ao esquecimento no caso do NCII. Para isso, diferentes acepções do direito ao esquecimento serão examinadas: a acepção tradicional (tópico 4.1.1), e as acepções que surgiram na era da Internet (tópico 4.1.2). Também será feita uma análise da relação entre o direito ao apagamento, disposto no artigo 17.º, e o "direito ao esquecimento" (tópico 4.1.3). Finalmente, o tópico 4.2 busca compreender quais atores serão obrigados a realizar o apagamento, tendo em vista que a NCII depende da ação de pessoas singulares na condição de usuários de redes sociais ou *sites* de compartilhamento, e das próprias plataformas e *sites*. Para isso, é preciso examinar a possibilidade de se considerar o usuário como responsável pelo tratamento dos dados disseminados (tópico 4.2.1), bem como o próprio provedor do serviço de rede social ou *site* de compartilhamento (tópico 4.2.2).

1. CONSIDERAÇÕES SOBRE O PROBLEMA DA DISSEMINAÇÃO NÃO CONSENSUAL DE IMAGENS ÍNTIMAS

1.1 A digitalização, o aumento da capacidade de armazenamento e processamento de dados, a *web 2.0* e a "ascensão da lembrança"

É possível identificar uma revolução nas tecnologias da informação a partir das últimas décadas do século XX. O aprimoramento dos *chips,* o advento do microprocessador e o lançamento dos primeiros microcomputadores de sucesso comercial foram alguns dos acontecimentos que modificaram de forma drástica a economia, a cultura e a sociedade. (CASTELLS, 2010, p. 43). É notável a evolução que a computação proporcionou na capacidade de acumulação, armazenamento e transmissão de informação. Anteriormente, informações eram armazenadas manualmente em livros ou ficheiros, por exemplo, através da técnica da escrita. A computação permitiu um aumento exponencial das informações processadas, que também passaram a ser acumuladas em outros formatos, como o *compact disk* (CD), o pen drive e o computador pessoal[3]. Além disso, observou-se uma evolução qualitativa no processamento de informações, que passaram a ser mais precisamente organizadas, facilitando, por exemplo, a localização de documentos através de ferramentas de busca (BIONI, 2019, cap. 1).

Nesse contexto, cada vez mais tipos de informação, como áudio e vídeo, passaram a ser digitalizados. Isso trouxe benefícios significativos, que incluem a possibilidade de compressão de dados e a correção de erros (NEGROPONTE, 1995, p. 15). A digitalização permite que o conteúdo de um arquivo não se perca no tempo. Diferentemente do que acontecia na era analógica, a qualidade daquilo que é gravado em formato digital (seja áudio, vídeo, ou outro tipo de arquivo) não se deteriora com o tempo. Uma cópia digital de uma imagem, por exemplo, é uma réplica exata do original, ainda que se trate da cópia de uma cópia. O uso também não afeta a integridade do conteúdo: é possível ouvir o mesmo arquivo de áudio repetidas vezes, sem que este seja danificado (diferentemente do que

[3] Estima-se que, de 1956 a 1996, os discos rígidos dos computadores multiplicaram por seiscentos a sua capacidade de estoque e por setecentos e vinte mil a densidade da informação registrada (LÉVY, 1997, p. 39).

ocorria, por exemplo, com o áudio gravado em fitas *cassette*) (MAYER-SCHÖNBERGER, 2009, cap. 3).

Na era digital, um único equipamento é capaz de acumular informações em diversos formatos. Um disco rígido de um computador comporta músicas, vídeos e arquivos de texto sem risco de a informação se misturar ou haver dano ao conteúdo ou ao equipamento. Essa padronização acabou por facilitar o compartilhamento e distribuição da informação em rede. Tal mudança é significativa quando se tem em conta que, antes da digitalização, informações eram distribuídas em infraestruturas separadas de acordo com o seu tipo: jornais eram enviados às bancas em automóveis, filmes eram enviados aos cinemas, rádios utilizavam um sistema de transmissores. Já a informação digital pode ser enviada através da mesma rede, independentemente do tipo de conteúdo (MAYER-SCHÖNBERGER, 2009, cap. 3).

Pode-se dizer que o *big data* representa o êxtase do progresso quantitativo e qualitativo da gestão da informação (BIONI, 2019, cap. 1). O termo *big data* normalmente é associado aos três "vs": volume, velocidade e variedade. O *big data* excede a capacidade das tecnologias tradicionais de processamento, e consegue organizar quantidades antes inimagináveis de informação em diversos formatos e em alta velocidade (BIONI, 2019, cap. 1; CASTRO, 2016, p. 1052). Através da análise de quantidades massivas de dados, são identificadas correlações entre fatos, e a partir destas, são feitas previsões, o que torna as informações extremamente valiosas. Por tal razão, dados são referidos como "o petróleo da economia da informação" (MAYER-SCHÖNBERGER e CUKIER, 2013, cap. 1).

A evolução na tecnologia da informação não significou apenas a melhoria qualitativa e quantitativa da capacidade de armazenamento e processamento de dados, mas também permitiu a conexão de pessoas em rede. A Internet teve modificações significativas desde a sua criação, incluindo, principalmente, o surgimento de *sites* e aplicativos baseados em conteúdo gerado pelos próprios usuários. O termo *web 2.0* foi o adotado por Tim O'Reilly para se referir a essa transformação (O'REILLY, 2005). Em seus primeiros anos, a Internet era utilizada para acessar informações e interagir com outras pessoas através da rede global (essa fase é chamada *web 1.0*). Por volta de 2001, a Internet passou a ser visualizada não apenas como um meio para receber informações, mas também para produzir e compartilhar informações com outros usuários, falando-se, assim, em *web 2.0* (MAYER-SCHÖNBERGER, 2009, cap. 1).

Helen Nissenbaum define *web 2.0* como um "*social software ecosystem*". De acordo com Nissenbaum, o termo corresponde a "uma ampla classe de *sites* dedicados a criar e manter laços sociais"[4] (2010, p. 59, tradução nossa). Assim, redes sociais como o *Facebook* e *sites* colaborativos como a *Wikipedia* são exemplos daquilo que se entende por *web 2.0*. *social softwares, e* permitem que indivíduos, mesmo com recursos tecnológicos modestos, publiquem opiniões, fotos, música e *links*. O próprio usuário também pode avaliar a qualidade ou a performance de serviços fornecidos pelos *sites* (2010, p. 59).

Ressalta-se que o avanço das tecnologias da informação e comunicação também fez com que dados pessoais de consumidores se tornassem extremamente valiosos do ponto de vista econômico. Informações sobre hábitos de consumo permitem empreender de forma mais eficiente no mercado (BIONI, 2019, cap. 1). Através das aplicações da Internet, consumidores passam a ter participação ativa no ciclo de consumo, fornecendo opiniões que podem orientar a confecção, distribuição ou segmentação de um bem. Redes sociais, por exemplo, recolhem vários tipos de dados sobre seus usuários ao longo da interação com a aplicação, de modo que o usuário fornece um perfil dos próprios hábitos, que pode ser utilizado para direcionamento de publicidade. A publicidade comportamental online reduz os custos da ação publicitária, correlacionando o bem de consumo "cirurgicamente aos interesses do consumidor abordado" (BIONI, 2019, cap. 1). A proliferação de dados em rede fornecidos pelos próprios utilizadores é uma consequência do princípio da participação ativa, apontado como um dos princípios da *web 2.0* (GONZÁLES FUSTER e GUTWIRTH, 2008, p. 350).

Outra questão que merece destaque é a Internet das coisas (também chamada de computação pervasiva ou ubíqua, ou *web 3.0*), que possibilita a obtenção de dados de formas antes inimagináveis. No passado, na maioria das vezes, o fornecimento de dados estava ligado a atividades das quais o titular de dados pessoais estava ciente, e sobre as quais tinha algum controle. Na era da Internet das coisas há uma vigilância pervasiva, sobre a qual o sujeito não tem mais controle (ČAS, 2011, p. 140). *Microchips* ou *nanochips* são incorporados a objetos (geladeiras, relógios, máquinas de café etc.) e, através da tecnologia RFID (*Radio Frequency Identification*) associada a meios de comunicação, são monitorados à distância, em tempo real. Por ser muito pequeno, o

[4] *"A loose class of Web sites dedicated to creating and maintaining social ties, groups, and networks"* (NISSENBAUM, 2010, p. 59).

transmissor incorporado ao objeto é imperceptível, o que torna seu controle invisível e potencialmente intrusivo (CASTRO, 2016, p. 1058).

Toda a conjuntura acima mencionada gera questionamentos no que toca à proteção de dados pessoais e à privacidade. Indivíduos podem perder o controle sobre quais informações circulam sobre si, quem as processa e para quais fins. Nesse sentido, Poullet afirma que as tecnologias podem representar um risco às liberdades tão grande quanto as vantagens que propõe. Tivemos de nos habituar a sermos vigiados constantemente, a sermos reduzidos a números e tivemos de aceitar a percepção de nossas informações pessoais como mercadoria (POULLET, 2009, p. 226).

Especialmente no contexto das redes sociais, podem ser identificados diversos problemas. Nesse sentido, Nissenbaum menciona três potenciais complicações. A primeira diz respeito a indivíduos que publicam informações sobre si próprios que, posteriormente, quando descobertas, trazem inconvenientes. Cita como exemplo o caso de uma família enfurecida após descobrir sobre o consumo de drogas da filha adolescente em sua página no *Facebook*, ou o caso de candidatos a empregos ou estágios que são descartados do processo seletivo devido a postagens comprometedoras no *Facebook* (2010, p. 59). O segundo tipo de problema mencionado por Nissenbaum diz respeito a indivíduos que publicam informações sobre terceiros, prática comum em *sites* como o *Facebook*, que possui uma função que permite identificar outros usuários em uma imagem, capturada e publicada com ou sem o seu consentimento. Já o terceiro problema diz respeito à capacidade de monitoramento e rastreamento dos usuários de redes sociais (2010, p. 60).

Mayer-Schönberger afirma que, com a revolução tecnológica mencionada e a chegada da "era digital", vive-se a "ascensão meteórica da lembrança" ("*meteoric rise of remembering*"). O armazenamento de dados torna-se cada vez mais barato, enquanto a capacidade de armazenamento torna-se cada vez maior. Além disso, a capacidade de extração de informação também foi facilitada: basta digitar algumas palavras em uma ferramenta de busca no computador, por exemplo, para que, em alguns segundos, seja gerada uma lista de arquivos com os termos pesquisados. Isso faz com que vastas quantidades de informação sirvam como uma extensão da memória humana. Por fim, redes globais digitais eliminaram a necessidade de deslocamento geográfico para acessar uma determinada base de dados. Como resultado, é cada vez mais difícil que algumas informações sejam esquecidas. Para Mayer-Schönberger, "o resultado é um mundo que é

programado para lembrar"[5] (MAYER-SCHÖNBERGER, 2009, cap. 3, tradução nossa).

Essa memória digital pode ser problemática. Mayer-Schönberger inicia seu livro mencionando o caso de Stacey Snyder, uma estudante de 25 anos que se preparava para ser professora em 2006. Apesar de ter obtido todos os créditos, passado nos exames e completado o treinamento para exercer a profissão, não obteve seu certificado. O motivo alegado foi que seu comportamento não condizia com o de uma professora. Uma foto em seu perfil na rede social *MySpace* mostrava Snyder em uma festa, vestindo uma fantasia de pirata e segurando um copo de plástico, com a legenda "*drunken pirate*" ("pirata bêbado"). A administração da Universidade considerou a fotografia como um exemplo de conduta não profissional, afirmando que poderia expor alunos à imagem de um professor consumindo álcool. Snyder considerou retirar a foto do *site*, mas a página já havia sido catalogada por motores de busca, e a imagem já havia sido arquivada por usuários da *web*. Nas palavras de Mayer-Schönberger, "a Internet lembrou o que Stacey queria ter esquecido"[6] (MAYER-SCHÖNBERGER, 2009, cap. 1, tradução nossa).

No mesmo sentido, Solove chama atenção para a rapidez com que informações pessoais são divulgadas na Internet, para a forma com que são permanentemente arquivadas e facilmente acessadas pelos motores de busca. O *Google* é capaz de vasculhar bilhões de páginas da *web* em uma fração de segundos. Para saber algo sobre uma determinada pessoa, basta digitar seu nome na ferramenta de busca do *Google* e é possível obter uma lista de *websites* contendo informações sobre esse indivíduo. No passado, mesmo publicações escritas poderiam ser esquecidas com o tempo. A sua extração seria mais difícil, já que uma busca em arquivos físicos de bibliotecas demandaria tempo. Com a Internet, contudo, publicações podem danificar permanentemente a reputação de uma pessoa. Um fato poderá ser acessado através do *Google* em menos de um segundo, e estará disponível em todo o mundo (SOLOVE, 2007, p. 33).

O fluxo espontâneo de informações da Internet pode, de acordo com Solove, restringir a nossa liberdade. Se cada má decisão que tomarmos for gravada em um "registro permanente", isso afetará nossa capacidade de definir nossas identidades, de conseguir emprego, e de participar na vida pública (2007, p. 17). Solove menciona o caso

[5] "*The result is a world that is set to remember"* (MAYER-SCHÖNBERGER, 2009, cap. 3)
[6] "*The Internet remembered what Stacy wanted to have forgotten*" (MAYER-SCHÖNBERGER, 2009, cap. 1).

real de um jovem norte americano de 19 anos, que publicou em 2004 um vídeo de si mesmo dançando ao som de "*Dragostea Din Tei*", uma canção romena popular na época. O vídeo tinha como intenção provocar o humor, e teve aproximadamente dois milhões de downloads, trazendo reconhecimento ao seu autor (2007, p. 42).

O jovem posteriormente tentou evitar a exposição e buscou refúgio na casa de sua família. Todavia, já não era possível desfazer a situação que havia se concretizado: vários outros *sites* já haviam reproduzido o vídeo, e já havia sido criada até mesmo uma página da *Wikipedia* dedicada ao vídeo. Se no passado, tolices cometidas na adolescência costumavam ser esquecidas, com a Internet, são preservadas para a eternidade, e tornam-se o motivo pelo qual uma pessoa será para sempre lembrada (SOLOVE, 2007, p. 42).

É nesse contexto de inovações tecnológicas, grande capacidade de armazenamento e compartilhamento de informações e "ascensão meteórica da lembrança" que se insere o problema da disseminação não consensual de imagens íntimas, o qual pretendemos discutir ao longo dos próximos capítulos. Trata-se da publicação ou distribuição de imagens íntimas ou sexualmente explícitas sem o consentimento da pessoa representada. Uma vez disponibilizado online, o número de pessoas que visualizam o material pode crescer exponencialmente em poucos dias, e é praticamente impossível remover as imagens (BEYENS e LIEVENS, 2016, p. 42).

1.2 A prática da disseminação não consensual de imagens íntimas

A Disseminação não consensual de imagens íntimas - NCII consiste na distribuição de imagens sexualmente explícitas ou imagens íntimas sem o consentimento da pessoa retratada (BEYENS e LIEVENS, 2016, p. 32; HENRY e POWELL, 2016, p. 399). A prática é popularmente referida como "*revenge porn*", ou "pornografia de vingança". O nome remete ao cenário comumente descrito na mídia convencional ao relatar episódios de disseminação não consensual de imagens íntimas: o caso de um ex-namorado ou ex-marido que publica imagens íntimas da ex-companheira como vingança pelo término do relacionamento. Essa descrição, porém, é bastante reducionista (BEYENS e LIEVENS, 2016, p. 32).

A adoção do termo "*revenge porn*", apesar de comum, é problemática por vários motivos. A palavra "*revenge*" ou "vingança" pode criar a impressão errônea de que os atos

são exclusivamente cometidos por ex-companheiros (BEYENS e LIEVENS, 2016, p. 33), ou de que são praticados tendo como motivação exclusiva a vingança. O termo não abrange, por exemplo, situações em que aquele que compartilha as imagens busca a humilhação ou a manipulação da pessoa retratada, a gratificação sexual, a notoriedade ou o lucro (HENRY e POWELL, 2016, p. 400; RYAN, 2018, p. 1054).

O uso da palavra "*porn*" ou "pornografia" também é apontado como inadequado, por focar indevidamente no conteúdo das imagens e nas ações da pessoa representada. Referir à prática como pornografia também acarreta o risco de minimizar o mal causado às vítimas, e de correlacionar as imagens a um subgênero aceitável e/ou desejável dentro da pornografia online comercial. A pornografia é algo notoriamente difícil de se definir, pela diversidade do conteúdo considerado como sexual, e pela interpretação deste conteúdo (se a intenção e o efeito são de excitação sexual). As imagens distribuídas sem o consentimento podem ter outros propósitos que não a excitação sexual, e o conteúdo pode não servir ao propósito da pornografia (HENRY e POWELL, 2016, p. 401).

Normalmente, presume-se que a pornografia comercial convencional seja produzida por pessoas adultas e que prestam o seu consentimento, o que não é o caso da NCII (BEYENS e LIEVENS, 2016, p. 33). Também se argumenta que o termo "pornografia" confere um sentido de escolha e legitimidade que não captura suficientemente a natureza não consensual do compartilhamento de imagens (MCGLYNN, RACKLEY e HOUGHTON, 2017, p. 38).

Por essas razões, alguns autores sugerem a adoção de termos como "pornografia não consensual" ("*nonconsensual pornography")* (CITRON e FRANKS, 2014), "abuso sexual baseado em imagem" ("*image-based sexual abuse*") (MCGLYNN, RACKLEY e HOUGHTON, 2017), "violência sexual facilitada pela tecnologia" ("*technology facilitated sexual violence*") (HENRY e POWELL, 2015), "disseminação não consensual de imagens sexuais" ("*non-consensual dissemination of sexual images*") (BEYENS e LIEVENS, 2016), e "disseminação não consensual de imagens íntimas" (CODING RIGHTS; e INTERNETLAB, 2017; VALENTE *et al.*, 2016). O presente trabalho opta pelo uso do último termo, buscando manter consistência com trabalhos publicados sobre o tema em língua portuguesa, bem como a adoção da sigla internacional NCII, que já é empregada na língua inglesa por algumas redes sociais como *Facebook* e *Twitter* (MADDOCKS, 2018,

p. 351), e que também é adotada por Valente *et al*. como forma de dialogar com a literatura internacional sem mais mediações (VALENTE *et al.*, 2016, p. 6).

Na prática do NCII, o material disseminado pode ser obtido de várias formas. As fotos ou vídeos podem ter sido produzidos pela própria vítima e enviados voluntariamente à pessoa que posteriormente os publicou sem o seu consentimento. Em outros casos, as imagens são produzidas através da sobreposição do rosto da vítima em uma imagem pornográfica pré-existente. O conteúdo também é muitas vezes obtido através de *hacking* no computador ou no smartphone da vítima. Além disso, há também casos em que as imagens são capturadas enquanto a vítima está dormindo, inconsciente, afetada por drogas ou álcool e/ou durante uma violação sexual, e em seguida compartilhadas online (HENRY e POWELL, 2016, p. 400).

Na maioria das vezes, as imagens são publicadas online, em redes sociais como o *Facebook*, em *sites* pornográficos convencionais ou em *sites* pornográficos dedicados ao "*revenge porn*",[7] e em aplicativos de foto ou vídeo. As imagens compartilhadas estão frequentemente acompanhadas de outras informações pessoais da vítima, como seu nome, endereço de residência, endereço do local de trabalho, número de telefone, e-mail e *links* para perfis nas redes sociais. Tal prática é conhecida como *doxing.* Também é comum o envio das imagens diretamente para os amigos, a família ou o empregador da vítima (BEYENS e LIEVENS, 2016, p. 32; RYAN, 2018, p. 1055).

É possível identificar a prática da disseminação não consensual de imagens íntimas mesmo antes da popularização da Internet e da criação das redes sociais. O caso Lajuan and Billy Wood v. Hustler Magazine, Inc., nos Estados Unidos, é um exemplo. LaJuan Wood teve sua residência invadida por um vizinho, que furtou algumas de suas fotos íntimas e as enviou para a revista *Hustle*. A revista, por sua vez, publicou as fotografias sem o consentimento de Wood, em uma seção dedicada a imagens de nudez,

[7] Um dos exemplos mais conhecidos de *sites* lucrativos dedicados ao "*revenge porn*" é o *IsAnyoneUp*, criado por Hunter Moore nos Estados Unidos. O *site* publicava imagens de nudez sem o consentimento das pessoas retratadas, supostamente enviadas por ex-namorados, identificando as vítimas pelo nome, pelos perfis nas redes sociais e informações de contato (OHLHEISER, 2015). O *site* já chegou a ter sessenta mil acessos por mês, e gerar oito mil dólares por mês em anúncios, o que permitiu que seu criador abandonasse o emprego para se dedicar exclusivamente à página, que foi desativada em 2012 (HALL e HEARN, 2018, p. 17; HILL, 2011). *Sites* dedicados ao "*revenge porn*" normalmente atraem um número significativo de visualizações. Além disso, como o conteúdo dessas páginas é normalmente gerado pelo próprio usuário, não é necessário grande investimento por parte do operador do *site*, o que torna o "*revenge porn"* atraente de um ponto de vista econômico em alguns casos (LANGLOIS e SLANE, 2017, p. 127). Alguns *websites* também cobram taxas para remover as imagens ou vídeos (HALL e HEARN, 2018, p. 18).

acompanhada de informações como o seu nome e a cidade onde morava (WOOD V. HUSTLER MAGAZINE, 1984).

Apesar de não ser um problema recente, a prática da disseminação não consensual de imagens íntimas tem sido muito frequente nos últimos anos devido a uma série de mudanças sociais trazidas por novas tecnologias, principalmente diante da ubiquidade das câmeras digitais, a fácil distribuição de conteúdo online, e o uso de armazenamento em nuvem (MCGLYNN, RACKLEY e HOUGHTON, 2017, p. 26; SINGLETON, SEIGNIOR e SUZOR, 2017, p. 1058; VALENTE *et al.*, 2016, p. 2). Observa-se que as tecnologias digitais passaram a desempenhar um papel também na comunicação sexual. A palavra "*sexting*"[8] passou a ser usada para descrever esse fenômeno, referindo-se ao envio de mensagens ou imagens sexualmente explícitas pelo telefone celular, e foi adicionada ao dicionário *Merriam-Webster* da língua inglesa em 2012 (DROUIN, ROSS e TOBIN, 2015, p. 197). Estudos sugerem que o *sexting* tornou-se relativamente comum em relacionamentos entre jovens adultos (DROUIN *et al.*, 2013; DROUIN e LANDGRAFF, 2012, p. 446; DROUIN, ROSS e TOBIN, 2015, p. 200).

A disseminação não consensual de imagens íntimas pode afetar tanto homens quanto mulheres. Contudo, apesar de pesquisas sobre a frequência de NCII ainda serem escassas, há indícios de que a prática atinge as mulheres com maior frequência (CITRON e FRANKS, 2014, p. 353; HENRY e POWELL, 2016, p. 399; MCGLYNN, RACKLEY e HOUGHTON, 2017, p. 29; VALENTE *et al.*, 2016, p. 54). Uma pesquisa conduzida nos Estados Unidos por Ruvalcaba e Eaton examinou as taxas de vitimização e perpetração da disseminação não consensual de imagens íntimas (referida na pesquisa como "pornografia não consensual"), bem como a correlação entre a vitimização e saúde. A análise revelou que as taxas de vitimização variaram significativamente entre participantes homens e mulheres, de modo que as mulheres reportaram taxas mais altas de vitimização e mais baixas de perpetração do que os homens (RUVALCABA e EATON, 2020, p. 5). Langlois e Slane realizaram uma pesquisa no *site* dedicado à pornografia de vingança "*myex.com*", e verificaram que 84,5% das vítimas eram mulheres, e 15,5% eram homens, tendo como

[8] Henry e Powell ressaltam que não há um consenso sobre a definição de "*sexting*", principalmente sobre se esse termo engloba tanto comportamentos consensuais como não consensuais. Uma definição ampla acarreta o risco de agrupar uma gama diversificada de comportamentos em um só termo. Isso pode ter efeitos problemáticos no tratamento da vítima, como presumir que o comportamento da vítima foi arriscado ou promíscuo, ou ainda negar o consentimento em situações em que a troca de mensagens foi consensual (2015, p. 108).

base o número total de publicações até 29 de outubro de 2015 (LANGLOIS e SLANE, 2017, p. 135).

Em alguns casos, a NCII pode se manifestar em um contexto de práticas de violência doméstica. Frequentemente os vídeos e imagens são produzidos mediante coerção da vítima e, em outras situações, pessoas ameaçam publicar imagens íntimas de seus parceiros como forma de impedi-los de terminar o relacionamento (CITRON e FRANKS, 2014, p. 351). Há também situações em que um parceiro ameaça revelar as imagens ou filmagens aos filhos do casal ou ao resto da família caso a esposa ou companheira tente denunciá-lo por violência doméstica (HENRY e POWELL, 2015, p. 113).

A disseminação não consensual de imagens íntimas traz sérias implicações à saúde psicológica das vítimas, bem como para suas vidas sociais, profissionais e familiares. Também há riscos para a segurança pessoal devido à possibilidade de perseguição ou assédio, riscos de violência doméstica, danos à reputação, perda de perspectiva de emprego, entre outras consequências (CITRON e FRANKS, 2014, p. 351; HENRY e POWELL, 2016, p. 403). Os efeitos das publicações são amplificados na Internet, já que milhares de pessoas podem ter acesso ao conteúdo e replicá-lo, aumentando o seu alcance de formas antes inimagináveis (CITRON e FRANKS, 2014, p. 350).

Devido à sua gravidade, a conduta já foi criminalizada em diversos Estados, como Reino Unido (*Abusive Behaviour and Sexual Harm Act*, 2016*; Criminal Justice and Courts Act,* 2015), França (*Code Pénal*, 1994), Bélgica (Code Pénal, 1867), Alemanha (Código Penal, 1998), Malta (Criminal Code, Chapter 9 of the Laws of Malta, 1854), Itália (Codice Penale, 1930), Brasil (Código Penal,1940) e Espanha (Código Penal, 1995). Em Portugal, a Lei n.º 44/2018 alterou o artigo 152.º do Código Penal Português, prevendo pena mínima maior para a difusão de imagem ou som relativos à intimidade da vida privada de alguém sem o seu consentimento, através da Internet ou outros meios de difusão pública generalizada, em um contexto de violência doméstica. A lei também alterou o artigo 197.º do Código Penal Português, para determinar que as penas previstas nos artigos 190.º a 195.º (crimes contra a reserva da vida privada) sejam elevadas de 1/3 nos seus limites mínimo e máximo se o fato for praticado através de meio de comunicação social, ou da

difusão através da Internet, ou de outros meios de difusão pública generalizada (Código Penal. Lei n.º 59/2007).

1.3. Os riscos associados à disseminação não consensual de imagens íntimas

A disseminação não consensual de imagens íntimas traz consequências particularmente graves às pessoas retratadas. Vítimas relatam dificuldade em confiar em outras pessoas e baixa autoestima em decorrência da exposição. Podem sofrer de ansiedade, ataques de pânico, transtorno de estresse pós-traumático, depressão, pensamentos suicidas e insônia (BATES, 2017, p. 23; CITRON e FRANKS, 2014, p. 358). Também há casos de vítimas que cometeram suicídio após a publicação das imagens (BATES, 2017, p. 31; FARIA, ARAÚJO e JORGE, 2015, p. 670; HALL e HEARN, 2018, p. 19), e relatos de consumo excessivo de álcool como forma de lidar com a ansiedade e a depressão. As consequências para a saúde mental das vítimas são semelhantes àquelas observadas em casos de violação sexual (BATES, 2017, p. 35).

Tendo em conta que as pessoas retratadas nas imagens são facilmente identificadas, e muitas vezes suas informações pessoais são publicadas junto às postagens, a disseminação não consensual de imagens íntimas aumenta o risco de *stalking* e de ataques físicos às vítimas. Muitas vezes, as fotos ou vídeos são acompanhados do endereço ou números de contato da pessoa retratada como forma de encorajar estranhos a contactá-la off-line. Algumas vítimas recebem ligações e e-mails de desconhecidos. Citron e Franks citam o exemplo de uma assistente de professor de trinta e três anos que relatou medo de sair de casa e de andar sozinha depois que suas imagens íntimas foram publicadas junto ao endereço de sua casa (CITRON e FRANKS, 2014, p. 351; HENRY e POWELL, 2016, p. 403).

Bates (2017) conduziu uma pesquisa qualitativa sobre os efeitos emocionais e para a saúde mental que a NCII provoca das vítimas. Em uma das entrevistas, uma vítima relatou que homens desconhecidos apareciam em sua casa em busca de sexo após a publicação de suas fotos e seu endereço por seu ex-namorado. Um homem chegou a invadir sua casa e a tentar estrangulá-la. Como resultado, a vítima passou a sofrer de ansiedade em público, particularmente à noite, e foi forçada a mudar sua rotina e hábitos. A insegurança e a vulnerabilidade geradas pela exposição contribuem para o surgimento de condições como ansiedade e ataques de pânico (BATES, 2017, p. 32).

Em muitos casos de disseminação não consensual de imagens íntimas, as vítimas são expostas de maneira humilhante. Em *sites* dedicados a *slut-shaming,*[9] usuários anônimos podem comentar as fotos publicadas, e ameaças de violação são frequentes. "*First I will rape you, then I'll kill you*" é o exemplo destacado por Citron e Franks (2014, p. 353). Algumas vítimas são reconhecidas quando saem de casa, e, para evitar maior exposição, tendem a se isolar. Vítimas mudam de residência e algumas modificam a própria aparência. É comum a deterioração das relações sociais, principalmente porque as vítimas são frequentemente culpadas por terem permitido que fotos e vídeos fossem capturados (BATES, 2017, p. 25; FARIA, ARAÚJO e JORGE, 2015 p. 671; HALL e HEARN, 2018, p. 21).

Ruvalcaba e Eaton (2020), em sua pesquisa sobre as taxas de vitimização e perpetração da disseminação não consensual de imagens íntimas e a correlação entre a vitimização e saúde, verificaram que as mulheres vítimas de NCII reportaram bem-estar psicológico mais baixo e níveis mais elevados de sintomas somáticos do que aquelas que não foram vítimas de NCII, em consonância com o que sugeriu Bates (2017) (RUVALCABA e EATON, 2020, p. 73).

São comuns casos de suicídio após a disseminação não consensual de imagens íntimas. Hall e Hearn mencionam notícias de mortes de adolescentes nos Estados Unidos, no Brasil e no Canadá (HALL e HEARN, 2018, p. 21). Na Itália, um dos casos com maior repercussão midiática foi a morte de Tiziana Cantone, uma mulher de 31 anos que apareceu em seis vídeos íntimos disseminados na Internet. Cantone havia enviado os vídeos para o ex-namorado e alguns amigos através do aplicativo *WhatsApp*. Pouco tempo depois, o conteúdo foi replicado em *sites* pornográficos e nas redes sociais, ganhou popularidade, e tornou-se alvo de piadas e paródias na Internet. Devido à grande repercussão, mudou seu nome para Tiziana Giglio e mudou-se também para uma nova casa. Suicidou-se um ano e meio após a publicação dos vídeos, tendo já atentado contra a própria vida em duas ocasiões (FORSTER, 2016).

Na Espanha, também foi amplamente divulgado o caso de Verónica, uma funcionária de uma fábrica da Iveco que se suicidou em maio de 2019, após a divulgação de vídeos sexuais nos quais ela aparecia. As filmagens circulavam entre seus colegas de

[9] *Slut shaming* é o termo em inglês que se refere ao ato de difamar mulheres por possíveis atividades sexuais(FARIA, ARAÚJO e JORGE, 2015, p. 671).

trabalho, primeiro em um grupo de 20 pessoas, depois entre mais de 200. Verónica sofria humilhação constante no ambiente de trabalho, onde frequentemente os colegas se aproximavam em grupo para verificar se era mesmo a pessoa retratada nos vídeos (VALDÉS, 2019).

Além dos efeitos para a saúde mental, a NCII pode trazer problemas financeiros e para a vida profissional das vítimas. São muitos os casos de pessoas que perderam o emprego devido à disseminação de suas imagens íntimas (BATES, 2017, p. 37; BEYENS e LIEVENS, 2016, p. 32; CITRON e FRANKS, 2014, p. 352; FRANKS, 2016, p. 1259). É comum que os autores das publicações enviem as imagens também para conhecidos da vítima, incluindo empregadores e colegas de trabalho. O ex-marido de uma das mulheres entrevistadas por Bates enviou um vídeo da ex-esposa sendo violada para a diretoria da escola onde trabalhava. A vítima foi demitida de seu cargo de superintendente escolar imediatamente após o envio da filmagem para seus colegas de trabalho (BATES, 2017, p. 37). Em alguns casos, a vítima se vê compelida a abandonar o trabalho devido à repercussão das imagens. Franks menciona a história de Lori Douglas, uma juíza canadense que se afastou do cargo em 2014, devido à descoberta de fotos íntimas publicadas por seu marido sem o seu consentimento em 2003 (FRANKS, 2016, p. 1265). O mesmo ocorreu com uma brasileira de 19 anos, retratada em um vídeo altamente popularizado em 2013, que deixou de trabalhar e estudar devido à sua repercussão (FARIA, ARAÚJO e JORGE, 2015, p. 670).

As vítimas também podem ter dificuldade de encontrar um novo emprego após a disseminação. É comum que empregadores e recrutadores pesquisem pelos nomes de candidatos em motores de busca antes da contratação (BAMBAUER, 2014, p. 2039; CITRON e FRANKS, 2014, p. 352). A pesquisa *Online Reputation in a Connected World,* conduzida em 2009 entre recrutadores, profissionais de recursos humanos e gerentes de contratação na França, na Alemanha, no Reino Unido e nos Estados Unidos, indicou essa tendência. Nos Estados Unidos, 79% dos recrutadores entrevistados relataram buscar informação adicional sobre a reputação dos candidatos online. No Reino Unido, a porcentagem foi de 47%, na França, 23%, e na Alemanha, 59% (MICROSOFT, 2010, p. 6). Além disso, 70% dos recrutadores nos Estados Unidos já haviam rejeitado candidatos com base em dados encontrados online. A porcentagem foi de 41% no Reino Unido, 16% na Alemanha e 14% na França (MICROSOFT, 2010, p. 5).

Empregadores tendem a evitar o risco de contratar uma pessoa que teve sua intimidade exposta na Internet, já que a reputação de um empregado pode comprometer a maneira como uma empresa é vista por seus clientes e sócios. Assim, por mais que as imagens ou vídeos em questão façam parte da esfera íntima da pessoa retratada e não envolvam condutas relacionadas ao desempenho do trabalho, a tendência é que esse tipo de informação afete as perspectivas de emprego dos candidatos (BAMBAUER, 2014), à semelhança do que ocorreu no incidente do "pirata bêbado", citado por Mayer-Schönberger, (MAYER-SCHÖNBERGER, 2009).

2. O DIREITO À PROTEÇÃO DE DADOS PESSOAIS COMO UM DOS DIREITOS AFETADOS PELA DISSEMINAÇÃO NÃO CONSENSUAL DE IMAGENS ÍNTIMAS

2.1 A proteção de dados pessoais e a tutela da personalidade

A Carta de Direitos Fundamentais da União Europeia, em seu artigo 8.º, n.º 1, determina que "Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito". No número 2, prevê que "Esses dados devem ser objecto 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 rectificação". Reitera, assim, alguns dos princípios já contidos na Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. A proteção de dados pessoais é, portanto, considerada um direito fundamental em âmbito europeu, sendo também prevista no artigo 16.º do Tratado sobre o Funcionamento da União Europeia.

O Regulamento (UE) 2016/679 do Parlamento e do Conselho (Regulamento Geral sobre a Proteção de Dados Pessoais – RGPD), publicado em abril de 2016 e aplicável a partir de 25 de maio de 2018, reconhece como válidos os princípios e objetivos da Diretiva 95/46/CE, mas considera que estes "não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, e nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrônica". Por tal razão, tem por objetivo assegurar um nível equivalente de proteção das pessoas singulares e a livre circulação de dados pessoais na União. Considera, portanto, a natureza de direito fundamental do direito à proteção de dados pessoais e busca assegurá-lo, ao mesmo tempo em que busca garantir a livre circulação dos dados, vendo-os também como um bem econômico (BIONI, 2019, cap. 2; FINOCCHIARO, 2017, p. 2).

Quando se fala em proteção de dados pessoais, é preciso ter em mente a proteção da pessoa humana. Como observou Mayer-Schonberger ao criticar a escolha do termo "proteção de dados", "não é o dado que precisa de proteção, mas o indivíduo com o qual o

dado se relaciona"(2001, p. 219).[10] É possível conceituar o direito à proteção de dados pessoais como "o direito do sujeito a quem os dados se referem de exercitar um controle, mesmo ativo, sobre seus dados, que se estende do acesso à retificação"[11] (FINOCCHIARO, 2014, p. 152). Tal conceito guarda relação com a ideia de autodeterminação informacional, popularizada pela Decisão do Tribunal Constitucional Alemão sobre a Lei dos Censos de 1983, como o direito que "garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais" (BVERFGE, 1983 *apud* MARTINS, 2005, p. 238).

É importante observar que a proteção de dados e a autodeterminação informacional têm como fundamento o princípio da dignidade humana. Tal constatação pode ser observada da própria construção do direito à proteção de dados no espaço europeu, tendo em conta a importante decisão do Tribunal Constitucional Alemão sobre a Lei dos Censos de 1983, que delineou o direito à autodeterminação informacional a partir do artigo 2 I da Constituição da República da Alemanha - referente ao livre desenvolvimento da personalidade - c/c o artigo 1 I da Constituição – referente à dignidade da pessoa humana (PINHEIRO, 2015, p. 778).[12] [13]

Pode-se dizer que o direito à proteção de dados pessoais pertence ao âmbito dos direitos da personalidade. Um dado pessoal, definido como "informação relativa a uma pessoa singular identificada ou identificável ('titular dos dados')",[14] pode ser considerado como uma projeção da sua identidade (BIONI, 2019, cap. 2; FINOCCHIARO, 2017, p.

---

[10] "*It is not the data that is in need of protection; it is the individual to whom the data relates*"(MAYER-SCHÖNBERGER, 2001, p. 219).

[11] "*Il diritto alla protezione dei dati personali consiste nel diritto del soggetto cui i dati si riferiscono di esercitare um controllo, anche ativo, su detti dati, che si estende dall'acesso alla rettifica*" (FINOCCHIARO, 2017, p. 161).

[12] Destaca-se, nesse ponto, a observação de Ana Isabel Herrán Ortiz: "*Por outra parte, se afirma con frecuencia que el derecho a la protección de datos costituye um médio o instrumento jurídico para la garantia de ejercicio de otros valores y princípios de la persona, tales como la dignidade humana y el libre desarollo de su personalidade, lo que se traduce em el desconocimiento de su identidade como derecho de la persona; ahora bien, precisamente por ser esato así, el derecho a la protección de datos alcanza la categoria de derecho fundamental, no em vano, todos los derechos fundamentales tienen vocación instrumental respecto de la dignidade y la personalidade humana*" (2003, p. 18). No mesmo sentido, Stefano Rodotà: "*La nozione di dignità dev'essere tenuta presente tutte le volte che bisogna identificarei l significato complessivo della protezione delle informazioni personali e, in questo quadro, della tutela della riservatezza e dell'identità*"(1997, p. 584).

[13] Danilo Doneda afirma que é possível interpretar a decisão alemã como sendo representativa de uma concepção segundo a qual "*os dados pessoais merecem proteção, visto que são manifestações diretas da personalidade, e, portanto, que sua proteção pertence à órbita dos direitos fundamentais e que, nessa condição, devem se relacionar com os demais interesses envolvidos*" (DONEDA, 2019, cap. 2).

[14] Essa é a definição de dado pessoal adotada pelo Regulamento (UE) 2016/679.

161). Capelo de Sousa se refere à identidade como um atributo que se insere na dimensão relacional eu-mundo da personalidade humana (assim como a liberdade, a igualdade, a segurança, a participação, a honra, a reserva e o desenvolvimento de cada homem). “Nas relações consigo mesmo, com os outros homens, com a Natureza e com Deus, ou pelo menos com a ideia d’Ele, cada homem é um ser em si mesmo e só igual a si mesmo” (2011, p. 244). De acordo com o autor, o “bem da identidade reside [...] na própria ligação de correspondência ou identidade do homem consigo mesmo e está pois ligado a profundas necessidades humanas, a ponto de o teor da convivência humana depender de sua salvaguarda em termos de plena reciprocidade” (2011, p. 245).

O direito à identidade será lesado não apenas quando elementos da identidade humana forem falsificados ou desviados dos fins próprios do titular, mas também nos casos de inexatidão da representação da pessoa, por omissão ou insuficiência dos elementos retratados. Conforme ressalta o autor, “a tutela juscivilística da identidade humana incide desde logo sobre a configuração somático-psíquica de cada indivíduo, particularmente sobre a sua imagem física, os seus gestos, a sua voz, a sua escrita e o seu retrato moral. Mas recai também sobre os termos da inserção sócio-ambiental de cada homem, *maxime*, sobre a sua história de vida, a sua história pessoal, o seu decoro, o seu crédito, a sua identidade sexual, familiar, racial, linguística, política, religiosa e cultural" (SOUSA, 2011, p. 248). O autor ressalta que no bem identidade podem ser incluídos, também, “os próprios sinais sociais de identificação humana, quer principais, como o nome e o pseudônimo, quer acessórios, como a filiação reconhecida, o estado civil, a naturalidade e o domicílio” (SOUSA, 2011, p. 250).

Conclui-se, assim, que os dados que dizem respeito a uma pessoa integram a sua identidade. Essa constatação é ainda mais significativa no contexto atual, na era *do Big Data*, em que é possível traçar um perfil comportamental de um indivíduo a partir de seus dados de navegação, por exemplo, como já mencionado.[15] Stefano Rodotà chama atenção para o fato de que, com a evolução dos sistemas de informação e num contexto de *social networking* e *web 2.0*, a identidade está cada vez mais exposta e cada vez mais disponível

[15] Tópico 1.1 do capítulo I

para o *data minig*[16] (2012, p. 322). Rodotà também aborda a problemática do *web 3.0* ou Internet das coisas, que determinam novas modalidades de aquisição de dados pessoais. Segundo Rodotà, nesse quadro de fluxos intensos de dados, se torna cada vez mais relevante o direito de acesso, "essencial para a construção da identidade, porque confere o poder de obter o apagamento de dados falsos ou ilegitimamente recolhidos ou conservados além dos termos previstos, a retificação daqueles inexatos, a integração daqueles incompletos" (2012, p. 327, tradução nossa).[17] [18]

É importante lembrar que nossa economia e nossa sociedade se movem a partir dos *signos identificadores* do cidadão. Por isso, os nossos "dossiês digitais" devem externar informações precisas, para uma projeção fidedigna da identidade do titular (BIONI, 2019, cap. 2). A proteção de dados é, portanto, fundamental para a salvaguarda da identidade pessoal, tendo em vista que a divulgação de dados pessoais torna os seus titulares vulneráveis à apropriação e à deturpação de suas identidades, de modo que uma pessoa pode ser confundida com outra, ou sua verdade pessoal pode ser desvirtuada (BARBOSA, 2017, p. 106).

A ideia de autodeterminação informacional é relevante para a tutela da identidade. Passa-se de uma visão da proteção de dados como um direito de afastar intrusões em dados pessoais para um direito muito mais participativo, que determina que o indivíduo tenha controle sobre o fluxo de dados que deseja transmitir. Assim, garante-se ao indivíduo a possibilidade de determinar como participará na sociedade (MAYER-SCHÖNBERGER, 2001, p. 228). A autodeterminação reconhece que o titular de dados deve ter controle sobre a projeção da própria identidade.

Também se observa uma forte ligação entre o direito à proteção de dados e o direito à privacidade. Cumpre lembrar que não existe um conceito universalmente aceito de privacidade, e uma definição rigorosa do termo é considerada uma tarefa quase

---

[16] Termo utilizado para descrever "o procedimento através do qual as bases de dados são "mineradas" por meio de algoritmos em busca de padrões de correlação entre dados. Essas correlações indicam relações entre dados, sem estabelecer causas ou razões" (HILDEBRANDT, 2008, p. 18).

[17] "*Diritto, questo, essenziale per la costruzione dell'identità, poiché conferisce il potere di ottenerela cancellazione dei dati falsi o illegittimamente raccolti o conservati oltre i termini previsti, la rettifica di quelli inesatti, l'integrazione di quelli incompleti*" (RODOTÀ, 2012, p. 327).

[18] Ao mesmo tempo, Rodotà reconhece que as possibilidades de apagamento e retificação se tornaram hoje um "empreendimento sem fim", já que há um registro contínuo de nossos rastros: "*Ma questa è divenuta ormai un'impresa senza fine, una ricerca inesauribile, poiché mai si arresta la registrazione d'ogni nostra traccia*." (2012, p. 327).

impossível (PINTO, 1993, p. 504). O artigo "*Right to Privacy*", de Samuel D. Warren e Louis D. Brandeis, de 1890, é reconhecido como o primeiro momento em que o direito à *privacy* foi autonomizado.[19] Nesse contexto, o direito foi concebido como forma de proteger pessoas de uma publicidade indesejada, quando não há um interesse legítimo em seus assuntos privados. A ideia era impedir que pessoas se vissem obrigadas a expor aspectos de suas vidas que gostariam que permanecessem privados (WARREN e BRANDEIS, 1890, pp. 214–215). Tal noção de privacidade se aproxima do conceito de "*right to be let alone*", ou "direito de ser deixado em paz", também traduzido como "direito a ser deixado só".

Capelo de Sousa, ao abordar o bem da reserva (resguardo e sigilo) do ser particular e da vida privada de cada indivíduo, afirma que, face à complexidade da vida social, cada pessoa deve ter "uma esfera privada onde possa recolher-se ('*right to be alone'*), pensar-se a si mesmo, avaliar sua conduta, retemperar as suas forças e superar as suas fraquezas [...]" (2011, p. 317). Essa esfera é uma decorrência da autonomia física e moral de cada pessoa para conduzir a própria vida, que é outorgada pelo princípio da dignidade humana. Tal esfera não deve ser violada pelos demais, "intrometendo-se nela e instrumentalizando e divulgando os elementos que a compõem" (2011, p. 317).[20]

O interesse na privacidade é identificado por Paulo Mota Pinto como um interesse de evitar ou controlar a tomada de conhecimento de informação que se pode razoavelmente

[19] Na concepção de Warren e Brandeis, o direito à *privacy* se apresenta como o direito de "estar a salvo de interferências alheias", e o direito de uma pessoa de "retrair aspectos de sua vida do domínio público" (BIONI, 2019, cap. 2) . Contudo, importa ressaltar que o direito à *privacy* no direito estadunidense evoluiu, de modo que é possível identificar uma distinção entre o que se chama de *informational privacy* e *decisional privacy*. Enquanto a *informational privacy* tem seu conceito vinculado a formas de tornar pública informação pessoal, aproximando-se da noção de proteção de dados pessoais do direito europeu, a *decisional privacy* diz respeito não à informação pessoal, mas a comportamentos, aplicando-se a situações como o aborto, uso de métodos contraceptivos e relações homossexuais. Desse modo, o direito à *privacy* estadunidense não corresponde ao direito à privacidade ou à proteção de dados no direito europeu, e abriga questões que vão muito além das noções de privacidade e proteção de dados (PINHEIRO, 2015, p. 267).

[20] O autor considera que o direito à reserva sobre a intimidade da vida privada presente no Código Civil Português abrange "não só o respeito da intimidade da vida privada, em particular a intimidade da vida pessoal, familiar, doméstica, sentimental e sexual e inclusivamente os respectivos acontecimentos e trajectórias, mas ainda o respeito de outras camadas intermédias e periféricas da vida privada, como as reservas do domicílio e de lugares adjacentes, da correspondência e de outros meios de comunicação privada, dos dados pessoais informatizáveis, dos lazeres, dos rendimentos patrimoniais e de demais elementos privados da atividade profissional e econômica, bem como também, last but not the least, a própria reserva sobre a individualidade privada do homem no seu ser para si mesmo, v.g., sobre o seu direito a estar só e sobre os caracteres de acesso privado do seu corpo, da sua saúde, da sua sensibilidade e da sua estrutura intelectiva e volitiva" (2011, p. 318).

esperar que o indivíduo considere como íntima ou confidencial.[21] Além disso, o autor aponta que nesse interesse também estão incluídos "o interesse na subtração à atenção dos outros (anonimato num sentido lato) e o interesse em excluir o acesso físico dos outros a si próprio (*solitude*)"[22] (1993, p. 508). Também conclui que o problema da tutela da privacidade é caracterizado por uma contraposição: de um lado, o interesse do indivíduo em "impedir a intromissão dos outros em sua esfera privada, e impedir a revelação de informação pertencente a essa esfera", e, do outro, "o interesse em conhecer e em divulgar a informação conhecida" (1993, p. 509).

Sem a pretensão de chegar a um conceito universal de privacidade, na mesma linha de Bioni, observamos que a lógica tradicional da privacidade é centrada em uma liberdade negativa de "não sofrer interferência alheia" (2019, cap. 2). Adriano De Cupis, por exemplo, define a "*riservatezza*" como um modo de ser de uma pessoa que exclui aquilo que diz respeito a ela do conhecimento dos outros (1973, p. 258). No mesmo sentido, Carlos Alberto da Mota Pinto, ao tratar do direito à reserva sobre a intimidade da vida privada no contexto português, identifica a pretensão de defender contra violações a paz, a tranquilidade e o resguardo de uma esfera íntima de vida (2012, p. 212).

Observa-se que, apesar de muitas vezes ser tratada dentro do âmbito da privacidade,[23] a proteção de dados pessoais não pode ser reduzida a uma categoria do

---

[21] Nesse ponto, Mota Pinto segue a definição de Raymond Wacks, afirmando que o interesse na *privacy* é o de evitar ou controlar a tomada de conhecimento de "factos, comunicações ou opiniões que se relacionam com o indivíduo e que é razoável esperar que ele encare como íntimos ou pelo menos como confidenciais e que por isso queira excluir ou pelo menos restringir a sua circulação" (WACKS *apud* PINTO, 1993, p. 508).

[22] O autor aborda aspectos realçados por Ruth Gavison no artigo *Privacy and the Limits of Law*. Nesse sentido: "*The concept of privacy suggested here is a complex of these three independent and irreducible elements: secrecy, anonymity, and solitude. Each is independent in the sense that a loss of privacy may occur through a change in any one of the three, without a necessary loss in either of the other two. The concept is nevertheless coherent because the three elements are all part of the same notion of accessibility, and are related in many important ways*" (GAVISON, 1980, p. 433 e ss.)

[23] Por exemplo, Pedro Pais de Vasconcelos trata do tema da proteção de dados pessoais inserido no contexto dos direitos da personalidade, mais especificamente do direito à privacidade (1999, p. 241). Capelo de Sousa também trata do direito à proteção de dados pessoais dentro do âmbito do direito à privacidade, mas também afirma que "a previsão do n.º 1 do artigo 35.º da Constituição Portuguesa diz respeito, mais propriamente, ao bem da identidade da pessoa"(2011, p. 322).

Stefano Rodotà considera o direito à proteção de dados pessoais como uma evolução do direito à privacidade, que passa a ser definida também como um "direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada": "*la privacy viene inoltre definita come 'diritto di mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata' e, in definitiva, come 'il diritto di scegliere liberamente il proprio modo di vivere'*" (2012, p. 327). Rodotà não deixa, porém, de reconhecer que o direito à proteção de dados é explicitamente considerado um direito fundamental autônomo na Carta de Direitos Fundamentais da União Europeia (2009, p. 77, 2012, p. 321). Danilo Doneda segue a consideração de Rodotà de que a proteção de dados pessoais é

direito à privacidade. Em primeiro lugar, pela própria definição de dado pessoal como qualquer "informação relativa a uma pessoa singular identificada ou identificável", a proteção não está restrita àqueles dados ligados à intimidade ou à vida privada de uma pessoa. Tal ideia foi abordada, por exemplo, na já mencionada Decisão dos Censos, do Tribunal Constitucional Alemão. Na ocasião, questionava-se sobre a constitucionalidade da Lei do Censo de 1983, que ordenava o recenseamento geral da população, e solicitava dados como moradia, profissão e local de trabalho, para fins estatísticos. O §9.º da referida lei - que foi considerado incompatível com o artigo 2 I (direito geral da personalidade) c/c o artigo 1 I (dignidade humana) da Constituição - previa a possibilidade de comparação dos dados levantados com os registros públicos e também a transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais para a finalidade genérica de "atividades administrativas" (BIONI, 2019, cap. 2; BVERFGE, 1983 *apud* MARTINS, 2005, p. 234; PINHEIRO, 2015).

Na decisão, o Tribunal Constitucional chegou à importante conclusão de que mesmo dados considerados insignificantes e que não afetam uma esfera íntima da pessoa podem adquirir um novo valor dependendo de sua finalidade e do contexto de sua utilização. Desse modo, não basta apenas considerar o tipo de dado - se este diz respeito a uma esfera íntima do cidadão ou não - para decidir sobre a licitude de seu tratamento. De acordo com o tribunal, só quando há clareza quanto às finalidades e possibilidades de uso e ligação dos dados recolhidos com outros dados é que se pode saber se uma restrição ao direito à autodeterminação informacional é aceitável (BVERFGE, 1983 *apud* MARTINS, 2005, p. 234).

Tal conclusão é relevante principalmente quando comparada a outra decisão, conhecida como Decisão do Microcenso, de 1969. Naquela ocasião, o mesmo Tribunal havia se manifestado pela constitucionalidade de uma lei que previa uma multa de até 10 mil marcos caso os entrevistados se recusassem a responder a perguntas sobre "viagens de férias" e "viagens de repouso". A fundamentação da decisão centrou-se na discussão sobre se as informações solicitadas atingiriam ou não a esfera mais íntima do cidadão, para

---

uma evolução da privacidade (DONEDA, 2019). Alexandre Dias Pereira considera que o direito à proteção de dados funda-se no direito ao respeito pela vida privada. Afirma, porém, que tal direito adquiriu "vida própria" com fundamento no direito à autodeterminação informativa, conforme a decisão do Tribunal Constitucional Alemão sobre a Lei dos Censos (2019, p. 1164).

determinar a licitude de seu tratamento. A Decisão dos Censos de 1983 foi relevante por não recorrer a uma lógica do que é público e o que é privado para construir o direito à proteção de dados, e pela consideração de que qualquer dado relativo a uma pessoa é potencialmente lesivo. A decisão construiu um direito à proteção de dados autônomo, destacado do direito à privacidade (BIONI, 2019, cap. 2; BVERFGE, 1983 *apud* MARTINS, 2005, p. 217; PINHEIRO, 2015, p. 487).

Mesmo que se adote uma concepção ampla de privacidade,[24] que não se limite à intimidade de uma pessoa, é possível constatar que o direito à proteção de dados vai além dessa noção, não podendo ser reduzido ao – nem englobado pelo - direito à privacidade. Isso, porque o direito à proteção de dados se aplica a uma gama mais ampla de dados e de operações feitas com esses dados. Em primeiro lugar, deve-se considerar que definir se um dado interfere ou não na privacidade de um indivíduo dependerá de um contexto, enquanto o enquadramento de um dado como pessoal ou não independe de uma análise contextual. Orla Lynskey, partindo de uma análise de casos do Tribunal de Justiça da União Europeia, fornece um exemplo claro dessa diferença. Um trecho de um documento referente a uma reunião de trabalho contendo os nomes dos participantes dessa reunião certamente está incluído na definição de dado pessoal. Há controvérsia, contudo, sobre se esse trecho está abrangido ou não pelo interesse do titular do dado na privacidade quanto ao seu nome. Tal conclusão dependerá de uma análise contextual (2014, p. 583).[25] [26] Também o fato de que

[24] O Tribunal Europeu dos Direitos do Homem, por exemplo, tem julgado casos referentes à proteção de dados pessoais à luz do artigo 8.º da Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, que dispõe sobre o direito ao respeito pela vida privada e familiar. A Convenção não dispõe sobre um direito à proteção de dados pessoais, e o referido tribunal adota um conceito de vida privada amplo o suficiente para abrigar um direito à proteção de dados. Contudo, há casos em que o tribunal considera que tratamentos de certos dados não constituem interferência com o direito ao respeito pela vida privada e familiar, ainda que constituam claramente tratamento de dados pessoais, o que sugere que o direito à proteção da vida privada e o direito à proteção de dados pessoais têm âmbitos diferentes.

[25] Nesse ponto, Lynskey usa como exemplo o caso *Bavarian Lager*, do Tribunal de Justiça da União Europeia. No caso, a companhia *Bavarian Lager* havia solicitado à Comissão Europeia o acesso a documentos referentes a uma reunião, com base no Regulamento n.º 1049/2001, relativo ao acesso do público de documentos. A Comissão havia respondido que alguns documentos poderiam ser exibidos, mas ressaltou que os nomes dos participantes haviam sido retirados da ata de reunião devido à ausência de consentimento por parte de alguns participantes. A companhia, então, enviou por e-mail um pedido de acesso às atas completas da reunião, incluindo os nomes dos participantes. A Comissão decidiu que a companhia não havia apresentado um propósito legítimo para a transmissão dos dados, e portanto as condições para transmissão de dados previstas no artigo 8.º do Regulamento 45/2001 não haviam sido cumpridas, e que seria aplicada a exceção prevista no artigo 4.º, n.º 1, alínea b), do Regulamento 1049/2001, que previa a recusa ao acesso de documentos nos casos em que fosse prejudicada "a vida privada e da integridade do indivíduo, nomeadamente nos termos da legislação comunitária relativa à protecção dos dados pessoais". O Tribunal Geral, na primeira instância, ao analisar a aplicabilidade do artigo 4.º, n.º 1, alínea b), ao caso, examinou,

o direito à proteção de dados pessoais envolve dados sobre pessoas identificadas ou identificáveis faz com que regras sobre proteção de dados sejam aplicáveis mesmo quando o titular não é identificado. Na análise sobre violação ao respeito pela vida privada, contudo, há muitas vezes ênfase na ponderação sobre se a pessoa é ou não identificada, o que sugere, mais uma vez, que o âmbito do direito à proteção de dados é mais amplo (LYNSKEY, 2014, p. 584).[27]

A definição de tratamento de dados na legislação europeia como "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados" também é extremamente abrangente, podendo incluir mais operações do que aquelas que sejam consideradas capazes de interferir na vida privada do sujeito.[28] Lynskey dá um exemplo hipotético: se

---

primeiramente, se a revelação das informações requeridas constituiria uma interferência na vida privada do indivíduo nos termos do artigo 8.º da CEDH, conforme a jurisprudência do TEDH. O Tribunal Geral considerou que o mero fato de que um documento contém dados pessoais não significa que a privacidade ou integridade das pessoas foi afetada, ainda que o conceito de vida privada seja amplo e não exclua, necessariamente, informações relacionadas à atividade profissional. No caso, decidiu que o respeito pela vida privada não havia sido comprometido, uma vez que os participantes da reunião estavam como representantes do órgão ao qual pertenciam, e não a título pessoal. Além disso, também observou que as atas não continham opiniões individuais atribuíveis a essas pessoas, mas sim aos órgãos os quais elas representavam. O Tribunal Geral considerou, então, que a exceção prevista no artigo 4.º, n.º1, alínea b), só se aplicaria a dados pessoais capazes de comprometer a proteção da privacidade e integridade do indivíduo, não sendo aplicável ao presente caso. Posteriormente, em sede de apelação, o Tribunal de Justiça reverteu a decisão, sob o argumento de que, ao limitar a aplicação do artigo 4.º, n.º1, alínea b), do Regulamento 1049/2001 às situações em que há violação da privacidade conforme o artigo 8.º da CEDH, o Tribunal Geral desconsiderou a redação do artigo, que requer a conformidade com a legislação da União Europeia sobre proteção de dados pessoais (COMISSÃO DAS COMUNIDADES EUROPEIAS CONTRA THE BAVARIAN LAGER CO. LTD., 2007; COMISSÃO EUROPEIA CONTRA THE BAVARIAN LAGER CO. LTD., 2010).

[26] Nesse sentido, Lynskey: "*However, what is notable for present purposes is that there is a clear lack of consensus regarding whether, and if so in what circumstances, an individual has a privacy interest in his name. In contrast, as the EDPS highlighted, 'a reference to the name of a participant in the minutes of a meeting constitutes personal data'. Thus, it can be seen that while the question of whether a 'privacy interest' exists in particular circumstances requires a context-dependent assessment, whether data constitutes personal data can be an easier issue to assess*"(LYNSKEY, 2014, pp. 583–584).

[27] Lynskey cita como exemplo o caso *Friedl v Austria*, no qual o recorrente alegava violação ao seu direito ao respeito pela vida privada por ter sido fotografado por policiais durante um protesto em via pública. O Tribunal Europeu dos Direitos do Homem removeu o caso da lista, e fez referência ao fato de que não haviam sido adotadas medidas para identificar as pessoas fotografadas (TEDH, 1995).

[28] Foram citadas duas decisões para exemplificar esse ponto. No primeiro caso, *Pierre Herbecq and the Association 'Ligue des droits de l'homme' v Belgium,* o apelante alegou violação ao seu direito ao respeito pela vida privada (artigo 8.º da CEDH) pelo fato de que o governo da Bélgica não havia adotado legislação no que diz respeito a filmagens de vigilância nos casos em que os dados não eram gravados. A Comissão Europeia dos Direitos do Homem considerou que os sistemas fotográficos em questão seriam provavelmente usados em locais públicos, ocupados legalmente pelos usuários desses sistemas, para monitorar as instalações por razões de segurança. Tendo em vista que as imagens não eram gravadas, julgou difícil identificar como as imagens poderiam ser disponibilizadas para o público geral ou usadas para outros propósitos. Considerou, assim, que não havia interferência com o direito ao respeito pela vida privada.

uma estudante compete em uma equipe de atletismo de sua universidade, seu nome e faixa etária de competição podem ser publicados no *website* da universidade. A publicação constitui tratamento de dados e entraria no âmbito da proteção de dados pessoais no direito europeu. Contudo, considerando que a informação seria pública e não teria sido sistematicamente coletada e organizada, não estaria no âmbito do direito ao respeito pela vida privada e familiar (2014, p. 585).

Lynskey também pontua que o direito à proteção de dados pessoais abrange outros direitos que não estão direcionados à proteção da privacidade. É o caso do direito do titular de dados de não ficar sujeito a uma decisão que se baseie exclusivamente no tratamento automatizado de seus dados, e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar. Nesse caso, o objetivo não é o de proteger a vida privada do indivíduo, mas de reduzir assimetrias entre o titular de dados pessoais e o responsável pelo tratamento (2014, p. 586).[29]

É verdade que o direito à proteção de dados e o direito à privacidade, muitas vezes, podem servir aos mesmos objetivos. Ambos os direitos podem servir como meios de evitar formas de vigilância não autorizada, permitindo aos sujeitos a manutenção de suas liberdades de associação e expressão sem o temor de repercussões (LYNSKEY, 2014, p. 587). A privacidade, como ressalta Ruth Gavison, é essencial para a democracia, já que é necessário que os indivíduos possam manter suas opiniões, seus votos, suas discussões no âmbito privado, para poderem exercer ao máximo sua liberdade (1980, pp. 455–456), e nesse ponto, a proteção de dados pessoais também serve ao propósito de garantir essa

---

O segundo caso mencionado por Lynskey para ilustrar o ponto foi o caso *Rundfunk*, do Tribunal de Justiça da União Europeia, que implicitamente reafirmou essa diferença entre o âmbito da proteção de dados pessoais e do direito ao respeito pela vida privada. No parágrafo 74, o Tribunal afirma: "*Há que reconhecer que, se a simples memorização pela entidade patronal de dados nominativos relativos às retribuições pagas ao seu pessoal não pode, enquanto tal, constituir uma ingerência na vida privada, a comunicação desses dados a um terceiro, neste caso, a uma autoridade pública, viola o direito ao respeito da vida privada dos interessados, seja qual for a utilização posterior das informações assim comunicadas, e apresenta a natureza de uma ingerência na acepção do artigo 8.° da CEDH.*" Tal memorização, porém, entraria no âmbito da proteção de dados pessoais.

[29] Lynskey também afirma que o direito ao esquecimento e o direito à portabilidade de dados, previstos no RGPD, também não se relacionam necessariamente com a privacidade: *"For example, although privacy law might recognize the right of the data subject to ensure the erasure of his personal data in certain instances, it does not recognize anything akin to the 'right to be forgotten' set out in the Proposed Regulation. Moreover, the ECtHR case law does not recognize a right to data portability. This confirms that the objective of such a right is not to protect individual privacy; it must therefore serve a different, independent objective"* (2014, p. 587).

liberdade ao indivíduo, ao permitir o controle sobre os dados que revela e sobre para quem os revela.

Apesar de consistirem em direitos diversos, e mesmo que o âmbito de relevância do direito à proteção de dados pessoais seja, muitas vezes, mais amplo do que o do direito à privacidade, em muitos casos os dois direitos se sobrepõem.[30] A proteção de dados pessoais pode servir para garantir o direito à privacidade, principalmente quando permite o controle de dados que possam revelar informações sobre a vida privada de uma pessoa. Como se verá adiante, a disseminação não consensual de imagens íntimas é o exemplo de uma situação em que tanto a reserva da vida privada como o direito à proteção de dados pessoais são afetados.

Para além de sua relação com a proteção da vida privada, a proteção de dados é fundamental para a promoção da igualdade, considerada por Capelo de Sousa como um elemento da própria noção de personalidade humana (2011, p. 289). Isso se evidencia com a proibição do tratamento de dados considerados sensíveis, normalmente tidos como dados referentes a saúde, etnia, credo político ou religioso, vida sexual e dados genéticos.[31] Tal proibição tem por objetivo impedir práticas discriminatórias entre os cidadãos (RODOTÀ, 1995, p. 86). Um exemplo do potencial lesivo do acesso a dados sensíveis foi mencionado por Charles Sykes: nos Estados Unidos, no Estado de Maryland, um banqueiro local que detinha um cargo público de comissário de saúde cruzou os dados de empréstimos bancários com aqueles referentes a pacientes com câncer, e em seguida cancelou os empréstimos destinados a esses pacientes (SYKES, 1999, p. 100).

Mesmo dados que não são necessariamente sensíveis, quando divulgados, podem acarretar efeitos discriminatórios. Como já mencionado,[32] informações pessoais tornadas públicas, acessíveis através da ferramenta de busca do *Google*, podem afetar a forma como

[30] No mesmo sentido, Finocchiaro chama atenção para o fato de que o direito à proteção de dados pessoais e o direito à reserva da vida privada têm âmbitos diversos e objetos diversos. Recorda que em muitas situações, tais direitos coincidem, como, por exemplo, dados de saúde em uma cartela clínica de um paciente são objeto seja do direito à reserva da vida privada, seja do direito à proteção de dados pessoais. Mas salienta que existem casos em que a informação é tutelada apenas pelo direito à proteção de dados pessoais (2017, p. 8). Mafalda Miranda Barbosa também tece considerações nesse sentido (2017, p. 105).

[31] No Regulamento (UE) 2016/679, tal categoria de dados é tratada no artigo 9.º: "1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. [...]"

[32] Tópico 1.3.

uma pessoa é tratada em seu meio social, bem como as oportunidades que a ela são oferecidas. Dados disponíveis em perfis de redes sociais, por exemplo, podem ser usados por possíveis empregadores para descartar candidatos (ROSENBLAT, KNEESE e BOYD, 2014, p. 5).

A proteção de dados pessoais hoje busca reduzir assimetrias de poder entre os titulares de dados pessoais e os responsáveis pelo tratamento de dados. Tal noção é especialmente significativa quando se tem em mente a realidade das técnicas de *profiling*. O *profiling* é o resultado do processo de *data mining* (mineração de dados), em que se busca correlações entre dados localizados em grandes bases de dados. A partir dessas correlações, é possível fazer previsões baseadas nos padrões de comportamento identificados, que podem ser humanos ou não humanos. Trata-se de um processo indutivo de conhecimento, que não pretende levar em consideração as razões pelas quais determinados comportamentos são previstos (HILDEBRANDT, 2008, p. 18).

O *profiling* permite que, através de dados pessoais não sensíveis, sejam revelados dados sensíveis sobre uma pessoa. Esta é uma das razões pelas quais a divisão entre dados pessoais sensíveis e não sensíveis é criticada, pois, nesses casos, não é o dado em si que é perigoso ou discriminatório, mas o seu uso (DONEDA, 2019, cap. 2). Um estudo conduzido nos Estados Unidos, baseado nas "curtidas" do perfil dos participantes no *site Facebook* revelou como inferências feitas a partir de dados triviais podem revelar dados sensíveis. Os pesquisadores conseguiram prever com 95% de exatidão os usuários afro-americanos e caucasianos, e com 93% de exatidão, os usuários do gênero masculino e feminino. Além disso, conseguiram identificar corretamente os usuários cristãos e muçulmanos em 82% dos casos, e os usuários republicanos e democratas em 85% dos casos. Também conseguiram prever corretamente a orientação sexual dos participantes masculinos em 88% dos casos, e femininos, em 75% dos casos (KOSINSKI, STILLWELL e GRAEPEL, 2013, p. 5803).

Os dados pessoais, mesmo os mais triviais, podem ser usados para decisões que terão influência sobre a vida de seus titulares. Daniel Solove afirma que, na era da informação, dados pessoais são combinados para criar uma "biografia digital" sobre nós. Informações sobre produtos que consumimos, por exemplo, podem servir como um reflexo de nossa personalidade. Tal reflexo é, porém, reducionista, já que captura apenas uma pequena parte de quem somos. Assim, a biografia digital de uma pessoa, "ainda que

contenha muitos detalhes sobre ela, captura uma persona distorcida, construída por uma variedade de detalhes externos" (SOLOVE, 2007, p. 45, tradução nossa).[33] Através do *profiling*, parte da personalidade de uma pessoa é reconstruída, mas de maneira padronizada; pessoas são categorizadas e estigmatizadas, o que pode trazer efeitos sociais profundos (SOLOVE, 2007, p. 46).

As relações de consumo são situações em que os efeitos discriminatórios potencializados pelo *profiling* se tornam mais visíveis. Solove menciona a tendência crescente das companhias em diferenciar entre clientes "anjos" e clientes "demônios". Os clientes "anjos" seriam aqueles que proporcionariam maior margem de lucro à empresa, por consumirem mais. Já os "demônios" seriam aqueles propensos a consumir em menores quantidades e fazer com que a companhia perca dinheiro de alguma forma. Um exemplo seriam consumidores que telefonam com mais frequência aos serviços de atendimento ao cliente, fazendo com que a companhia tenha de despender recursos. Ao deter dados pessoais dos consumidores e identificar aqueles que seriam os mais promissores, as empresas poderão estabelecer formas diferentes de tratar os seus clientes. Podem escolher servir os clientes "anjos" primeiro e os "demônios" depois, ou podem oferecer preços mais baixos aos clientes "anjos", por exemplo. Podem, inclusive, tentar afastar os clientes indesejados. Solove cita uma estratégia discriminatória estabelecida antes que a ideia de consumidores "anjos" e "demônios" fosse articulada: nos Estados Unidos, um banco tinha por hábito negar pedidos de cartão de crédito a estudantes universitários dos cursos de História, Inglês e Arte, por presumir que suas perspectivas de empregabilidade seriam pequenas (SMITH, 1994, p. 123; SOLOVE, 2007, p. 50).

Discriminações de preço são potencializadas com a criação de perfis comportamentais a partir de dados pessoais. Tal prática consiste na venda de diversas unidades de um bem ou serviço com diferenças nos preços que não correspondem diretamente a diferenças nos custos de fornecimento. Discriminações desse tipo ocorrem, por exemplo, quando um negócio oferece descontos a idosos ou estudantes. Podem ocorrer também, contudo, quando uma empresa altera o preço de um bem para obter do consumidor o valor máximo que este está disposto a pagar. Assim, uma empresa, ao identificar um potencial consumidor que estaria disposto a comprar seu bem ou serviço por

[33] "*Although the digital biography contains a host of details about a person, it captures a distorted persona, one who is constructed by a variety of external details*" (SOLOVE, 2007, p. 45).

um valor inferior ao valor corrente, poderá oferecê-lo por um valor menor a esse consumidor, se os custos de produção compensarem a redução de preço. Porém, o inverso também poderá ocorrer: uma empresa poderá escolher vender seu produto por um valor maior do que aquele inicialmente proposto se identificar, a partir de diversos dados pessoais colhidos de seus consumidores, clientes dispostos a pagar mais pelo mesmo produto (ROTENBERG, 2001, p. 31).[34]

Os exemplos acima mencionados evidenciam que, em certos contextos, verificam-se assimetrias de informação e assimetrias de poder na relação entre o titular de dados pessoais e o responsável pelo tratamento de dados. Titulares de dados têm acesso a menos informação e estão em situação de vulnerabilidade em comparação àqueles que tratam seus dados. Em virtude dessas assimetrias, titulares normalmente têm dificuldade em tomar decisões informadas sobre permitir que determinados dados sejam tratados, uma vez que não conseguem compreender inteiramente a possibilidade de que o uso desses dados acarrete efeitos lesivos, ou a seriedade desses possíveis efeitos. Além disso, as assimetrias de informação são um obstáculo para que o indivíduo possa identificar corretamente e responsabilizar aqueles que tratam os seus dados (LYNSKEY, 2014, p. 593).

Devido às assimetrias de informação, os titulares têm menos poder de barganha em relação a quem trata seus dados. O exemplo das discriminações de preço é significativo nesse sentido, já que muitas vezes os consumidores revelam qual o preço máximo que estão dispostos a pagar, mesmo inadvertidamente, através de seus dados de navegação e compras, enquanto que o vendedor nunca revela o preço mínimo pelo qual está disposto a vender o produto (LYNSKEY, 2014, p. 593; ROTENBERG, 2001, p. 32). O problema, como afirma Daniel Solove, não é simplesmente a coleta de dados em si, mas a possível falta de controle sobre o modo como os dados serão empregados no futuro (SOLOVE, 2007, p. 51).

O direito à proteção de dados, dessa forma, busca tutelar a igualdade não só quando impede a divulgação, ou permite maior controle sobre certos dados que possam gerar discriminação em relação ao seu titular, mas também quando atua para reduzir assimetrias entre o titular e o responsável pelo tratamento. Nesse caso, pretende-se fazer

[34] Por exemplo, em 2000, um consumidor da empresa Amazon.com havia apagado os cookies de seu computador e, como resultado, um DVD que era em oferta por $26,24 passou a ser oferecido por $22,74 (RAMASASTRY, 2005).

com que o responsável pelo tratamento adira a limites estabelecidos para a forma como os dados são tratados. O princípio da limitação de finalidades, presente no artigo 5.º, n.º 1, alínea b), do RGPD, e no artigo 8.º da Carta de Direitos Fundamentais da União Europeia é um exemplo disso (LYNSKEY, 2014, p. 594).

A disseminação não consensual de imagens íntimas é um exemplo de situação em que o direito à proteção de dados pessoais pode servir para tutelar diversos bens da personalidade. Em primeiro lugar, por consistir na divulgação não autorizada da imagem de uma pessoa, a NCII já se enquadra em uma violação do direito à imagem, que pode ser definido como o direito de uma pessoa a não ter o seu retrato exposto, reproduzido ou lançado no comércio sem o seu consentimento (PINTO, 2012, p. 212). Uma pessoa pode limitar voluntariamente o seu direito à imagem fornecendo o seu consentimento. Todavia, a eficácia desse consentimento será restrita aos sujeitos para os quais foi dado. Assim, Adriano De Cupis ressalta que uma pessoa pode se deixar fotografar como forma de deixar uma recordação de si a uma determinada pessoa querida, sem a intenção de que esse retrato circule pelo mundo, tornando-se objeto visível a todos. Também se nota que o consentimento pode ser dado para determinados modos de difusão da própria imagem, e não outros (alguém que consente em ter seu retrato exposto na vitrine de um fotógrafo não permite a reprodução da fotografia em cartões postais por exemplo) (1973, p. 268).[35] Desse modo, observa-se que o consentimento para o acesso de uma pessoa às imagens íntimas de outra não pode ser interpretado como autorização para sua ampla divulgação.

Uma imagem ou vídeo de uma pessoa pode constituir um dado pessoal, enquadrando-se na definição de "informação relativa a uma pessoa singular identificada ou identificável",[36] por conter elementos específicos da sua identidade física.[37] A Diretiva 95/46/CE já previa, em seu considerando 14, a aplicação da norma ao tratamento de dados de som e de imagem relativos às pessoas singulares.[38] De acordo com o Grupo de Trabalho

[35] Adriano De Cupis trata o direito à imagem como uma manifestação do direito à reserva da vida privada ("*diritto alla riservatezza*"), sendo o "direito de manter a própria imagem fora do conhecimento dos outros" (1973, p. 258). Paulo Mota Pinto afirma que, apesar de o direito à imagem ser um dos direitos que mais têm sido aproximados ao direito à reserva sobre a intimidade da vida privada, não há que se falar em coincidência total entre os dois. O direito à reserva pode ser violado sem que haja violação do direito à imagem, assim como o direito à imagem pode ser violado fora da vida privada (1993, p. 549).

[36] É essa a definição prevista no artigo 4.º, n.º 1, do RGDP.

[37] O TJUE já decidiu no sentido de que a imagem de uma pessoa gravada por uma câmara constitui um «dado pessoal» nos acórdãos Ryneš (2014, par. 22) e Buivids (2019, par. 31).

[38] "(14) Considerando que, tendo em conta a importância do desenvolvimento que, no âmbito da sociedade de informação, sofrem actualmente as técnicas de captação, transmissão, manipulação, gravação,

do Artigo 29.º (GT 29), "quando uma imagem digital contém o rosto de um indivíduo que é claramente visível e permite que este indivíduo seja identificado, será considerado um dado pessoal" (2012, p. 4., tradução nossa).[39] O GT 29 esclarece, porém, que tal enquadramento dependerá de alguns parâmetros, como a qualidade da imagem e o ponto de vista. Imagens de indivíduos a uma longa distância, ou com os rostos borrados provavelmente não serão consideradas dados pessoais. Em alguns casos específicos, imagens poderão ser consideradas como dados sensíveis, principalmente se forem usadas para obter informações sobre a origem étnica, religião, ou saúde de uma pessoa, por exemplo.

A NCII também configura, evidentemente, uma ofensa ao já mencionado direito à privacidade, uma vez que os dados publicados dizem respeito à vida sexual da pessoa retratada, o que é certamente abrangido pela noção de vida privada. A pessoa têm interesse na privacidade de certos atributos pessoais, que incluem dotes artísticos, deformidades físicas e hábitos sexuais (1993, p. 529).[40] Ressalta-se que dados relativos à vida sexual são inseridos dentro das categorias especiais de dados pessoais no artigo 9.º do RGPD. Para além da ofensa à privacidade, a NCII envolve violação ao direito à honra, entendido por Capelo de Sousa como a projeção na consciência social do conjunto de valores pessoais de cada indivíduo, desde aqueles que derivam de sua pertença ao gênero humano como aqueles adquiridos por meio de seu esforço pessoal. A honra abrange a projeção do valor da dignidade humana e, em sentido amplo, inclui o bom nome e a reputação. Inclui, também, o simples decoro, tido como a "projeção dos valores comportamentais do indivíduo no que se prende ao trato social" (2011, p. 305).

Cumpre lembrar que, para que se configure lesão à honra de uma pessoa, não é imprescindível que a ela seja imputado um fato inverídico. Como ressalta Paulo Mota

---

conservação ou comunicação de dados de som e de imagem relativos às pessoas singulares, há que aplicar a presente directiva ao tratamento desses dados;
(15) Considerando que o tratamento desses dados só é abrangido pela presente directiva se for automatizado ou se os dados tratados estiverem contidos ou se destinarem a ficheiros estruturados segundo critérios específicos relativos às pessoas, a fim de permitir um acesso fácil aos dados pessoais em causa;"

[39] "*When a digital image contains an individual's face which is clearly visible and allows for that individual to be identified it would be considered personal data*" (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2012).

[40] Anderson Schreiber apresenta um caso de NCII em seu livro Direitos da Personalidade, comentando especificamente sobre a violação da intimidade e do direito à imagem: "artefatos simples, a que quase todos têm acesso, permitem o registro eletrônico com detalhamento irrefutável da intimidade mais profunda de uma menina, sem qualquer possibilidade de reparação efetiva" (2013, p. 124).

Pinto, é possível que o direito à honra seja atingido com a imputação de fatos correspondentes à verdade, o que possibilita a configuração tanto da violação da honra quanto da privacidade (1993, p. 543).[41] Mesmo imagens e notícias verdadeiras podem trazer lesões injustificadas à reputação social da pessoa envolvida (SCHREIBER, 2013, p. 82). Adriano De Cupis afirma que o direito à honra pode ser, em alguns casos, um direito a uma dignidade fictícia. A dignidade entendida como valor real que existe em cada indivíduo humano como tal nunca será fictícia. Porém, aspectos particulares da dignidade de uma pessoa podem ser somente aparentes, e, nesses casos, é possível falar em tutela de uma dignidade fictícia. Segundo De Cupis, a aparência de dignidade constitui uma qualidade da pessoa, refletindo-se na opinião de terceiros e projetando-se externamente (CUPIS, 1973, p. 235). Sendo assim, no caso da disseminação não consensual de imagens íntimas, ainda que os dados revelados correspondam a uma verdade – se a pessoa retratada esteve realmente naquela situação, em que foi filmada ou fotografada – a publicação não deixa de ser ofensiva à sua honra.

É interessante notar que a atividade sexual não é necessariamente um fato desonroso, já que a sexualidade inevitavelmente faz parte da vivência humana. Contudo, a divulgação de imagens íntimas pode acarretar lesões à reputação de uma pessoa principalmente por contrariar as expectativas sociais em relação a certos grupos. Existem normas sociais e expectativas quanto ao gênero feminino, por exemplo, que se tornam evidentes em situações como a NCII. Durante muito tempo, a castidade de uma mulher solteira foi considerada não só uma virtude, mas também uma obrigação.[42] Assim, para

[41] A *exceptio veritatis* só é aceita como causa de exclusão da ilicitude quando a imputação é feita para realizar o interesse público ou por justa causa (PINTO, 1993, p. 543; SOUSA, 2011, p. 311).

[42] Exemplos dessas expectativas em relação à sexualidade feminina estiveram presentes também no Direito. Por exemplo, o Código Civil Português chegou a estabelecer, no artigo 1636.º (alterado pelo Decreto-Lei n.º 496/77), "a falta de virgindade da mulher ao tempo do casamento" como uma das hipóteses de erro que vicia a vontade, se fosse desconhecida pelo marido. O Código Civil Brasileiro de 1916 continha disposição semelhante no artigo 219, inciso IV. O código Penal Português de 1886 fazia menção explícita à virgindade da mulher no tipo penal do artigo 392.º ("aquele que, por meio de sedução, estuprar mulher virgem, maior de doze e menor de dezoito anos [...]"). O artigo 396.º previa como circunstância agravante de estupro "o rapto de qualquer mulher virgem, maior de doze e menor de dezoito anos, da casa ou lugar em que com a devida autorização ela estiver, que for cometido com o seu consentimento". Além disso, no artigo 400.º, § único, previa-se que, em casos de atentado ao pudor, estupro e violação, "cessará lodo o procedimento ou toda a pena, quando o criminoso casar com a mulher ofendida". Da mesma forma, o artigo 544 do Código Penal Italiano (revogado pela Lei 5 agosto 1981, n. 442) também determinava que, para alguns crimes de violência sexual, o casamento entre o autor e a vítima extinguiria o crime e, caso tivesse havido condenação, cessaria a execução e os efeitos penais. Essa previsão era conhecida como "casamento reparador", e também esteve presente no Código Penal Brasileiro, em seu artigo 107, inciso VII. O Código Penal Português de 1852, em seu artigo 392.º, estipulava pena de degredo temporário para aquele que estuprasse "mulher virgem ou viúva

muitas mulheres, a atividade sexual exposta é motivo de vergonha e desonra (HENRY e POWELL, 2016, p. 399; HILL, 2015, p. 122). Para além disso, a forma como as imagens são difundidas e os meios nos quais são publicadas podem ser especialmente danosos para sua reputação, considerando que as pessoas retratadas podem ter própria imagem associada a *sites* e vídeos pornográficos, por exemplo, o que pode ofender não só sua honra mas também sua identidade.

Cumpre lembrar ainda que, como já mencionado no capítulo 1, a disseminação não consensual de imagens íntimas também tem interferência na igualdade. Por sua natureza sexual, as imagens constituem um tipo de dado capaz de gerar discriminação. O maior exemplo disso é a dificuldade que muitas pessoas retratadas nas imagens têm em encontrar trabalho, principalmente pelo fato de que basta uma pesquisa pelo seu nome em motores de busca ou redes sociais para que um possível empregador tome conhecimento da publicação de suas imagens íntimas. A NCII é, portanto, um exemplo de situação em que o direito à proteção de dados pode servir como forma de tutela da privacidade, da igualdade, da honra, da imagem e da identidade. O presente trabalho tem por objetivo abordar o tema da disseminação não consensual de imagens íntimas na perspectiva da proteção de dados, especificamente considerando o quadro europeu do Regulamento Geral sobre a Proteção de Dados.

2.2 A Integridade Contextual e a disseminação não consensual de imagens íntimas como uma violação ao direito à proteção de dados pessoais.

Helen Nissenbaum apresenta a ideia de integridade contextual como uma referência para a privacidade. A autora afirma que, ao longo de suas vidas, as pessoas não "agem e transacionam como indivíduos em um mundo social indiferenciado", mas como

honesta". O artigo 393.º também recorria a essa expressão. A mesma noção estava presente no Código Penal Brasileiro: o crime de "posse sexual mediante fraude" (revogado pela Lei n.º 12.015, de 2009) previa em seu tipo penal "ter conjunção carnal com mulher honesta, mediante fraude". O conceito de "mulher honesta" implicava um juízo de valor de acordo com padrões ético-sociais vigentes na comunidade (BITENCOURT, 2014). Poderia ser adotado para excluir da proteção jurisdicional as adúlteras, mulheres de comportamento sexual liberal e prostitutas, por exemplo (RODRIGUES e ARAÚJO, 2016). A virgindade da vítima era uma causa qualificadora nesse caso.

"indivíduos agindo e transacionando em certas capacidades"[43] conforme se movimentam dentro e fora de diferentes contextos sociais (2010, p. 129, tradução nossa). Os contextos são entendidos como "ambientes sociais com características que evoluíram com o tempo, e são sujeitos a uma série de causas e contingências de propósito, lugar, cultura, acidente histórico, entre outros"[44] (2010, p. 130, tradução nossa).

No conceito de integridade contextual, todas as áreas da vida são governadas por normas de fluxo informacional. Ou seja, não existem áreas da vida em que "vale tudo", em que qualquer informação pode ser exposta. A vida das pessoas normalmente envolve uma pluralidade de domínios distintos: uma pessoa vai ao médico, fica em casa com a família, vai ao trabalho, visita amigos, consulta com um psiquiatra, vai ao banco, consulta advogados, faz compras, vota, frequenta cerimônias religiosas etc. Cada uma dessas esferas ou contextos é definida por um conjunto de normas distinto, que governa seus aspectos: papéis, expectativas, ações e práticas. Tais normas podem ter inúmeras fontes (história, cultura, lei, convenção etc.), e dentre elas estão as normas que governam a informação, chamadas por Nissenbaum de normas informacionais. A integridade contextual é mantida quando são cumpridas as normas informacionais. (2004, p. 120, 2010, p. 140).

Nissenbaum afirma que a indignação e a resistência em relação aos sistemas de informação baseados em tecnologia surgem a partir de violações de normas informacionais relativas a contextos. Tais normas prescrevem, para um determinado contexto, quais são as partes que são sujeitos da informação, bem como as que a enviam e recebem, e os princípios segundo os quais a transmissão de informação se dará. A dicotomia público/privado seria uma versão mais grosseira da integridade contextual, postulando apenas dois contextos com dois conjuntos de normas informacionais: a proteção da vida privada, em privado, e a ideia de que "vale tudo" ("*anything goes*") em público. De acordo com a moldura da integridade contextual, porém, considera-se uma ampla gama de contextos sociais, cada um com diferentes conjuntos de normas que governam fluxos informacionais (2010, p. 141).

---

[43] "*In the course of people's lives we act and transact not simply as individuals in an undiff erentiated social world, but as individuals acting and transacting in certain capacities as we move through, in, and out of a plurality of distinct social contexts*."(NISSENBAUM, 2010, pp. 129–130).

[44] "*By contexts, I mean structured social settings with characteristics that have evolved over time (sometimes long periods of time) and are subject to a host of causes and contingencies of purpose, place, culture, historical accident, and more*"(NISSENBAUM, 2010, p. 130).

Normas informacionais também determinarão os atores, que poderão ser colocados em três posições: emissores, destinatários e sujeitos de informação ("*senders of information, recipients of information, and information subjects*"). Nissenbaum dá o exemplo do contexto de serviços de saúde, em que as normas informacionais prescrevem situações de transmissão de informação em que os emissores e sujeitos de informação são os pacientes, e os destinatários são os médicos. É importante que os papeis estejam bem especificados, pois as capacidades nas quais os atores agem dão legitimidade a certos fluxos de informação. A autora aponta que, normalmente, quando as pessoas se referem a certo tipo de informação como secreta, na verdade o que querem dizer é que tal informação é secreta em relação a alguns atores, ou restrita por algum princípio de transmissão, e não absolutamente secreta. A relação que os atores têm um com o outro determinará se o fluxo de informação entre eles é ou não apropriado (2010, p. 143).

Outra questão que deve ser levada em consideração são os tipos ou natureza da informação transmitida. Assim, normas informacionais variam de acordo com os papéis dos atores e com o tipo de informação em questão. Alguns tipos de informação serão apropriados ou não para determinados atores. Por exemplo, no contexto de saúde, é apropriado que médicos questionem seus pacientes sobre as condições de seus corpos. Já num contexto de trabalho, o mesmo tipo de informação seria, na maioria das vezes, inapropriado. Em contrapartida, seria inapropriado que um médico interrogasse seu paciente a respeito de sua religião ou de suas finanças (NISSENBAUM, 2010, p. 144).

Há ainda outro parâmetro das normas informacionais: os princípios de transmissão, definidos como restrições do fluxo de informação entre os atores em um contexto. Expressam os termos nos quais a transmissão poderá ou não ocorrer. Um dos exemplos mais marcantes é o princípio da confidencialidade, que estipula que o destinatário de uma informação não pode compartilhá-la com terceiros. Nissenbaum afirma que a lista de princípios de transmissão é provavelmente indefinida. Um princípio de transmissão pode, por exemplo, determinar que uma informação só deve ser compartilhada voluntariamente, ou consensualmente. Pode, também, requerer que o sujeito seja informado através de uma notificação antes de dar o seu consentimento para que haja transmissão. Pode, ainda, permitir trocas comerciais de informação, de acordo com regras de mercado (2010, p. 145).

Nissenbaum argumenta que as noções tradicionais de privacidade já não se mantinham aptas para lidar com os novos desafios provocados por sistemas técnico-sociais e práticas que alteraram de forma radical o fluxo de informações na sociedade, afetando instituições, estruturas de poder, relacionamentos, entre outros, e gerando novas ansiedades. A autora propõe o conceito de integridade contextual como uma concepção alternativa da "*informational privacy*", sem a pretensão de capturar todo o significado de privacidade, mas buscando caracterizar sistematicamente e precisamente a natureza dessas alterações radicais. Nissenbaum procura entender as razões pelas quais algumas das mencionadas alterações provocam resistência e ansiedade legítima. Propõe que a integridade contextual sirva como uma heurística, um quadro para detectar violações (2010, p. 148).

Um exemplo utilizado por Nissenbaum para abordar a integridade contextual é o caso dos usuários de redes sociais. Muitas vezes, pessoas publicam seus pensamentos, informações pessoais e fotografias de si próprios e de outras pessoas em perfis de *social media*, o que gera a sensação de que "'a juventude de hoje' não se importa com a privacidade". Preocupações controversas relacionadas com a privacidade em redes sociais envolvem terceiros reunindo informações pessoais de usuários a partir de seus perfis, pessoas que têm seu desenvolvimento profissional impedido porque suas publicações desagradaram seus superiores e informações pessoais publicadas em perfis de outras pessoas (2010, pp. 225–226).

Quando se olha para estes problemas tendo em conta apenas a dicotomia público/privado, considera-se que "ou algo é privado e está fora dos limites, ou é público e disponível" (NISSENBAUM, 2010, pp. 224–225, tradução nossa)[45] . Pensando em termos de integridade contextual, porém, argumenta-se que existem nuances que devem ser consideradas, e que a indignação perante tais problemas pode ser justificada. Para Nissenbaum, em muitos desses casos, as surpresas evidenciam um choque de contextos, de modo que usuários acreditavam estar agindo em uma capacidade dentro de um contexto, e foram tratados como se estivessem agindo em outra, dentro de outro contexto. Empregados ou candidatos a um emprego que são prejudicados porque materiais publicados por seus amigos foram visualizados por empregadores e recrutadores, por exemplo, podem

[45] *"Either something is private and off limits or it is public and up for grabs"* (NISSENBAUM, 2010, pp. 224–225).

considerar que estes não respeitaram princípios de transmissão ao vasculhar conteúdo que era destinado aos amigos. No caso de serviços que agregam informações pessoais a partir de perfis de redes sociais (que podem incluir nome, idade, universidade onde estudou e afiliação partidária), informação que originalmente circulava dentro de um círculo social passou para outros recipientes sem o consentimento do usuário ou seu conhecimento. Quando amigos ou conhecidos compartilham informações sobre uma pessoa em seus perfis, normalmente a situação é caracterizada como uma quebra da confidencialidade (2010, p. 226).

Assim, pode-se dizer que a privacidade, nessa perspectiva, é um direito não propriamente de ter controle sobre informação ou de ter o acesso a essa informação restrito, mas "de viver num mundo em que as nossas expectativas sobre o fluxo de informação são, em geral, atendidas". Tais expectativas se baseiam não somente em hábitos e convenções, mas também na confiança de que os fluxos serão orientados de acordo com os princípios da vida social (NISSENBAUM, 2010, p. 231). Trazendo a ideia de integridade contextual para a proteção de dados pessoais, Bruno Bioni afirma que, a partir desse conceito, tem-se uma alternativa normativa em que a proteção de dados não se baseia totalmente no consentimento do titular. A integridade contextual compreende a ideia de que a privacidade não beneficia somente o indivíduo, mas toda a sociedade, na medida em que viabiliza a democracia e a participação deliberativa entre os cidadãos (BIONI, 2019, cap. 5; NISSENBAUM, 2010, p. 76). De acordo com Bioni, a integridade contextual traz essa mensagem para a proteção de dados pessoais, ao se propor a investigar as implicações do fluxo informal para as interações sociais. Considerando a intensa datificação da vida das pessoas, e a utilização de seus dados para decisões automatizadas que afetam suas vidas, é preciso que os dados pessoais tenham sua negociabilidade limitada. Bioni propõe, assim, que a integridade contextual seja encarada como uma vertente normativa complementar à autodeterminação informacional, limitando-a a situações que não esvaziem a importância do papel desempenhado pela proteção de dados pessoais. A autonomia do titular de dados não pode ser tratada como uma armadilha. Assim, é preciso investigar se o fluxo informacional é apropriado e se não apresenta interferência excessiva com o desenvolvimento da personalidade do titular (2019, cap. 5).

Também se apoiando na integridade contextual de Nissenbaum, Franck Dumortier analisou os riscos de "descontextualização" que derivam das interações através do *site*

Facebook. De acordo com Dumortier, o conceito de "descontextualização" da informação é particularmente interessante no caso da rede social, devido às suas propriedades arquitetônicas, temporais e intersubjetivas, que geram disparidades entre os sentimentos do usuário e a forma como a informação pode ser propagada. Destaca três características principais que contribuem para a descontextualização: a simplificação das relações sociais, a grande disseminação de informação e os efeitos de globalização e normalização do *Facebook* (2010, p. 121).

A simplificação das relações sociais ocorre porque, enquanto no "mundo *off-line*" relações são multifacetadas, a rede de contatos das pessoas nos *social media* engloba conhecidos, amigos, colegas de trabalho, familiares, empregadores etc., ou seja, abrange vínculos de diversos níveis, reduzindo-os a relações binárias: "amigo ou não" (DUMORTIER, 2010, p. 122) . A disseminação de informação é ampla, pelo fato de que o *Facebook* permite grandes redes de contatos (como os grupos de determinadas áreas geográficas, que podem ter centenas de milhares de membros), e as conexões de uma pessoa estão muitas vezes visíveis em seu perfil (DUMORTIER, 2010, pp. 123–126). Além disso, funções da própria rede social, aplicativos de terceiros e o próprio aplicativo da rede para *smartphones* promove compartilhamento de dados cada vez mais intenso. Dumortier chama de "efeito de globalização" o fato de que, mesmo sem se inscrever como usuário da rede social, pessoas podem ser titulares de dados presentes na rede, através de fotos e artigos publicados por terceiros. Sem ter conhecimento ou possibilidade de responder, uma pessoa pode se tornar objeto de um tópico de discussão amplamente disseminado. Já o "efeito de normalização" se refere ao fato de que cada vez mais pessoas aderem à rede social, de modo que alguém que não tenha um perfil registrado no *site* pode passar a ser considerado como anormal (2010, p. 127). O autor afirma que essa descontextualização traz consequências para o direito à privacidade e para o direito à proteção de dados pessoais. No que toca à privacidade, segundo Dumortier, o *Facebook* apresenta uma ameaça à integridade contextual por dificultar a possibilidade de que cada um construa sua identidade através de relacionamentos diferenciados. A plataforma apresenta um colapso de contextos e funde todos os relacionamentos em um espaço social único (2010, p. 131).

Segundo Dumortier, o direito à proteção de dados pessoais pode ser visto como um meio de controle sobre uma projeção parcial da identidade de uma pessoa. A partir de

trabalhos como o de Williams (2005) e Deleuze (1992), o autor sustenta que, através dos dados coletados sobre nós, as tecnologias de controle conseguem separar quem somos de nossos seres físicos, e os dados passam a ser uma representação de nós mesmos na rede de relações sociais. Somos, assim, reduzidos aos nossos interesses e comportamentos documentados. Dumortier caracteriza a proteção de dados como um direito proporcionado a "*dividuals*", ou seja, a "sujeitos humanos infinitamente divisíveis e reduzíveis a representações de dados pelas tecnologias modernas de controle, como sistemas baseados em computadores" (WILLIAMS, 2005, p. 104, tradução nossa)[46]. O termo inglês "*dividual*", significa "dividido, compartilhado", e é adotado por Deleuze em suas descrições de sociedades de controle (DUMORTIER, 2010).

Devido à divisibilidade de dados pessoais em vários contextos de representação, somos expostos ao risco de que a informação seja descontextualizada, principalmente considerando a fluidez dos dados eletrônicos. A informação coletada em um contexto pode ser facilmente usada em outro, de forma muitas vezes inapropriada. Segundo Dumortier, a legislação europeia sobre proteção de dados foi desenhada para garantir ao titular de dados pessoais (referido como um "*dividual*") meios de evitar a descontextualização da informação. As previsões de que os dados deverão ser "recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades", e também de que deverão ser "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados" (artigo 5.º, n.º 1, alíneas b) e c), do RGPD, e antigo artigo 6.º, n.º 1, alíneas b) e c), da Diretiva 95/46/CE) podem ser interpretadas como uma consagração da integridade contextual. O autor também propõe que os direitos de informação, acesso, retificação e oposição podem ser vistos como meios para garantir a integridade contextual dos dados de uma pessoa (2010, p. 134).

Na visão de Dumortier, o fenômeno da descontextualização em *sites* como o *Facebook* é particularmente danoso para o direito à proteção de dados pessoais. O propósito de redes sociais é amplo demais para que se possa determinar qual tipo de dados é adequado, relevante e não excessivo em relação à sua finalidade. Ao fundir vários contextos em apenas um ambiente, a rede social nega a existência das dividualidades de

[46] Esta é a definição do termo "*dividuals*" fornecida por Robert W. Williams, e mencionada também por Dumortier (WILLIAMS, 2005, p. 104).

seus usuários. O autor destaca nesse ponto o parecer do Grupo de Trabalho do Artigo 29.º sobre *online social networking* em que demonstra preocupação pela disseminação e uso de informação disponível nas redes para finalidades secundárias e não pretendidas, sugerindo a adoção de configurações de segurança robustas e configurações de privacidade por definição[47] (2009, p. 3, tradução nossa).

A partir das considerações sobre a integridade contextual e sua relação com o direito à proteção de dados pessoais, especialmente no que diz respeito às redes sociais, podemos examinar a disseminação não consensual de imagens íntimas, que se manifesta como violação ao direito à proteção de dados. Quando as imagens ou vídeos (dados pessoais) de uma pessoa são retirados de um determinado contexto (uma conversa em aplicativo, um arquivo de computador ou na nuvem) e transportadas a outro contexto (uma publicação em redes sociais ou *websites*), tornando-as visíveis e disponível a todos, podemos identificar uma violação daquilo que Nissenbaum chama de normas informacionais. O fluxo informacional não é adequado, já que não se espera que aquele tipo de informação (imagens com conteúdo íntimo ou sexual) seja compartilhado com aqueles atores (o público geral).

Da mesma forma, podemos identificar violações à legislação europeia sobre a proteção de dados pessoais: o tratamento é ilícito principalmente pelo fato de que o titular de dados pessoais, que é a pessoa retratada nas imagens, não consentiu em sua divulgação, contrariando o disposto no artigo 6.º, n.º 1, alínea a), do Regulamento. Importa destacar que, como em muitos dos casos mencionados no capítulo 1, mesmo quando uma pessoa consente que outra tenha acesso às suas imagens e vídeos, tal consentimento não legitimará a divulgação posterior dos dados a outras pessoas, já que o contexto deve ser específico para uma finalidade. Essa ideia está em consonância com os já mencionados princípios da limitação das finalidades e da minimização dos dados, previstos no artigo 5.º, n.º 1, alíneas b) e c), do Regulamento, e com a própria noção de integridade contextual, segundo a qual esse fluxo externo de informações seria inapropriado por violar as expectativas relativas àquele contexto, assim como seria inapropriado que um médico compartilhasse dados de saúde fornecidos consensualmente pelo paciente com o empregador deste.

[47] "*The dissemination and use of information available on SNS for other secondary, unintended purposes is of key concern to the Article 29 Working Party. Robust security and privacy-friendly default settings are advocated throughout the Opinion as the ideal starting point with regard to all services on offer*" (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2009, p. 3).

No caso da NCII, verifica-se uma espécie de descontextualização semelhante àquela identificada por Dumortier nas redes sociais como o *Facebook*. Ao se disseminar uma imagem ou vídeo em *sites* e redes sociais, rompe-se com a separação entre cada um dos contextos nos quais uma pessoa pode interagir, expondo a diversos atores de diversos contextos (família, empregador, amigos, colegas de trabalho) dados referentes a uma dimensão que deveria ser mantida em um contexto mais restrito: a vida sexual. Nos próximos capítulos analisaremos o problema da disseminação não consensual de imagens íntimas na perspectiva da legislação sobre proteção de dados da União Europeia.

3. O CONSENTIMENTO E SEUS LIMITES

3.1 O direito à proteção de dados pessoais ao longo dos tempos.

3.1.1 Observações sobre a evolução do *right to privacy* no contexto Estadunidense

O presente tópico pretende abordar a construção do direito à *privacy* nos Estados Unidos, destacando a diferenciação entre o modelo norte-americano e o modelo europeu de proteção de dados pessoais. Em alguns aspectos, nomeadamente no que diz respeito à vertente "*informational privacy*", a *privacy* norte-americana guarda semelhanças com aquilo que se entende por proteção de dados pessoais no contexto da União Europeia, principalmente por surgir a partir de receios semelhantes àqueles que impulsionaram o surgimento das primeiras normas de proteção de dados na Europa. Contudo, como se observará adiante, é preciso esclarecer que *privacy* e proteção de dados não se equivalem, e o direito à *privacy* nos Estados Unidos engloba situações que vão muito além da noção europeia de proteção de dados (PINHEIRO, 2015, p. 267).

O artigo "*Right to Privacy*", de Samuel D. Warren e Louis D. Brandeis, publicado em 1890 na *Harvard Law Review*, é referido como o primeiro momento em que o direito à *privacy* foi autonomizado (CASTRO, 2005, p. 17), e sua publicação é frequentemente identificada com o início do debate moderno a respeito da privacidade[48] (DONEDA, 2019, cap. 1; MEZZANOTTE, 2009, p. 51; PINTO, 1993, p. 513). Os autores do artigo mencionam a necessidade de se "adotar um próximo passo para a proteção da pessoa e para assegurar ao indivíduo (...) o "direito a ser deixado em paz"[49] (WARREN e BRANDEIS, 1890, p. 195), diante das invenções e modelos de negócios que surgiam à época. Warren e Brandeis demonstraram preocupação no que diz respeito a empreendimentos jornalísticos e às novas tecnologias - nomeadamente o surgimento de

[48] Doneda chama atenção para o fato de que o marco inicial do debate não foi tão abrupto, e o assunto já havia sido mencionada na jurisprudência do *common law* e em literatura anterior (DONEDA, 2019, cap. 1). No mesmo sentido, Pinheiro: "o ano de 1890 marcou a origem da *privacy* com contornos dogmáticos próprios. O estudo das fontes demonstra que, rigorosamente, não foi de Warren e Brandeis a "primeira palavra" sobre o Right to Privacy" (PINHEIRO, 2015, p. 279).

[49] "*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person and for securing the individual what Judge Cooley calls the 'right to be let alone'*"(WARREN e BRANDEIS, 1890).

fotografias instantâneas - que poderiam resultar em invasões à vida privada e doméstica (WARREN e BRANDEIS, 1890, p. 195).

O artigo é concebido em um contexto de preocupação quanto à invasão da vida privada não por parte de entidades públicas, mas por particulares, como a imprensa ou qualquer indivíduo que obtenha fotografias ou imagens sem o consentimento dos titulares. Afirma-se que o artigo foi motivado por acontecimentos da própria vida de Samuel Warren, descendente de uma família tradicional de Boston e casado com a filha de um senador, cujas festas eram reportadas em crônicas sociais com riqueza de detalhes (CASTRO, 2005, p. 18; PINHEIRO, 2015, p. 282; PROSSER, 1960, p. 383).

Em seu artigo, Warren e Brandeis mencionam o "*right to be let alone*" ("direito de ser deixado em paz"), que havia sido descrito por Thomas Cooley em sua obra *Treatise on the Law of Torts, or the Wrongs Which Arise Independent of Contract*. Cooley identifica tal direito como um "direito de completa imunidade", sendo o dever a ele correspondente o de "não causar qualquer lesão e de não, dentro de tal proximidade que possa tornar a ação bem-sucedida, tentar infligir uma lesão".[50] (COOLEY, 1888, p. 29, tradução nossa). Tal direito baseia-se na defesa do corpo e da "paz singular do indivíduo". É possível dizer que Warren e Brandeis "definem o conteúdo de um novo direito, o '*right to privacy'*, a partir de uma fórmula já conhecida, o '*right to be let alone*'" (PINHEIRO, 2015, p. 295).

Os autores buscaram distinguir a *privacy* de figuras conhecidas que com ela tinham alguma semelhança, como por exemplo a difamação. Ao contrário do que ocorre em casos de calúnia e difamação, em que está em causa um dano à reputação de um indivíduo e a redução de sua estima por parte da comunidade, no direito à *privacy* está em jogo não uma ofensa ao seu caráter, mas à sua privacidade. Assim, a verdade do que é publicado também não tem relevância para a configuração de uma ofensa ao direito, e tampouco releva a intenção do agente (WARREN e BRANDEIS, 1890, p. 197 e 218).

O artigo estabeleceu o direito à *privacy* como um direito pessoal, que não é protegido através da tutela da propriedade (DONEDA, 2019, cap. 1). Os autores afirmam que "o direito que protege escritos pessoais e todas as demais produções pessoais, não

[50] "*Personal Immunity. The right to one's person may be said to be a right of complete immunity: to be let alone. The corresponding duty is, not to inflict any injury, and not, within such proximity as might render it successful, to attempt the infliction of an injury*" (COOLEY, 1888, p. 29).

contra furto ou apropriações físicas, mas contra publicação sob qualquer forma, é, na realidade, não o princípio da propriedade privada, mas da personalidade inviolada" (PIERFELICI, 1999, p. 63; WARREN e BRANDEIS, 1890, p. 205).

De acordo com Warren e Brandeis, o que se busca é proteger "pessoas com cujos assuntos o público não tem qualquer interesse legítimo" de uma "publicidade indesejada", e proteger "todas as pessoas, independentemente de sua posição, de ter assuntos que provavelmente prefeririam que permanecessem privados, tornados públicos contra sua vontade" (WARREN e BRANDEIS, 1890, p. 214 e 215). Assim, observam os autores que o direito à *privacy* não é um direito absoluto, já que se pode argumentar que existem pessoas que renunciaram ao direito de não terem suas vidas expostas ao olhar do público. Questões que, para um cidadão comum, diriam respeito apenas à sua pessoa, podem ser de interesse legítimo dos demais cidadãos quando se trata de um candidato a um cargo público, por exemplo. A pertinência de uma publicação, porém, mesmo quando diz respeito a pessoas que concorrem a cargos públicos ou que pretendem participar da vida pública de algum modo, dependerá ainda do seu conteúdo. Assuntos que concernem à "vida privada, hábitos, atos e relações de um indivíduo e não têm conexão legítima com a sua aptidão para o cargo público o qual almeja, ou para o qual foi nomeado", por exemplo, devem ser reprimidas (WARREN e BRANDEIS, 1890, p. 216).

O *right to privacy* também não proíbe publicações feitas em tribunais, em órgãos legislativos, assembleias municipais, ou outros tipos de organismo público, nem publicações necessárias para cumprimento de algum dever público ou privado. Os autores também ressaltam que, caso a violação da *privacy* seja feita através de publicação oral, provavelmente não será autorizada uma compensação se não tiver sido configurado algum dano (WARREN e BRANDEIS, 1890, p. 217). Finalmente, o direito à *privacy* cessa com a publicação dos fatos pelo indivíduo ou com o seu consentimento (WARREN e BRANDEIS, 1890, p. 218).

Pode-se dizer que o artigo "*The Right to Privacy*" tratava, principalmente, do direito à imagem e sua reserva (apesar de que o bem jurídico *privacy* vai bem além disso), como uma reação ao perigo das pequenas câmeras que poderiam registrar momentos sem autorização das pessoas em causa (PINHEIRO, 2015, p. 317). Nesse momento, o direito à *privacy* apresenta-se como o direito de "estar a salvo de interferências alheias", e o direito de uma pessoa de "retrair aspectos de sua vida do domínio público". O seu conteúdo está,

então, “centrado na liberdade negativa de o indivíduo não sofrer interferência alheia” (BIONI, 2019, cap. 2).

Apesar de já conhecida, a *privacy* só foi estabelecida na doutrina em 1960, pelo artigo *Privacy* de William Prosser, em que foram determinadas quatro categorias de *torts*, que correspondem a quatro tipos de interesses: “(i) interesse da preservação do indivíduo contra intrusões alheias (...); (ii) interesse na não publicação de fatos privados sobre o indivíduo (...); (iii) interesse na não divulgação de fatos privados que podem criar uma imagem pública falsa (...); (iv) interesse na não divulgação do nome do indivíduo (...)” (PINHEIRO, 2015, p. 321; PROSSER, 1960, p. 389).

O primeiro *tort* especificado, “*intrusion upon the plaintiff’s seclusion or solitude*”, diz respeito a casos em que há uma intrusão na reclusão ou solidão de um indivíduo, como, por exemplo, casos de intrusão de domicílio, de quarto de hotel, e mesmo no caso de uma revista ilegal em uma sacola de supermercado (PINHEIRO, 2015, p. 322; PROSSER, 1960, p. 390). O segundo, “*public disclosure of private facts*”, refere-se a situações como as descritas no artigo de Warren e Brandeis, em que há publicação de fatos privados do indivíduo (PINHEIRO, 2015, p. 325; PROSSER, 1960, p. 392).

A terceira forma de invasão da privacidade, segundo Prosser, é a de “*publicity that places the plaintiff in a false light in the public eye*”, que se refere a fatos erroneamente atribuídos a um indivíduo. O primeiro exemplo citado por Prosser é um caso em que um poema de qualidade inferior havia sido atribuído a Lord Byron. Uma das formas mais frequentes se manifesta quando opinião ou frase é atribuída falsamente ao indivíduo (PINHEIRO, 2015, p. 334; PROSSER, 1960, p. 398). Finalmente, o tort de “*appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness*” diz respeito à “exploração dos atributos da identidade do autor” (PROSSER, 1960, p. 401). Ocorre quando, por exemplo, o nome, a foto, ou as características do indivíduo são usados sem o seu consentimento para promover produtos ou aumentar as vendas de artigos (PINHEIRO, 2015, p. 337; PROSSER, 1960, p. 402).

O sentido de *privacy* para o direito estadunidense evoluiu, e pode-se identificar uma distinção entre o que se chama de *informational privacy* e *decisional privacy*. A primeira assemelha-se mais à proteção de dados Europeia, e seu conceito está vinculado a formas de tornar pública informação pessoal. Já a segunda não diz respeito a informação pessoal, mas a comportamentos (PINHEIRO, 2015, p. 365 e 366). A *decisional privacy*

pode ser descrita como "o direito de tomar decisões reprodutivas e outras decisões íntimas sem a interferência do governo"[51] (RICHARDS, 2007, p. 265, tradução nossa).

Nesse sentido, o caso Griswold v. Connecticut, de 1965, é considerado como aquele que serviu de base para as futuras decisões sobre *decisional privacy.* Trata-se do caso em que a diretora executiva e o diretor médico da organização *Planned Parenthood League* de Connecticut haviam sido condenados por fornecerem informações em conselhos médicos sobre contracepção a pessoas casadas, e prescreverem materiais contraceptivos. No estado de Connecticut, era considerado crime o uso de droga ou qualquer artigo para prevenção da concepção (GRISWOLD V. CONNECTICUT, 1965). O Supremo Tribunal dos Estados Unidos considerou inconstitucional a lei que criminalizava o uso de contraceptivos por ser inconsistente com o direito à *privacy* (no que se referia a pessoas casadas). O Tribunal reconheceu, assim, a existência desse direito, referindo-se a emendas que já haviam sido de alguma forma fundamento para a aplicação do *right to privacy* (PINHEIRO, 2015, p. 371; RICHARDS, 2007, p. 265; ROPPO, 1984, p. 68).

A decisão de Griswold v. Connecticut serviu de modelo para diversas outras decisões que envolviam a *decisional privacy*. No caso *Eisenstadt v. Baird*, de 1972, por exemplo, o Tribunal considerou inconstitucional uma lei que proibia que indivíduos não casados acedessem a contraceptivos. O direito à *privacy* foi aqui entendido como "o direito de um indivíduo de estar livre de intrusões do Estado quanto a decisões tão fundamentais como a de ter ou não um filho"[52] (EISENSTADT V. BAIRD, 1973, tradução nossa). A decisão de Griswold também serviu de base para *Roe v. Wade*, de 1973, em que se reconheceu um direito a abortar fundado no direito à *privacy* (DONEDA, 2019, cap. 3; PINHEIRO, 2015, p. 374; RICHARDS, 2007, p. 265).

No que diz respeito à *informational privacy*, destaca-se que a noção de *privacy* como "o direito de indivíduos, grupos ou instituições de determinar por si próprios quando, como, e em qual extensão a informação sobre si será comunicada a outros", de Alan Westin, se aproxima do direito à proteção de dados na concepção europeia, especialmente no que diz respeito à ideia de autodeterminação informacional, que será desenvolvida

[51] *"(...) the right to make reproductive and other intimate decisions without government Interference*" (RICHARDS, 2007).
[52] "*If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child*" (EISENSTADT V. BAIRD, 1972).

posteriormente na Alemanha, pela ênfase na autonomia do indivíduo em controlar suas próprias informações (BIONI, 2019, cap. 3; DONEDA, 2019, cap. 2; WESTIN, 1967). A *privacy* informacional começou a ser regulada principalmente no fim dos anos 70 do século passado, com ênfase a partir de 1974, o que foi motivado não só pela expansão do uso de computadores, mas também por questões de política interna dos Estados Unidos. A preocupação estava voltada para o armazenamento de dados pela Administração, por bancos e instituições de crédito (PINHEIRO, 2015, p. 401).

O caso paradigmático no que diz respeito à *informational privacy* nos Estados Unidos foi o projeto de criação do *National Data Center*. Por volta de 1965, o Escritório de Orçamento apresentou uma proposta para a construção de uma central única de armazenamento de informações pessoais, reunindo informações sobre cidadãos norte-americanos disponíveis em vários órgãos da administração federal. O projeto pretendia unificar os cadastros do censo, dos registros trabalhistas, do fisco e da previdência social, o que apresentaria vantagens em termos de eficiência administrativa, já que é mais dispendioso localizar informações armazenadas em bancos de dados dispersos, por exemplo.

Em resposta ao projeto, surgiram debates em torno dos possíveis problemas causados pela concentração de dados pessoais em um único polo. Havia um receio generalizado de que a unificação dos bancos de dados, concentrando as informações nas mãos da administração, poderia atribuir um poder excessivo ao governo. O Congresso realizou uma série de audiências com o intuito de discutir os efeitos da criação desse banco de dados, e por fim recomendou que não se estabelecesse um banco de dados nacional sem que a proteção da privacidade fosse observada e garantida ao máximo nível possível para os cidadãos cujas informações seriam usadas. Posteriormente, o projeto foi encerrado (DONEDA, 2019, cap. 2; HOUSE OF REPRESENTATIVES, 1966, p. 318).

Os trabalhos de Alan Westin e Arthur Miller foram os de maior destaque na área, e são frequentemente referidos em obras sobre a *informational privacy* e proteção de dados. Já nos anos 60 e início dos anos 70, refletiram a preocupação quanto à proteção de dados pessoais no contexto da expansão do uso e da capacidade dos computadores. Na obra *The Assault on Privacy*, de 1971, Miller já prevê que “pode não demorar muito para que computadores se comuniquem entre si e com seus operadores da mesma maneira que

humanos comunicam entre si"[53] (1971, p. 14, tradução nossa). Miller identifica dois possíveis danos infligidos ao titular de dados pessoais ("*data subject*") pelos computadores que trabalham com informação pessoal. Em primeiro lugar, há o risco de disseminação de informações sobre atos ou associações presentes ou passados para um público maior do que aquele antecipado pelo titular ou para o qual havia dado seu consentimento, quando inicialmente forneceu a informação. Em segundo lugar, há possibilidade de introdução de inexatidões factuais ou contextuais nos dados, que pode criar impressões errôneas das reais condutas do sujeito (1971, p. 26).

Da mesma forma, Alan Westin, na obra *Privacy and Freedom* de 1967, sustenta que a coleta e o tratamento de dados para diversos propósitos públicos e privados, se não controlada, podem levar a um poder extenso de vigilância do governo sobre a vida e as atividades do indivíduo (1967, p. 158). Westin comenta sobre seis tendências que geravam ameaças à *privacy* na época. Em primeiro lugar, observa a tendência de que o ser humano tenha que fornecer uma corrente constante de informações sobre si, tanto para ajudar a sociedade a funcionar de forma mais eficiente, como para ajudar a si mesmo. Tais informações são gravadas em registros, como, por exemplo, registros de nascimento, de casamento, documentos escolares, dados de censo, militares, de passaporte e de emprego. Em segundo lugar, menciona o fato de que a mobilidade das pessoas e a padronização da vida em sociedade conduziu ao desenvolvimento de sistemas de investigação e a acumulação de dossiês sobre cidadãos estadunidenses. Esses dossiês, muitas vezes, eram desconhecidos pelos próprios indivíduos, de modo que geralmente não havia um meio para questionar a exatidão dos dados armazenados (1967, p. 159).

Em terceiro lugar, Westin comenta que a capacidade de coleta de dados e de elaboração de dossiês foi radicalmente acelerada pelo advento do computador eletrônico digital. A quarta tendência identificada pelo autor é o fato de que o desenvolvimento de alguns programas governamentais gerou uma demanda por mais dados pessoais do que aqueles que eram anteriormente recolhidos em pesquisa nos Estados Unidos. Como exemplo, menciona o *Civil Rights Act*, de 1964, que passou a exigir que o departamento do censo obtivesse informações sobre o registro de votos. Em quinto lugar, o autor identificou a tendência de aceleração do compartilhamento de dados entre usuários de computadores,

[53] "*It may not be long before computers are communicating with each other and their operators in much the same manner as humans communicate among themselves*" (MILLER, 1971, p. 14).

em decorrência da padronização das linguagens de computação e do aperfeiçoamento de máquinas que traduzem uma linguagem para a outra, possibilitando que computadores se comuniquem diretamente uns com os outros. Finalmente, a sexta tendência identificada por Westin é a substituição gradual das transações tradicionais em dinheiro pelo processamento automático de dados, como no caso dos cartões de crédito (1967, pp. 160–163).

Apesar de o trabalho de Warren e Brandeis ser considerado um marco no que diz respeito à *privacy,* sendo frequentemente referido em obras sobre a privacidade e proteção de dados fora do sistema Common Law (BIONI, 2019, cap. 2; CASTRO, 2005, p. 17; DONEDA, 2019, cap. 2; FINOCCHIARO, 2014, p. 159), resta claro que o direito à *privacy* para o direito estadunidense não corresponde ao direito à privacidade ou à proteção de dados no Direito Europeu. "*Privacy* e privacidade não se equivalem, *privacy* e proteção de dados não são sinônimos com regimes variados" (PINHEIRO, 2015, p. 267). A *privacy* para o direito estadunidense abriga questões que vão muito além das noções de privacidade e proteção de dados no contexto europeu, como a possibilidade de recurso a anticoncepcionais, o aborto e as relações homossexuais.

3.1.2 O direito à proteção de dados no contexto europeu

Neste tópico, abordaremos a evolução geracional das normas em matéria de proteção de dados pessoais na Europa. Para isso, utilizaremos a classificação de Viktor Mayer-Schönberger, que divide a evolução da legislação em quatro gerações.[54] Cumpre, porém, fazer uma ressalva quanto a essa abordagem. Alexandre de Sousa Pinheiro, apesar de abordar essa taxonomia em sua obra, apresenta objeções ao tratamento científico do direito à proteção de dados pessoais através de uma divisão dessa natureza. Segundo o autor, a divisão geracional não leva em conta a diversidade de vias de incorporação do direito à proteção de dados pessoais nos ordenamentos jurídicos nacionais. Pinheiro também chama atenção para o fato de que a evolução das telecomunicações eletrônicas criou elementos que dividiriam a proteção de dados em duas áreas: antes e depois das redes sociais e da recolha à distância de imagens para finalidades distintas da videovigilância (PINHEIRO, 2015, p. 572).

Contudo, apesar de oferecer um retrato reducionista do desenvolvimento da legislação sobre a matéria na Europa, como destaca Bioni, a divisão geracional fornece algumas noções que devem ser consideradas quando se pensa no direito à proteção de dados pessoais no contexto europeu. Destaca-se, principalmente, a noção de autodeterminação informacional, o papel de protagonista do consentimento, e como este tem sido revisitado e revigorado ao longo do processo evolutivo. Desse modo, mesmo tendo em conta as limitações dessa abordagem, a divisão de Mayer-Schönberger pode fornecer "uma amostra de como o progresso geracional das leis de proteção de dados pessoais teve curso no direito comunitário europeu" (BIONI, 2019, cap. 3).

3.1.2.1 As primeiras gerações de leis em matérias de proteção de dados

As primeiras leis em matéria de proteção de dados pessoais publicadas na Europa surgiram ao longo dos anos 70, como resultado da percepção de mudanças tecnológicas no processamento de informações (MAYER-SCHÖNBERGER, 2001, p. 219). A primeira lei

[54] Reconhece-se, porém, que existe outro referencial teórico que estabelece apenas três gerações (POULLET, 2010). Contudo, este trabalho opta por adotar a evolução geracional elaborada por Mayer- Schönberger, no artigo "*Generational Development of Data Protection in Europe*" (MAYER-SCHÖNBERGER, 2001).

sobre proteção de dados pessoais a entrar em vigor foi a do estado de Hesse, na Alemanha. Em seguida, a lei sueca de proteção de dados pessoais, a lei do estado alemão de Rheinland-Pfalz, os vários projetos de lei federal na Alemanha, os projetos de lei da Áustria e a lei federal alemã de proteção de dados também surgiram no mesmo contexto, e podem ser vistos como reações diretas a planos de centralização de bancos de dados nacionais (MAYER-SCHÖNBERGER, 2001, p. 221).

Nesse primeiro momento, a preocupação era voltada para o crescimento do processamento eletrônico de dados por governos ou grandes empresas. Para implementar reformas sociais e estender seus sistemas de bem-estar social, os governos europeus tinham de não só coletar quantidades crescentes de informação dos cidadãos, como processar e estabelecer vínculos entre os dados coletados. Dessa forma, governos começavam rapidamente a entender os benefícios dos computadores, assim como grandes empresas passaram a perceber as vantagens da computação para melhor gerir seus empreendimentos. Surgiram, assim, propostas para centralizar a informação a nível nacional. Cresceu o receio quanto à centralização de arquivos de dados pessoais em grandes bancos de dados nacionais, e temia-se uma situação de total vigilância, como descrito na obra de George Orwell, 1984 (MAYER-SCHÖNBERGER, 2001, p. 223).

Mayer-Schönberger identifica essa como a primeira geração de legislação sobre proteção de dados. Nesse caso, o foco está na proteção de dados como ferramenta para conter os perigos do uso de computadores no processamento de informações sobre humanos. Assim, a maioria das normas de primeira geração não teve como enfoque principal a privacidade individual, mas considerava que, "se o ato do processamento é o problema, a legislação deveria ter como alvo o funcionamento do computador" (2001, p. 223, tradução nossa).[55] As normas de proteção de dados eram vistas como parte de uma tentativa de "domar" a tecnologia" (2001, p. 223). A construção da proteção de dados na Europa estava voltada para a blindagem dos dados pessoais e tinha um caráter mais proibitivo (FUSTER e GUTWIRTH, 2013, p. 534).

O surgimento e a crescente difusão dos microcomputadores, porém, provocou uma mudança na discussão sobre proteção de dados pessoais. Se antes o receio estava restrito a alguns bancos de dados centralizados, com o uso dos microcomputadores,

[55] "*If the act of processing is the actual problem, the legislation should target the workings of the computer*" (MAYER-SCHÖNBERGER, 2001, p. 223).

passou-se a adotar um processamento de dados descentralizado. Já não havia apenas a figura de um "Big Brother" a ser temido, mas uma gama muito mais ampla de possíveis infratores de normas de proteção de dados pessoais (BIONI, 2019, cap. 3; MAYER-SCHÖNBERGER, 2001, p. 224).

A legislação existente até então era inadequada para responder a uma realidade já não de apenas dezenas, mas de milhares de unidades processadoras de dados, impondo procedimentos demasiado complexos e morosos, que passaram a ser abertamente desconsiderados pela administração pública e por empresas. Os cidadãos temiam a coleta e processamento irrestritos de dados pessoais, e, como resultado, passaram a reivindicar direitos de privacidade e de proteção de dados, o que ia além das tentativas da legislação de controlar a tecnologia existente. É esse o contexto no qual se insere a segunda geração de normas em matéria de proteção de dados pessoais identificada por Mayer-Schönberger (2001, p. 224).

Desse modo, a segunda geração teve como enfoque os direitos individuais de privacidade do cidadão, e o direito à proteção de dados passou a ser explicitamente ligado ao direito à privacidade, tornando-se um direito garantido nas constituições da Espanha, Áustria e Portugal[56]. As normas passaram a ser mais abstratas e menos ligadas a um

[56] Cumpre fazer uma observação quanto à presença do direito à proteção de dados pessoais no texto constitucional português. A Constituição Portuguesa de 1976 foi a primeira Constituição europeia a integrar um dispositivo especial sobre proteção de dados pessoais, em seu artigo 35.º (CASTRO, 2005, p. 32). O direito foi tratado de forma indireta, porém, já que o texto original não fazia menção, em qualquer dos três números, à "proteção de dados" ou ao "direito à proteção de dados". O texto de 1976 já previa, contudo, o direito ao conhecimento da informação, à retificação de dados e sua atualização, também fazia menção ao "tratamento de dados" e suas limitações, e à proibição da criação de um número nacional único. Também era proibido o uso da informática para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, exceto no caso de processamento de dados não identificáveis para fins estatísticos. Alexandre Sousa Pinheiro chama atenção para o fato de que a epígrafe do artigo 35.º não reconhece qualquer direito, mas apenas "um 'problema/*quaestio*' gerador de direitos": a utilização da informática, que, nesse sentido, se assume "como um fenômeno autônomo de proteção jurídica, não subsumido à protecção da intimidade da vida privada' ou aos 'direitos da personalidade'. (2015, p. 666). Catarina Sarmento e Castro comenta que a consolidação desse direito foi influenciada pela já mencionada decisão do Tribunal Constitucional Alemão sobre a Lei do Censo de 1983, em que se construiu o direito à autodeterminação informacional a partir da interpretação da Constituição Alemã. Castro também sustenta que, apesar da epígrafe, o direito citado se refere não apenas à proteção de dados face à informática, mas também em relação a outros meios. Nesse sentido, a partir da Revisão Constitucional de 1997, o artigo 35.º foi acrescido do número 7, que determina que: "os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei". Desse modo, o artigo 35.º da Constituição consolida um conjunto de direitos fundamentais que buscam impedir que o cidadão seja tratado como mero "objeto de informações" (2005, p. 33). Após as revisões constitucionais, o artigo 35.º foi alargado. Passou a incluir, em seu número 2, disposição determinando que a lei definirá o conceito de dados pessoais, bem como as condições aplicáveis ao tratamento, transmissão, conexão e utilização, e garantirá a sua proteção através de entidade administrativa independente. A proibição do tratamento de dados sensíveis passou a ser prevista no número

estágio específico da tecnologia. Mayer-Schönberger identifica como pertencentes à segunda geração de normas sobre a proteção de dados as legislações da França (1978) e da Áustria (1978), e, em certos aspectos, da Dinamarca (1978 e 1987) e da Noruega (1978) (MAYER-SCHÖNBERGER, 2001, p. 226).

Na segunda geração, de acordo com Mayer-Schönberger, os indivíduos passaram a ter mais poder de decisão sobre o processo de tratamento de dados. O consentimento era, muitas vezes, uma condição necessária para o tratamento, e, em outros casos, poderia prevalecer sobre uma presunção de proibição de tratamento de dados. Esperava-se "que o indivíduo fosse o melhor garante de uma implementação bem-sucedida de proteção de dados" (MAYER-SCHÖNBERGER, 2001, p. 227). Todavia, para que cidadãos pudessem usufruir de serviços prestados pelo Estado, por exemplo, ainda era necessário um fluxo de informação contínuo dos indivíduos para a administração pública. A mesma situação se verificava em ações como ter uma conta bancária, agendar uma viagem e votar. Optar por não fornecer dados traria custos insustentáveis ao indivíduo. Surge, então, uma questão: "alcançamos um nível ótimo de proteção de dados se garantirmos direitos de privacidade que, quando exercidos, essencialmente expulsarão o cidadão individual da sociedade?" (MAYER-SCHÖNBERGER, 2001, p. 229).

3.1.2.2 As gerações subsequentes e a Decisão dos Censos de 1983

Esse cenário levou à terceira geração identificada por Mayer-Schönberger, em que a liberdade individual de um cidadão de negar invasões aos seus dados pessoais transformou-se em um direito muito mais participativo de autodeterminação informacional. Nesse sentido, é destacada como fundamental a já mencionada decisão do Tribunal Constitucional Alemão sobre a Lei do Censo de 1983 (BIONI, 2019, cap. 3; MAYER-SCHÖNBERGER, 2001, p. 229). Como já referido anteriormente, a lei do censo alemã ordenava o recenseamento geral da população, com a obtenção de dados como moradia,

---

3, incluindo, além da proibição de tratamento de dados referentes à fé religiosa ou vida privada, a proibição do tratamento de dados sobre convicções filosóficas ou políticas, filiação partidária ou sindical e origem étnica. Foi incluído o número 4, que proíbe o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei. A proibição de atribuição de um número nacional único foi deslocada para o número 5, e acrescentou-se o número 6, que estabelece uma garantia de livre acesso às redes informáticas de uso público, além do já mencionado número 7, que expande a proteção para os dados presentes em ficheiros manuais.

profissão e local de trabalho, para fins estatísticos. O objetivo era "reunir dados sobre o estágio do crescimento populacional, a distribuição espacial da população no território federal, sua composição segundo características demográficas e sociais, assim como também sobre sua atividade econômica" (BVERFGE, 1983 *apud* MARTINS, 2005, p. 234). Contudo, a lei previa a possibilidade de comparação dos dados coletados com dados armazenados em registros públicos, e também a transmissão de dados tornados anônimos a repartições públicas federais para a finalidade genérica de "atividades administrativas" (BIONI, 2019, cap. 2; BVERFGE, 1983 *apud* MARTINS, 2005, p. 234).

Foram ajuizadas várias Reclamações Constitucionais em face da Lei do Censo de 1983, e o Tribunal Constitucional declarou a sua inconstitucionalidade parcial, popularizando o termo "autodeterminação informacional".[57] De acordo com a decisão do Tribunal, o § 9.º, I a III (referente à possibilidade de comparação dos dados levantados com os registros públicos e também à transmissão de dados tornados anônimos a repartições públicas federais) da Lei do Censo era incompatível com o artigo 2 I da Constituição da República da Alemanha (referente ao livre desenvolvimento da personalidade) c/c o artigo 1 I da Constituição (dignidade da pessoa humana) (BVERFGE, 1983 *apud* MARTINS, 2005, p. 235).

Assim, como parâmetro para a decisão, o Tribunal utilizou o direito geral de personalidade, que estava previsto no artigo 2 I GG c/c o artigo 1 I GG. (BIONI, 2019, cap. 2; BVERFGE, 1983 *apud* MARTINS, 2005, p. 234). Considera-se que o livre desenvolvimento da personalidade pressupõe "a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais" (BVERFGE, 1983 *apud* MARTINS, 2005, p. 238), e esse direito fundamental "garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais" (BVERFGE, 1983 *apud* MARTINS, 2005, p. 238). Dessa forma, o Tribunal Constitucional Alemão delineia o direito à autodeterminação informacional valendo-se do direito geral de personalidade (BIONI, 2019, cap. 2).

O Tribunal chama atenção para o fato de que, nesse contexto, não basta simplesmente levar em consideração o tipo de dado que será recolhido e tratado, uma vez

[57] É importante destacar que a decisão do Tribunal Constitucional não criou a expressão "autodeterminação informacional", que havia sido referida pela primeira vez na década de 70 do século XX, num parecer de caráter dogmático elaborado a pedido do Ministério do Interior alemão (PINHEIRO, 2015, p. 464).

que, dependendo de sua utilidade e possibilidade de uso, “um dado em si insignificante pode adquirir um novo valor”. Assim, a Corte afirmou que o fato de um dado concernir ou não questões íntimas não determinará, por si só, se este é um dado sensível ou não, tendo em vista que somente a clareza quanto à finalidade para a qual os dados são solicitados e as possibilidades de uso e ligação desses dados com outros poderá indicar se a restrição ao direito de autodeterminação informacional é aceitável (BVERFGE, 1983 *apud* MARTINS, 2005, p. 239).

A decisão também determina uma distinção entre dados referentes à pessoa, que são manipulados de forma individualizada e não anônima e aqueles destinados a fins estatísticos. Ressaltou que o levantamento obrigatório de dados relativos à pessoa não é admissível de forma irrestrita, especialmente quando tais dados devem ser usados para a função administrativa. Também afirmou que, quando há obrigação de fornecer dados pessoais, o legislador deve definir a finalidade de uso de forma precisa, e os dados devem ser adequados e necessários para essa finalidade. Dessa forma, é vedado o armazenamento de dados reunidos, não anônimos, para fins indeterminados ou ainda indetermináveis (BVERFGE, 1983 *apud* MARTINS, 2005, p. 240).

No caso de levantamento e manipulação de dados para fins estatísticos, o Tribunal Constitucional reconheceu que não se pode exigir uma ligação estrita e concreta de dados à finalidade, pois, segundo a essência da estatística, os dados devem ser utilizados para as tarefas mais diversas, não determináveis de antemão. As proibições de transmissão e uso de dados preparados estatisticamente também seriam contrárias à sua finalidade. Sendo assim, o Tribunal menciona a necessidade de criar limites compensatórios, “condições de manipulação claramente definidas que garantam que o indivíduo não se torne um simples objeto de informação, no contexto de um levantamento e manipulação automáticos dos dados relativos à sua pessoa” (BVERFGE, 1983 *apud* MARTINS, 2005, p. 241).

A decisão também ressalta que mesmo no levantamento de dados individuais para fins estatísticos, o legislador deve examinar a possibilidade de que tais dados possam expor o cidadão a alguma forma de discriminação social (como, por exemplo, vício em drogas, antecedentes criminais, insanidade mental) (BVERFGE, 1983 *apud* MARTINS, 2005, p. 242). Devem ser garantidos, portanto, o anonimato dos dados e a sua manifestação em sigilo, uma vez que, apenas quando estão presentes tais condições é que se pode esperar que as informações exigidas coercitivamente do cidadão possam ser fornecidas por ele. Em

outras palavras, só se pode garantir a veracidade dos dados coletados se tiver sido criada no cidadão a confiança necessária na proteção de seus dados coletados (BVERFGE, 1983 *apud* MARTINS, 2005, p. 243).

Conforme ressalta Alexandre Sousa Pinheiro, a Decisão dos Censos terá, reflexamente, influência determinante na futura dogmática da proteção de dados, na medida em que estabelece uma separação radical entre dados pessoais e outros instrumentos jurídicos de defesa da pessoalidade. Assim, a proteção de dados tem autonomia em relação à privacidade, tal como é entendida no espaço europeu (PINHEIRO, 2015, p. 487). O Tribunal Constitucional não recorre ao discurso do que é público e o que é privado para abordar o direito à autodeterminação informacional, e a sua fundamentação acaba por transpor essa dicotomia[58] (BIONI, 2019, cap. 2).

A terceira geração de normas é caracterizada pelo enfoque no princípio da autodeterminação informacional, e na crença de que o indivíduo exerceria esse direito. Mayer-Schönberger identifica uma série de reformas legislativas nesse contexto, como os estatutos alemães de proteção de dados após a decisão do Tribunal Constitucional, a alteração geral da lei federal de proteção de dados alemã em 1990, a alteração da lei de proteção de dados austríaca em 1986, a extensão de direitos de participação individuais na lei norueguesa, a adoção de uma previsão constitucional de autodeterminação informacional nos Países Baixos, e algumas partes da lei finlandesa de registro de pessoas. Nessa geração, havia maior compreensão de que, numa sociedade cada vez mais interconectada, não era possível exigir do indivíduo que optasse pela não participação. Assim, os direitos de participação individuais foram estendidos. (MAYER-SCHÖNBERGER, 2001, p. 231).

Mesmo com as mudanças observadas na terceira geração de legislação sobre proteção de dados, "as pessoas não estavam dispostas a pagar o alto custo monetário e social necessário para exercer rigorosamente seu direito de autodeterminação informacional". Além de temerem o alto risco financeiro de possíveis ações judiciais, muitas pessoas, inadvertidamente, renunciavam ao seu direito à autodeterminação

[58] Tal constatação é ainda mais nítida quando se considera uma decisão precedente do Tribunal Constitucional, conhecida como Decisão do Microcenso. Naquela ocasião, o Tribunal declarou constitucional uma norma da lei do microcenso de 1957, que previa multa de até dez mil marcos para os entrevistados que se recusassem a responder aos quesitos "viagens de férias" e "viagens de repouso". Na fundamentação, o Tribunal considerou que os dados levantados não atingiam a esfera íntima intocável do indivíduo (BIONI, 2019, cap. 2; BVERFGE, 1969 *apud* MARTINS, 2005, p. 215).

informacional como parte de um contrato, em que davam o seu consentimento para o tratamento de dados. (MAYER-SCHÖNBERGER, 2001, p. 232).

Desse modo, as leis da quarta geração surgem a partir da consciência dos legisladores do baixo poder de barganha do indivíduo ao exercer o seu direito. Essas normas buscaram fortalecer a posição do indivíduo frente às instituições mais poderosas, o que demonstra que ainda há uma crença na possibilidade de exercício da autodeterminação informacional do indivíduo se um equilíbrio for estabelecido. Porém, outra estratégia adotada pelos legisladores foi, paradoxalmente, a de retirar parte da liberdade de participação dadas ao indivíduo na segunda e terceira gerações. Isso decorre da compreensão de que alguns tipos de informação devem ser absolutamente protegidos e não podem ser negociados individualmente (MAYER-SCHÖNBERGER, 2001, p. 232).

A Diretiva UE 95/46/CE é um exemplo dessa abordagem, ao determinar a proibição do tratamento de dados sensíveis, definidos na diretiva como dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como relativos à saúde e à vida sexual, em seu artigo 8.º, n.º 1. (MAYER-SCHÖNBERGER, 2001, p. 232). A mesma proibição se observa no artigo 9.º, n.º 1 do Regulamento UE 2016/679, que inclui, ainda, dados genéticos, dados biométricos, e dados sobre a orientação sexual de uma pessoa.

Além disso, a quarta geração também é caracterizada pela disseminação do modelo de autoridades independentes para a atuação da lei, e o surgimento de normas específicas para determinados setores de tratamento de dados (DONEDA, 2019, cap. 2; MAYER-SCHÖNBERGER, 2001, p. 233). Os legisladores tentam resgatar a imagem de um direito à autodeterminação informacional, que continua, segundo Mayer-Schönberger, a ser o coração de todo o modelo da proteção de dados.

A Diretiva UE 95/46/CE foi descrita por Mayer-Schönberger como um documento que reflete a evolução geracional. Os direitos de participação individuais tinham posição de destaque na diretiva, e o consentimento era uma das bases legais que autorizavam o tratamento de dados (artigo 7.º, alínea a)), bem como a transmissão de dados pessoais a Estados que não garantem regimes de proteção de dados considerados adequados (artigos 25.º e 26.º, n.º 1, alínea a)). O consentimento também devia ser informado e explícito para o caso de dados sensíveis (artigo 8.º, n.º 2, alínea a)). Havia, ainda, o direito do cidadão de proibir o tratamento de dados para o propósito de marketing

direto (artigo 14.º, alínea b)), e a determinação, nos artigos 22.º e 23.º, de compensação monetária pelas violações de direitos. Ao contrário das normas de primeira geração, em que se buscava dominar a tecnologia, a diretiva europeia abrangia não somente tratamento de dados em computador, mas também de forma manual (MAYER-SCHÖNBERGER, 2001, p. 235).

Nesse ponto, importa destacar a observação de Bioni a respeito da evolução geracional das normas sobre proteção de dados pessoais. Bioni afirma que a quarta geração, trazendo disseminação de autoridades independentes e proposições que não deixavam a cargo do indivíduo a decisão sobre o tratamento de certos tipos de dados, relativiza a centralidade do consentimento. Ainda assim, o consentimento não perdeu seu protagonismo, e, ao longo desse processo evolutivo, passou a ser adjetivado, como livre, informado, inequívoco, explícito e/ou específico. Identifica-se, assim, um processo em que "o consentimento emerge, é questionado, e se reafirma como sendo o seu vetor central" (BIONI, 2019, cap. 3).

De acordo com Bioni, o direito comunitário europeu "exprime bem a travessia do consentimento no percurso geracional das leis de proteção de dados pessoais, cuja linha evolutiva permanece em curso até hoje" (2019, cap. 3). Bioni começa por observar a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal do Conselho da Europa (Convenção 108), considerada como o ponto de referência inicial do modelo europeu de proteção de dados pessoais (DONEDA, 2019, cap. 3). A Convenção 108 correlacionou a proteção de dados pessoais ao livre fluxo informacional, reconhecendo ser necessário conciliar os valores fundamentais do respeito pela vida privada e da livre circulação de informação entre os povos em seu preâmbulo (BIONI, 2019, cap. 3). Foi influenciada pelas *guidelines* da OCDE de 1980, que estabeleciam uma série de princípios, tidos como *Fair Information Practice Principless,* e incorporou-os em seu texto[59].

A Diretiva 45/96/CE, nesse sentido, também manteve a noção de que é preciso conciliar a proteção de dados pessoais e o desenvolvimento econômico. No considerando (3), por exemplo, mencionou-se a necessidade de assegurar que os dados pessoais possam

[59] As *guidelines* previam os seguintes princípios: a) Limitação da Coleta; b) Qualidade dos Dados; c) Especificação dos Propósitos; d) Limitação de Uso; e) Mecanismos de Segurança; f) Abertura; g) Participação Individual; h) Responsabilidade (OCDE, 1980).

circular livremente de um Estado-membro para outro, mas, igualmente, que sejam protegidos os direitos fundamentais das pessoas. O considerando (5), ainda, reconhecia que a integração econômica e social provocaria um aumento sensível nos fluxos transfronteiriços de dados pessoais (BIONI, 2019, cap. 3).

A Diretiva 95/46/CE adotou os princípios consagrados na Convenção 108 "como sua espinha dorsal", traduzindo-os em normas mais específicas. É possível dizer que, na diretiva, a autodeterminação do indivíduo "é o que parametriza a (i)licitude do tratamento de dados pessoais" (BIONI, 2019, cap. 3). A diretiva adjetivou o consentimento como forma de operacionalizá-lo, colocando-o como livre, específico e informado (artigo 2.º alínea h)), inequívoco (artigo 7.º, alínea a)), e explícito (artigo 8.º, número 2, alínea a)). Essa, segundo Bioni, é uma característica marcante do progresso geracional das leis de proteção de dados, pois tenta responder ao problema de um possível "controle ilusório e pouco efetivo" de dados pessoais por parte de seu titular (BIONI, 2019, cap. 3).

Outra característica que merece destaque é o fato de que a diretiva europeia se centrou tanto no titular de dados pessoais como no responsável pelo tratamento, dispondo sobre direitos dos titulares e impondo, simetricamente, deveres aos responsáveis. A minimização dos dados coletados, por exemplo, acarretava um dever de cooperação por parte do responsável na diretiva. Este, segundo Bioni, é um aspecto que situa a Diretiva 95/46/CE na quarta geração, pois, para tentar garantir ao titular o controle das suas próprias informações, "expande seu espectro para todos os sujeitos inseridos ao longo da cadeia do fluxo informacional", não focando apenas no papel do titular, como em gerações anteriores (BIONI, 2019, cap. 3).

A Diretiva 2002/58/CE, continuando essa tendência, reafirma a necessidade de um consentimento livre, específico e informado[60], e exercido preferencialmente de forma prévia à coleta e ao tratamento. Contém, ainda, disposições mais específicas sobre como deve ser prestado o consentimento em alguns casos, como nos testemunhos de conexão ou

[60] (17) Para efeitos da presente directiva, o consentimento por parte do utilizador ou assinante, independentemente de este ser uma pessoa singular ou colectiva, deve ter a mesma acepção que o consentimento da pessoa a quem os dados dizem respeito conforme definido e especificado na Directiva 95/46/CE. O consentimento do utilizador pode ser dado por qualquer forma adequada que permita obter uma indicação comunicada de livre vontade, específica e informada sobre os seus desejos, incluindo por via informática ao visitar um sítio na Internet.

cookies, por exemplo[61] (BIONI, 2019, cap. 3). A mesma tendência é observada no Regulamento UE 2016/679, ao elencar uma série de qualificadores para o consentimento, deixando claro que são cumulativos pelo uso da partícula "e". Estabelece-se, também, como o consentimento deverá ser prestado: por meio de uma afirmação ou de um ato positivo inequívoco.[62] Há, ainda, o artigo 7.º, que estipula quais as condições aplicáveis ao consentimento, determinando, por exemplo, que se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples (BIONI, 2019, cap. 3).

3.1.2.3 Considerações sobre a proteção de dados no contexto europeu

A breve leitura da evolução geracional das normas europeias sobre a proteção de dados pessoais, apesar de reducionista, pode fornecer indícios das principais questões que devem ser consideradas quando se tem em mente o quadro europeu sobre proteção de dados pessoais. Se inicialmente a legislação europeia tinha como foco o próprio funcionamento do computador e tentava regular a própria tecnologia, em resposta ao crescimento do processamento de dados, em um segundo momento, passou a ter enfoque maior nos direitos individuais de privacidade do cidadão, que começava a ter maior poder de decisão sobre o tratamento de seus dados, principalmente porque o consentimento já era, em alguns casos, condição necessária para o tratamento. Posteriormente, passou-se a tutelar não só o direito de afastar intrusões alheias nos dados pessoais do titular, mas um

[61] (25) [...] A informação e o direito a recusar poderão ser propostos uma vez em relação aos diversos dispositivos a instalar no equipamento terminal do utente durante a mesma ligação e deverá também contemplar quaisquer outras futuras utilizações do dispositivo durante posteriores ligações. As modalidades para prestar as informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão conviviais quanto possível. O acesso ao conteúdo de um sítio *web* específico pode ainda depender da aceitação, com conhecimento de causa, de um testemunho de conexão ("cookie") ou dispositivo análogo, caso seja utilizado para um fim legítimo.

[62] Artigo 4.º
Definições
Para efeitos do presente regulamento, entende-se por:
[...]
11) «Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

direito mais participativo de autodeterminação informacional. Finalmente, a legislação europeia evoluiu para um momento em que, apercebendo-se do baixo poder de barganha do titular para o exercício de seu direito, busca estabelecer um equilíbrio entre as posições de barganha, fortalecendo a posição do indivíduo diante das instituições que coletam dados, e, ao mesmo tempo, removendo parte das liberdades conferidas ao indivíduo nas gerações de normas anteriores, submetendo-o a proteção legal obrigatória em alguns casos (BIONI, 2019, cap. 3; MAYER-SCHÖNBERGER, 2001, p. 235).

Destaca-se a Decisão dos Censos de 1983 como fundamental na evolução do tema, pois marca o debate futuro sobre a proteção de dados ao abordar o conceito de autodeterminação informacional (PINHEIRO, 2015, p. 479). Tida como um direito do indivíduo de decidir quando e dentro de quais limites seus dados poderão ser revelados, a autodeterminação informacional exerce grande influência até hoje sobre a proteção de dados nos países do sistema romano-germânico (DONEDA, 2019, cap. 2), e se mantém relevante no contexto da Internet e das redes sociais (FISCHER-HÜBNER *et al.*, 2013). É preciso notar, contudo, que a autodeterminação informacional não se resume à possibilidade de dar ou não o consentimento. A decisão reconhece a necessidade de se observar o princípio da finalidade, principalmente nas situações em que o consentimento não é requerido, como forma de evitar que o indivíduo seja reduzido a um mero "objeto informacional"[63] (BIONI, 2019, cap. 2; DONEDA, 2019, cap. 2; BVERFGE, 1983 *apud* MARTINS, 2005, p. 241).

A evolução geracional das normas europeias de proteção de dados reflete tanto o surgimento do consentimento como uma condição para o tratamento de dados, como também o questionamento sobre eficácia de uma legislação focada no poder de escolha dos indivíduos. Com o progresso geracional, a legislação passou a relativizar a centralidade do consentimento, retirando do âmbito de escolha do indivíduo a decisão sobre tratamento de certos tipos de dados como, por exemplo, os dados sensíveis. Ao mesmo tempo, também passou a atribuir qualificadores ao consentimento, na tentativa de garantir que ele reflita uma decisão genuína do titular de dados pessoais. O consentimento, portanto, apesar de questionado e relativizado, não chega a perder a sua centralidade. A seguir, abordaremos o

[63] "[...]a falta de vinculação a um propósito definido, reconhecível e compreensível a qualquer momento, e o uso multifuncional dos dados, fortalecem as tendências que devem ser identificadas e restringidas pelas leis de proteção aos dados, que concretizam o direito garantido constitucionalmente à autodeterminação sobre a informação" (BVERFGE, 1983 *apud* MARTINS, 2005, p. 242).

tema do consentimento no contexto do Regulamento Geral de Proteção de Dados Pessoais da União Europeia (BIONI, 2019, cap. 3).

3.2 O consentimento como forma de legitimação do tratamento de dados no Regulamento (UE) 2016/679

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho estabelece, em seu artigo 6.º, seis condições para a licitude do tratamento de dados pessoais. São elas: a) o consentimento do titular dos dados para tratamento de seus dados pessoais para uma ou mais finalidades específicas; b) se o tratamento for necessário para a execução de um contrato no qual o titular é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) se o tratamento for necessário para cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) se o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) se o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Assim, existem cinco bases legais que autorizam o tratamento de dados para além do consentimento. Contudo, o consentimento ainda é considerado por alguns autores como a base legal mais importante. As outras situações previstas no artigo 6.º se referem a cenários específicos que estão, na maior parte dos casos, fora da esfera de controle do titular. Observa-se, ainda, que a maioria das atividades ordinárias e diárias de tratamento de dados usam o consentimento como base legal. (HERT e PAPAKONSTANTINOU, 2016, p. 187). Como visto no tópico anterior, ao longo do progresso geracional das leis de proteção de dados pessoais, "o consentimento emerge, é questionado e se reafirma como seu vetor central" (BIONI, 2019, cap. 3).

Na linha da Diretiva 95/46/CE e da Diretiva 2002/58/CE, o RGPD também teve uma preocupação nuclear em torno do consentimento, mantendo o seu processo de adjetivação (BIONI, 2019, cap. 3). Conforme elencado no artigo 4.º, n.º 11 do

Regulamento, o consentimento deve ser uma manifestação de vontade livre, específica, informada e inequívoca,[64] pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que seus dados pessoais sejam objeto de tratamento. Conforme afirmado nas Diretrizes do Comitê Europeu para a Proteção de Dados (CEPD) sobre consentimento, o termo "livre" implica que o titular possa fazer uma escolha real e tenha um controle real sobre os dados. Se o titular se sente compelido a dar seu consentimento para evitar consequências negativas, tal consentimento não será considerado válido. Da mesma forma, não será válido o consentimento se o titular não tiver possibilidade de recusá-lo ou retirá-lo sem ter prejuízos (2020a, p. 7). Não existe, portanto, a figura do consentimento obrigatório (PINHEIRO, 2018, p. 167).

Tal observação é relevante quando se pensa, por exemplo, em serviços que estipulam contratualmente a obrigatoriedade de concordar com a utilização de seus dados para além do necessário. Um exemplo citado pelo CEPD é o caso de um aplicativo de edição de fotos que requer que seus usuários mantenham sua localização de GPS ativada para utilizarem o *app*, e que empregará os dados coletados para fins de publicidade direcionada. Nem a localização nem a publicidade direcionada são necessários para o serviço de edição de fotografias e, como os usuários não conseguem ter acesso aos serviços sem consentir para tais finalidades, o consentimento não pode ser considerado livre (EUROPEAN DATA PROTECTION BOARD, 2020a, p. 8).

O Regulamento também prevê, no considerando (43), que o consentimento não será considerado válido caso haja um desequilíbrio manifesto entre o titular dos dados e o responsável pelo tratamento, nomeadamente quando o responsável for uma autoridade pública. Nesse cenário, na maioria dos casos, o titular não terá alternativas reais a aceitar o tratamento nos termos estipulados pelo responsável. Sendo assim, considera-se mais apropriado que o tratamento seja fundado em outras bases legais. Como ressaltado pelo CEPD, outro contexto que normalmente pressupõe desequilíbrios de poder é o das relações empregatícias, já que, dada a dependência da relação entre empregado e empregador, é pouco provável que o empregado tenha possibilidade de responder de maneira livre a uma

[64] Como se verá adiante, optamos por utilizar a palavra "inequívoca" como tradução do termo inglês "*unambiguous*", em vez do termo "explícito", adotado na versão em português do Regulamento.

solicitação de seu empregador para tratamento de seus dados pessoais, sem que se sinta pressionado a aceitá-la[65] (EUROPEAN DATA PROTECTION BOARD, 2020a, p. 9).

O artigo 7.º, n.º 4, aprofunda esse ponto importante sobre o que deve ser considerado um consentimento dado livremente. Prevê que, ao avaliar se o consentimento é ou não dado de forma livre, deve-se verificar se a execução de um contrato ou a prestação de um serviço está subordinada ao consentimento para um tratamento de dados pessoais que não é necessário para a execução do contrato. Busca-se assegurar que o propósito do tratamento de dados pessoais não é disfarçado ou agrupado à provisão de um serviço para o qual esses dados pessoais não são necessários. Nesse aspecto, Fausto Caggia nota que o Regulamento, em comparação às normas precedentes, leva o juízo sobre a existência de liberdade do consentimento de um nível abstrato de avaliação para um nível de verificação que observe de maneira mais penetrante a estrutura da relação entre o titular dos dados e o responsável pelo tratamento (2019, p. 264). Tal regra reflete uma orientação já difusa no contexto europeu, que já era manifestada nas decisões de autoridades administrativas de proteção de dados (CAGGIA, 2019, p. 265; ZENO-ZENCOVICH e RESTA, 2018, p. 428)[66].

Outra característica do consentimento livre no RGPD é a granularidade. De acordo com o considerando (43), presume-se que o consentimento não é dado de livre vontade se não for possível dá-lo separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico. O considerando (32) também aborda a ideia de granularidade, estabelecendo que o consentimento deverá

[65] O Comitê Europeu para a Proteção de Dados ressalta que existem situações em que é possível aceitar o tratamento de dados com base no consentimento, ainda que o responsável seja uma autoridade pública. Dá exemplos de casos em que o cidadão poderá recusar um tipo de tratamento sem que isso acarrete a perda de acesso a algum serviço essencial. Por exemplo, o caso hipotético de um município que realizará um serviço de manutenção de estradas e oferece aos moradores a possibilidade de se inscrever em uma lista de e-mails para receber atualizações sobre o progresso das obras e os possíveis atrasos. A municipalidade deixa claro que não existe a obrigação de participar, e solicita o consentimento para acesso aos endereços de e-mail dos cidadãos exclusivamente para esse propósito. Sendo assim, os moradores não perderão a possibilidade de receber qualquer serviço essencial nem o exercício de algum direito, podendo dar ou não seu consentimento livremente. Da mesma forma, o CEPD chama atenção para o fato de que, em situações excepcionais, empregadores também podem adotar o consentimento como base legal para o tratamento de dados de seus empregados, desde que não haja quaisquer consequências adversas se o empregado der ou não seu consentimento (2020a, p. 9).

[66] Um exemplo nesse sentido, mencionado por Zeno-Zencovich e Resta, são as orientações da autoridade italiana de proteção de dados de 4 de julho de 2013, que exemplificam que não é livre o consentimento prestado quando uma sociedade condiciona o registro ao seu *site* por parte dos usuários e o uso de seus serviços ao fornecimento de consentimento para tratamento de dados para fins promocionais (GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 2013).

abranger todas as atividades de tratamento realizadas com a mesma finalidade, e que, nos casos em que o tratamento sirva a fins múltiplos, deverá ser dado consentimento para todos eles. A granularidade está intimamente relacionada à especificidade do consentimento (EUROPEAN DATA PROTECTION BOARD, 2020a, p. 12; PINHEIRO, 2018, p. 168)(EUROPEAN DATA PROTECTION BOARD, 2020, p. 12; PINHEIRO, 2018, p. 168). É uma forma de tentar atribuir ao titular uma autonomia genuína sobre o fluxo de suas informações pessoais, abandonando a lógica do "tudo ou nada" (BIONI, 2019, cap. 4), e, aliada ao princípio da limitação das finalidades, evita a "*function creep*", ou seja, evita que o responsável pelo tratamento, após recolher o consentimento para uma finalidade, altere seus termos de uso para ampliar a funcionalidade do tratamento (GIOVANNANGELI, 2019, p. 130).

Finalmente, deve-se atentar para a previsão do considerando (42), que determina que o consentimento não será considerado livre se não houver possiblidade de o titular de dados pessoais recusá-lo ou retirá-lo sem ser prejudicado. O responsável pelo tratamento deverá comprovar que a retirada do consentimento não acarreta maiores custos ou desvantagens, como piora na performance do serviço. O RGDP não impede que sejam estabelecidos incentivos, mas o responsável deverá demonstrar que o consentimento foi livre nessas circunstâncias (EUROPEAN DATA PROTECTION BOARD, 2020a, p. 13).

O segundo adjetivo atribuído ao consentimento no artigo 4.º, n.º 11, do Regulamento é "específico". O artigo 6.º, n.º 1, alínea a), ressalta que o consentimento do titular deve ser dado "para uma ou mais finalidades específicas". De acordo com as orientações do CEPD, essa qualificação busca assegurar ao titular um grau de controle sobre seus dados pessoais e de transparência. Guarda relação com a exigência de que o consentimento seja informado e, como já mencionado, deve ser interpretado de acordo com a exigência de granularidade. Cumpre lembrar que, conforme determinado no artigo 5.º, n.º 1, alínea b), do Regulamento, a obtenção do consentimento deve ser sempre precedida pela definição de finalidades determinadas, explícitas e legítimas para o tratamento pretendido, o que também funciona como uma salvaguarda contra a já mencionada "*function creep*" O consentimento pode abranger uma ou mais operações, contanto que sirvam à mesma finalidade, como destacado no considerando (32). (EUROPEAN DATA PROTECTION BOARD, 2020a, p. 14).

O consentimento deve ser granular não apenas para cumprir o requisito "livre", mas também para cumprir o requisito "específico". Se o responsável pelo tratamento deseja obter o consentimento do titular para várias finalidades, deverá fornecer a opção de consentir ("*opt in*") para cada uma delas. O responsável também deverá fornecer informações específicas para cada pedido de consentimento separadamente, o que se relaciona com o terceiro adjetivo empregado na definição de consentimento no RGPD: "informado". Tal requisito está em consonância com o princípio da transparência, previsto no artigo 5.º, n.º 1, alínea a), do Regulamento. Se o responsável não provê informações acessíveis, o consentimento não será uma base legal válida para o tratamento, por ser tido como ilusório (2020a, p. 15).

De acordo com o Comitê Europeu para a Proteção de Dados, para que se considere o consentimento informado, é necessário que o titular seja comunicado sobre alguns elementos cruciais para sua decisão, que são: i. a identidade do responsável pelo tratamento; ii. a finalidade de cada operação de tratamento para a qual o consentimento é requerido; iii. qual tipo de dado será coletado e usado; iv. a existência do direito de retirar o consentimento; v. informações sobre o uso de dados para decisões individuais automatizadas, para o caso previsto no artigo 22.º, n.º 2, alínea c), e vi. os possíveis riscos da transferência de dados para países terceiros ou organizações internacionais, devido à ausência de uma decisão de adequação nos termos do artigo 45.º, n.º 3, e de garantias adequadas nos termos do artigo 46.º (2020a, p. 15).

Não há uma exigência quanto à forma utilizada para informar o titular dos dados no RGPD, o que significa que a informação pode ser prestada de vários modos, como declarações orais ou escritas, mensagens de áudio ou vídeo. Contudo, vários requisitos para o consentimento informado estão previstos no Regulamento. A informação deve ser facilmente compreensível para o cidadão médio, e não somente para advogados. O responsável deve identificar qual é o público-alvo que fornecerá os dados para tratamento, para que possa adequar a informação a esse público. Se o público for de menores, por exemplo, o responsável deve se certificar de que a informação é compreensível para menores (2020a, p. 16).

Conforme disposto no artigo 7.º, n.º 2, caso o consentimento seja prestado no contexto de uma declaração escrita que também diga respeito a outros assuntos, o pedido deverá ser claramente distinguível desses outros assuntos, "de modo inteligível e de fácil

acesso numa linguagem clara e simples". O CEPD ressalta que, se um contrato em papel inclui vários aspectos que não têm relação com o consentimento para o tratamento de dados, a questão do consentimento deve ser tratada de maneira que claramente se sobressai, ou em um documento separado. Já no caso de contratos eletrônicos, o pedido de consentimento deve ser separado e distinto, e não pode ser feito simplesmente em um parágrafo dentro dos termos e condições de uso, conforme considerando (32) (EUROPEAN DATA PROTECTION BOARD 2020a, p. 17).

Finalmente, o artigo 4.º, n.º 11, também estipula que o consentimento deve ser uma manifestação de vontade explícita. Cabe aqui, porém, um esclarecimento quanto ao emprego desse termo. Como aponta Alexandre Sousa Pinheiro, o termo "não tem natureza generalizada no RGPD, projetando-se nos artigos 9.º, 22.º e 49.º, atendendo à sensibilidade quer dos dados pessoais, quer dos tratamentos em causa" (2018, p. 169). É possível observar que, apesar de a proposta de regulamento definir, em seu artigo 4.º, n.º 8, o consentimento como uma manifestação de vontade "livre, específica, informada e explícita",[67] o texto foi alterado após a intervenção do Parlamento e do Conselho, e o termo foi removido na versão final, de modo que o consentimento passa a ser descrito como uma "manifestação de vontade, livre, específica, informada e inequívoca" (em inglês: "*any freely given, specific, informed and unambiguous indication of the data subject's wishes*").[68] Duarte também chamou atenção para o fato de que a tradução portuguesa do artigo 4.º, n.º 11, do RGPD não refletiu a sutileza do significado da palavra inglesa "*unambiguous"*, adotando o adjetivo "explícito", que é muito mais amplo, em vez de empregar o termo "inequívoco" (2018, p. 247).

Sendo assim, parece-nos que o consentimento não deve ser explícito como regra geral, mas em situações específicas. Todavia, o Regulamento requer que se configure uma manifestação de vontade inequívoca, e "mediante declaração ou ato positivo inequívoco", exigências que representam adições importantes em relação aos termos da Diretiva 95/46/CE,[69] e que refletem entendimentos criados a partir de experiências recorrentes que

---

[67] Na versão em inglês: "(8) *'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed*".

[68] Por exemplo, em italiano, utiliza-se o termo "*inequivocabile*", e em francês, o termo "*univoque*", não havendo referência à natureza explícita do consentimento no artigo 4.º.

[69] Artigo 2.º
Definições

passaram e ser evitadas, como as caixas de diálogo previamente selecionadas ("*pre-ticked opt in boxes"*), ou o consentimento implícito no estabelecimento de uma relação contratual (HERT e PAPAKONSTANTINOU, 2016, p. 187).

O Comitê Europeu para a Proteção de Dados esclarece que considerar que o consentimento deve ser dado mediante um "ato positivo inequívoco" significa que o titular dos dados deve realizar uma ação deliberada para consentir ao tratamento. O considerando (32) aborda essa exigência de forma mais detalhada, exemplificando que o consentimento pode ser dado "mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral", e "validando uma opção ao visitar um sítio *web* na Internet". Contudo, o considerando ressalta que, como já afirmado, o silêncio, as opções pré-validadas ou a omissão" não constituem consentimento válido. Os responsáveis pelo tratamento têm certa liberdade para desenvolver um fluxo de consentimento compatível com o seu negócio. Isso significa que movimentos físicos podem ser tidos como consentimento, desde que os mecanismos sejam desenhados de modo claro para os titulares. Assim, passar o dedo por uma barra na tela, acenar em frente a uma câmera "*smart*", girar um *smartphone* em sentido horário, por exemplo, podem ser opções válidas para indicar o consentimento, desde que sejam fornecidas informações claras, e que esteja claro que aquele movimento corresponde à concordância com aquela requisição específica (2020, p. 19).

O consentimento também deve sempre ser obtido anteriormente ao tratamento de dados. Apesar de não haver previsão literal quanto a isso no artigo 4.º, n.º 11, o CEPD chama atenção para o fato de que o artigo 6.º, n.º 1, alínea a), utiliza as palavras "tiver dado o seu consentimento", o que corrobora com essa interpretação. Além disso, a ideia de consentimento prévio é uma decorrência lógica do próprio artigo 6.º e do considerando (40), que determina que "para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo [...]". A princípio, pode ser suficiente requerer o consentimento do titular apenas uma vez. Contudo, o pedido deve ser renovado se a finalidade do tratamento for modificada, ou se o responsável pretende tratar os dados para uma finalidade adicional (EUROPEAN DATA PROTECTION BOARD, 2020, p. 20).

[...]
h) «Consentimento da pessoa em causa», qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento.

3.3 Os limites do consentimento

O consentimento para o tratamento de dados é um tema frequentemente discutido, já que existem várias ressalvas quanto à sua eficácia. Deve-se ter em consideração, como salientado por Solove (2013, pp. 1883–1893), problemas cognitivos e problemas estruturais. A ideia de que o titular será capaz de controlar o uso e a disseminação dos próprios dados pressupõe uma pessoa informada e que atua com racionalidade, capaz de tomar uma decisão adequada sobre consentir ou não a um determinado tratamento. Porém, evidências demonstram que o poder de decisão da maioria das pessoas não funciona dessa maneira. Dentre os problemas cognitivos observa-se, em primeiro lugar, a dificuldade de informar corretamente o titular de dados, usuário de um serviço, para que possa prestar consentimento para o tratamento de seus dados de maneira adequada.

Solove chama atenção para o fato de que os termos de uso de aplicativos e *sites*, na maioria das vezes, sequer são lidos pelos usuários.[70] Uma das razões apontadas para a falta de engajamento dos usuários é o fato de que grande parte dos textos das políticas de privacidade são longos e de difícil compreensão (2013, p. 1885). Um estudo feito nos Estados Unidos em 2019, por exemplo, aplicou testes de legibilidade linguística aos contratos de adesão dos quinhentos *websites* mais populares dos Estados Unidos. Os resultados indicaram que os contratos de adesão são geralmente ilegíveis, e a pontuação obtida era semelhante à encontrada em artigos acadêmicos, que normalmente não são direcionados ao público geral. Um dos testes realizados concluiu que 99,6% dos contratos

[70] Solove menciona uma pesquisa de 2006, discutida por Nissenbaum (2010, p. 105), que revelou que apenas 20% dos entrevistados afirmaram ler as políticas de privacidade "na maioria das vezes" (TRUSTe, 2006). Também menciona o artigo *The Failure of Fair Information Practice Principles* (CATE, 2006, p. 362), que discute a falta de clareza quanto ao que deveria constituir uma política de privacidade adequada, indicando que as notificações de privacidade nos Estados Unidos se tornaram longas e complexas, resultando em informação que na maioria das vezes não é lida pelos cidadãos e não afeta o seu comportamento. Em 2013, um estudo conduzido em um laboratório de uma universidade pública em Israel, com equipamento para monitorar os movimentos dos olhos dos participantes, buscou averiguar se a apresentação da política de privacidade por predefinição ("*by default*") encoraja sua leitura, e como os usuários a leem. Os resultados indicaram que, quando a política de privacidade é apresentada aos usuários por predefinição, estes tendem a dedicar um tempo significativo à sua leitura. Porém, se os usuários têm a opção de aceitar os termos e condições sem antes ler a política de privacidade, geralmente evitam a leitura do documento, e, mesmo quando clicam em um link não obrigatório que redireciona para a política de privacidade, tendem a gastar menos tempo e esforço na leitura. Do grupo de participantes ao qual a política de privacidade não foi apresentada por predefinição, apenas 20,3% optaram por clicar o link para leitura do documento, e os demais 79,7% concordaram com os termos sem leitura prévia. (STEINFELD, 2016, p. 998).

dificilmente serão compreendidos pelos consumidores (BENOLIEL e BECHER, 2019, pp. 2277–2278).

Sobre propostas para notificações simplificadas ou mais viscerais (como os avisos sobre perigo de doenças e morte em embalagens de cigarros), Solove aponta uma outra dificuldade: tornar a informação mais simples e mais fácil de entender pode comprometer o objetivo de garantir que o usuário esteja totalmente informado sobre as consequências do fornecimento dos seus dados naquela situação. Explicar as possíveis consequências será uma tarefa complexa, se o que se pretende é expô-las de forma suficientemente detalhada para que sejam entendidas de maneira significativa. Outro problema comentado por Solove é a forma como estão dispostas as possíveis escolhas dos usuários. Em muitos casos, as opções de controle de dados são oferecidas de forma binária, mas a granularidade nas escolhas, na visão de Solove, também pode adicionar maior complexidade e aumentar os riscos de confusão (2013, p. 1885).

Para além do problema quanto à informação do usuário, há que se considerar que as decisões dos titulares de dados podem ser distorcidas em muitos casos. Mesmo se a maioria das pessoas lesse as políticas de privacidades de *sites* e aplicativos rotineiramente, não se pode dizer que as decisões quanto ao compartilhamento de seus dados ao utilizar esses serviços refletiriam um controle perfeito de seus dados. Isso se deve ao fato de que, na maioria dos casos, as pessoas não têm expertise suficiente para avaliar adequadamente as consequências de se concordar com certos tratamentos de dados. É comum que pessoas aceitem entregar seus dados em troca de benefícios muito pequenos. Existem inconsistências entre a forma como as pessoas valorizam a proteção de seus dados pessoais e suas atitudes diante do compartilhamento de suas informações e seus possíveis riscos (ACQUISTI, 2009, pp. 82–83; SOLOVE, 2013, p. 1887). O ser humano tem uma racionalidade limitada, que faz com que, frequentemente, o processo de decisão racional seja substituído por modelos mentais simplificados e heurística (ACQUISTI e GROSSKLAGS, 2008, p. 369).

Tais modelos de raciocínio simplificados também são adotados em decisões sobre proteção de dados pessoais. Por exemplo, Alessandro Acquisti e Jens Grossklags encontraram evidências de racionalidade limitada em uma pesquisa na qual uma parte dos entrevistados associou segurança à proteção dos dados pessoais, tratando-os como sinônimos. Alguns entrevistados manifestaram a crença de que, se uma transação

comercial for segura, ninguém poderá ver os dados referentes a ela. Contudo, a segurança de uma transação não implica a proteção de seus dados (2006, p. 26). Da mesma forma, existem indícios de que o termo "política de privacidade" ("*privacy policy*") gera confusão entre os consumidores: muitos acreditam que o simples fato de que um *site* tem uma política de privacidade significa que a informação inserida pelo usuário não será compartilhada com outros *websites* ou empresas (TUROW *et al.*, 2006, p. 9).

As preferências ajustadas pelos usuários em relação à proteção de seus dados pessoais não são desenvolvidas em abstrato, mas dentro de um contexto. A maneira como as possibilidades de escolha são elaboradas pode direcionar as decisões dos usuários. Estudos indicam, por exemplo, que as pessoas têm a tendência de revelar mais informações pessoais quando sentem que têm controle da situação, ainda que tal controle seja ilusório (BRANDIMARTE, ACQUISTI e LOEWENSTEIN, 2013, p. 345; SOLOVE, 2013, p. 1887). Solove resume os problemas cognitivos da seguinte forma: " (1) as pessoas não leem as políticas de privacidade; (2) se as leem, não as compreendem; (3) se as leem e compreendem, na maioria dos casos não têm o conhecimento necessário para fazer uma escolha informada; (4) se as leem, compreendem e fazem uma escolha informada, a escolha pode ter sido influenciada por várias dificuldades na tomada de decisão"[71] (SOLOVE, 2013, p. 1888, tradução nossa).

Além das limitações cognitivas do ser humano, há que se considerar os problemas estruturais que também colocam em dúvida a efetividade do consentimento em muitos casos. Solove aponta, em primeiro lugar, o problema da escala. Mesmo que uma pessoa consiga controlar de forma adequada o uso de seus dados por alguns atores, existem tantas entidades que coletam, usam e publicam dados pessoais, que o controle em relação a cada uma delas se torna impossível. Tendo em consideração a quantidade de *websites* e aplicativos de empresas utilizados por uma pessoa diariamente para diversos fins (compras, finanças, viagens, seguros etc.), é simplesmente inverossímil que ela consiga dedicar tempo e atenção a cada uma das políticas de privacidade. Uma pesquisa conduzida por Aleecia M. McDonald e Lorrie Faith Cranor concluiu que o usuário de Internet americano

[71] "(*1) people do not read privacy policies; (2) if people read them, they do not understand them; (3) if people read and understand them, they often lack enough background knowledge to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various decisionmaking difficulties*" (SOLOVE, 2013, p. 1888).

gastaria aproximadamente 201 horas por ano e o equivalente a US$3.534 só com a leitura de políticas de privacidade (2008, p. 565).

A agregação de dados também é um fator problemático. Como já visto, uma pessoa pode consentir em revelar partes de dados que individualmente são inofensivas, mas que, combinadas com outras partes de dados não sensíveis fornecidas pelo mesmo indivíduo em outras ocasiões, podem revelar dados sensíveis. Esse efeito de agregação torna praticamente impossível a gestão dos próprios dados. Prever como os pedaços de dados poderão ser combinados seria uma atividade extremamente complexa, e é muito difícil para o titular avaliar se a informação poderá, posteriormente, revelar dados que ele gostaria que não fossem tratados. Para que uma pessoa possa decidir racionalmente sobre compartilhamento dos seus dados, é preciso que ela compreenda toda a gama de possibilidades de prejuízos e vantagens daquele compartilhamento, para que faça uma análise de custo-benefício. Isso também se agrava pelo fato de que, muitas vezes, um dado que inicialmente não permite a identificação de uma pessoa pode se tornar identificável dependendo do contexto (SOLOVE, 2013, pp. 1890–1891).

Finalmente, há o problema de como as pessoas tendem a analisar os possíveis danos derivados de suas decisões. Em geral, as pessoas têm a tendência de optar por benefícios a curto prazo, mesmo quando há possibilidade de implicações negativas no futuro. O controle dos dados pessoais implica o gerenciamento dos dados a longo prazo, enquanto a maioria das decisões relacionadas ao tratamento está ligada a benefícios a curto prazo. Como o consentimento normalmente é dado no início, os usuários têm dificuldade em fazer a análise de custo/benefício antecipadamente. O modelo de gestão dos próprios dados (chamado por Solove de "*privacy self-management*"), por sua própria estrutura, impede o alcance de um controle significativo dos dados pessoais por parte dos titulares (SOLOVE, 2013, pp. 1891–1893).

Solove tenta apontar algumas saídas para esse problema. Segundo o autor, fortalecer ainda mais a autogestão dos dados ("*privacy self-management*") não é a resposta correta, mas tampouco se deve abandoná-la por completo, adotando-se uma legislação paternalista (2013, p. 1893). Tendo em vista que as pessoas, na maioria das vezes, não conseguem prestar um consentimento significativo no tratamento de seus dados, a alternativa mais óbvia seria regular certas escolhas quanto à proteção de dados através da lei. Contudo, "ironicamente, uma regulação paternalista pode limitar a liberdade de escolha

das pessoas em nome do aprimoramento de sua autonomia"[72] (2013, p. 1894, tradução nossa). Essa situação é chamada de "dilema do consentimento". Medidas paternalistas nem sempre serão as mais adequadas. Uma pessoa pode escolher revelar publicamente determinados dados sobre si com o intuito de compartilhar experiências e gerar conscientização a respeito de determinada situação, ainda que isso possa gerar alguns prejuízos a ela (Solove cita o exemplo de uma pessoa que sofreu de bulimia e decide compartilhar sua experiência com a doença para ajudar outros pacientes a superarem o problema). Da mesma forma, algumas pessoas querem a publicidade direcionada, e escolhem ter seus perfis traçados (2013, p. 1895).

De acordo com Solove, a mudança para um sistema de "opt-in" (em vez de "opt-out" ou seja, de caixas de diálogo pré-selecionadas) não necessariamente traz benefícios em termos de proteção de dados. Mencionando o exemplo da política de privacidade da Apple's ITunes Store, o autor ressalta que, ainda que notificações apareçam na tela do usuário, requerendo o consentimento prestado através de um ato inequívoco, não há muito poder de barganha por parte do consumidor: se o usuário quer baixar um aplicativo daquela loja, deverá concordar com aqueles termos (2013, p. 1898). Mesmo considerando as suas limitações, Solove acredita que não se deve abandonar a ideia de controle dos dados por parte do usuário. É preciso que as pessoas tenham garantido o seu direito de saber como seus dados são usados e de tomar decisões sobre esses usos (2013, pp. 1899–1900).

Esforços para aprimorar a gestão dos dados por parte do usuário através de educação do consumidor, de informativas mais salientes e mais escolhas são desejáveis e importantes. O processo de criação de notificações sobre a proteção de dados não só informa os usuários e aprimora o controle sobre os dados, mas também força mudanças internas nas próprias empresas que realizam o tratamento, promovendo autoconsciência sobre coleta e uso de dados. Para além disso, negar às pessoas a possibilidade de gerir os próprios dados significaria restringir sua liberdade (SOLOVE, 2013, p. 1900).

Diante das limitações observadas na solução do consentimento, sugere-se que este deve ser repensado. Requerer o consentimento com base em uma lógica binária (lógica do "take it or leave it") pode não fazer sentido, tendo em vista que o consentimento é algo complexo e matizado. Em seu artigo, Solove sugere medidas que combinem o

[72] "*Ironically, paternalistic regulation might limit people's freedom to choose in the name of enhancing their autonomy*" (SOLOVE, 2013, p. 1894).

consentimento e o paternalismo, como as formas de “paternalismo libertário”, que busca arquitetar as escolhas oferecidas à pessoa de modo a aprimorar, e, em alguns casos, influenciar a escolha individual e o bem estar social (ACQUISTI, 2009, p. 84; SOLOVE, 2013, p. 1901).

Essa forma de paternalismo não proíbe nem onera comportamentos, pois tende a preservar a liberdade de escolha pessoal. Acquisti dá um exemplo desse *soft paternalism* referindo-se ao caso de redes sociais que permitem que os usuários publiquem suas datas de nascimento, informação que pode levar a inferências de dados sensíveis. Uma abordagem fortemente paternalista proibiria a publicação de datas de nascimento. No entanto, os usuários podem ter razões legítimas para desejar publicar tais informações pessoais. O paternalismo libertário poderá, simplesmente, fornecer uma contextualização para auxiliar a decisão do usuário, como, por exemplo, representar visualmente quantos outros usuários poderão acessar a informação e o que poderão fazer com ela (ACQUISTI, 2009, p. 84).

Ao indicar possíveis saídas, Solove também afirma que a maioria das pessoas não tem interesse em gerir todo e qualquer aspecto sobre os próprios dados. Do mesmo modo como os consumidores não precisam se tornar especialistas em carros para conseguirem escolher modelos que respeitem os parâmetros de segurança, não deveria ser esperado que as pessoas se tornassem especialistas em proteção de dados para se assegurarem de que seus dados estarão protegidos. Uma solução para essa questão seria encontrar formas de universalizar as preferências de privacidade, para que as pessoas possam gerir globalmente os seus dados para várias entidades, sem ter que analisar as condições de cada uma delas. Pode ser difícil, porém, encontrar um conjunto de regras que faça sentido para todas as entidades (2013, p. 1901).

É preciso, ainda, que o tempo e o foco do consentimento sejam ajustados. Normalmente, tem-se o momento inicial, anterior à coleta dos dados, como o momento para recolha do consentimento. Contudo, ao longo do tratamento, o surgimento de novas formas de combinar e agregar dados, novas técnicas e tecnologias podem alterar os custos e os benefícios daquela atividade. Como já visto, é difícil prever as implicações de um tratamento de dados no momento inicial da coleta. Desse modo, Solove ressalta a necessidade de que algumas decisões quanto ao consentimento sejam tomadas quando se iniciam determinados usos de dados, e não somente em uma ocasião, anteriormente à

coleta. Também destaca a importância de se limitar o consentimento em alguns casos e de permitir sua revogação (2013, p. 1902).

É possível dizer que há uma crescente conscientização quanto às limitações que afetam as decisões dos titulares de dados pessoais. Como já visto, é possível identificar no RGPD tentativas de responder às limitações do consentimento, procurando facilitar uma escolha genuína por parte do titular. O regulamento não permite, por exemplo, a adoção de caixas pré-selecionadas ("*opt-in*") para fornecimento do consentimento, já que a mera aceitação de termos gerais não pode ser considerada como consentimento, e é necessário um ato positivo inequívoco que autorize o tratamento (EUROPEAN DATA PROTECTION BOARD, 2020a, pp. 18–19).

O RGPD também dispõe expressamente sobre a adoção dos conceitos de "*privacy by design*" e "*privacy by default*", conforme se depreende do considerando (78).[73] O princípio da "proteção desde a concepção", ou "*privacy by design*", envolve a ideia de que a proteção de dados pessoais deve orientar a concepção de produtos e serviços. Está previsto no artigo 25.º, n.º 1, do RGPD, que impõe ao responsável pelo tratamento a obrigação de implementar medidas técnicas e organizativas adequadas para aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento. Essas medidas técnicas e organizativas podem envolver várias situações, desde o uso de soluções técnicas avançadas ao treinamento de pessoal (EUROPEAN DATA PROTECTION BOARD, 2019a, p. 6).

As chamadas *Privacy Enhancing Technologies (PETs)* podem ser empregadas como forma de cumprir com os requisitos do RGPD para o princípio de "*privacy by design"* PET é um "termo guarda-chuva" para aludir a toda e qualquer tecnologia amigável e facilitadora da privacidade (BIONI, 2019, cap. 4). O Comitê Europeu de Proteção de

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

Dados, em suas Diretrizes sobre os referidos princípios, afirmou que PETs que representem o estado da arte podem ser empregadas com o intuito de cumprir o disposto no artigo 25.º, numa abordagem baseada em risco. Ressaltou, porém, que a adoção de PETs não necessariamente abarca todas as obrigações do artigo. (EUROPEAN DATA PROTECTION BOARD, 2019a, p. 30). Por sua vez, o princípio da proteção de dados por defeito, ou "*privacy by default*" se refere às escolhas feitas pelo responsável pelo tratamento para quaisquer configurações ou opções de processamento atribuídas a um software, computador, programa ou dispositivo. Tais configurações devem ser ajustadas para coletar e tratar apenas os dados necessários para alcanças as finalidades daquele tratamento (2019a, pp. 10–11). Tal princípio está previsto no artigo 25.º, n.º 2, do Regulamento.[74]

A própria ideia de granularidade do consentimento também é uma tentativa de superar algumas das suas limitações e garantir maior autodeterminação informacional. Ao determinar que o consentimento deve ser dado separadamente para cada uma das finalidades do tratamento, o Regulamento busca evitar uma lógica binária de "tudo ou nada" ("*take it or leave it*"). O Regulamento (UE) 2016/679 é considerado uma referência de legislação mais protetiva no que diz respeito aos dados pessoais, principalmente em comparação a legislações de países como os Estados Unidos, por exemplo. Isso se observa também nas condições estabelecidas para um consentimento válido (PEÑA e VARON, 2019, p. 25).

3.4 A Disseminação de imagens íntimas e o Regulamento (UE) 2016/679: tratamento ilícito de dados sensíveis

Em situações que comportam sérios riscos no que diz respeito à proteção de dados, o Regulamento (UE) 2016/679 estabelece que o consentimento deve ser dado de forma explícita. Nesses casos, um nível maior de controle individual sobre os dados é considerado apropriado. É o caso do artigo 9.º, que versa sobre o tratamento de categorias

[74] 2. "O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares."

especiais de dados. Como já mencionado, tais categorias acarretam maiores riscos de efeitos discriminatórios, usurpação ou roubo de identidade, perdas financeiras, prejuízos para a reputação, perda de confidencialidade de dados protegidos por sigilo profissional, entre outros (DUARTE, 2018, p. 237; EUROPEAN DATA PROTECTION BOARD, 2020, p. 20).

A proibição de tratamento dessas categorias de dados deve ser compreendida como uma salvaguarda de direitos fundamentais em face do tratamento de dados pessoais, como o direito à intimidade da vida privada e a igualdade. O artigo 9.º, n.º 2, estabelece as exceções a essa proibição, que se constituem estruturalmente como causas de exclusão da ilicitude. As exceções admissíveis têm como objetivo garantir o exercício de direitos ou interesses do titular ou a prossecução de interesses considerados juridicamente relevantes, como o interesse público, a realização da justiça, a saúde pública ou o interesse de organizações que tenham um objeto relevante (DUARTE, 2018, p. 238).

O número 2 do artigo 9.º prevê dez situações que autorizam o tratamento nesses casos, sendo o consentimento do titular a primeira delas.[75] O consentimento constitui o

[75] Outras hipóteses são: tratamento necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social (alínea b)); o tratamento necessário para proteção de interesses vitais do titular de dados ou de outra pessoa singular, caso o titular esteja física ou legalmente incapacitado de dar o seu consentimento (alínea c)); se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contatos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares (alínea d)); tratamento de dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular (alínea e)); tratamento necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional (alínea f)); se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados (alínea g)); Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.o 3 (alínea h)); se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional (alínea i)); se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a

fundamento residual para tratamento de dados sensíveis, nos casos em que não for aplicável nenhuma das demais exceções previstas. Nessas categorias especiais de dados, há uma exigência a mais para que o consentimento dado pelo titular seja válido. Além de ser uma manifestação de vontade livre, específica, informada e inequívoca, o consentimento também deve ser explícito quando se trata de dados sensíveis. Isso significa que deve haver uma expressão de vontade precisa, escrita ou oral, e não basta que o titular adote um comportamento concludente coerente com a sua vontade de autorizar o tratamento (DUARTE, 2018, p. 244).

Como ressalta Alexandre Sousa Pinheiro, o direito à proteção de dados pessoais foi concebido em um contexto no qual ainda não havia "um universo cibernético que comportasse a vivência em rede, a socialização electrónica – com maior exposição do sujeito à comunidade – e a proliferação informativa em redes abertas" (2015, p. 777). A proteção de dados foi historicamente aplicada a casos de "*back-end processing*", ou seja, tratamento em que não há interação dos usuários, como registros hospitalares e registros de usuários da Internet (KELLER, 2018, pp. 308–309). O próprio intuito do RGPD, de conjugar a exigência de tutela da pessoa com a realidade inevitável da circulação dos dados pessoais (CUFFARO, 2018, p. 12), já indica que o regulamento foi pensado tendo em consideração situações como o tratamento de dados pessoais por empresas, por exemplo, que envolve termos de uso e políticas de privacidade relativas ao tratamento, e não casos de descontextualização como o da NCII. Ainda assim, as imagens íntimas disseminadas constituem uma forma de dado pessoal de acordo com a definição do RGPD, a sua publicação sem o consentimento explícito da pessoa retratada é uma forma ilícita de tratamento de dados.

Quando se pensa na prática da disseminação de imagens íntimas na perspectiva do RGPD, é possível concluir que o ato constituirá um tratamento ilícito de dados pessoais quando não houver a configuração de uma das hipóteses do artigo 9.º, n.º 2, do Regulamento, já que os dados tratados podem ser considerados sensíveis: são dados relativos à vida sexual de uma pessoa que, como visto no capítulo precedente, acarretam riscos discriminatórios. A principal base legal capaz de autorizar tal disseminação seria o consentimento da pessoa retratada, conforme disposto na alínea a) do número 2 do artigo

essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados (alínea j)).

9.º, já que não se configuram situações de tratamento necessário para o cumprimento de obrigações, para a proteção de interesses vitais do titular, para efeitos de medicina preventiva ou do trabalho, ou para interesse público, por exemplo.

O consentimento, como já mencionado, é um conceito chave na definição da disseminação não consensual de imagens íntimas. Nesse ponto, Beyens e Lievens fazem uma observação pertinente. A disseminação é ilegal mesmo se a pessoa retratada (titular dos dados pessoais) deu seu consentimento explícito para a produção das imagens. Se, por exemplo, fotografias foram tiradas com o consentimento da pessoa A (retratada), e enviadas pela pessoa A à pessoa B, ou tiradas pela pessoa B com o consentimento de A, o consentimento inicial dado por A não abrange uma posterior publicação ou um compartilhamento com a pessoa C, ou outras. As autoras ressaltam que, ainda que tal observação pareça óbvia, não é raro o questionamento quanto à aplicabilidade de noções tradicionais de consentimento para o que se conhece popularmente como "*revenge porn*" (BEYENS E LIEVENS, 2016, p. 33).

Admitir que o consentimento de uma pessoa para a produção de imagens íntimas e seu armazenamento também serve para autorizar a sua disseminação seria contrário à própria lógica do regulamento, levando em conta a construção do consentimento no RGPD como uma manifestação de vontade específica. À luz do princípio da limitação das finalidades, o consentimento deve ser específico para cada uma das finalidades do tratamento. A publicação das imagens fora do contexto em que inicialmente haviam sido partilhadas, e para um público maior do que aquele inicial guarda semelhanças com o já mencionado "*function creep",* ou seja, com a prática de coletar dados com base no consentimento para uma finalidade, e realizar o tratamento para uma finalidade distinta. Viola a própria ideia de granularidade do consentimento, permite que o titular emita autorizações fragmentadas no tocante ao fluxo de seus dados (BIONI, 2019, cap. 4).

Identifica-se, nesse caso, uma violação à autodeterminação informacional: o titular de dados pessoais perde o controle sobre quem tem acesso às suas imagens. Além disso, pode-se dizer que o fluxo informacional não atende às legítimas expectativas do titular, violando o próprio desenvolvimento de sua personalidade (BIONI, 2019, cap. 4). Tendo em vista, portanto, que a NCII constitui um tratamento ilícito de dados pessoais conforme disposto no RGPD, pretende-se examinar no próximo capítulo, o possível direito

do titular de dados pessoais de obter o apagamento de suas imagens íntimas, na forma do artigo 17.º do Regulamento.

4 O DIREITO AO APAGAMENTO DE DADOS COMO RESPOSTA À DISSEMINAÇÃO NÃO CONSENSUAL DE IMAGENS ÍNTIMAS: ALGUMAS QUESTÕES

4. 1 O Direito ao apagamento dos dados (direito a ser esquecido) no caso da disseminação não consensual de imagens íntimas

Nas discussões sobre possíveis remédios para o caso de disseminação não consensual de imagens íntimas, é frequentemente mencionado o direito ao esquecimento, principalmente na perspectiva do caso *Google Spain.*[76] Em resposta a uma pergunta parlamentar de 2015 sobre o tema, por exemplo, a Comissão Europeia afirmou que a Diretiva 95/46/CE era aplicável ao tratamento de dados de imagem de pessoas naturais, e que determinava as condições para o tratamento legítimo de dados pessoais, bem como os direitos do titular de dados pessoais, incluindo o direito ao apagamento de dados, se não forem mais necessários para fins legítimos. Também afirmou que, conforme a decisão do Tribunal de Justiça da União Europeia no caso *Google Spain*, os cidadãos da União Europeia têm o direito, sob determinadas condições, de obter a remoção de seus dados pessoais dos motores de busca. Sustenta, ainda, que o "direito a ser esquecido" previsto na proposta de reforma da legislação em matéria de proteção de dados, constrói-se a partir desses direitos existentes (EUROPEAN COMMISSION, 2015).

Em resposta a uma pergunta semelhante, em 2017, a Comissão também chamou atenção para o fato de que indivíduos podem solicitar aos fornecedores de *websites* e aos motores de busca a remoção de informações pessoais sobre si de acordo com a legislação sobre proteção de dados da União Europeia (EUROPEAN COMMISSION, 2017). Nesse sentido, David Ryan aborda o tema do direito ao esquecimento como um remédio para a disseminação não consensual de imagens íntimas, afirmando que o direito tem "potencial

[76] Nesse sentido, o artigo publicado no jornal *The Guardian*, intitulado *Revenge porn: why the right to be forgotten is the right remedy*, chegou a referir-se à decisão do caso *Google Spain* como uma "dádiva divina" para as vítimas de "*revenge porn*", considerando que o *Google* é o motor de busca escolhido pela grande maioria dos usuários europeus. O artigo chegou a afirmar que "se o link desaparece do *index,* o conteúdo praticamente deixa de existir". Tal conclusão, porém, é inexata, visto que a remoção de links dos resultados de busca no nome do titular de dados pessoais não impede que o material seja acessado por outros meios (EDWARDS, 2014).

para oferecer alívio rápido e a curto prazo para as vítimas e alguma atenuação dos danos em suas vidas pessoais" (RYAN, 2018, p. 1067).

O Regulamento (UE) 2016/679 prevê, em seu artigo 17.º, o direito ao apagamento dos dados ("direito a ser esquecido"). Trata-se do direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, quando presentes as condições previstas nas alíneas a) a f) do número 1. O presente capítulo tem como objetivo analisar alguns aspectos do direito ao apagamento de dados no caso da disseminação não consensual de imagens íntimas. Para isso, começaremos por examinar as diversas acepções do direito ao esquecimento.

4.1.1 A perspectiva tradicional do direito ao esquecimento

Como já visto, o artigo 17.º do Regulamento é intitulado "Direito ao apagamento dos dados («direito a ser esquecido»)". Conforme ressalta Annarita Ricci, o título "justapõe dois termos: 'apagamento' e 'esquecimento', que remetem a conceitos jurídicos distintos" (2017, p. 200). É preciso esclarecer, portanto, o que significam esses termos. Di Ciommo ressalta que, dentre as novidades mais importantes trazidas pelo Regulamento no que toca aos direitos do titular de dados pessoais, está a referência expressa ao "direito ao esquecimento". É a primeira vez que uma norma europeia reconhece a existência desse direito (2019, p. 371).

Tradicionalmente, o termo "direito ao esquecimento" é utilizado para se referir a um direito de matriz jurisprudencial, que pode ser compreendido como o direito de uma pessoa de que uma notícia relativa a si própria, ainda que verdadeira e legitimamente publicada, não seja reproposta à opinião pública depois de certo lapso de tempo da sua primeira difusão ou do fato ao qual a notícia se refere (CIOMMO, 2019). Essas notícias, ainda que legitimamente publicadas em um momento histórico, tornam-se esquecidas ou ignoradas em decorrência do decurso do tempo (RICCI, 2017, p. 202). De acordo com Massimiliano Mezzanotte, o papel do "*diritto all'oblio*" é de "tutelar as escolhas de vida contra o controle público e a reprovação social, num quadro caracterizado pela liberdade

das escolhas existenciais" (2009, p. 121, tradução nossa).[77] Assim, consiste em um "meio para reconstruir a dimensão social do indivíduo, evitando que a vida passada possa constituir um obstáculo para a vida presente"[78] (2009, p. 121, tradução nossa).

O direito ao esquecimento envolve inevitavelmente o fator tempo. Não se trata de uma avaliação qualitativa da notícia. Em outras palavras: para que se reconheça a pretensão do titular do direito, não se deve avaliar se a reportagem em questão será lesiva para a sua reputação e identidade. É o decurso do tempo que torna a republicação da notícia ilícita, fazendo com que se perca a finalidade originária de divulgação. Isso ocorre porque, com o passar do tempo, o interesse coletivo à notícia se perde (RICCI, 2017, pp. 202–203). Annarita Ricci ressalta que o direito ao esquecimento tutela o interesse do sujeito de não sofrer alterações do seu patrimônio moral e social, ainda que tal patrimônio tenha sido adquirido através do esquecimento da notícia a seu respeito. Assim, a autora identifica uma ligação entre o direito ao esquecimento e a reputação e, mais em geral, com a identidade pessoal (2017, pp. 203–204).

Um dos principais casos precursores[79] [80] do direito ao esquecimento é a decisão Lebach, do Tribunal Constitucional Alemão, em 1973 (VLACHOPOULOS, 2018, p. 113).

---

[77] "*Questa è la ratio del diritto all'oblio, il cui ruolo è quello di tutelare le scelte di vita contro il controlo pubblico e la riprovazione sociale, in un quadro caratterizatto della libertà dele scelte esistenziali*" (MEZZANOTTE, 2009, p. 121).

[78] "*Esso è il mezzo per ricostruire la dimensione sociale dell'individuo, evitando che la vita passata possa costituire un ostacolo per la vita presente*" (MEZZANOTTE, 2009, p. 121).

[79] De acordo com Francesco Di Ciommo, o "*diritto all'oblio*" surgiu primeiramente nos Estados Unidos (2019, p. 378). Di Ciommo menciona a decisão do caso *Melvin v. Reid*, de 1931. O caso versava sobre uma mulher que, antes de 1918, trabalhava como prostituta e naquele ano foi acusada de homicídio, tendo sido absolvida em tribunal. Em 1919, ela mudou seu estilo de vida, casou-se e passou a ter uma vida respeitável. Em 1925, foi produzido um filme intitulado "*The Red Kimono*", que retratava sua história de vida, usando seu nome de solteira como o nome da personagem principal do filme. O Tribunal da Califórnia decidiu que o filme causou danos à autora que deveriam ser ressarcidos. Afirmou-se que "uma pessoa não consegue perseguir e obter felicidade se às demais é permitido transmitir detalhes desagradáveis de sua vida passada sem justa causa" (PINHEIRO, 2015, p. 305; COURT OF APPEALS OF CALIFORNIA, 1931 *apud* S. G. P., 1931). Di Ciommo também cita o caso Sidis v. FR Publishing Corp (2019, p. 378). William James Sidis adquiriu fama em 1910, por ser uma "criança-prodígio". Aos 11 anos, já dava palestras a matemáticos de renome, e, aos 16, graduou-se na *Harvard College*, tendo atraído atenção considerável. Desde então, Sidis foi referido pela imprensa apenas em publicações esporádicas. Decidiu afastar-se de sua vida de fama e estudos e seguiu carreira em um emprego comum, que não requeria talentos matemáticos atípicos. Em 1937, a revista semanal *The New Yorker* publicou textos e *cartoons* biográficos sobre a história de Sidis, descrevendo suas conquistas na área da Matemática e evocando seu colapso e a repulsa que sentiu por sua vida anterior. Sidis alegou que seu "*right to privacy*" foi atingido pelo fato de a imprensa dar publicidade à sua vida à época da reportagem. Nesse caso, porém, o tribunal considerou que não havia qualquer violação à privacy, tratando-se apenas de mera publicação de informações corretas (U.S. COURT OF APPEALS, 1940).

[80] No contexto francês, afirma-se que o "*droit à l'oubli*" foi colocado em discussão pela primeira vez no chamado "*Affaire Landru*", em uma decisão de 1965. Trata-se do caso de uma pessoa que havia sido amante de um criminoso muito conhecido, e que demandava a reparação dos prejuízos causados por um filme que

O autor da reclamação constitucional havia participado de um crime violento em 1969, que chamou atenção da opinião pública e teve ampla cobertura da imprensa e televisões locais, conhecido como "assassinato dos soldados de *Lebach*". Foi condenado a seis anos de reclusão por ter auxiliado na preparação do crime. Um canal de televisão alemão produziu um documentário sobre o ocorrido, no qual, além de outros dois condenados pelo crime, o reclamante foi apresentado com foto e nome, sendo também representado por atores. Foram retratados detalhes da relação dos condenados entre si, incluindo relações homossexuais, além dos pormenores da noite do crime e da perseguição policial. O documentário seria transmitido pouco antes da soltura do reclamante (BVERFGE, 1973 *apud* MARTINS, 2005, p. 487).

O Tribunal Constitucional identificou um conflito entre a liberdade de radiodifusão (artigo 5, I, 2, da GG) e o interesse da pessoa em questão contra a divulgação e apresentação da sua imagem, reforçado pela garantia constitucional de proteção da personalidade (artigo 2, I c.c. artigo 1, I, da GG). Ressaltou que não se pode outorgar a nenhum dos valores constitucionais, em princípio, a prevalência sobre o outro, e que, no caso particular, a intensidade da intervenção no âmbito da personalidade deveria ser ponderada com o interesse de informação da população. Decidiu que a publicação feria o direito fundamental do reclamante ao livre desenvolvimento da personalidade, considerando que não se admite que "a televisão se ocupe com a pessoa do criminoso e sua vida privada por tempo ilimitado". Afirmou, ainda, que um noticiário posterior será inadmissível se tiver o condão de provocar prejuízo considerável novo ou atual à pessoa do criminoso, principalmente se ameaçar a sua reintegração na sociedade (BVERFGE, 1973 *apud* MARTINS, 2005, p. 488).

Nesse sentido, para identificar os traços distintivos do direito ao esquecimento, Mezzanotte (2009, p. 121) menciona uma decisão da *Corte di Cassazione* italiana de 1998

---

retratou um período distante de sua vida, que gostaria que ficasse esquecido no passado. A autora não invocou propriamente o "*droit à l'oubli*", mas a chamada "*prescription du silence"*. O pedido foi negado, contudo. Considerou-se que a autora não poderia exigir tal reparação, já que ela mesma tinha publicado suas memórias, e que o filme se referia a fatos que figuravam em crônicas judiciárias acessíveis (LETTERON, 1996, pp. 411–412; T.G.I DE LA SEINE, 1965 *apud* LINDON, 1983, p. 271). Posteriormente, em uma decisão de 1983 (Madame M. c. Filipacchi et Cogedipresse), o *Tribunal de Grande Instance de Paris* afirmou que qualquer pessoa que participou de eventos públicos pode, com o passar do tempo, invocar o direito ao esquecimento, e que relembrar esses eventos será uma atividade ilegítima, se não for fundada nas necessidades da história, ou se for feita de forma ofensiva. Também ressalta que o direito poderá ser reivindicado por todos, incluindo condenados que já cumpriram a sua pena e que pretendem se reinserir na sociedade (T.G.I. DE PARIS *apud* LETTERON, 1996, p. 412).

sobre a publicação de notícia em uma revista semanal, em que o jornalista correlacionou uma das partes a acontecimentos ligados à máfia siciliana. Na decisão, o Tribunal aborda o direito ao esquecimento. Afirma que não se trata, simplesmente, de aplicar o princípio da atualidade do interesse público à informação, já que o interesse não está estritamente ligado à atualidade do fato. O interesse permanece enquanto se mantém atual a relevância pública do fato, ou mesmo ressurge, caso a relevância pública do fato torne a ser atual. Considera o direito ao esquecimento como um novo perfil do direito à reserva da vida privada, e o define como "o justo interesse de cada pessoa a não permanecer indeterminadamente exposta a danos ulteriores causados à sua honra e reputação pela reiterada publicação de uma notícia legitimamente divulgada no passado"[81] (CORTE DI CASSAZIONE, 1998, tradução nossa) A antiguidade dos fatos é o que diferencia o direito ao esquecimento do direito à reserva da vida privada. Desse modo, a publicação de fatos datados é considerada ilícita, a menos que eventos supervenientes tornem aqueles fatos novamente atuais, fazendo ressurgir um novo interesse público à informação (CORTE DI CASSAZIONE, 1998, MEZZANOTTE, 2009, p. 124).

É evidente que o direito ao esquecimento não é um direito absoluto, e existem situações em que a nova divulgação de um fato poderá ser considerada lícita. Mezzanotte aborda algumas dessas possibilidades, tendo em conta o direito constitucional italiano. O direito à liberdade de imprensa e de informação, por exemplo, pode prevalecer sobre o direito à reserva da vida privada e o direito ao esquecimento. Como mencionado na decisão da *Corte di Cassazione* de 1998, acontecimentos supervenientes podem fazer com que fatos já publicados tornem a ser atuais, e, nesse caso, o direito à liberdade de imprensa passa a ser legitimamente exercido, já que o interesse público naquela informação está configurado (2009, pp. 142–143). O direito ao esquecimento também pode não ser aplicado em casos de pesquisa ou crítica histórica. Nessas situações, ao contrário do que ocorre com o direito à liberdade de imprensa, o interesse no acontecimento permanece estável com o passar dos anos. Não se pode exigir que certas informações relativas a personagens históricos sejam esquecidas pelo mero decurso do tempo. O personagem histórico não perde a notoriedade com o passar dos anos (MEZZANOTTE, 2009, p. 144).

[81] "[...] *giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata"* (CORTE DI CASSAZIONE, 1998).

4.1.2 O direito ao esquecimento na Internet e o caso *Google Spain*

Com a evolução da Internet, o direito ao esquecimento adquiriu um novo significado. Ao contrário do que ocorre com publicações em jornais e revistas em papel, uma notícia difundida na rede permanece disponível, ou ao menos abstratamente disponível. Basta realizar uma pesquisa através de um motor de busca como o *Google*, por exemplo, para que notícias publicadas no passado sobre um determinado assunto sejam elencadas nos resultados. O problema passa a não ser só ou necessariamente a republicação da informação, mas a sua permanência na rede. Assim, o tempo a ser considerado não é mais aquele entre a publicação e a republicação de uma informação, mas a sua permanência na rede (FINOCCHIARO, 2015, p. 31).

Nesse sentido, como indica Finocchiaro (2015, pp. 31–32), identifica-se, na Itália, uma segunda acepção do direito ao esquecimento, que é entendido nesse caso como um direito à contextualização da informação. O problema em questão é o de atribuir um peso à informação, que muitas vezes é exibida na Internet de forma reducionista. Essa acepção foi adotada em uma decisão italiana da *Corte di Cassazione*, de 2012. Trata-se do caso de um político que foi preso por corrupção em 1993, mas que foi absolvido ao fim do processo judicial. Ele afirmava que, mesmo depois de muitos anos da sentença que o absolveu, a notícia de sua prisão era elencada em qualquer pesquisa pelo seu nome no *Google*, sem que houvesse alguma referência à sua absolvição (CORTE DI CASSAZIONE, 2012; PARDOLESI e CIOMMO, 2012, p. 703; RICCI, 2017, pp. 205–206).

A *Corte di Cassazione* não reconheceu o direito de pedir a eliminação da notícia, já que não estava em causa a veracidade do ocorrido, e nem a utilidade pública da informação. Considerou que ao sujeito deve ser reconhecido o direito ao controle de seus dados, mesmo quando se trata de uma notícia verdadeira e de utilidade pública. Tal controle pode se traduzir na pretensão à contextualização e atualização dos arquivos em que a notícia foi publicada e, se for o caso, ao seu apagamento. Assim, reconheceu-se o direito de integrar a notícia com as informações necessárias, que diziam respeito à absolvição do réu (PARDOLESI e CIOMMO, 2012, p. 703; RICCI, 2017, pp. 205–206). Nesse caso, fala-se em direito ao esquecimento ("*diritto all'oblio*") em um sentido lato, já que não se trata tanto do direito de esquecer, mas de contextualizar (FINOCCHIARO, 2015, p. 32).

Nesse mesmo contexto digital, em que qualquer um pode ter acesso a arquivos ilimitados em termos de conteúdo e tempo, através de motores de busca generalistas ou específicos de arquivos digitais de periódicos, Finocchiaro (2015, p. 35) identifica uma terceira acepção de direito ao esquecimento, que se aproxima mais da eliminação de dados pessoais. A decisão do Tribunal de Justiça da União Europeia no caso *Google Spain SL e Google Inc. v Agencia Española de Protección de Datos (AEPD) e Mario Costeja González,* de 2014, é considerada como aquela que estabeleceu essa nova forma de pensar no direito ao esquecimento, como "direito a não ser encontrado online" (RICCI, 2017, p. 207).

Em 2010, o Senhor M. Costeja González apresentou uma reclamação à Agência Espanhola de Proteção de Dados (AEPD) contra um jornal de grande tiragem na Catalunha (*La Vanguardia Ediciones SL*), bem como contra a *Google Spain* e a *Google Inc*. A reclamação referia-se ao fato de que, quando um internauta inseria o nome do Senhor González no motor de busca do *Google*, apareciam nos resultados duas ligações para publicações do Jornal *La Vanguardia* de 19 de janeiro e 9 de março de 1998, anunciando a venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Segurança Social, que mencionava o nome do Senhor González (TJUE, 2014, par. 14).

Na reclamação, M. Costeja González pedia que o jornal suprimisse ou alterasse as páginas referentes à venda dos imóveis, para que seus dados pessoais deixassem de aparecer, ou que utilizasse ferramentas disponibilizadas pelos motores de busca para proteger esses dados. Além disso, pedia que se ordenasse à *Google Spain* ou à *Google Inc*. que suprimissem ou ocultassem os dados pessoais, para que deixassem de aparecer nos resultados de pesquisa e entre os links do *La Vanguardia*. Alegava que o processo de arresto tinha sido encerrado há muito tempo, e que a referência a esse processo carecia de pertinência. Quanto ao jornal *La Vanguardia*, a AEPD indeferiu a reclamação, considerando que a publicação das informações estava legalmente justificada, já que tinha sido feita por ordem do Ministério do Trabalho e dos Assuntos Sociais, tendo por finalidade publicitar ao máximo a venda em hasta pública, com o objetivo de reunir o maior número possível de licitantes (TJUE, 2014, par. 15-16).

No que diz respeito à reclamação em face da *Google Spain* e da *Google Inc*., a AEPD deferiu o pedido, considerando que os operadores de motores de busca estão

sujeitos à legislação em matéria de proteção de dados pessoais, pois realizam um tratamento de dados pelo qual são responsáveis e atuam como intermediários da sociedade de informação. A *Google Spain* e a *Google Inc.* interpuseram recursos à Audiência Nacional, que suspendeu a instância e submeteu questões prejudiciais ao Tribunal de Justiça da União Europeia (TJUE, 2014, par. 17-20). Questionado se é possível considerar a atividade do motor de busca como tratamento de dados pessoais conforme a Diretiva 95/46/CE, o Tribunal considerou que, entre os dados encontrados, indexados, armazenados e colocados à disposição pelo motor de busca figuram, evidentemente, dados pessoais. Além disso, as ações de "recolher", "recuperar", "registrar", "organizar", "conservar" e "disponibilizar" dados pessoais estavam claramente referidas nas definições de tratamento de dados da Diretiva (TJUE, 2014, par. 27-28).

Quanto ao papel do motor de busca no tratamento de dados nesse caso, o Tribunal ressaltou que é o operador que "determina as finalidades e os meios dessa atividade" que está em causa no processo principal, devendo ser considerado responsável por esse tratamento na forma do artigo 2.º, alínea d), da Diretiva. Também salientou que excluir a o motor de busca da definição de responsável pelo tratamento, sob o argumento de que ele não exerce controle sobre os dados publicados nas páginas da *web* de terceiros, seria contrário não só à redação da diretiva, mas também aos seus objetivos, já que ela, através de uma definição ampla do conceito de "responsável pelo tratamento", buscou assegurar uma proteção eficaz e completa das pessoas em causa. Ressaltou, ainda, que o tratamento efetuado pelo motor de busca se distingue daquele efetuado pelo editor da página da *web*, e acresce a ele. O tratamento feito pelo operador do motor de busca tem papel decisivo na difusão global dos dados, pelo fato de tornar as informações acessíveis a qualquer usuário que efetue uma pesquisa a partir do nome da pessoa em causa, podendo afetar significativamente os seus direitos à privacidade e proteção de dados pessoais[82] (TJUE, 2014, par. 33-36).

[82] Quanto ao âmbito de aplicação da legislação nacional que transpõe a Diretiva, o Tribunal analisou se o referido tratamento era efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento no território de um Estado-Membro, conforme disposto no artigo 4.º, número 1, alínea a). Observou que, conforme o considerando (19), um "estabelecimento no território de um Estado-Membro pressupõe o exercício efetivo e real de uma atividade mediante instalação estável", e que a forma jurídica desse estabelecimento, quer seja sucursal ou filial com personalidade jurídica, não é determinante. A *Google Spain*, filial da *Google Inc*. com personalidade jurídica própria na Espanha, dedica-se ao exercício efetivo e real de uma atividade, que consiste na promoção e venda de espaços publicitários, através de uma instalação estável no território espanhol. É, portanto, um estabelecimento na acepção do artigo 4.º, número 1, alínea a),

Um dos pontos mais importantes esclarecidos pelo tribunal foi quanto ao alcance da responsabilidade do operador do motor de busca. O TJUE, nesse ponto, ressaltou o direito da pessoa em causa de obter a retificação, apagamento ou bloqueio de dados do responsável pelo tratamento, caso este não cumpra o disposto na Diretiva 95/46/CE, que estava claramente previsto em seu artigo 12.º, alínea b). A não conformidade com a Diretiva poderia decorrer do incumprimento de qualquer uma das condições de licitude impostas pela Diretiva ao tratamento de dados pessoais. Além disso, mesmo que a conformidade do tratamento com os princípios relativos à qualidade dos dados (artigo 6.º da Diretiva) e a necessidade do tratamento para prosseguir interesses legítimos do responsável (artigo 7.º, alínea f), da Diretiva) pudessem ser verificadas no âmbito de um pedido na acepção do artigo 12.º, alínea b), a pessoa em causa ainda teria o direito de se opor, em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito fossem objeto de tratamento, salvo disposição em contrário do direito nacional (artigo 14.º, primeiro parágrafo, alínea a)) (TJUE, 2014, par. 70-76).

O Tribunal considerou que um tratamento de dados como o que estava em questão era capaz de afetar significativamente os direitos previstos nos artigos 7.º e 8.º da CDFUE, por permitir que qualquer um que busque pelo nome da pessoa em causa encontre numerosos aspectos de sua vida privada nos resultados, e que dificilmente seriam descobertos sem a atuação do referido motor de busca. Tal ingerência foi considerada potencialmente grave, não podendo ser simplesmente justificada pelo interesse econômico do operador do motor de busca. Dessa forma, o TJUE considerou necessário procurar um justo equilíbrio entre os direitos à privacidade e proteção de dados da pessoa em causa e esse interesse econômico, além do interesse dos internautas em ter acesso à informação. Ressaltou, porém, que os direitos da pessoa em causa, geralmente, prevaleceriam também sobre os referidos interesses dos internautas. Essa ponderação dependerá, contudo, da natureza da informação em questão, bem como da sua sensibilidade pela pessoa em causa, além do interesse do público em dispor dessa informação (TJUE, 2014, par. 80-81).

---

da Diretiva. O Tribunal ressaltou que a Diretiva não exige que o tratamento seja efetuado pelo próprio estabelecimento em causa, mas "no contexto das atividades" deste. Dessa forma, ainda que a atividade de indexação seja desenvolvida pelo *Google Search*, que por sua vez é operado pela *Google Inc*., e não pela *Google Spain*, observa-se que as atividades de indexação e promoção e venda de espaços publicitários estão indissociavelmente ligadas (TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, 2014, par. 48-60).

Como resultado da aplicação dos artigos 12.º, alínea b) (direito de acesso, retificação, apagamento ou bloqueio) e 14.º, primeiro parágrafo, alínea a) (direito de oposição ao tratamento) da Diretiva, o Tribunal concluiu que, diante de um pedido como aquele feito pelo Sr. González, a autoridade de controle ou o tribunal poderiam ordenar ao operador do motor de busca que suprimisse da lista de resultados as ligações a páginas da *web* publicadas por terceiros e que contivessem informações sobre a pessoa em causa, sem que o editor tivesse de eliminar os dados previamente da página. Tal conclusão decorre da já mencionada constatação de que o tratamento efetuado pelo operador do motor de busca se distingue daquele efetuado pelos editores dos *websites*, e acresce a ele. Dessa forma, o responsável por esse tratamento deve, também, certificar-se de que o tratamento satisfaça as exigências da diretiva (TJUE, 2014, par. 82-83).

Nesse ponto, o TJUE salientou que, muito facilmente, as informações publicadas em um *website* poderiam ser copiadas e reproduzidas em outro, e os responsáveis pela publicação podem não estar sujeitos à legislação da União Europeia. Dessa forma, não seria possível assegurar uma proteção eficaz e completa das pessoas em causa se, para suprimir links dos resultados de busca, elas devessem obter, prévia ou paralelamente, a supressão das informações que lhes dizem respeito junto aos editores dos *sites*. Do mesmo modo, acrescentou que o tratamento feito pelo editor da página da *web* pode ser efetuado para fins exclusivamente jornalísticos, sendo, portanto, beneficiado pelas derrogações previstas no artigo 9.º da Diretiva. Assim, não se pode excluir que, em determinados casos, a pessoa em causa possa exercer os direitos previstos nos artigos 12.º, alínea b), e 14.º, primeiro parágrafo, alínea a), contra o operador do motor de busca, mas não contra o editor do *site* (TJUE, 2014, par. 84-85).

Além disso, o Tribunal acrescentou que os motivos que justificam a publicação de dados pessoais num *site* não necessariamente coincidem com os que se aplicam às atividades dos motores de busca, e, mesmo que haja coincidência, o resultado da ponderação dos interesses em conflito também poderá divergir. Assim, o Tribunal considera que, para respeitar os direitos previstos nos artigos 12.º, alínea b), e 14.º, primeiro parágrafo, alínea a), da Diretiva, o motor de busca é obrigado a suprimir da lista de resultados obtida na pesquisa pelo nome da pessoa em causa as ligações a páginas da *web* publicadas por terceiros e que tenham informações sobre essa pessoa, ainda que a publicação de tais dados nessas páginas seja, em si mesma, lícita (TJUE, 2014, par. 86).

Finalmente, no que diz respeito ao alcance dos direitos da pessoa em causa garantidos pela Diretiva, o Tribunal considerou que mesmo um tratamento inicialmente lícito de dados exatos pode tornar-se, com o tempo, incompatível com os princípios relativos à qualidade dos dados. Tal situação ocorre quando os dados são inadequados, não pertinentes, não mais pertinentes ou excessivos em relação aos propósitos para os quais foram recolhidos, e à luz do tempo decorrido. O Tribunal também ressalta que a constatação do direito da pessoa em causa de solicitar que informações sobre si deixem de ser associadas ao seu nome nas listas de resultados de busca não pressupõe que a inclusão da informação nas referidas listas cause algum prejuízo a ela. Considerando o caso concreto, o Tribunal chamou atenção para o fato de que as informações contidas nos links relacionados nos resultados de busca no nome do Sr. González eram de caráter sensível para a sua vida privada, e para o fato de que a publicação havia sido feita 16 anos antes. Além disso, ressaltou que não havia, aparentemente, razões especiais que justificassem um interesse preponderante do público em ter acesso a esses dados no âmbito dessa pesquisa (TJUE, 2014, par. 92-98).

Assim, o Tribunal conclui que, tendo em conta o disposto nos artigos 12.º, alínea b), e 14.º, primeiro parágrafo, alínea a), da Diretiva, bem como os direitos fundamentais previstos nos artigos 7.º e 8.º da Carta, a pessoa em causa pode requerer que informações pessoais deixem de estar à disposição do grande público pela inclusão na lista de resultados de pesquisa. Esses direitos prevalecem, em princípio, não só sobre o interesse econômico do operador do motor de busca, mas também sobre o interesse do público em aceder à informação através da pesquisa no nome da pessoa. Esses direitos não prevalecerão, porém, se houver interesse preponderante do público em ter acesso àquela informação, como, por exemplo, no caso de pessoas que desempenham papeis na vida pública (TJUE, 2014, par. 97-99).

Como observa Annarita Ricci, o Tribunal, nesse caso, reconheceu um direito ao apagamento da indexação dos dados (“desindexação”) e, consequentemente, à remoção das condições para seu conhecimento generalizado, desde que esses dados fossem inadequados, não pertinentes, ou não mais pertinentes em relação às finalidades do motor de busca. Em síntese, o Tribunal afirmou a aplicação dos princípios gerais sobre a qualidade dos dados previstos pela Diretiva ao tratamento de dados efetuado pelos motores de busca (2017, p. 209). Nota-se que na decisão o Tribunal não se propõe a considerar o

que significa o "esquecimento", e nenhuma das respostas às quatro questões referidas inclui a noção de "direito ao esquecimento" (HOFFMAN, BRUENING e CARTER, 2015).

Não há consenso quanto a vários aspectos do direito envolvido na decisão *Google* Spain (UNCULAR, 2019, p. 310). Alguns autores ressaltaram que, ao contrário do que foi sugerido em várias notícias, o Tribunal não criou o direito ao esquecimento através da decisão do *Google Spain*, mas apenas afirmou o direito do cidadão de, em certas circunstâncias, ter resultados de busca em seu nome removidos (KULK e BORGESIUS, 2014, p. 397). Afirma-se que o Tribunal não poderia fazer cumprir um direito que não existisse na legislação corrente (POLITOU, ALEPIS e PATSAKIS, 2018, p. 10). Costescu (2016, p. 71) acredita que o Tribunal apenas reconheceu que o direito ao esquecimento existia. Em contrapartida, Bunn (2015, p. 350) entende que a decisão somente aplicou um direito ao apagamento existente na diretiva. Da mesma forma, Bougiakiotis (2016, p. 312) considera que o Tribunal nada mais fez do que interpretar, talvez de forma mais dinâmica, a legislação em vigor.

Hoffman, Bruening e Carter (2015, p. 441) chamam atenção para o fato de que a decisão não tem como resultado um verdadeiro esquecimento, já que a informação ainda pode ser encontrada usando outros termos de busca. De acordo com os autores, em vez de "esquecimento", o que a decisão proporciona é um "direito à obscuridade". Na mesma linha, Uncular (2019, p. 311) afirma que a decisão não criou – e nem poderia criar – um direito ao esquecimento, já que é impossível que os dados sejam completamente esquecidos simplesmente pela remoção das listas de um motor de busca. Lynskey (2015, p. 528) considera que o Tribunal, ao afirmar a desnecessidade de prejuízo à pessoa em causa para que se configure o direito, não reconhece um "direito ao esquecimento". Segundo Lynskey, o direito ao apagamento só se aplica quando o tratamento é incompatível com a Diretiva, e o rótulo "direito ao esquecimento" para esse caso é equivocado.

O entendimento do Tribunal foi objeto de várias críticas, principalmente no que toca ao conflito entre o direito à liberdade de expressão e informação e os direitos à privacidade e proteção de dados pessoais. Alguns autores afirmam que o Tribunal não deu a atenção devida ao direito à liberdade de expressão e informação ao afirmar que os direitos à privacidade e à proteção de dados da pessoa em causa prevalecem, como regra, sobre o interesse dos internautas em ter acesso à informação. Kulk e Borgesius (2014, p. 392) e Lynskey (2015, p. 530), por exemplo, ressaltam que o julgado não contém

referência explícita ao direito à liberdade de expressão e informação, mencionando apenas o "interesse dos internautas" em ter acesso à informação. Contudo, o direito à liberdade de expressão protege não só o usuário em busca de informação, mas também quem fez a publicação original, bem como o próprio operador do motor de busca. Apesar de afirmar a necessidade de se estabelecer um justo equilíbrio entre os referidos direitos, o Tribunal, ao determinar que os direitos previstos nos artigos 7.º e 8.º da CDFUE prevalecerão como regra sobre a liberdade de expressão, acabou por contrariar o entendimento do Tribunal Europeu dos Direitos do Homem, que atribui igual peso à privacidade e à liberdade de expressão (BUNN, 2015, p. 345; HOFFMAN, BRUENING e CARTER, 2015, pp. 460–464; KULK e BORGESIUS, 2014, pp. 393–394).

Desde a publicação da decisão, o *Google* recebeu um número elevado de solicitações de remoção de *links*.[83] Uma das críticas frequentes sobre o caso se refere ao fato de que o direito à desindexação pode onerar significativamente os motores de busca e outros serviços online, como redes sociais (ABRIL e LIPTON, 2014, p. 380; HOFFMAN, BRUENING e CARTER, 2015, p. 478; UNCULAR, 2019, p. 319). O julgado impõe aos motores de busca como o *Google* a obrigação de determinar se certos dados pessoais são ou não de interesse público, uma tarefa que tradicionalmente era atribuída a autoridades públicas, e não a empreendimentos privados (LYNSKEY, 2015, p. 532). Afirma-se que a liberdade de expressão é um direito muito significativo para ser deixado ao alvedrio de empresas privadas, em vez de autoridades imparciais (UNCULAR, 2019, p. 318). Alguns autores comentam que os mecanismos de remoção adotados pelo *Google* não são transparentes (HOFFMAN, BRUENING e CARTER, 2015, p. 478; KULK e BORGESIUS, 2014, p. 395).

Críticos argumentam que o posicionamento da decisão *Google* Spain pode acarretar problemas de implementação. Empresas privadas como o *Google* podem optar pela precaução ao avaliar os pedidos de remoção de links, e, para evitar sanções, podem determinar a remoção mesmo em situações em que ela não seria justificada. Tal cenário pode resultar em menos liberdade e expressão maior desigualdade, já que os mais abastados e com maior escolaridade ter mais ferramentas para pressionar legalmente os

[83] Desde 29 de maio de 2014, o *Google* recebeu mais de 980.000 pedidos de desindexação, requerendo a remoção de mais de 3.840.000 *links* (GOOGLE, 2020).

operadores para que cumpram os pedidos (ABRIL e LIPTON, 2014, p. 383; BOUGIAKIOTIS, 2016, p. 323; HOFFMAN, BRUENING e CARTER, 2015, p. 478).[84]

Em contrapartida, Gorzeman e Korenhof, por exemplo, consideraram a decisão do TJUE "uma solução elegante", tendo em vista o papel crucial desempenhado pelos motores de busca na manutenção de uma memória eterna coletiva online (2017, p. 89). Os autores argumentaram que o direito reconhecido pelo TJUE é a forma menos pesada e mais efetiva de se obter a quantidade mínima de censura e, ao mesmo tempo "permitir que as pessoas possam evoluir para além de suas opiniões passadas" (2017, p. 73). Kieron O'Hara, ao analisar os pontos positivos da decisão, afirma que seus efeitos na liberdade de expressão são proporcionais, uma vez que a informação permanece online, e ainda pode ser encontrada através dos motores de buscas, se forem usados termos específicos (2015, p. 75). A autora também comenta que o julgado restaura um pouco da obscuridade que protegia nossa esfera privada no passado, quando a informação disponível estava em arquivos de papel e, mesmo que fosse pública, era mais difícil de se obter (2015, p. 76).

4.1.3 O Artigo 17.º do Regulamento e o "direito a ser esquecido"

O artigo 17.º do Regulamento (UE) 2016/679 afirma o direito do titular de dados pessoais de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, nas seguintes situações:

"a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;

b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;

c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2;

d) Os dados pessoais foram tratados ilicitamente;

[84] O Advogado-Geral apresenta esse argumento em suas conclusões: "Tais procedimentos de informação e de supressão («*notice and take down*»), caso sejam exigidos pelo Tribunal, podem conduzir à remoção automática de hiperligações a quaisquer conteúdos contestados ou a um número incontrolável de pedidos recebidos pelos prestadores do serviço de motor de pesquisa na Internet" (JÄÄSKINEN, 2013, par. 133).

e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;

f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1."

O artigo refere-se ao "direito ao apagamento dos dados («direito a ser esquecido»)", que foi considerado como uma inovação do Regulamento (POLITOU, ALEPIS e PATSAKIS, 2018, p. 11). Contudo, observa-se que o previsto no artigo 17.º "não parece representar uma mudança revolucionária nas regras já existentes quanto a esse direito" (MANTELERO, 2013, p. 229, tradução nossa).[85] [86] O artigo reproduz o conteúdo essencial do direito ao apagamento já previsto na Diretiva 95/46/CE, identificando especificamente os casos de violação da norma que justificam o apagamento, acrescentando a revogação do consentimento, o exercício do direito de oposição, a obrigação legal e o tratamento de dados de menores no contexto da oferta de serviços da sociedade da informação (RICCI, 2017, p. 197).

A maior novidade em relação à Diretiva parece ser o disposto no seu número 2, que determina que, quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los conforme o número 1, "deverá tomar as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos" (FINOCCHIARO, 2015, p. 34; MANTELERO, 2013, p. 233; POLITOU, ALEPIS e PATSAKIS, 2018, p. 11; RICCI, 2017, p. 197). O responsável pelo tratamento deve, ainda, comunicar o apagamento a cada destinatário a quem os dados pessoais tenham sido transmitidos, conforme disposto no artigo 19.º do Regulamento, salvo se a comunicação se revelar impossível ou implicar um esforço desproporcionado. Nesses casos, configura-se, portanto, uma obrigação de meio para o responsável pelo tratamento, impondo a adoção

[85] "*the new provisions do not seem to represent a revolutionary change to the existing rules with regard to the right granted to the individual*" (MANTELERO, 2013, p. 229).
[86] Finocchiaro e Ricci fazem observações no mesmo sentido (FINOCCHIARO, 2015, p. 34; RICCI, 2017, p. 197).

das medidas técnicas e organizativas que seriam razoavelmente esperadas considerando a tecnologia disponível e os custos de atuação (RICCI, 2017, p. 198).

O número 3 do artigo 17.º apresenta um elenco de hipóteses em que o direito ao apagamento não se aplica. Tal direito pode não ser reconhecido nos casos em que o apagamento é necessário: a) ao exercício da liberdade de expressão e de informação; b) ao cumprimento de uma obrigação legal, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; c) por motivos de interesse público no domínio da saúde pública; d) para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, ou e) para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

De acordo com Ricci, o artigo 17.º surge da necessidade de reforçar a pretensão do interessado de obter a remoção de informações sobre si próprio cujo tratamento não é mais justificado, e que poderiam prejudicar a sua esfera individual, tendo em conta principalmente o mundo digital. Segundo a autora, desse fato provém a qualificação do direito ao apagamento como instrumento de implementação do direito ao esquecimento (2017, p. 199). Como já mencionado, uma das novidades mais importantes do Regulamento foi a expressa menção ao direito ao esquecimento, pela primeira vez em uma norma europeia. A referência é feita da seguinte forma: ao lado da expressão "direito ao apagamento" lê-se, entre parênteses, a expressão "direito a ser esquecido", que também está presente nos considerandos (65), (66) e (156) (CIOMMO, 2019, p. 371).

Francesco Di Ciommo chama atenção para o fato de que o legislador europeu, através dessa justaposição de expressões, mencionando o direito ao esquecimento somente entre parênteses no contexto de um artigo dedicado ao direito ao apagamento de dados pessoais, "parece ter desejado enquadrar o instituto trazendo-o ao contexto do tema relativo ao apagamento de dados" (2019, p. 371). Ressalta-se que na proposta de Regulamento, o título do artigo era "direito a ser esquecido e ao apagamento" (em inglês "*right to be forgotten and to erasure*"), sendo posteriormente alterado. Ainda assim, a disposição do texto definitivo continua a ser criticada e considerada ambígua (CIOMMO, 2019, p. 374; RICCI, 2017, p. 200; UNCULAR, 2019, p. 311).

Várias questões quanto ao direito ao esquecimento não estão claras no Regulamento. A norma não fornece uma definição nítida do que se entende por "direito a ser esquecido" (CIOMMO, 2019, p. 372; POLITOU, ALEPIS e PATSAKIS, 2018, p. 11).

Diante disso, Francesco Di Ciommo alerta para a possibilidade de que a nova norma seja interpretada de modo a esvaziar, ao menos em parte, o próprio conteúdo do direito ao esquecimento. Se o direito ao esquecimento fosse considerado mera expressão do direito ao apagamento, ou de qualquer forma incluído neste, perderia muito da sua conotação típica, já que o esquecimento pode envolver outras situações como desindexação e contextualização de uma informação, que não implicam o seu apagamento total (2019, p. 372).

Observa-se que, apesar do que consta do título, a intenção do artigo não foi de disciplinar de forma específica o direito ao esquecimento. O artigo simplesmente disciplina o direito ao apagamento, sem tecer qualquer consideração particular relativamente ao "*right to be forgotten*" (CIOMMO, 2019, p. 373). Assim, é preciso ressaltar que, embora justapostos no artigo 17.º, o direito ao esquecimento e o direito ao apagamento não são sinônimos. Nesse ponto, Ricci afirma que o direito ao apagamento pode ser exercido quando se configuram circunstâncias taxativamente previstas no Regulamento, e é expressamente previsto como pretensão autônoma e distinta do titular de dados pessoais. Já o direito ao esquecimento, para Ricci, não se configura como um direito autônomo, formalizado pelo Regulamento. O esquecimento, mais do que objeto de uma específica pretensão do titular, é um possível efeito que se obtém com o exercício do direito ao apagamento de dados. Ou seja, o direito ao apagamento pode comportar o efeito do esquecimento (2017, p. 201). Bunn afirma que o direito ao esquecimento é mais difícil de ser concebido como um mecanismo legal, e menciona que o direito pode ser realizado através de outros meios que não sejam o apagamento. O direito ao esquecimento, segundo a autora, é mais bem interpretado como uma justificativa para direitos existentes e medidas tecnológicas, ou para a criação de novos direitos e medidas, do que como um direito em si (2015, pp. 338–339).

Importa evidenciar, ainda, outro fator relevante para a diferenciação entre o direito ao apagamento de dados e o direito ao esquecimento. Ainda que existam diversas acepções do direito ao esquecimento, é possível afirmar, sem pretensão de criar uma definição compreensiva desse direito, que o tempo desempenha um papel fundamental para a sua configuração (BUNN, 2015, p. 338; FINOCCHIARO, 2015, p. 31; MEZZANOTTE, 2009, p. 123). A noção de tempo é intrínseca à compreensão do direito ao esquecimento. Já o direito ao apagamento pode ser exercido em várias situações, que podem ou não envolver a

passagem do tempo (BUNN, 2015, p. 338). No caso de dados tratados ilicitamente, por exemplo, não é preciso o decurso de um lapso de tempo para que a possibilidade de apagamento se configure.

Ao analisar a proposta de Regulamento, Mantelero considera que a noção de direito ao esquecimento adotada no Regulamento é diferente do conceito definido pela jurisprudência da Europa e dos Estados Unidos. O autor recorda que, em casos envolvendo a noção tradicional de direito ao esquecimento, não existe sequer a possibilidade de retirar o consentimento, já que, no que diz respeito à publicação original, o interesse público na informação faz com que o consentimento não seja considerado relevante. Segundo Mantelero, a representação do direito ao esquecimento como direito de ter os dados pessoais completamente removidos é consistente com a noção tradicional de "*droit à l'oubli"*, mas tem um escopo mais amplo, uma vez que o apagamento de dados não está apenas relacionado à perda de interesse em eventos passados, mas também a outras situações, que não dizem respeito à dicotomia mídia/vida individual (2013, p. 233).

4.2 A NCII, o apagamento e o esquecimento

Como já mencionado nos capítulos anteriores,[87] a disseminação de imagens íntimas de uma pessoa se enquadra como tratamento de dados pessoais, de acordo com o Regulamento Geral de Proteção de Dados. A imagem de uma pessoa pode constituir dado pessoal na forma do artigo 4.º, número 1, do Regulamento, por ser informação relativa a uma pessoa singular identificada ou identificável. Tal enquadramento já havia sido comentado inclusive pelo Grupo de Trabalho do Artigo 29.º, nas Diretrizes sobre reconhecimento facial (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2012, p. 4). Além disso, imagens íntimas, por serem dados relativos à vida sexual do indivíduo, são consideradas dados sensíveis, na forma do artigo 9.º, número 1, do RGPD, tendo seu tratamento, por regra, proibido.

A publicação de um dado pessoal constitui tratamento, na forma do artigo 4.º, n.º 2, do RGPD, que o define como "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou

[87] tópicos 2.1 e 3.4

não automatizados", incluindo a "divulgação por transmissão, difusão ou qualquer outra forma de disponibilização". No caso, a base legal capaz de autorizar esse tratamento seria o consentimento.[88] Sendo assim, se a pessoa retratada não deu seu consentimento através de uma manifestação de vontade, livre, específica, informada, inequívoca e explícita, a disseminação de suas imagens íntimas constitui tratamento ilícito de dados. Desse modo, é possível concluir que uma pessoa que teve suas imagens íntimas disseminadas sem seu consentimento terá o direito de solicitar o apagamento de seus dados pessoais na forma do artigo 17.º, n.º 1, alínea d), tal como sugerido pela Comissão Europeia nas respostas às perguntas parlamentares sobre a disseminação não consensual de imagens íntimas (EUROPEAN COMMISSION, 2015, 2017).

Contudo, é preciso fazer uma distinção importante no que toca à disseminação não consensual de imagens íntimas. No caso, trata-se de uma publicação que é ilícita pelo fato de conter dados sensíveis sem autorização do titular para seu tratamento, em violação ao disposto no artigo 9.º, número 1 e número 2, alínea a), do Regulamento. O direito envolvido, no caso da NCII, não é propriamente o de não estar indefinidamente ligado a informações sobre o próprio passado. O tempo não é um fator relevante para que se configure a ilicitude do tratamento nesse caso. A publicação dos dados já nasce ilícita, não se torna ilícita com o decurso do tempo. Por isso, não se trata de um caso de direito ao esquecimento, ao menos não na sua acepção tradicional, discutida no tópico 4.1.1. A NCII também se diferencia, em parte, da situação descrita no caso *Google Spain*[89]. Naquele cenário, a publicação original pelo jornal *La Vanguardia* foi feita por ordem do Ministério do Trabalho e dos Assuntos Sociais, tendo como finalidade publicitar ao máximo a venda em hasta pública, para atingir o maior número de licitantes. Era, portanto, lícita, ao contrário do que ocorre na NCII. Isso significa que o pedido de apagamento feito por uma vítima de NCII poderá ter como alvo a publicação original, e não somente a sua indexação.

Um ponto importante a ser examinado é a quem pode ser direcionado o pedido de apagamento de dados em casos de NCII. A proteção de dados pessoais, como já mencionado, foi tradicionalmente aplicada ao tratamento de dados armazenados em bancos de dados, como no caso de hospitais, ou de empresas que geram dados a partir do

[88] Tendo em conta que não se configuram situações de tratamento necessário para o cumprimento de obrigações, para a proteção de interesses vitais do titular, para efeitos de medicina preventiva ou do trabalho, ou para interesse público, por exemplo, que estão descritas nas alíneas b) a j) do artigo 9.º do RGPD.
[89] Tópico 4.1.2.

monitoramento das atividades do usuário, por exemplo. Esse tipo de dado é diferente dos dados publicados por usuários de plataformas e redes sociais, embora ambos possam constituir dados pessoais[90] (KELLER, 2018, p. 309). Como ressalta Keller, a estrutura da proteção de dados europeia surgiu de uma era em que o tratamento de dados dizia respeito a bancos, empregadores, médicos, e outras entidades. Por ter sido desenhada tendo bancos de dados em mente, tal estrutura fornece um bom quadro regulatório para muitas das atividades desempenhadas por empresas que atuam na Internet, como recolha, conservação e monitoramento ("tracking"). Porém, o surgimento e a expansão de redes sociais e plataformas que suportam publicações do usuário criaram dificuldades em aplicar a estrutura de proteção de dados a casos de expressão do usuário (2018, p. 307).

Como disposto no artigo 17.º, o pedido de apagamento deve ser feito ao responsável pelo tratamento (*controller*, na versão em inglês). O Regulamento define "responsável pelo tratamento" como "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais" (artigo 4.º, n.º 7, do RGPD). Outro conceito central utilizado no Regulamento é o de subcontratante (*processor*, em inglês), que é a "pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes" (artigo 4.º, n.º 8, do RGPD). Como já visto,[91] a disseminação não consensual de imagens íntimas é feita, normalmente, através de redes sociais, *sites* pornográficos convencionais e *sites* dedicados a "*revenge porn*". O conteúdo publicado nessas páginas é, por regra, compartilhado pelo próprio usuário, e não criado pelo *website* ou rede social em que foi publicado. O apagamento deverá ser efetuado, portanto, por aquele que for considerado o responsável pelo tratamento dos dados pessoais sensíveis compartilhados. O Regulamento não fornece uma resposta clara, contudo, sobre quem será considerado o responsável pelo tratamento nesse caso.

Os tópicos a seguir têm como objetivo buscar compreender a quem poderá ser direcionado o pedido de apagamento conforme o artigo 17.º do Regulamento. Para isso, serão analisados os papeis de "responsável pelo tratamento" e "subcontratante", tendo em

[90] O GT 29 aborda esse tipo de dado pessoa no Parecer 5/2009, sobre redes sociais: "*The personal information a user posts online, combined with data outlining the users actions and interactions with other people, can create a rich profile of that person's interests and activities*" (2009, p. 4)(2009, p. 4).
[91] Tópico 1.2.

vista os usuários de redes sociais ou *sites* de compartilhamento e as próprias plataformas, no cenário da NCII. A discussão sobre o tema da responsabilidade civil pela violação de dados pessoais não será objeto do presente trabalho.[92]

4.2.1 O papel do usuário de rede social ou *site* de compartilhamento de imagens e vídeos

Primeiramente, é preciso destacar que muitos dos *sites* pornográficos nos quais é compartilhado conteúdo de NCII funcionam como redes sociais em vários aspectos. O termo *Porn2.0* foi adotado para descrever os *sites* pornográficos que se tornaram populares nos anos 2000, que apresentam ferramentas como *tags*, grupos de discussão, comentários e classificações de usuários para formar uma comunidade onde usuários podem explorar e compartilhar conteúdo (FREEMAN, 2007; MARSHALL, 2009). A título de exemplo, o *site* pornográfico *PornHub* estabelece em seus Termos e Condições a possibilidade de o usuário fazer *upload* e compartilhamento de vídeos. O *website* também ressalta que não tem qualquer responsabilidade pelo conteúdo submetido pelo usuário, e que não controla ou oferece qualquer garantia em relação a tal conteúdo (PORNHUB, 2020a). O *site*, assim como uma rede social, oferece ao usuário a possibilidade de ter "amigos", inscrever-se nos canais de outros usuários para acompanhar suas últimas publicações, bem como enviar mensagens privadas aos "amigos" (PORNHUB, 2020b).

Quanto ao usuário que publica as imagens íntimas de uma pessoa em uma rede social ou plataforma, cabe fazer algumas considerações. Ao definir o que se entende por responsável pelo tratamento de dados, o Regulamento, em princípio, não limita qual o tipo de ator que pode assumir esse papel, mencionando que pode se tratar de uma pessoa singular ou coletiva (ALSENOY, 2019, p. 49). É verdade que, em geral, nas normas relativas à proteção de dados pessoais, os indivíduos são vistos sobretudo como

[92] Quando se fala em "responsável pelo tratamento", a ideia de responsabilidade assume o sentido de "*role-responsibility*", ou seja, remete a um dever atribuído a uma pessoa, que é responsável pelo desempenho desse dever, na divisão proposta por Hart (1975, p. 212). Mafalda Miranda Barbosa chama atenção para essa distinção, ressaltando que o conceito de "responsável pelo tratamento" remete à responsabilidade enquanto assunção de um especial encargo, que implica deveres especiais de salvaguarda dos dados pessoais alheios. Tal noção é diferente da ideia de "*liability*", que remete à responsabilidade civil. É possível, contudo, que o responsável pelo tratamento (*controller*) se torne responsável, no sentido da "*liability*", pela violação dos deveres de proteção de dados pessoais (2018, pp. 424–425) No entanto, essa "*liability*" não será o foco do presente trabalho.

"beneficiários" da proteção. Contudo, em algumas situações, poderão ser considerados como responsáveis pelo tratamento (ALSENOY, 2015, p. 5). Um usuário de uma rede social que publica dados pessoais de outras pessoas pode livremente determinar a finalidade daquela divulgação de dados. Quanto aos meios de tratamento, apesar de poder alterar algumas das configurações, o usuário, em geral, não tem controle sobre a maneira como o tratamento é conduzido dentro da plataforma que escolhe. Ainda assim, o indivíduo tem o poder de decidir se deseja publicar um determinado dado e qual plataforma ele usará para isso. Dessa forma, pode-se considerar que ele efetivamente determina as finalidades e meios de tratamento quando publica dados de terceiros através de uma rede social, por exemplo (ALSENOY, 2019, pp. 413–414; EECKE e TRUYENS, 2010, pp. 537–538).

O artigo 2.º, n.º 2, alínea c), do RGPD determina que o Regulamento não se aplica ao tratamento efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas. Essa é a chamada *household exemption*, que também tinha previsão no artigo 3.º, n.º 2, segundo travessão, da Diretiva 95/46/CE. O considerando (18) do Regulamento também dispõe que atividades pessoais ou domésticas podem incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrônico no âmbito dessas atividades. É preciso verificar, portanto, se a publicação de dados pessoais de terceiros pelo usuário de um *site* ou rede social é considerada uma atividade exclusivamente doméstica. No caso *Lindqvist,*[93] o Tribunal de Justiça da União Europeia fornece alguns parâmetros para compreender a questão. No

[93] O Tribunal também se pronunciou sobre a *household exemption* em outros casos. No caso *Ryneš,* que dizia respeito ao uso de videovigilância para fins de segurança do lar, o TJUE considerou que "a exploração de um sistema de câmara que dá lugar a uma gravação vídeo de pessoas, guardada num dispositivo de gravação contínua, como um disco rígido, sistema esse instalado por uma pessoa singular na sua casa de família, para proteger os bens, a saúde e a vida dos proprietários dessa casa, e que vigia igualmente o espaço público não constitui um tratamento de dados efetuado no exercício de atividades exclusivamente pessoais ou domésticas, na aceção desta disposição." (TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, 2013, par. 35). No caso *Jehovan todistajat*, o Tribunal considerou uma comunidade religiosa conjuntamente responsável com os seus membros pregadores pelo tratamento de dados pessoais efetuado por estes últimos no âmbito de uma atividade de pregação porta a porta organizada, coordenada e promovida pela comunidade. O Tribunal afirmou que o tratamento de dados efetuado no âmbito do exercício de atividade de pregação porta a porta tem o objetivo de difundir a fé da comunidade de testemunhas de Jeová junto de pessoas que não pertencem ao círculo dos membros pregadores, sendo, portanto, uma atividade dirigida para o exterior da esfera privada dos membros. Além disso, tendo em conta que alguns dos dados recolhidos eram transmitidos às congregações, que conservam listas de pessoas que já não querem receber visitas dos membros, o que indica que alguns dos dados recolhidos são acessíveis a um número potencialmente indefinido de pessoas. Assim, a exceção prevista no artigo 3.º, número 2, segundo travessão, da Diretiva 95/46/CE não se aplica (2018, par. 44-45).

caso, a Sra. Lindqvist exercia funções de catequista em uma paróquia na Suécia, e frequentou um curso de informática no âmbito do qual devia criar uma página da Internet. Assim, em 1998, criou páginas com o objetivo de fornecer informações aos paroquianos que preparam o crisma. As páginas foram criadas em sua casa, a partir de seu computador pessoal. O administrador da *webpage* da Igreja da Suécia, a pedido de Lindqvist, criou links entre as referidas páginas e o *site* da Igreja (TJUE, 2003, par. 12).

As páginas continham informações sobre a própria Lindqvist e 18 dos seus colegas de paróquia, incluindo nome completo e, às vezes, somente o nome próprio. Também continha a descrição das funções desempenhadas pelos colegas, bem como dos seus hábitos de lazer, em termos ligeiramente humorísticos. O *site* apresentava, em muitos casos, a situação familiar dos colegas, o número de telefone, e outros dados. Além disso, a página mencionava que uma das colegas tinha uma lesão num pé e que estava com baixa por doença a meio tempo. Lindqvist não informou seus colegas sobre a criação das páginas, não obteve o seu consentimento, nem declarou a sua atuação ao organismo público para a proteção dos dados transmitidos por via informática. Logo que tomou conhecimento de que alguns colegas não apreciaram as páginas, Lindqvist suprimiu-as. O Ministério Público intentou uma ação contra B. Lindqvist, por violação da Lei Sueca de Proteção de Dados (TJUE, 2003, par. 13-15).

Uma das questões referidas ao Tribunal de Justiça da União Europeia foi se a conduta de Lindvist poderia ser abrangida por qualquer das exceções previstas no artigo 3.º, número 2, da Diretiva 95/46/CE. Quanto à aplicação da *household exemption*, o Tribunal determinou que tal exceção deveria ser "interpretada como tendo unicamente por objecto as actividades que se inserem no âmbito da vida privada ou familiar dos particulares", o que não era o caso do tratamento feito por Lindqvist, que consistia na publicação dos dados na Internet, de modo que estes eram disponibilizados a um número indefinido de pessoas (TJUE, 2003, par. 47).

No Parecer 5/2009 sobre redes sociais, o GT 29 também forneceu alguns esclarecimentos sobre a possibilidade de um usuário de rede social desempenhar o papel de *controller*. O GT 29 afirmou que a maioria dos usuários de redes sociais seria considerada titular de dados pessoais (pessoa em causa, nos termos da Diretiva). Contudo, apresentou dois critérios para definir se a *household exemption* seria ou não aplicada. Em primeiro lugar, importa observar se a rede social é usada como uma plataforma de colaboração para

uma associação ou empresa. Se o usuário age em benefício de uma empresa, ou se o SNS é utilizado com propósitos comerciais, políticos ou filantrópicos, a exceção não se aplica, e o usuário normalmente assume o papel de responsável pelo tratamento. O segundo critério apresentado pelo GT 29 é o acesso à informação do perfil. Quando o acesso às informações publicadas se estende para além de contatos selecionados, considera-se que vai além da esfera exclusivamente pessoal ou doméstica do usuário. Assim, aquele que decide estender suas publicações para além de uma rede de amigos pré-selecionada poderá assumir o papel de *controller* (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2009, p. 5).

Contudo, é importante ressaltar que, anteriormente à adoção do RGPD, e no âmbito das discussões sobre a reforma da Diretiva 95/46/CE, o Grupo de Trabalho do Artigo 29.º afirmou que a exceção prevista no artigo 3.º, n.º 2, da Diretiva tinha um âmbito irrealisticamente restrito, que já não era capaz de refletir a capacidade dos indivíduos para tratar dados para atividades pessoais ou domésticas. O GT 29 considerou que o acesso à tecnologia da informação por parte dos "cidadãos comuns" expandiu muito desde a elaboração da Diretiva nos anos 90, o que causa certa insegurança jurídica, já que indivíduos podem disponibilizar informações sobre si e terceiros a qualquer pessoa instantaneamente (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2013, pp. 2–3). O Grupo de Trabalho demonstrou preocupação com a possibilidade de centenas de milhões de usuários de redes sociais com perfis públicos serem considerados responsáveis pelo tratamento no âmbito do Regulamento (2013, p. 9).

Nesse sentido, sugeriu cinco perguntas a serem feitas para determinar se um certo tratamento está ou não abarcado pela exceção estabelecida no artigo 2.º, n.º 2, alínea c), do RGPD: a) "os dados pessoais são divulgados a um número indefinido de pessoas, em vez de a uma comunidade limitada de amigos, familiares ou conhecidos?"; b) "os dados pessoais referem-se a indivíduos que não têm nenhuma relação pessoal ou familiar com a pessoa que os publica?"; c) "a escala e a frequência do tratamento de dados pessoais sugerem atividade profissional ou a tempo integral?"; d) "há evidências de vários indivíduos agindo juntos de forma coletiva e organizada?"; e) "existe potencial impacto adverso sobre os indivíduos, incluindo intrusão em sua privacidade?"[94] (ARTICLE 29

[94] "*Is the personal data disseminated to an indefinite number of persons, rather than to a limited community of friends, family members or acquaintances?*

DATA PROTECTION WORKING PARTY, 2013, p. 9, tradução nossa). O GT 29 ressalta, porém, que nenhum dos critérios apontados é, por si só, necessariamente determinante, e que uma combinação desses fatores pode ser usada para determinar se um tratamento está ou não no âmbito da *household exemption* (2013, p. 9).

Em 2019, no caso *Buivids*, o Tribunal de Justiça da União Europeia se pronunciou sobre uma situação que também guarda semelhanças, em alguns aspectos, com a disseminação não consensual de imagens íntimas. No caso, Sergejs Buivids filmou suas declarações no âmbito de um procedimento contraordenacional, quando se encontrava nas instalações de uma esquadra policial. Na filmagem, são visíveis dois agentes de polícia, e suas atividades na esquadra. Buivids publicou o vídeo na plataforma *YouTube*, sem ter informado os agentes da polícia, na sua qualidade de pessoa em causa, do tratamento de dados que lhes diziam respeito. Também não havia comunicado à Agência Nacional de Proteção de Dados as informações relativas à finalidade da gravação do vídeo em causa e da sua publicação. O TJUE considerou que a publicação da filmagem, sem restrição de acesso, num *site* em que os utilizadores podem carregar, visualizar e partilhar vídeos, tornando assim acessíveis dados pessoais a um número indefinido de pessoas, não se insere no âmbito do exercício de atividades exclusivamente pessoais ou domésticas. Citou como precedentes os casos *Lindqvist*, *Ryneš* e outros (TJUE, 2019, par. 43).

Brendan Van Alsenoy chama atenção para o fato de que, em comparação à Diretiva, o Regulamento acrescentou o considerando (18), que menciona como exemplo de atividade pessoal ou doméstica o uso de redes sociais.[95] Esse pode ser um indício de que o Tribunal adotará uma interpretação mais ampla da *household exemption*. Contudo, o Regulamento manteve no artigo 2.º, n.º 2, alínea c), o mesmo texto adotado anteriormente

---

Is the personal data about individuals who have no personal or household relationship with the person posting it?
Does the scale and frequency of the processing of personal data suggest professional or full-time activity?
Is there evidence of a number of individuals acting together in a collective and organised manner?
Is there the potential adverse impact on individuals, including intrusion into their privacy?" (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2009, p. 3).

[95] Por essa razão, Alexandre Dias Pereira considera que, em geral, as atividades de usuários de redes sociais estão incluídas na *household exemption*, e, por isso, não estão sujeitas ao RGPD. Contudo, ressalta que o referido considerando também determina que o Regulamento ainda será aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas. Diante disso, afirma que as plataformas serão responsáveis pelo tratamento. Os operadores de redes sociais e plataformas, segundo Pereira, não são considerados prestadores intermediários de serviços para efeitos do regime de responsabilidade estabelecido na diretiva sobre comércio eletrônico (2019, p. 1170).

pela Diretiva, o que indica que o valor do julgamento *Lindqvist* e de outros julgamentos na interpretação da exceção se mantém em princípio (2019, p. 416). No caso da NCII, pode-se dizer que a atividade de publicar as imagens e vídeos em *sites* ou redes sociais não se insere no âmbito da vida privada ou familiar do responsável pela publicação. Verifica-se, em primeiro lugar, que os dados são acessíveis a um número indefinido de pessoas, havendo possibilidade de serem visualizados e compartilhados sem restrição de acesso, o que, de acordo com o entendimento do TJUE nos casos *Lindqvist* e *Buivids*, por exemplo, indica a não aplicação da exceção prevista (TJUE, 2003, par. 47; 2019, par. 43). Para além disso, como já visto,[96] observa-se que a NCII geralmente tem impacto adverso sobre os indivíduos retratados, incluindo intrusão em sua privacidade, o que foi um dos critérios apontados pelo Grupo de Trabalho do Artigo 29.º para ajudar na identificação de situações fora do âmbito da exceção do artigo 2.º, n.º 2, alínea c) (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2013, p. 4). Assim, é possível que o indivíduo que publica as imagens e vídeos de NCII seja considerado o responsável pelo tratamento de dados.

Considerar uma pessoa singular usuária de rede social ou *site* como responsável pelo tratamento pode acarretar alguns problemas práticos para os quais ainda não há respostas claras. Ter um indivíduo como "*controler"* poderá significar impor a ele as mesmas obrigações impostas a qualquer outro responsável pelo tratamento. No entanto, como relembram Helberger e Hoboken, a norma europeia de proteção de dados não foi escrita tendo em mente "*amateur data controllers*" ("responsáveis pelo tratamento amadores") nem redes sociais. Algumas previsões em matéria de proteção de dados até podem ser facilmente aplicadas, em teoria, a usuários individuais. Um exemplo é a obrigação de obter o consentimento dos titulares de dados pessoais antes da publicação de fotos, vídeos, ou outros dados pessoais, informando sobre a publicação e a sua finalidade, que pode fazer parte de uma norma social de etiqueta na Internet. Contudo, na prática, a aplicação dessas previsões pode gerar questões difíceis. Helberger e Hoboken chamam atenção para o fato de que, para a maioria dos usuários de redes sociais, expressões como "dados pessoais", "dados sensíveis" e "consentimento" são "termos abstratos e com pouco significado prático" (2010, p. 104).

[96] Tópico 1.3.

Algumas previsões do Regulamento simplesmente não se adaptam bem ao contexto de uma pessoa singular usuária de rede social ou *site*. Pode ser difícil, por exemplo, exigir que um "*amateur data controller*" garanta a segurança do tratamento de dados, "incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas" (princípio da integridade e confidencialidade, previsto no artigo 5.º, n.º 1, alínea f), do RGPD).[97] Da mesma forma, parece difícil aplicar à pessoa singular a exigência prevista no artigo 5.º, n.º 1, alínea e), do Regulamento, que determina que os dados sejam "conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados" (princípio da limitação da conservação), e a previsão da alínea d), que determina que os dados devem ser exatos e atualizados sempre que necessário (princípio da exatidão) (ALSENOY, 2019, pp. 454–455; HELBERGER e HOBOKEN, VAN, 2010, p. 105).

Ao analisarem a aplicação da Diretiva 95/46/CE para usuários e operadores de redes sociais, Eecke e Truyens comentam o fato de que, no caso dos perfis de redes sociais, as bases legais que autorizam o tratamento de dados muitas vezes não são atendidas por usuários que publicam dados de terceiros. Isso ocorre especialmente no caso de dados sensíveis, em que é exigido o consentimento explícito do titular de dados pessoais. Muito frequentemente, perfis de redes sociais publicam dados sensíveis direta ou indiretamente. Um texto em um blog sobre a doença de um amigo, ou contendo fotos de atividades religiosas, é um exemplo desse tipo de publicação. Muitos desses perfis podem ser considerados ilícitos à luz do entendimento do caso *Lindqvist* (2010, p. 543). Assim, há possibilidade de que as autoridades de controle sejam sobrecarregadas com reclamações relacionadas a imagens ou comentários sobre terceiros em redes sociais (EECKE e TRUYENS, 2010, p. 546; WONG, 2009, p. 143). Nesse sentido, Eecke e Truyens

[97] Tal dever é previsto também no artigo 32.º do Regulamento, que prevê que o responsável pelo tratamento e o subcontratante devem adotar medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: a pseudonimização e a cifragem de dados; a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; e um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento. Alexandre Dias Pereira aborda os deveres do responsável pelo tratamento em seu artigo (2019, pp. 1170–1180).

questionaram a aptidão da então vigente Diretiva 95/46/CE para tratar do caso das redes sociais (2010, p. 546).

Tendo em conta o direito ao apagamento previsto no artigo 17.º e as situações de disseminação não consensual de imagens íntimas, considerar a pessoa singular que fez a publicação no *site* ou rede social como único responsável pelo tratamento de dados poderá significar, na prática, uma dificuldade de garantir o cumprimento do apagamento. O responsável pode ser uma pessoa desconhecida para o titular de dados pessoais, e pode não ser possível contactá-lo se ele utilizar uma identidade virtual, por exemplo. O responsável também pode simplesmente não responder aos pedidos individuais. Nessas situações, o titular de dados pode não conseguir exigir seus direitos (HELBERGER e HOBOKEN, VAN, 2010, p. 108).

4.2.2 O papel do provedor do serviço de rede social ou *site* de compartilhamento de imagens ou vídeos

Nesse ponto, é possível perguntar se o pedido de apagamento de dados no caso de NCII poderia ser feito ao próprio *site* ou rede social. Para isso, é preciso examinar se a plataforma poderá ser considerada como responsável pelo tratamento. Geralmente, o provedor do serviço de rede social (também referido como *SNS provider*)[98] pode ser facilmente identificado como *controller* em relação a tratamentos de dados como: a) coleta e uso de dados explicitamente solicitados (como os dados requisitados para inscrição dos usuários na rede social, como nome, idade, local de residência); b) tratamento de dados de usuários para propósitos de publicidade direcionada (como dados relativos ao comportamento do usuário); c) tratamento de dados de usuários com o objetivo de melhorar a qualidade do serviço ou fornecer ferramentas adicionais (como, por exemplo,

[98] O presente trabalho adota o termo "provedor de serviço de rede social" para referir-se às plataformas de comunicação online que permitem a conexão entre usuários e a criação de redes de pessoas conhecidas. O termo em inglês *"Social Network Service Provider*" ou "*SNS Provider*" foi adotado pelo GT 29 no Parecer 5/2009 (2009, p. 4). Outros termos usados para esses provedores de serviço são: "*social network operators*" (EECKE e TRUYENS, 2010), "operadores de redes sociais" (PEREIRA, 2019, p. 1170) e "*online social network providers*" ou "*OSN providers*" (ALSENOY, 2019). Em geral, *sites* que possibilitam o compartilhamento de conteúdo pelo usuário também são referidos como "*online service providers*" (KELLER, 2018), ou simplesmente "*providers*" (SARTOR, 2013), e "plataformas de partilha de conteúdo" (PEREIRA, 2019, p. 1170). Em geral, o presente trabalho também adota o termo "plataforma" para referir-se tanto a provedores de redes sociais (como *Facebook* e *Twitter*), como *sites* de compartilhamento de conteúdo de usuários em geral.

uso de técnicas de reconhecimento facial) (ALSENOY, 2019, p. 410). O GT 29 se pronunciou nesse sentido no Parecer 5/2009, sobre redes sociais[99] (2009, p. 5). Assim, quando o provedor do serviço de rede social atua como proprietário de bancos de dados e sistemas de armazenamento contendo registros dos cliques, compras e comportamento *online* dos usuários, é visto como responsável pelo tratamento. Já quanto ao conteúdo gerado e compartilhado pelos usuários da rede social, incluindo imagens, vídeos e comentários contendo dados pessoais, o papel desempenhado pelo *SNS provider* não é tão claro (KELLER, 2018, p. 308).

Existe a possibilidade de que o provedor do serviço de rede social seja considerado responsável pelo tratamento mesmo em casos de publicação de conteúdo gerado pelo usuário. Brendan Van Alsenoy et al. entendem que o *SNS Provider* determina as próprias finalidades do tratamento de dados que realiza. Na maioria dos casos, o tratamento é feito tendo como principal finalidade o ganho monetário. Além das operações estritamente necessárias para fornecimento dos serviços, esse tipo de plataforma geralmente pressupõe tratamentos adicionais, como aqueles que facilitam o marketing direto. Da mesma forma, os autores acrescentam que o *SNS Provider* determina quase inteiramente os meios para alcançar essas finalidades, ao configurar e operar os serviços usufruídos pelos usuários, escolher como tornar a informação disponível a terceiros para propósitos de marketing, determinar quanto espaço será destinado à publicidade etc. (2009, p. 70).

Alsenoy et al argumentam que o provedor do serviço de rede social define tanto as finalidades como os meios para o serviço como um todo. Quanto ao conteúdo que é publicado na plataforma, geralmente exerce pouco controle no momento em que a informação é submetida pelo usuário. Não obstante, os autores defendem que a o provedor do serviço de rede social também age como responsável pelo tratamento ao fornecer o serviço e distribuir essa informação. Assim, consideram que o *SNS Provider* pode ser tido como *controller* em conjunto com o usuário, já que, quando a informação é disponibilizada

[99] "*SNS providers are data controllers under the Data Protection Directive. They provide the means for the processing of user data and provide all the "basic" services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the use that may be made of user data for advertising and marketing purposes – including advertising provided by third parties* " (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2009, p. 5).

pelo usuário para o operador, este realiza operações naqueles dados pessoais, para as quais já havia determinado as finalidades e os meios previamente (2009, p. 71).

Hoboken e Helberger chamam atenção para o fato de que o modelo de negócios da maioria dos serviços de redes sociais é construído em torno da atividade de publicação de conteúdos pessoais pelos usuários em seus perfis e nos perfis de outros usuários. Os *SNS providers* fornecem meios e recursos que possibilitam que o usuário se envolva em atividades que oferecem risco à privacidade de outros sujeitos, ou atividades ilegais, e podem até, de certa maneira, se beneficiar dessas atividades. Assim, argumenta-se que não é aceitável que o provedor do serviço de rede social negue qualquer responsabilidade sobre o que acontece nos perfis de seus usuários. Contudo, é preciso reconhecer que seria invasivo e praticamente impossível determinar que o provedor do serviço de rede social fosse obrigado a supervisionar e controlar todas as atividades de seus usuários, sendo razoável atribuir alguma responsabilidade aos usuários. Os autores consideram essa situação como um dilema, já que os usuários não têm o conhecimento e os recursos técnicos e organizacionais necessários para serem responsáveis pelo tratamento. A solução sugerida pelos autores é um modelo de "responsabilidade compartilhada", ou uma divisão de tarefas para garantir a conformidade do tratamento dos dados pessoais que constam dos perfis dos usuários (2010, p. 106). Nessa perspectiva, usuários e redes sociais seriam conjuntamente responsáveis pelo tratamento (artigo 26.º do RGPD).[100]

O Tribunal de Justiça da União Europeia já adotou uma abordagem ampla do conceito de responsável pelo tratamento, citando a necessidade de garantir a proteção completa e efetiva dos titulares de dados pessoais.[101] Como visto na primeira parte do

[100] A diferença entre responsáveis conjuntos pelo tratamento e diferentes responsáveis pelo tratamento pode ser difícil de identificar em algumas situações. O CEPD (*European Data Protection Board, EDPB*), em Diretrizes publicadas recentemente, afirma que a responsabilidade conjunta pode ser identificada quando há decisões convergentes de duas ou mais entidades sobre as finalidades e os meios do tratamento. Tais decisões serão convergentes, por exemplo, se o tratamento depender da participação de ambas as partes. (2020b, p. 18) Pode-se argumentar que a publicação do NCII dependerá tanto da decisão do usuário de publicar os dados através do *site* ou rede social, quanto da decisão da própria plataforma de viabilizar ferramentas de compartilhamento, sugestão e organização de conteúdo em um *feed*, por exemplo.

[101] Um exemplo dessa interpretação é o caso *Facebook Fanpages* ("*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*"), em que o Tribunal considerou a *Facebook Inc.* e a *Facebook Ireland* responsáveis pelo tratamento em conjunto com o administrador de uma página de fãs alojada no *Facebook*, relativamente às informações sobre visitantes da página, fornecidas ao administrador através da ferramenta *Facebook Insight*, contendo dados recolhidos através de *cookies* (TJUE, 2018, par. 26-31).

capítulo,[102] no caso *Google Spain*, o Tribunal decidiu que uma interpretação restritiva do conceito de "responsável pelo tratamento" seria contrária não só à redação da diretiva, mas também a seus objetivos. O caso demonstra, dessa forma, que a ausência de controle sobre o conteúdo original referenciado pelo *Google* não impediu a sua classificação como *controller* (BUCKLEY, 2020, p. 93).

A posição adotada pelo *Information Commission's Office*, no Reino Unido, sobre a questão foi de que, mesmo se o conteúdo publicado pelo usuário não for moderado previamente pelo *site* ou rede social, a plataforma pode ser considerada responsável pelo tratamento. Se o *site* apresenta termos e condições que determinam qual o conteúdo aceitável, e se tiver o poder de remover conteúdos que violem esses termos, pode-se dizer que determina, até certo ponto, as finalidades e os meios pelos quais os dados são tratados (2013, p. 11). Cumpre lembrar que os termos de serviço da rede social *Facebook*, por exemplo, determinam que o usuário não poderá compartilhar conteúdo que constitua infração aos termos, padrões da comunidade, e outros termos e políticas aplicáveis, além de proibir conteúdo "ilegal, enganador, discriminatório ou fraudulento", ou que desrespeite os direitos de outra pessoa (FACEBOOK, 2020b). Nos Padrões da Comunidade, o site afirma que remove por padrão imagens sexuais para impedir o compartilhamento de conteúdo de menores ou não consentido (FACEBOOK, 2020a). O *site* pornográfico *PornHub* também estabelece uma série de conteúdos não autorizados em seus Termos e Serviços, incluindo atividade sexual não consensual e "*revenge porn*". Também se reserva o direito de, a seu próprio critério, remover qualquer conteúdo do *site*. Adverte, ainda, que removerá conteúdos que envolvam menores de idade, ou qualquer forma de força, fraude ou coerção (PORNHUB, 2020a).[103]

Alguns autores se posicionam de forma contrária à classificação desse tipo de plataforma como responsável pelo tratamento, tendo como argumento o nível de influência exercida pelo *site* ou rede social no conteúdo que é disponibilizado em suas páginas. Em regra, como já mencionado, esses provedores de serviços não determinam o conteúdo dos *posts* e têm pouco controle sobre a fase anterior à publicação (BUCKLEY, 2020, p. 94). Assim, argumenta-se que essas plataformas não são responsáveis pelo tratamento, por não terem o controle sobre o que é publicado. Nessa perspectiva, as plataformas são tidas como

[102] Tópico 4.1.2
[103] Existem previsões semelhantes em *sites* como o *XVideos* (2020) e o *YouPorn* (YOUPORN, 2016).

subcontratantes[104] seguindo as instruções dos usuários (responsáveis pelo tratamento) (KELLER, 2018, p. 323).

Nesse sentido, destaca-se uma decisão espanhola em que a *Audiencia Nacional*, ao aplicar a legislação nacional que transpunha a Diretiva 95/46/CE, considerou que uma plataforma que armazena um *blog* não é responsável pelo tratamento relativamente aos dados publicados pelo nesse *blog*. No caso, o titular dos dados havia solicitado o apagamento de dados pessoais publicados em um *blog* hospedado na plataforma *Blogger*. A autoridade espanhola de proteção de dados pessoais (AEPD) havia determinado que o *Google Spain,* enquanto proprietário do *Blogger*, procedesse ao apagamento dos referidos dados do *blog*, além da desindexação dos *links* para os dados do motor de busca *Google*. O Tribunal deu provimento parcial ao recurso, mantendo a decisão quanto à obrigação de desindexação dos dados, mas determinou que a atividade do *Google* em relação ao *blog* era de meramente armazenar o conteúdo que o editor decidia publicar, e que não houve comprovação de qualquer tratamento adicional, para além daquele decidido livremente pelo editor do *blog*. Tal atividade, segundo o tribunal, não converte o *Google* em responsável pelo tratamento dos dados publicados no *blog*, sendo impossível impor a ele a obrigação de apagamento. O responsável pelo tratamento, de acordo com o Tribunal, é exclusivamente o responsável pelo *blog*, sendo o *Google* um mero intermediário (AUDIENCIA NACIONAL, 2014).

Keller comenta que classificar *SNS providers* como responsáveis pelo tratamento de dados gerados pelo usuário pode significar sujeitá-los a obrigações que não podem cumprir. Keller cita como exemplo o provedor de serviço de rede social *Twitter*. Sempre que um usuário publicasse um *tweet* sobre o estado de saúde de um amigo, por exemplo, o *Twitter* estaria fazendo um tratamento ilícito de dados a partir do momento da postagem, e seria obrigado a obter o consentimento da pessoa mencionada no *tweet*, que poderia nem

[104] Alsenoy vê com certo estranhamento a interpretação segundo a qual o provedor de serviço de rede social é um subcontratante, quando leva em consideração as disposições sobre realização de tratamento em subcontratação. O artigo 28, número 3, alínea a), do RGPD dispõe que haja a vontade, por parte do subcontratante, de tratar os dados apenas mediante as instruções do responsável pelo tratamento, o que não acontece na dinâmica entre usuários e o provedor de serviço de rede social. O artigo também dispõe que essa vontade deve ser expressa na forma de um contrato. Alsenoy sugere que os *SNS providers* não sejam considerados subcontratantes, mas responsáveis pelo tratamento separados, cujo controle se estende em diferentes partes do tratamento (2019, p. 411).

sequer ser usuária da plataforma[105] (2018, pp. 310, 323). No mesmo sentido, Sartor ressalta que tais plataformas são incapazes de filtrar ou remover toda a informação ilegal, considerando o grande volume de dados publicados online diariamente. Considerá-las como *controllers* poderá ter o efeito prático de fazer com que interfiram no conteúdo publicado pelos usuários, o que, por um lado, reduziria sua liberdade, e, por outro, traria custos muito altos às plataformas (2013, p. 4).

Giovanni Sartor argumenta que, no caso de material livremente publicado pelos usuários, os *SNS providers* são "meros facilitadores neutros do compartilhamento de informações geradas pelo usuário" (2013, p. 3, tradução nossa),[106] ainda que atuando no seu próprio interesse (2013, p. 3). Desse modo, ao desempenhar uma atividade neutra em relação ao conteúdo gerado pelo usuário, o *SNS provider* age apenas como subcontratante, não tendo obrigação de monitorar ou verificar as informações que recebe do responsável pelo tratamento, seja em relação aos dados enviados, seja em relação aos meios pelos quais esses dados são tratados de forma neutra pela plataforma do *SNS Provider* (SARTOR, 2013, p. 5). Sartor propõe essa interpretação aplicando à definição de *controllers* e *processors* a lógica da Diretiva 2000/31/CE, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio eletrônico, no mercado interno (conhecida como "Diretiva sobre o comércio eletrônico" ou "*E-commerce Directive*").

Cumpre fazer um esclarecimento quanto à Diretiva 2000/31/CE. Tal diretiva tem o objetivo de contribuir para o correto funcionamento do mercado interno, garantindo a livre circulação dos serviços da sociedade da informação entre Estados-Membros. Dispõe, entre outros assuntos, sobre a responsabilidade de prestadores de serviço intermediários. Em seu artigo 14.º, determina que, em caso de prestação de um serviço da sociedade da informação que consista no armazenamento de informações prestadas por um destinatário do serviço (também conhecida como "*hosting*"), o prestador intermediário de serviço que armazena conteúdo de terceiros em sua plataforma não terá sua responsabilidade invocada em relação a conteúdos ilícitos publicados pelo usuário, se não tiver conhecimento do conteúdo ou atividade ilegal, ou se, a partir do momento em que tiver conhecimento da

[105] O GT29 afirmou, no Parecer n.º 5/2009 sobre redes sociais, que, como responsáveis pelo tratamento, os serviços de rede social não podem tratar dados sensíveis sobre usuários ou não usuários sem seu consentimento explícito (2009, p. 8).
[106] "*I shall only address the role of providers as neutral (though self-interested) enablers of the sharing of user-generated information [..]*" (SARTOR, 2013, p. 3).

ilicitude, atuar com diligência no sentido de retirar ou impossibilitar o acesso à informação (artigo 14, n.º 1, alínea a), da Diretiva 2000/31). A Diretiva também dispõe, no seu artigo 15.º, que os prestadores intermediários de serviço não serão submetidos a uma obrigação geral de vigilância sobre as informações que estes transmitam ou armazenem, ou uma obrigação geral de procurar ativamente fatos ou circunstâncias que indiciem ilicitudes. Redes sociais e *sites* que abrigam conteúdo publicado por usuários, por exemplo, seriam classificados como intermediários nesse cenário.

O artigo 1.º, n.º 5, alínea b), da Diretiva 2000/31/CE, no entanto, determina que esta não se aplica às questões respeitantes aos serviços da sociedade da informação abrangidas pelas Diretivas 95/46/CE e 97/66/CE. O considerando (14) da Diretiva 2000/31/CE também ressalta que a proteção dos indivíduos no que se refere ao tratamento dos dados pessoais "é regida exclusivamente pela Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e pela Directiva 97/66/CE […]", completando que "não é necessário tratar essa questão na presente directiva". Dessa forma, ao longo dos anos, as determinações da Diretiva 2000/31/CE sobre a responsabilidade dos prestadores de serviço intermediários foram, em geral, interpretadas como não aplicáveis à proteção de dados pessoais (GREGORIO, 2019, p. 3; KELLER, 2018, p. 357; SARTOR, 2013, p. 8).

Contudo, é preciso observar que o artigo 2.º, n.º 4, do Regulamento Geral sobre a Proteção de Dados Pessoais determina que o regulamento "não prejudica a aplicação da Diretiva 2000/31/CE, nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12.º a 15.º". Tal disposição, aparentemente, passa a autorizar a aplicação do disposto na Diretiva sobre o comércio eletrônico à proteção de dados pessoais. No entanto, Keller ressalta que o significado de tal disposição ainda está aberto à interpretação (2018, p. 358). Como aponta Sartor, o artigo 94.º do RGPD determina que "as remissões para a diretiva revogada são consideradas remissões para presente regulamento". Desse modo, a disposição que excluía a proteção de dados pessoais do âmbito de aplicação da Diretiva sobre comércio eletrônico ainda estaria em vigor, referindo-se, agora, ao RGPD, e não mais à Diretiva 95/46/CE. Ainda há dúvidas, portanto, quanto à possibilidade de se aplicar as disposições sobre

responsabilidade de intermediários da Diretiva 2000/31/CE ao contexto de proteção de dados pessoais (SARTOR, 2013, p. 8).

Analisando o direito ao apagamento previsto no artigo 17.º do RGPD, Sartor propõe que, nos casos de conteúdo publicado na plataforma por terceiros, o usuário que realiza a publicação seja o único responsável pelo tratamento, e a rede social ou *site* em que os dados foram publicados seja apenas subcontratante. Desse modo, o pedido de apagamento com base no artigo 17.º, n.º 1, do RGPD só poderá ser direcionado ao usuário individual que publicou os dados. Sartor sugere, ainda, que a pessoa que teve seus dados publicados poderá, eventualmente, requerer a remoção de conteúdo ao provedor do serviço de rede social ou *site*, mas tendo como fundamento para tal remoção o disposto na Diretiva sobre comércio eletrônico (e não o artigo 17.º do RGPD),[107] de modo que a plataforma só será responsabilizada a partir do momento em que tem conhecimento da ilegalidade do conteúdo hospedado em sua página (o que dependerá, portanto, de uma interpretação segundo a qual a Diretiva 2000/31/CE pode ser aplicada à proteção de dados pessoais) .

Essa sugestão feita por Sartor demonstra uma preocupação com as consequências de se considerar a plataforma como responsável pelo tratamento de dados. O autor alerta que, se fosse considerado *controller*, o *site* ou rede social, temendo a possibilidade de responsabilização na forma do artigo 82.º do RGPD,[108] acabaria por acatar qualquer pedido de apagamento de dados, mesmo quando ausentes os motivos elencados nas alíneas a) a f)

[107] Alsenoy ressalta que as diferenças práticas dessas conclusões podem ser bem pequenas, já que pode-se argumentar que um procedimento de "*notice and takedown"* baseado na Diretiva 2000/31/CE, pode ter resultados semelhantes aos do RGPD, principalmente se for adotada uma perspectiva em que, mesmo se for considerada um *controller*, a plataforma não é obrigada a analisar a legalidade de cada item submetido por seus usuários. Ainda assim, a sugestão de Sartor pode significar que, em alguns casos, obter o apagamento será mais difícil, já que as regras para o procedimento de remoção na Diretiva 2000/31/CE não são harmonizadas. Em Itália, por exemplo, considera-se que o conhecimento dos fatos por parte do prestador intermediário só se configura mediante comunicação de uma autoridade competente. Isso significaria que o titular de dados que teve suas imagens disseminadas teria de aguardar a comunicação da autoridade à plataforma sobre a ilegalidade dos dados para que fossem removidas (Decreto Legislativo 9 aprile 2003, artigo 16).

[108] "Artigo 82 1. Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos.

2. Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. O subcontratante é responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento [...]".

do artigo 17.º, o que resultaria em violação de direitos fundamentais dos usuários, em particular do direito à liberdade de expressão e informação (2013, p. 10).

Keller defende que,[109] no caso de conteúdo gerado pelo usuário, o procedimento de remoção de conteúdo com fundamento no direito ao apagamento previsto no artigo 17.º do Regulamento deve seguir as disposições da Diretiva sobre o comércio eletrônico, uma vez que as plataformas que armazenam conteúdo de terceiros são intermediários. (2018, p. 351). De acordo com Keller, as disposições da Diretiva 2000/31/CE equilibram melhor os direitos de todas as partes afetadas pelo apagamento de dados, incluindo usuários da Internet, cujo direito à liberdade de expressão também está envolvido. Por exemplo, segundo Keller, a determinação do artigo 14.º, n.º 1, alínea a), de que o prestador intermediário não será responsabilizado se não tiver conhecimento efetivo da atividade ou informação ilegal, pode assegurar que a plataforma não será obrigada a remover publicações de usuários com base em pedidos sem fundamentação. A previsão do artigo 15.º da Diretiva, no sentido de que a plataforma não terá obrigação geral de vigilância sobre as informações transmitidas e armazenadas também ajudaria a evitar o apagamento excessivo de dados sem fundamentação, protegendo, assim, a liberdade de expressão e informação dos usuários (2018, pp. 351–353).

Keller reconhece, contudo, que não há clareza quanto à aplicabilidade das disposições da Diretiva 2000/31/CE ao direito ao apagamento de dados. Por um lado, o artigo 17.º pode se referir a uma situação em que um prestador de serviço intermediário (como uma rede social) é obrigado a remover conteúdo criado pelo usuário. Por outro lado, o artigo 17.º do RGPD, ao contrário do artigo 14.º da Diretiva 2000/31/CE, não dispõe sobre responsabilidade civil pela violação de dados pessoais, mas sim sobre um dever de apagar dados pessoais quando presentes os critérios dispostos nas alíneas do artigo (2018, p. 354). Ainda assim, Keller defende que as previsões da Diretiva sobre o comércio eletrônico podem ser aplicadas ao caso do artigo 17.º como forma de limitar as obrigações da plataforma com relação a conteúdo publicado pelo usuário (2018, pp. 355–356).

Uma decisão da *Corte di Cassazione*, na Itália, buscou conciliar as duas disciplinas. O caso diz respeito a um vídeo publicado na plataforma *Google Video*, contendo imagens de uma pessoa portadora de síndrome de *Down* sendo provocada com

[109] Ressalta-se que Keller também chega a sugerir a exclusão de serviços de *hosting* das obrigações previstas no artigo 17.º do RGPD como solução para as possíveis ameaças à liberdade de expressão no Regulamento.

frases ofensivas e ações vexatórias sobre sua síndrome por outros indivíduos menores de idade. Em primeira instância, o Tribunal de Milão condenou os dirigentes do *Google* pelo crime de tratamento ilícito de dados, previsto no decreto legislativo que transpôs a Diretiva 95/46/CE para o ordenamento italiano, decisão que foi revertida pelo tribunal de segunda instância. A *Corte di Cassazione*, ao julgar o caso, levou em consideração também o disposto no decreto legislativo que transpõe a Diretiva 2000/31/CE, na parte em que dispõe sobre a limitação da responsabilidade dos prestadores de serviço de armazenagem em servidor, e sobre a ausência de obrigação geral de vigilância (CORTE DI CASSAZIONE, 2013).

A interpretação da *Corte di Cassazione* foi de que, enquanto o dado ilícito é desconhecido pelo prestador de serviço, este não pode ser considerado o *controller* (responsável pelo tratamento). Assim, como regra geral, os usuários serão considerados os únicos responsáveis pelo tratamento. Contudo, quando a plataforma toma conhecimento do tratamento ilícito e não atua para sua imediata remoção ou para impossibilitar o acesso às informações, assume a qualificação de responsável pelo tratamento. Segundo o Tribunal, a disciplina sobre o comércio eletrônico é realçada não de forma direta, mas interpretativa. O Tribunal considera que o artigo 1.º, n.º 2, alínea b), da diretiva sobre o comércio eletrônico não tem a função de tornar as normas em matéria de comércio eletrônico totalmente inoperantes em todos os fatos que dizem respeito à proteção de dados (CORTE DI CASSAZIONE, 2013).

Nesse entendimento, o *host* se torna *controller* a partir da notificação de que armazena conteúdo em violação à legislação sobre proteção de dados pessoais. Tal visão poderá evitar alguns problemas de atribuição de obrigações impossíveis de serem cumpridas, como a questão identificada por Keller, relativa à possível obrigação do *Twitter* de obter o consentimento de todas as pessoas cujos dados pessoais são mencionados em *tweets* de seus usuários (2018, p. 337).

Também buscando conciliar as duas disciplinas, Erdos observa que, ao contrário de alguns tipos de *hosts* de *websites* ou *blogs*, intermediários como *sites* de compartilhamento de vídeos (e.g. *Youtube*) e redes sociais mantém serviços que não limitam o tratamento relacionado à publicação às instruções diretas de quem submete o conteúdo, mas fundem essas ações com outras que eles mesmo determinam, por exemplo, combinando conteúdo para apresentá-lo aos outros usuários (como o "*feed*" do *Facebook* e

as recomendações automatizadas).[110] Assim, esses provedores de serviços seriam corretamente classificados como *controllers*. Contudo, segundo Erdos essas plataformas devem ser consideradas como "responsáveis pelo tratamento de tipo especial", de modo que não podem ser responsabilizados por algumas ilegalidades sem que tenham conhecimento delas. Isso não impede que tenham de cumprir com alguns deveres de cuidado especificados na legislação sobre proteção de dados. Assim, é possível que esses *controllers* sejam obrigados a fazer valer direitos dos titulares de dados *ex post*. Erdos afirma que seria razoável conceber essas plataformas como responsáveis em conjunto com os usuários pelo tratamento de dados publicados na plataforma (ERDOS, 2018, pp. 214–216).

4.2.3 Conclusões sobre o responsável pelo tratamento no caso da disseminação não consensual de imagens íntimas

Em suma, existem várias interpretações sobre o papel do responsável pelo tratamento no caso de dados pessoais sensíveis de terceiros publicados por usuários de *sites* de compartilhamento de conteúdo e redes sociais e, consequentemente, quanto ao seu dever de cumprir as determinações do artigo 17.º do RGPD. No que diz respeito à pessoa singular que publica os dados, como já visto, é possível considerá-la responsável pelo tratamento, uma vez que ela determina livremente as finalidades e os meios das publicações de dados pessoais de terceiros. Por mais que o usuário normalmente não tenha poder de decisão real sobre como o tratamento é conduzido pelo *site* ou rede social (a não ser quanto à alteração de algumas configurações), tem o poder de escolher se compartilhará ou não determinado dado pessoal usando a plataforma, o que indica que, de certa forma, também determina livremente os meios da publicação. Como visto,[111] a jurisprudência do TJUE nos casos *Lindqvist* e *Buivids* corrobora a interpretação segundo a qual o tratamento que consiste na publicação de dados sensíveis de terceiros em páginas abertas ao público por pessoas singulares não é abarcado pela exceção prevista no artigo 2.º, n.º 2, alínea c).

[110] Esse tipo de autonomia é o que diferencia as redes sociais e *sites* de compartilhamento de conteúdo das plataformas que hospedam *blogs,* como o caso do *Google Blogger*, na já mencionada decisão da *Audiencia Nacional*, na Espanha (ERDOS, 2018, pp. 212–214).
[111] Tópico 4.2.1.

Assim, usuários provavelmente terão obrigação de fazer valer o direito ao apagamento previsto no artigo 17.º no caso de NCII.

Já no que diz respeito ao *site* ou serviço de rede social no qual são publicados os dados pessoais de terceiros, há várias interpretações possíveis. Como já visto, existe a perspectiva de que os provedores de serviço de rede social, nesses casos, serão responsáveis pelo tratamento. Apesar de exercerem pouco controle sobre o conteúdo no momento em que o usuário submete a informação na plataforma, também agem como *controllers* ao fornecerem o serviço e distribuírem a informação. Ressalta-se que, uma vez disponibilizada a informação na plataforma, redes sociais realizam operações naqueles dados, para as quais já haviam determinado as finalidades e os meios previamente (como conservação, análise, disseminação, controle de acesso). Nessa ótica, as plataformas serão responsáveis pelo tratamento em conjunto com os usuários que submeteram os dados pessoais (ALSENOY, 2019, p. 412; ALSENOY *et al.*, 2009, p. 71).

Contudo, existe uma outra interpretação, segundo a qual essas plataformas não devem ser consideradas responsáveis pelo tratamento, mas sim subcontratantes, atuando de acordo com as instruções dos usuários que publicam os dados (KELLER, 2018, p. 323). Tal interpretação decorre da visão de que esse tipo de plataforma apenas viabiliza de forma neutra o compartilhamento de conteúdo gerado pelo usuário (ainda que agindo em interesse próprio) (SARTOR, 2013, pp. 3–5). Nesse sentido, o apagamento só poderá ser requerido ao usuário. Dentro dessa perspectiva, Sartor propõe a aplicabilidade da Diretiva 2000/31/CE a esse tipo de situação, sugerindo que o pedido de apagamento baseado no artigo 17.º só poderá ser direcionado ao usuário que compartilhou os dados pessoais de terceiro, mas que seria possível um eventual pedido de remoção seguindo as normas sobre comércio eletrônico, segundo as quais o intermediário não pode ser responsabilizado sem conhecimento da ilegalidade dos dados (2013, p. 10).

Finalmente, existe também a perspectiva que busca conciliar a disciplina do RGPD com a Diretiva sobre o comércio eletrônico. Nesse ponto de vista, a rede social ou *site* em que é compartilhado o conteúdo ilícito só se torna responsável pelo tratamento (*controller*) quando toma conhecimento da ilegalidade do tratamento de dados. Essa é a interpretação adotada no caso italiano envolvendo o *Google Video.* Nesse cenário, uma rede social ou *site* pode ser obrigada a fazer valer o direito ao apagamento previsto no artigo 17.º do Regulamento após ser notificado do conteúdo ilegal.

Nenhum dos cenários acima descritos é isento de problemas. Considerar o usuário de uma rede social ou *site* de compartilhamento de conteúdo como responsável pelo tratamento de dados poderá significar submetê-lo a obrigações difíceis de serem cumpridas por pessoas singulares (como as determinações do artigo 5.º, n.º 1, alíneas d) a f) (ALSENOY, 2019, pp. 454–455; HELBERGER e HOBOKEN, VAN, 2010, p. 105). Da mesma forma, identificam-se possíveis dificuldades de aplicação do disposto no Regulamento quando se considera a plataforma onde os dados pessoais são publicados como responsável pelo tratamento desses dados. Além de levantar questões para as quais não há resposta clara, como, por exemplo, o questionamento se uma rede social será obrigada a obter o consentimento de terceiros cujos dados pessoais são mencionados nas publicações de seus usuários (KELLER, 2018, p. 310), há a possibilidade de que essas plataformas sejam motivadas a remover conteúdo excessivamente, o que pode ferir direitos fundamentais de usuários e internautas, nomeadamente o direito à liberdade de expressão e informação (KELLER, 2018, p. 323; SARTOR, 2013, p. 10). Esses problemas decorrem do fato de que a legislação europeia em matéria de proteção de dados pessoais não foi projetada tendo usuários amadores ou redes sociais em mente (HELBERGER e HOBOKEN, VAN, 2010, p. 104).

Analisando o caso da disseminação não consensual de imagens íntimas, considerar o usuário que fez a publicação e a plataforma como responsáveis pelo tratamento dos dados publicados parece ser a solução mais benéfica do ponto de vista da efetividade do direito ao apagamento. Conceber o usuário de rede social como o único responsável pelo tratamento pode inviabilizar o cumprimento do direito previsto no artigo 17.º do RGPD, já que este pode ter publicado os dados usando uma identidade virtual, ou um perfil falso, sendo difícil a sua identificação. Também é possível que o usuário simplesmente não responda ao pedido feito pelo titular de dados pessoais (HELBERGER e HOBOKEN, VAN, 2010, p. 108). Além disso, é preciso considerar que, no caso do NCII, as imagens e vídeos são muitas vezes copiados e replicados por vários usuários diferentes (o que é referido como "*amplification effect*") (BROWN, 2018, p. 159). Assim, determinar que o titular tenha de encaminhar o pedido de apagamento individualmente para cada um dos usuários que publicaram seus dados em uma ou mais plataformas, em vez de contactá-las diretamente, inviabilizaria o apagamento efetivo. Uma interpretação que concilie o disposto no artigo 17.º com a Diretiva 2000/31/CE, como na decisão da *Corte di*

Cassazione sobre o caso do *Google Video*, não impedirá que a plataforma seja obrigada a cumprir com o direito ao apagamento se, após a notificação, for considerada como responsável pelo tratamento.

Observa-se que, principalmente no caso de *sites* pornográficos, a própria plataforma apresenta ferramentas para viabilizar o compartilhamento de material por usuários, sendo evidente, em alguns casos, que se beneficia desse tipo de atividade. A plataforma *PornHub*, por exemplo, tem sido criticada por abrigar em sua página vídeos não consensuais criados utilizando inteligência artificial, em que rostos de pessoas são inseridos em vídeos pornográficos (conhecidos como "*deepfakes*"). O *PornHub* também se beneficia da visualização desse tipo de conteúdo, já que pode trazer renda de anúncios (COLE, 2020). Também há relatos de vídeos de NCII em um dos canais mais populares do *site* (COLE, 2019). As professoras Clare McGlynn e Fiona Vera-Gray comentam o fato de que uma quantidade significativa dos vídeos apresentados em *sites* pornográficos comuns é contrária aos próprios termos e condições do *site*, o que inclui NCII (MCGLYNN e VERA-GRAY, 2019). Nesse sentido, não parece ser razoável apontar a falta de controle por parte da plataforma sobre o conteúdo como razão para que não seja obrigada a removê-lo.

Nada impede que o titular dos dados pessoais também faça o pedido de desindexação aos motores de busca. Contudo, enquanto a remoção dos *links* para *sites* contendo imagens íntimas de uma pessoa dos resultados de busca pode ter um papel importante ao dificultar o acesso do público a esses dados sensíveis, não impede que os dados continuem a ser visualizados. A publicação no *site* ou rede social permanecerá, e poderá ser acessada diretamente na página original, ou através de pesquisas contendo outros termos.[112] Dessa forma, o pedido de desindexação com base no artigo 17.º parece ser mais útil em casos nos quais os responsáveis pelo tratamento de dados na publicação original não estão sujeitos à legislação da UE. Ressalta-se que, diferentemente do caso

[112] O CEPD, nas Diretrizes n.º 5/2019 sobre os critérios para o direito ao esquecimento no caso de motores de busca conforme o RGPD, ressaltou que remover os links contendo dados pessoais da lista de resultados não resulta no apagamento total daqueles dados da página original em que foram publicados, nem do *index* e *cache* do motor de busca, de modo que os dados ainda estão publicamente disponíveis e podem ser acessados através de buscas que não incluam o nome do titular de dados pessoais. O CEPD reconhece, contudo, que em casos excepcionais, o motor de busca pode ser obrigado a realizar o apagamento total de seu *index* ou *cache* (EUROPEAN DATA PROTECTION BOARD, 2019b, p. 5). Essa remoção total, para um titular de dados pessoais vítima de NCII, pode ter consequências mais interessantes do que apenas remover os *links* dos resultados de busca em seu nome.

Google Spain, em que a publicação original dos dados feita pelo jornal espanhol foi considerada lícita, nos casos de NCII a publicação constitui tratamento ilícito de dados desde o início.

Por último, é preciso reconhecer que a implementação do direito ao apagamento no ambiente digital não é uma tarefa simples. Como destacado por Politou et al. (2018, p. 12), existem vários argumentos contrários à viabilidade do apagamento total de dados na Internet, tendo em conta a facilidade de se copiar e replicar a informação. Mesmo que seja adotada uma tecnologia capaz de programar dispositivos para apagar fotos e publicações quando atingem as datas de validade, como sugerido por Mayer-Schönberger (2009, cap. 6), problemas ainda podem surgir devido à cópia de dados.

A Agência da União Europeia para a Cibersegurança (ENISA)[113] se manifestou no sentido de que, num sistema aberto como a Internet de hoje, é praticamente impossível que uma pessoa localize todos os dados sobre si. Além disso, cópias de determinados conteúdos são difíceis de serem evitadas. Os dados podem ser digitalmente copiados e conservados em dispositivos não conectados à Internet, e em seguida reinseridos na Internet. As cópias podem, ainda, ser obtidas por meios não digitais, que não são detectados, como é o caso de alguém que tira uma fotografia de uma tela contendo dados pessoais. Por isso, a ENISA conclui que garantir um "direito ao esquecimento" com uma solução puramente técnica na Internet é inverosímil. No entanto, afirma que, apesar de ser praticamente improvável uma remoção completa dos dados, pode-se limitar o seu acesso, impedindo que apareçam em resultados de busca, e em redes sociais e *sites* de compartilhamento (EUROPEAN UNION AGENCY FOR CYBERSECURITY, 2012, pp. 11–13). Nesse sentido, destaca-se a atuação do *Facebook* para remover imagens íntimas e, usando tecnologia de reconhecimento de imagem, evitar que sejam compartilhadas novamente. O *site* tem desenvolvido ferramentas para detectar proativamente o conteúdo não-consensual e removê-lo mesmo antes que alguém o sinalize (FACEBOOK, 2019).

[113] Ressalta-se que o relatório da ENISA foi elaborado anteriormente à decisão do caso *Google Spain*.

CONCLUSÕES

1. A disseminação não consensual de imagens íntimas se torna um problema relevante na era digital. Apesar de já existir antes da popularização da Internet, foi potencializada pelo surgimento da *web 2.0*. A popularização da NCII é uma consequência da evolução da tecnologia da informação, que facilita a obtenção, o armazenamento e o compartilhamento de imagens e vídeos digitais, e que também viabiliza a conexão de pessoas em rede, com o surgimento e ampliação de aplicativos e *sites*, cuja atividade se baseia na publicação de conteúdo gerado pelo próprio usuário. As consequências da NCII para as vítimas são especialmente graves, considerando outra importante característica da Internet: a memória. Uma imagem compartilhada estará potencialmente acessível em um registro permanente.

2. Uma imagem íntima de uma pessoa pode constituir um dado pessoal, por conter elementos específicos da sua identidade física, enquadrando-se na definição de informação relativa a uma pessoa singular identificada ou identificável. A publicação de imagens desse tipo sem autorização da pessoa retratada viola seu direito à imagem. Também configura ofensa ao direito à privacidade, por envolver dados sobre a vida sexual da pessoa, abrangida pela noção de vida privada. Viola, ainda, o direito à honra, já que a exposição da vida sexual de uma pessoa pode lesar a sua reputação. A forma como a disseminação é feita também pode deturpar a identidade da pessoa retratada, associando-a a *sites* pornográficos, por exemplo. Ademais, pode configurar ofensa ao direito à igualdade, já que os dados publicados podem gerar discriminação do titular. Dessa forma, observa-se que a NCII é um exemplo de situação em que o direito à proteção de dados serve como forma de tutela de outros bens da personalidade.

3. Tendo em mente a ideia de integridade contextual, concebida por Helen Nissenbaum, observa-se que a NCII é um exemplo de situação em que normas informacionais são violadas, de modo que não é mantida a integridade contextual: dados sobre a intimidade de uma pessoa, e que estão restritos em um contexto específico (sua vida sexual), são publicados e transmitidos também a atores de outros contextos (familiar, laboral etc.), desrespeitando, portanto, um princípio de confidencialidade. As expectativas da pessoa retratada quanto ao fluxo informacional, nesse caso, não são atendidas. Trazendo a ideia de integridade contextual para a proteção de dados pessoais, vendo-a como uma

vertente complementar à autodeterminação informacional, observamos que, ainda que o titular de dados pessoais tenha dado seu consentimento para que um terceiro tivesse acesso às suas imagens íntimas, a publicação das imagens em outras plataformas ou *sites*, transportando-as a um contexto diverso, estabelece um fluxo informacional inadequado e fere os princípios da limitação das finalidades e da minimização dos dados, que estão previstos no artigo 5.º, alíneas b) e c), do RGPD.

4. A figura do consentimento teve papel de destaque na evolução da legislação sobre proteção de dados pessoais na Europa. O Regulamento (UE) 2016/679 estabelece o consentimento como uma das seis condições para a licitude do tratamento de dados pessoais. Atribui diversos adjetivos ao consentimento, entendido como uma "manifestação de vontade, livre, específica, informada e inequívoca", dada "mediante declaração ou ato positivo inequívoco". Essa adjetivação busca garantir um controle real do titular sobre os dados, evitando situações em que o titular se sinta compelido a dar o consentimento para algum tipo de tratamento, ou que o consentimento dado para uma finalidade específica seja expandido para outras finalidades com as quais o titular não concordou. Também se busca garantir a transparência quanto aos tratamentos e suas finalidades, a fim de evitar um consentimento ilusório.

4.1. Tendo em vista o disposto no artigo 9.º do RGPD, referente ao tratamento de categorias especiais de dados pessoais, a disseminação das imagens íntimas de uma pessoa só constituirá tratamento lícito de dados quando houver consentimento explícito da pessoa retratada para a publicação de suas imagens, já que o artigo 9.º prevê, em seu número 2, alínea a), o consentimento explícito do titular como uma exceção à proibição do tratamento de dados sensíveis. Considerando que na prática da NCII não se configuram as situações previstas nas alíneas b) a j) do número 2 do referido artigo (como tratamento necessário para o cumprimento de obrigações, para a proteção de interesses vitais do titular, para efeitos de medicina preventiva ou do trabalho, ou para interesse público, por exemplo), o consentimento seria a principal base legal capaz de autorizar a disseminação. Analisando o NCII do ponto de vista da proteção de dados, observamos que tal disseminação será um tratamento ilícito de dados pessoais mesmo no caso em que a pessoa retratada inicialmente dá seu consentimento para a produção das imagens. Se o titular de dados dá o seu consentimento para que alguém faça uma filmagem de si, por exemplo, ou mesmo envia, ele próprio, imagens a uma outra pessoa através de um app ou rede social, essa autorização

não permite uma publicação ou encaminhamento das imagens para terceiros. Tal conduta violaria a construção do consentimento como manifestação de vontade específica, tendo em vista o princípio da limitação das finalidades, previsto no artigo 5.º, n.º 1, alínea b), do RGPD.

5. O artigo 17.º do RGPD dispõe sobre o direito do titular de dados pessoais de obter do responsável pelo tratamento o apagamento dos seus dados, sem demora injustificada, nas situações elencadas nas alíneas de a) a f). A alínea d), mais especificamente, determina que o direito ao apagamento pode ser invocado em casos de tratamento ilícito de dados pessoais. Tendo em consideração que a imagem de uma pessoa pode constituir dado pessoal conforme artigo 4.º, n.º 1, do RGPD, e considerando, ainda, que a imagem íntima de uma pessoa constitui dado sensível na forma do artigo 9.º, número 1, do Regulamento, de modo que a sua disponibilização sem consentimento explícito do titular de dados pessoais configura tratamento ilícito, é possível concluir que o NCII é uma situação que dá ensejo à aplicação do direito ao apagamento.

6. O artigo 17.º faz menção expressa ao "direito a ser esquecido", previsto entre aspas ao lado do termo "direito ao apagamento dos dados". Em sua acepção tradicional, o direito ao esquecimento corresponde a um direito de matriz jurisprudencial, que consiste no direito de uma pessoa de que uma notícia sobre si não seja proposta à opinião pública depois de certo lapso de tempo da sua primeira difusão ou do fato a que se refere. Assim, o fator tempo é essencial para a configuração do direito ao esquecimento, já que é o decurso do tempo que torna a notícia lesiva, pela perda de interesse coletivo nela. Existe, porém, uma outra acepção do direito ao esquecimento, que envolve a Internet. Diferentemente do que ocorre com publicações de jornais ou revistas em papel, uma notícia difundida na Internet permanece disponível ou pelo menos abstratamente disponível, podendo ser facilmente localizada graças a motores de busca como o *Google*. Assim, o problema não é a republicação de um fato, mas a sua permanência na rede. Nesse cenário, identifica-se, ainda, uma terceira acepção do direito, que é a ideia de direito ao esquecimento como "direito a não ser encontrado online". Essa ideia está presente na decisão do TJUE no caso *Google Spain*, que reconheceu a possibilidade de requerer a "desindexação", ou seja, solicitar que informações sobre si deixem de estar à disposição do grande público através da remoção dos links contendo esses dados da lista de resultados de busca efetuada no nome da pessoa em causa.

6.1. O artigo 17.º do RGPD, apesar da menção explícita ao direito ao esquecimento, não parece ter como objetivo disciplinar especificamente esse direito. O direito ao esquecimento pode ser exercido de outras formas, que não envolvem apagamento dos dados. Ademais, o direito ao apagamento pode se configurar em várias hipóteses, mencionadas nas alíneas a) a f) do número 1 do artigo 17.º, que podem ou não envolver a passagem do tempo, não estando a sua configuração condicionada à verificação de um direito ao esquecimento. Apesar de alguns autores usarem os dois termos indiscriminadamente, confundindo os dois conceitos, apagamento e esquecimento não são sinônimos. No caso específico da NCII, observa-se que o direito envolvido não é propriamente o de não estar indefinidamente ligado a informações sobre o próprio passado, mas de obter o apagamento de dados tratados ilicitamente, de modo que o tempo não é um fator relevante. Ao contrário do que ocorreu no caso *Google Spain*, em que a publicação original feita pelo jornal espanhol era lícita e servia à finalidade de dar publicidade a uma venda em hasta pública, nos casos de NCII, a publicação já é ilícita desde o início, pelo fato de conter dados sensíveis tratados sem o consentimento do titular. Dessa forma, verifica-se que o que se busca no caso do NCII não é propriamente um direito ao esquecimento.

7. Tendo em vista a possibilidade de apagamento de dados pessoais conforme disposto no art. 17.º, número 1, alínea d), do RGPD, no caso de disseminação não consensual de imagens íntimas, surgem algumas questões para as quais não há resposta clara no Regulamento. A legislação europeia sobre proteção de dados pessoais foi tradicionalmente aplicada ao tratamento de dados armazenados em bancos de dados, como no caso de hospitais, ou empresas que geram dados com base no monitoramento da atividade de usuários. Esse tipo de dado é diferente dos dados pessoais que constam de publicações feitas em redes sociais e *sites* de compartilhamento de conteúdo pelo usuário, por exemplo. A estrutura da proteção de dados europeia foi pensada numa época em que o tratamento de dados dizia respeito a bancos, empregadores, médicos e outras entidades. Contudo, com o surgimento e expansão de redes sociais e outras plataformas da *web 2.0*, surgiram dificuldades de aplicação dessa estrutura aos casos de expressão do usuário. Considerando que as imagens íntimas normalmente são compartilhadas em redes sociais e *sites* pornográficos que oferecem conteúdo compartilhado pelo usuário (de forma análoga a uma rede social), uma das perguntas que surgem nesse contexto é quem deverá realizar o

apagamento no caso de NCII. Conforme disposto no artigo 17.º, n.º 1, o titular tem o direito de obter o apagamento do responsável pelo tratamento dos seus dados pessoais. Assim, é preciso identificar quem será o responsável pelo tratamento dos dados que constam da publicação ilícita.

7.1. Quanto ao usuário do *site* ou rede social que publica as imagens íntimas de uma pessoa, conclui-se que poderá ser considerado responsável pelo tratamento. O Regulamento não limita o tipo de ator que pode assumir o papel de responsável pelo tratamento, podendo este ser uma pessoa singular. Um usuário de rede social ou *site* que publica dados de terceiros pode livremente decidir a finalidade daquela divulgação. Quanto aos meios, é verdade que o usuário, apesar de pode alterar algumas configurações da rede social ou *site*, não tem controle, em geral, sobre a maneira como o tratamento é conduzido dentro da plataforma que escolhe. Ainda assim, tem o poder de decidir ou não se deseja publicar determinado e qual a plataforma usada para isso. Considerando que os dados pessoais, nesse caso, são divulgados a um número indefinido de pessoas e que existe potencial impacto adverso sobre a pessoa retratada, é provável que o NCII não seja considerado como um tratamento efetuado no exercício de atividades exclusivamente pessoais ou doméstica, tendo em conta a jurisprudência do TJUE nos casos *Lindqvist* e *Buivids*, por exemplo. Dessa forma, não se aplica o disposto no artigo 2.º, n.º 2, alínea c), do Regulamento. O usuário poderá ser obrigado, portanto, a cumprir com o disposto no artigo 17.º do RGPD.

7.2. Já no que diz respeito ao serviço de rede social ou *site* em que ocorre o compartilhamento de imagens íntimas, não há ainda um consenso sobre o papel desempenhado no caso do tratamento de dados pessoais de terceiros publicados pelo usuário. Existe a perspectiva segundo a qual o provedor do serviço de rede social é responsável pelo tratamento. Apesar de ter pouco controle no momento em que o usuário decide submeter a informação, considera-se que a rede social define as finalidades e os meios do tratamento ao fornecer o serviço e distribuir aquela informação. Uma vez que a informação é disponibilizada na plataforma, esta realiza operações nos dados, para as quais já havia definido as finalidades e os meios previamente (como conservação, análise, disseminação, controle de acesso etc.). Nessa perspectiva, a rede social ou *site* será responsável pelo tratamento em conjunto com o usuário que fez a publicação de NCII.

7.3 Contudo, também há a ideia de que plataformas como redes sociais não devem ser consideradas responsáveis pelo tratamento nesses casos, por não determinarem o conteúdo dos posts e terem pouco controle sobre a fase anterior à publicação. A rede social seria, assim, uma subcontratante, seguindo as instruções dos usuários. Desse modo, a plataforma não seria obrigada a cumprir com o apagamento previsto no artigo 17.º do Regulamento. Um dos argumentos nesse sentido é o de que a rede social é um mero facilitador neutro do compartilhamento de informações, não podendo ser responsabilizada. Essa visão aplica à definição de responsável pelo tratamento e contratante a lógica da Diretiva sobre comércio eletrônico, que determina que intermediários não poderão ser responsabilizados por conteúdo publicado na plataforma sem seu conhecimento. Tal ponto de vista leva em conta a preocupação de alguns autores com os efeitos da classificação de redes sociais como *controllers*, que pode resultar na sua sujeição a obrigações que não podem cumprir. Também há o receio de que, temendo uma possível responsabilização pelo conteúdo publicado pelo usuário, a plataforma acabe por acatar pedidos de apagamento infundados, o que violaria o direito à liberdade de expressão e informação dos usuários e dos internautas como um todo.

7.4. Finalmente, existe a possibilidade de se adotar uma perspectiva que busque conciliar as disciplinas do RGPD e da Diretiva 2000/31/CE. Essa foi a abordagem adotada pela *Corte di Cassazione* italiana no caso *Google Video*. Nessa concepção, considera-se que, como regra geral, os usuários serão os únicos responsáveis pelo tratamento dos dados pessoais de terceiros que publicam numa plataforma. Contudo, as plataformas, quando tomam conhecimento do tratamento ilícito, adquirem o *status* de responsável pelo tratamento. Tal posicionamento poderá evitar alguns dos problemas observados quanto à classificação de intermediários como *controllers*, no que diz respeito à possível imposição de obrigações que estas não conseguem cumprir pela falta de controle prévio do que é publicado pelos usuários. Nessa visão, após serem notificados e tomarem conhecimento da presença de material de NCII, redes sociais e *sites* também seriam obrigados a cumprir o disposto no artigo 17.º do RGPD.

7.5. Ainda há incertezas quanto ao papel das redes sociais e *sites* de compartilhamento no tratamento de dados pessoais de terceiros publicados por usuários na plataforma, e, consequentemente, quanto à sua obrigação de apagar dados pessoais publicados ilicitamente nesse contexto. Do ponto de vista da NCII, tendo em vista a

efetividade do direito ao apagamento do titular de dados pessoais previsto no artigo 17.º do Regulamento, conclui-se que a abordagem mais conveniente será considerar tanto o usuário como a rede social ou *site* de compartilhamento responsáveis pelo tratamento. Conceber o usuário como o único responsável pelo tratamento poderia inviabilizar o cumprimento do referido artigo. O usuário pode ter disseminado os dados utilizando uma identidade virtual ou um perfil falso, o que dificulta sua identificação. Também é possível que simplesmente não responda à notificação do titular de dados pessoais. Além disso, é preciso considerar que imagens íntimas normalmente são replicadas diversas vezes e compartilhadas por usuários diferentes em várias plataformas. Determinar que o titular de dados pessoais tenha de encaminhar o pedido de apagamento a cada um dos usuários que publicaram os dados em uma ou mais plataformas, em vez de contactá-las diretamente, inviabilizaria o seu direito ao apagamento. Uma possível abordagem que concilie o RGPD e a Diretiva sobre o comércio eletrônico não impediria o cumprimento do artigo 17.º, já que, após notificação da ilegalidade, a plataforma seria classificada como responsável pelo tratamento.

8. Reconhece-se que a implementação do direito ao apagamento, diante da facilidade de cópia e disseminação de conteúdo publicado por terceiros na Internet, não é uma tarefa simples, e provavelmente não garantirá o apagamento total. Contudo, o apagamento das imagens íntimas de redes sociais e *sites*, além de links de motores de busca, com base no artigo 17.º do RGPD, pode ser uma forma de reduzir o compartilhamento de conteúdo não consensual e evitar a configuração desse aspecto negativo da *web 2.0*.

REFERÊNCIAS

ABRIL, Patricia Sánchez; LIPTON, Jacqueline D. - The right to be forgotten: who decides what the world forgets? *Kentucky Law Journal* [Em linha]. Vol. 103, n.º 3 (2014), p. 363–389. [Consult. 27 Out. 2020]. Disponível em: WWW:<URL: https://uknowledge.uky.edu/klj/vol103/iss3/4/>. ISSN 0023-026X.

ACQUISTI, Alessandro - Nudging privacy: the behavioral economics of personal information. *Security & Privacy Economics* [Em linha]. Vol. 7, n.º 6 (2009), p. 82–85. [Consult. 27 Out. 2020]. Disponível em: WWW:<URL: https://ieeexplore.ieee.org/document/5370707>. ISSN: 1558-4046. DOI: 10.1109/MSP.2009.163.

ACQUISTI, Alessandro; GROSSKLAGS, Jens - Privacy and rationality: a survey. In STRANDBURG, KATHERINE J.; RAICU, DANIELA STAN (Eds.) - *Privacy and Technologies of Identity: a Cross-Disciplinary Conversation*. New York: Springer, 2006. ISBN 10:0-387-28222-X. p. 15–29.

ACQUISTI, Alessandro; GROSSKLAGS, Jens - What Can Behavioral Economics Teach Us about Privacy? In ACQUISTI, ALESSANDRO et al. (Eds.) - *Digital Privacy: Theory, Technologies and Practices*. New York : Auerbach Publications, 2008. ISBN 13: 978-1-4200-5217-6. p. 363–377.

ALSENOY, Brendan Van et al. - Social networks and web 2.0: Are users also bound by data protection regulations? *Identity in the Information Society* [Em linha]. Vol. 2, n.º 1 (2009), p. 65–79. [Consult. 27 Out. 2020]. Disponível em: WWW:<URL: https://link.springer.com/article/10.1007/s12394-009-0017-3>. ISSN: 1876-0678. DOI: 10.1007/s12394-009-0017-3.

ALSENOY, Brendan Van - The evolving role of the individual under EU data protection law. *CiTiP Working Paper 23/2015* [Em linha]. (2015), p. 1-35. [Consult. 27 Out. 2020].

Disponível em: WWW:<URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2641680#>.

ALSENOY, Brendan Van - *Data Protection Law in the EU: Roles, Responsibilities and Liability*. Cambridge : Intersentia, 2019. 694 p. ISBN 978-1-78068-828-2.

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 5/2009 on Online Social Networking* [Em linha]. 2009. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf >.

ARTICLE 29 DATA PROTECTION WORKING PARTY - *Opinion 02/2012 on Facial Recognition in Online and Mobile Services* [Em linha]. 2012. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf>.

ARTICLE 29 DATA PROTECTION WORKING PARTY - *Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities*. [Em linha]. 2013. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf>.

BAMBAUER, Derek E. - Exposed. *Minnesota Law Review* [Em linha]. Vol. 98, n.º 6 (2014), p. 2025–2102. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2315583 >. ISSN 0026-5535.

BARBOSA, Mafalda Miranda - Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil. *Estudos de Direito do Consumidor* [Em linha]. n.º 12 (2017), p. 75–131. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://www.fd.uc.pt/cdc/pdfs/rev_12_completo.pdf>. ISSN 1646-0375.

BARBOSA, Mafalda Miranda - Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil. *Revista de Direito Comercial* [Em linha]. (2018), p. 423–494. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://www.revistadedireitocomercial.com/data-controllers-e-data-processors>. ISSN 2183-9824.

BATES, Samantha - Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors. *Feminist Criminology* [Em linha]. Vol. 12, n.º 1 (2017), p. 22–42. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://journals.sagepub.com/doi/abs/10.1177/1557085116654565>. ISSN 1557-086X. DOI: 10.1177/1557085116654565.

BENOLIEL, Uli; BECHER, Shmuel - The duty to read the unreadable. *Boston College Law Review* [Em linha]. Vol. 60, n.º 8 (2019), p. 2255–2296. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3313837 >. ISSN 0161-6587. DOI: 10.2139/ssrn.3313837.

BEYENS, Jolien; LIEVENS, Eva - A legal perspective on the non-consensual dissemination of sexual images: identifying strengths and weaknesses of legislation in the US, UK and Belgium. *International Journal of Law, Crime and Justice* [Em linha]. Vol. 47, (2016), p. 31–43. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://www.sciencedirect.com/science/article/abs/pii/S1756061616300027>. ISSN 1756-0616. DOI: 10.1016/j.ijlcj.2016.07.001.

BIONI, Bruno - *Proteção de Dados Pessoais: A Função e os Limites do Consentimento* [Em linha]. São Paulo : Forense, 2019. [Consult. 27 Out. 2020]. Disponível em: WWW:<URL: https://ler.amazon.com.br/?asin=B07K8X28TC>. ISBN 978-85-309-8328-4.

BITENCOURT, Cezar Roberto - *Tratado de Direito Penal. Crimes Contra a Dignidade Sexual Até Crimes Contra a Fé Pública*. 8. ed. São Paulo : Saraiva, 2014. 4 vol. 608 p. ISBN 978-85-02-21732-4.

BOUGIAKIOTIS, Emmanouil - The enforcement of the Google Spain ruling. *International Journal of Law and Information Technology* [Em linha]. Vol. 24, n.º 4 (2016), p. 311–342. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://www.researchgate.net/publication/307142867_The_enforcement_of_the_Google_Spain_ruling>. ISSN 0967-0769. DOI: 10.1093/ijlit/eaw008.

BRANDIMARTE, Laura; ACQUISTI, Alessandro; LOEWENSTEIN, George - Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* [Em linha]. Vol. 4, n.º 3 (2013), p. 340–347. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://journals.sagepub.com/doi/abs/10.1177/1948550612455931>. ISSN 1948-5514. DOI: 10.1177/1948550612455931.

BROWN, Elizabeth - Protecting Does and Outing Mobsters: Recalibrating Anonymity Standards in Revenge Porn Proceedings. *Duke Journal of Gender Law & Policy* [Em linha]. Vol. 25, n.º 2 (2018), p. 155–190. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://scholarship.law.duke.edu/djglp/vol25/iss2/1/>. ISSN 2328-9732.

BUCKLEY, Shay - Defamation online - Defamation, Intermediary Liability and the Threat of Data Protection Law. *Hibernian Law Journal* [Em linha]. Vo. 19, (2020), p. 82–109. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://heinonline.org/HOL/LandingPage?handle=hein.journals/hiblj19&div=1&src=home>. ISSN 1393-8940.

BUNN, Anna - The curious case of the right to be forgotten. *Computer Law & Security Review* [Em linha]. Vol. 31, n.º 3 (2015), p. 336–350. [Consult. 27 Out. 2020] Disponível em WWW:<URL:

https://www.sciencedirect.com/science/article/abs/pii/S0267364915000606>. ISSN 0267-3649. DOI: 10.1016/j.clsr.2015.03.006.

CAGGIA, Fausto - Libertà ed espressione del consenso. In CUFFARO, VINCENZO; D'ORAZIO, ROBERTO; RICCIUTO, VINCENZO (Eds.) - *I Dati Personali nel Diritto Europeo*. Torino : Giappichelli, 2019. ISBN 9788892112742. p. 249–273.

ČAS, Johann - Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions. Em GUTWIRTH, SERGE et al. (Eds.) - *Computers, Privacy and Data Protection: an Element of Choice*. Dordrecht : Springer, 2011. ISBN 978-94-007-0641-5. p. 139–169.

CASTELLS, Manuel - *The rise of the network society*. 2. ed. Malden : Wiley-Blackwell, 2010. 597p. ISBN 978-1-4051-9686-4.

CASTRO, Catarina Sarmento E - *Direito da informática, privacidade e dados pessoais : a propósito da legalização de tratamentos de dados pessoais (incluindo videovigilância, telecomunicações e Internet) por entidades públicas e por entidades privadas, e da sua comunicação e acesso*. Coimbra : Almedina, 2005. 374p. ISBN 978-9724024240..

CASTRO, Catarina Sarmento E - A Jurisprudência do Tribunal de Justiça da União Europeia, o Regulamento Geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa. Em AMARAL, MARIA LÚCIA (Ed.) - *Estudos em homenagem ao Conselheiro Presidente Rui Moura Ramos*. Coimbra : Almedina, 2016. ISBN 9789724065786 p. 1047–1070.

CATE, Fred H. - The Failure of Fair Information Practice Principles. Em WINN, JANE K. (Ed.) - *Consumer Protection in the Age of the Information Economy*. London : Routledge, 2006. ISBN 9781315573717. p. 343–379.

CIOMMO, Francesco Di - Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblìo. Em CUFFARO, VINCENZO; D'ORAZIO, ROBERTO; RICCIUTO,

VINCENZO (Eds.) - *I Dati Personali nel Diritto Europeo*. Torino : Giappichelli, 2019. ISBN 978-88-921-1274-2. p. 353–395.

CITRON, Danielle Keats; FRANKS, Mary Anne - Criminalizing Revenge Porn. *Wake Forest Law Review* [Em linha]. Vol. 49, (2014), p. 345–391. [Consult. 27 Out. 2020] Disponível em WWW:< https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368946>. ISSN 0043-003X.

CODING RIGHTS; INTERNETLAB - *Violências de gênero na internet: diagnóstico, soluções e desafios. Contribuição conjunta do Brasil para a relatora especial da ONU sobre violência contra a mulher* [Em linha]. São Paulo, 2017. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://www.internetlab.org.br/wp-content/uploads/2017/11/Relatorio_ViolenciaGenero_ONU.pdf>.

COLE, Samantha - How Pornhub Enables Doxing and Harassment. *Vice*. [Em linha].16 jul. 2019. [Consult. 27 Out. 2020] Disponível em WWW:<URL:https://www.vice.com/en/article/mb8zjn/pornhub-doxing-and-harassment-girls-do-porn-lawsuit>.

COLE, Samantha - The Ugly Truth Behind Pornhub's «Year In Review». *Vice*. [Em linha] 18 fev. 2020. [Consult. 27 Out. 2020] Disponível em WWW:<URL:https://www.vice.com/en/article/wxez8y/pornhub-year-in-review-deepfake>.

COOLEY, Thomas M. - *Treatise on the Law of Torts, or the Wrongs Which Arise Independent of Contract.* 2. ed. Chicago : Callaghan & Co., 1888. 899p.

COSTESCU, Nicolae Drago? - Google Spain Decision – An analysis of the Right to be Forgotten – A regression from past interpretations of ECJ. *Annals of the Bucharest University - The Law Series* [Em linha]. n.º 1 (2016), p. 64–71. [Consult. 27 Out. 2020] Disponível em WWW:<URL: https://www.ceeol.com/search/journal-detail?id=1531>. ISSN 1011-0623.

CRIDDLE, Cristina - «Revenge porn new normal» after cases surge in lockdown. *BBC* [Em linha], atual. 16 set. 2020. [Consult. 23 out. 2020]. Disponível em WWW:<URL:https://www.bbc.com/news/technology-54149682>.

CUPIS, Adriano De - *I diritti della personalità - Tomo I*. Milano : Giuffrè, 1973. 371p.

DELEUZE, Gilles - Postscript on the societies of control. *October* [Em linha]. n.º 59 (1992), p. 3–7. [Consult. 27 out. 2020]. Disponível em WWW:<URL: https://www.jstor.org/stable/778828?seq=1#metadata_info_tab_contents>. ISSN 1536-013X.

DONEDA, Danilo - *Da privacy à proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados* [Em linha]. São Paulo : Thomson Reuters Brasil, 2019 [Consult. 27 Out. 2020]. Disponível em: WWW:<URL: https://proview.thomsonreuters.com/library.html#/library>. ISBN 978-85-5321-904-9.

DROUIN, Michelle et al. - Let's talk about sexting, baby: Computer-mediated sexual behaviors among young adults. *Computers in Human Behavior* [Em linha]. Vol. 29, n.º 5 (2013), p. A25–A30. [Consult. 27 Out. 2020]. Disponível em: WWW:<URL: https://www.sciencedirect.com/science/article/pii/S074756321200372X>. ISSN 0747-5632. DOI: 10.1016/j.chb.2012.12.030.

DROUIN, Michelle; LANDGRAFF, Carly - Texting, sexting, and attachment in college students' romantic relationships. *Computers in Human Behavior* [Em linha]. Vol. 28, n.º 2 (2012), p. 444–449. [Consult. 27 Out. 2020]. Disponível em: WWW:<URL: https://www.sciencedirect.com/science/article/pii/S0747563211002329 >. ISSN 0747-5632. DOI: 10.1016/j.chb.2011.10.015.

DROUIN, Michelle; ROSS, Jody; TOBIN, Elizabeth - Sexting: A new, digital vehicle for intimate partner aggression? *Computers in Human Behavior* [Em linha]. Vol. 50, (2015), p. 197–204. [Consult. 27 Out. 2020]. Disponível em: WWW:<URL:

https://www.sciencedirect.com/science/article/pii/S0747563215002836>. ISSN 0747-5632. DOI: 10.1016/j.chb.2015.04.001.

DUARTE, Tatiana - Artigo 9o. Em PINHEIRO, ALEXANDRE SOUSA (Ed.) - *Comentário ao Regulamento Geral de Proteção de Dados.* Coimbra : Amedina, 2018. ISBN 978-972-40-7786-4. p. 234–334.

DUMORTIER, Franck - Facebook and Risks of "De-contextualization" of Information. Em GUTWIRTH, SERGE; POULLET, YVES; HERT, PAUL DE (Eds.) - *Data Protection in a Profiled World*. Brussels : Springer, 2010. ISBN 978-90-481-8865-9. p. 119-137.

EDWARDS, Lilian - Revenge porn: why the right to be forgotten is the right remedy. *The Guardian* [Em linha]. 29 jul 2014. [Consult. 27 Out. 2020]. Disponível em WWW:<URL:https://www.theguardian.com/technology/2014/jul/29/revenge-porn-right-to-be-forgotten-house-of-lords#:~:text=Revenge porn is an undoubtedly vile phenomenon.&text=Revenge porn can cut across,as the other way round.>.

EECKE, Patrick Van; TRUYENS, Maarten - Privacy and social networks. *Computer Law & Security Review* [Em linha]. Vol. 26, n.º 5 (2010), p. 535–546. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://www.sciencedirect.com/science/article/pii/S0267364910001093.>. ISSN 0267-3649. DOI: 10.1016/j.clsr.2010.07.006.

ERDOS, David - Intermediary publishers and European data protection: Delimiting the ambit of responsibility for third-party rights through a synthetic interpretation of the EU acquis. *International Journal of Law and Information Technology* [Em linha]. Vol. 26, n.º 3 (2018), p. 189–225. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://academic.oup.com/ijlit/article/26/3/189/5033541.>. ISSN 1464-3693. DOI: 10.1093/ijlit/eay007.

EUROPEAN COMMISSION - *Answer given by Ms Jourová on behalf of the Commission Question reference: E-010481/2015* [Em linha], 2015. [Consult. 27 Out. 2020]. Disponível

em WWW:<URL:https://www.europarl.europa.eu/doceo/document/E-8-2015-010481-ASW_EN.html>.

EUROPEAN COMMISSION - Answer given by Vice-President Ansip on behalf of the Commission Question reference: E-000950/2017 [Em linha], 2017. [Consult. 27 Out. 2020]. Disponível em WWW:<URL:https://www.europarl.europa.eu/doceo/document//E-8-2017-000950-ASW_EN.html>.

EUROPEAN DATA PROTECTION BOARD. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* [Em linha]. 2019a. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en >.

EUROPEAN DATA PROTECTION BOARD. *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) Version 2.0* [Em linha]. 2019b. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf>.

EUROPEAN DATA PROTECTION BOARD. *Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1* [Em linha]. 2020a. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf >.

EUROPEAN DATA PROTECTION BOARD. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0*. 2020b. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf>.

EUROPEAN UNION AGENCY FOR CYBERSECURITY - *The right to be forgotten – between expectations and practice*. 2012. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://www.enisa.europa.eu/publications/the-right-to-be-forgotten >.

FACEBOOK - *Detecting Non-Consensual Intimate Images and Supporting Victims* [Em linha]. 2019. [Consult. 14 out. 2020]. Disponível em WWW:<URL:https://about.fb.com/news/2019/03/detecting-non-consensual-intimate-images/>.

FACEBOOK - *Padrões da Comunidade* [Em linha]. 2020a. [Consult. 27 out. 2020]. Disponível em WWW:< https://www.facebook.com/communitystandards/>.

FACEBOOK - *Termos de Serviço*. [Em linha]. 2020b. [Consult. 27 out. 2020]. Disponível em WWW:< https://pt-pt.facebook.com/legal/terms/>.

FARIA, Fernanda Cupolillo Miana De; ARAÚJO, Júlia Silveira De; JORGE, Marianna Ferreira - Caiu na Rede é Porn: Pornografia de Vingança, Violência de Gênero e Exposição da "Intimidade". *Contemporânea: Revista de Comunicação e Cultura* [Em linha]. Vol. 13, n.º 3 (2015), p. 659–677. [Consult. 27 out. 2020]. Disponível em WWW:< https://cienciasmedicasbiologicas.ufba.br/index.php/contemporaneaposcom/article/view/13999>. ISSN 1809-9386. DOI: 10.9771/1809-9386contemporanea.v13i3.13999.

FINOCCHIARO, Gusella - La protezione dei dati personali e la tutela dell'identità. In FINOCCHIARO, GIUSELLA; DELFINI, FRANCESCO (Eds.) - *Diritto dell'informatica*. San Mauro Torinese : UTET giuridica, 2014. ISBN 9788859811305. p. 150-181.

FINOCCHIARO, Giusella - ll diritto all'oblio nel quadro dei diritti della personalità. In ZENO-ZENCOVICH, VINCENZO; RESTA, GIORGIO (Eds.) - *Il diritto all'oblio su internet dopo la sentenza Google Spain*. Roma : Roma Tre-Press, 2015. ISBN 978-88-97524-27-4. p. 29-42.

FINOCCHIARO, Gusella - Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali. In FINOCCHIARO, GIUSELLA (Ed.) - *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*. Bologna : Zanichelli, 2017. ISBN 978-8808521057 p. 1–21.

FISCHER-HÜBNER, Simone et al. - Online Privacy – Towards Informational Self-Determination on the Internet. In HILDEBRANDT, MIREILLE; O'HARA, KIERON; WAIDNER, MICHAEL (Eds.) - *Digital Enlightenment Yearbook 2013*. Amsterdam : IOS Press, 2013. ISBN 978-1-61499-295-0. p. 123–138.

FORSTER, Katie - Tiziana Cantone: Woman's suicide after sex tape went viral prompts calls for stronger online privacy laws. *Independent* [Em linha]. 16 set. 2016. [Consult. 27 Out. 2020]. Disponível em WWW:< https://www.independent.co.uk/news/world/europe/tiziana-cantone-sex-tape-revenge-porn-suicide-death-italy-online-privacy-laws-campaign-overhaul-a7310956.html>.

FRANKS, Mary Anne - Redefining "Revenge Porn" Reform: A View From the Front Lines. *Florida Law Review* [Em linha]. Vol. 69, n. 5 (2016), p. 1251–1337. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://scholarship.law.ufl.edu/flr/vol69/iss5/2/.>. ISSN 1045-4241.

FREEMAN, Sunny - Porn 2.0, and Its Victims. *The Tyee* [Em linha]. 6 jul. 2007. [Consult. 27 Out. 2020]. Disponível em WWW:<URL:https://thetyee.ca/Mediacheck/2007/07/06/Porn2-0/>.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI - *Linee guida in materia di attività promozionale e contrasto allo spam*. 2013 [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2542348>.

GAVISON, Ruth - Privacy and the limits of law. *The Yale Law Journal* [Em linha].Vol. 89, n.º 3 (1980), p. 421–471. [Consult. 28 Out. 2020]. Disponível em WWW:<URL:

https://www.jstor.org/stable/795891?seq=1#metadata_info_tab_contents.>. ISSN 0044-0094. DOI: 10.2307/795891.

GIOVANNANGELI, Selvaggia Fausta - L'informativa agli interessati e il consenso al trattamento. In PANETTA, ROCCO (Ed.) - *Circolazione e Protezione dei Dati Personali, tra Libertà e Regole del Mercato: Commentario al Regolamento UE n. 2016/679 (GDPR) e al Novellato D.lgs. n. 196/2003 (Codice Privacy): Scritti in Memoria di Stefano Rodotà*. Milano : Giuffrè Francis Lefebvre, 2019. ISBN 9788828809692. p. 99–141.

GONZÁLES FUSTER, Gloria; GUTWIRTH, Serge - Privacy 2.0? *Revue du droit des Technologies de l'Information* [Em linha]. n.º 32, (2008) 349–359. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://works.bepress.com/serge_gutwirth/12/>. ISSN 1781-054X.

GOOGLE - *Requests to delist content under European privacy law* [Em linha], atual. 2020. [Consult. 28 out. 2020]. Disponível em WWW:<URL:https://transparencyreport.google.com/eu-privacy/overview?hl=en>.

GORZEMAN, Ludo; KORENHOF, Paulan - Escaping the Panopticon Over Time. Balancing the Right To Be Forgotten and Freedom of Expression in a Technological Architecture. *Philosophy & Technology* [Em linha]. Vol. 30, n.º 1 (2017), p. 73–92. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://link.springer.com/article/10.1007/s13347-016-0238-y >. ISSN 2210-5441. doi: 10.1007/s13347-016-0238-y.

GREGORIO, Giovanni De - The e-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society? *Robert Schuman Centre for Advanced Studies Research Paper EUI RSCAS; 2019/36* [Em linha]. (2019), p. 1–13. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3393557>.

HALL, Matthew; HEARN, Jeff - *Revenge Pornography: gender, sexualities and motivations*. New York : Routledge, 2018. 151 p. ISBN 978-1-138-12440-0.

HART, H. L. A. - *Punishment and Responsibility - Essays in the Philosophy of Law*. Oxford : Oxford University Press, 1975. 271 p. ISBN 0195003306.

HELBERGER, Natali; HOBOKEN, Joris VAN - Little Brother is tagging you - Legal and policy implications of amateur data controllers. *Computer Law International* [Em linha]. Vol. 11, n.º 4 (2010), p. 101–109. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://www.researchgate.net/publication/228218972_Little_Brother_Is_Tagging_You_-_Legal_and_Policy_Implications_of_Amateur_Data_Controllers>. ISSN 2194-4164. DOI: 10.9785/ovs-cri-2010-101.

HENRY, Nicola; POWELL, Anastasia - Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law. *Social & Legal Studies* [Em linha]. Vol. 25, n.º 4 (2016), p. 397–418. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://journals.sagepub.com/doi/full/10.1177/0964663915624273 >. ISSN 1461-7390 DOI: 10.1177/0964663915624273.

HENRY, Nicola; POWELL, Anastasia - Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. *Australian & New Zealand Journal of Criminology* [Em linha]. Vol. 48, n.º 1 (2015), p. 104–118. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://journals.sagepub.com/doi/10.1177/0004865814524218>. ISSN 1837-9273. DOI: 10.1177/0004865814524218.

HERT, Paul De; PAPAKONSTANTINOU, Vagelis - The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review* [Em linha]. Vol. 32, n.º 2 (2016), p. 179–194. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://www.sciencedirect.com/science/article/pii/S0267364916300346 >. ISSN 0267-3649. DOI: 10.1016/j.clsr.2016.02.006.

HILDEBRANDT, Mireille - Defining Profiling: A New Type of Knowledge? In HILDEBRANDT, MIREILLE; GUTWIRTH, SERGE (Eds.) - *Profiling the European citizen: Cross-disciplinary perspectives*. New York : Springer, 2008. ISBN 978-1-4020-6914-7. p. 17-45.

HILL, Kashmir - Revenge Porn With A Facebook Twist. *Forbes* [Em linha]. 6 jul. 2011. [Consult. 28 out. 2020]. Disponível em WWW:< https://www.forbes.com/sites/kashmirhill/2011/07/06/revenge-porn-with-a-facebook-twist/#30c6250d1d2e>.

HILL, Rachel - Cyber-Misogyny: Should 'Revenge Porn' be Regulated in Scotland, and If So, How? *Scripted* [Em linha]. Vol. 12, n.º 2 (2015), p. 117–140. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://www.researchgate.net/publication/297604362_Cyber-Misogyny_Should_'Revenge_Porn'_be_Regulated_in_Scotland_and_if_so_how >. ISSN 1744-2567. DOI: 10.2966/script.120215.117.

HOFFMAN, David; BRUENING, Paula; CARTER, Sophia - The Right to Obscurity: How we can implement the Google Spain decision. *North Carolina Journal of Law & Technology* [Em linha]. Vol. 17, n.º 3 (2015), p. 437–481. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://scholarship.law.unc.edu/ncjolt/vol17/iss3/2/>. ISSN 1542-5177.

HOUSE OF REPRESENTATIVES - *The Computer and Invasion Of Privacy: Hearings Before a Subcommittee of the Committee on Government Operations*. Washington : U.S. Government Printing Office, 1966. 318 p.

INFORMATION COMMISSIONER'S OFFICE - *Social networking and online forums – when does the DPA apply?* [Em linha]. 2013. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf>.

JÄÄSKINEN, Niilo - *Conclusões do Advogado-Geral no Processo C-131/12, Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*. [Em linha]. 2013. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62012CC0131&from=PT>.

KELLER, Daphne - The right tools: Europe's intermediary liability laws and the EU 2016 General Data Protection Regulation. *Berkeley Technology Law Journal* [Em linha]. Vol. 33, n.º 1 (2018), p. 287–364. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://heinonline.org/HOL/Page?handle=hein.journals/berktech33&div=10&g_sent=1&casa_token=&collection=journals>. ISSN 1086-3818.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore - Private traits and attributes are predictable from digital records of human behavior. P*roceedings of the National Academy of Sciences of the United States of America* [Em linha]. Vol. 110, n.º 15 (2013), p. 5802–5805. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://www.pnas.org/content/110/15/5802>. ISSN 1091-6490. DOI: 10.1073/pnas.1218772110.

KULK, Stefan; BORGESIUS, Frederik Zuiderveen - Google Spain v. González: Did the Court Forget about Freedom of Expression? *European Journal of Risk Regulation* [Em linha]. Vol. 5, n.º 3 (2014), p. 389–398. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://www.jstor.org/stable/24323469?seq=1#metadata_info_tab_contents>. ISSN 2190-8249.

LANGLOIS, Ganaele; SLANE, Andrea - Economies of reputation: the case of revenge porn. *Communication and Critical/Cultural Studies* [Em linha]. Vol. 14, n.º 2 (2017), p. 120–138. doi: [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://www.tandfonline.com/doi/abs/10.1080/14791420.2016.1273534?src=recsys&journalCode=rccc20>. ISSN 14791420 , 14794233. DOI: 10.1080/14791420.2016.1273534.

LETTERON, Roseline - Le droit à l'oubli. *Revue du Droit Public et de la Politique en France et a L'Etranger*. Vol. 112, n.º 2 (1996), p. 385–424.

LÉVY, Pierre - *Cyberculture: rapport au Conseil de l'Europe dans le cadre du project «Nouvelles technologies: coopération culturelle et communication».* Mesnil-sur-l'Estrée : Odile Jacob, 1997. 313 p. ISBN 2-7381-0512-2.

LINDON, Raymond - *Les droits de la personnalité*. Paris : Dalloz, 1983. 321 p. ISBN 2247004334.

LYNSKEY, Orla - Deconstructing data protection: The 'added-value' of a right to data protection in the EU legal order. *International and Comparative Law Quarterly* [Em linha]. Vol. 63, n.º 3 (2014), p. 569–597. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/deconstructing-data-protection-the-addedvalue-of-a-right-to-data-protection-in-the-eu-legal-order/95BD4CCF4670466FD4F6EBAD7DDB4E76>. ISSN 1471-6895. DOI: 10.1017/S0020589314000244.

LYNSKEY, Orla - Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez. *The Modern Law Review* [Em linha]. Vol. 78, n.º 3 (2015), p. 522. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2601584>. ISSN 1468-2230 DOI: 10.1111/1468-2230.12126.

MADDOCKS, Sophie - From Non-consensual Pornography to Image-based Sexual Abuse: Charting the Course of a Problem with Many Names. *Australian Feminist Studies* [Em linha]. Vol. 33, n.º 97 (2018), p. 345–361. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://www.tandfonline.com/doi/abs/10.1080/08164649.2018.1542592 >. ISSN 1465-3303. DOI: 10.1080/08164649.2018.1542592.

MANTELERO - The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law and Security Review* [Em linha]. Vol. 29, n.º 5 (2013), p. 229–235. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://www.sciencedirect.com/science/article/pii/S0267364913000654>. ISSN 0267-3649. DOI: 10.1016/j.clsr.2013.03.010.

MARSHALL, Carrie - Porn 3.0: the next gen of sex biz tech. *Techradar.* [Em linha]. 30 jun. 2009. [Consult. 28 Out. 2020]. Disponível em WWW:<URL:https://www.techradar.com/news/world-of-tech/porn-3-0-the-next-gen-of-sex-biz-tech-612328?artc_pg=2>.

MARTINS, Leonardo - *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão. Montevidéu : Fundación Konrad-Adenauer*, 2005. 993 p. ISBN 9974-7942-1-8. 993 p.

MAYER-SCHÖNBERGER, Viktor - Generational Development of Data Protection in Europe. In AGRE, PHILIP; ROTENBERG, MARC (Eds.) - *Technology and Privacy: the new landscape*. 3. ed. Cambridge : The MIT Press, 1997. ISBN 0-262-01162-X. p. 219–241.

MAYER-SCHÖNBERGER, Viktor - *Delete: the virtue of forgetting in the Digital Age* [Em linha]. New Jersey : Princeton University Press, 2009. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://www.jstor.org/stable/j.ctt7t09g>. ISBN 978-0-691-13861-9.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth - *Big data: a revolution that will transform how we live, work and think* [Em linha]. New York : Houghton Mifflin Harcourt, 2013. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://www.amazon.com/Big-Data-Essential-Learning-Insight-ebook/dp/B00BCK1A5Q/ref=tmm_kin_swatch_0?_encoding=UTF8&qid=&sr=>. ISBN 978-0-544-00293-7.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith - The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society* [Em linha]. Vol. 4, n.º 3 (2008), p. 543–568. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://heinonline.org/HOL/Page?handle=hein.journals/isjlpsoc4&div=27&g_sent=1&casa_token=&collection=journals>. ISSN 2372-2959.

MCGLYNN, Clare; RACKLEY, Erika; HOUGHTON, Ruth - Beyond 'Revenge Porn': The Continuum of Image- Based Sexual Abuse. *Feminist Legal Studies* [Em linha]. Vol. 25, n.º 1 (2017), p. 25–46. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://link.springer.com/article/10.1007/s10691-017-9343-2>. ISSN 1572-8455. doi: 10.1007/s10691-017-9343-2.

MCGLYNN, Clare; VERA-GRAY, Fiona - Porn Website T&Cs Are A Works Of Fiction. We Need Radical Measures To Take Them On. *Huffpost* [Em linha] 28 jun. 2019. [Consult. 28 Out. 2020]. Disponível em WWW:<URL:https://www.huffingtonpost.co.uk/entry/porn-website-tcs_uk_5d132febe4b09125ca466358>.

MEZZANOTTE, Massimiliano - *Il diritto all'oblio. Contributo allo studio della privacy storica*. Napoli : Edizioni Scientifiche Italiane, 2009. 311 p. ISBN 978-88-495-1740-8.

MICROSOFT - *Online Reputation in a Connected World* [Em linha]. 2010. [Consult. 28 Out. 2020]. Disponível em WWW:<URL:https://webcache.googleusercontent.com/search?q=cache:V0M7mabcuG4J:https://download.microsoft.com/download/C/D/2/CD233E13-A600-482F-9C97-545BB4AE93B1/DPD_Online%2520Reputation%2520Research_overview.doc+&cd=3&hl=en&ct=clnk&gl=br>.

MILLER, Arthur Raphael - *The Assault on Privacy*. Ann Arbor : The University of Michigan Press, 1971. 333 p. ISBN 0-472-65500-0.

NEGROPONTE, Nicholas - *Being digital*. New York : Vintage Books, 1995. 255 p. ISBN 0-679-76290-6.

NISSENBAUM, Helen - Privacy as contextual integrity. *Washington Law Review* [Em linha]. Vol. 79, n.º 1 (2004), p. 101–139. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://heinonline.org/HOL/Page?handle=hein.journals/washlr79&div=16&g_sent=1&casa_token=&collection=journals>. ISSN 1942-9983.

NISSENBAUM, Helen - *Privacy in context: Technology, Policy, and the Integrity of Social Life*. Stanford : Stanford University Press, 2010. 288 p. ISBN 978-0-8047-5236-7.

O'HARA, Kieron - The Right to Be Forgotten: The Good, the Bad, and the Ugly. *IEEE Internet Computing* [Em linha]. Vol. 19, n.º 4 (2015), p. 73–79. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://ieeexplore.ieee.org/document/7131393 >. doi: 10.1109/MIC.2015.88.

O'REILLY, Tim - *What Is Web 2.0: Design Patterns And Business Models For The Next Generation Of Software* [Em linha]. 30 set. 2005. [Consult. 28 Out. 2020]. Disponível em WWW:<URL:https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>.

OHLHEISER, Abby - Revenge porn purveyor Hunter Moore is sentenced to prison. *Washington Post* [Em linha]. 3 dez. 2015. [Consult. 28 Out. 2020]. Disponível em WWW:<URL:https://www.washingtonpost.com/news/the-intersect/wp/2015/12/03/revenge-porn-purveyor-hunter-moore-is-sentenced-to-prison/>.

ORTIZ, Ana Isabel Herrán - El derecho a la protección de datos personales en la sociedad de la información. *Cuadernos Deusto de Derechos Humanos*. n. 26 (2003), p. 9–92. ISSN 1130-8354.

PARDOLESI, Roberto; CIOMMO, Francesco Di - Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la Rete, bellezza! *Danno e Responsabilità*. n.º 7 (2012), p. 701–716. ISSN 1973-8099.

PEÑA, Paz; VARON, Juana - Consent to our Data Bodies: lessons from feminist theories to enforce data protection. *Coding Rights* [Em linha]. (2019). [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://codingrights.org/docs/ConsentToOurDataBodies.pdf>.

PEREIRA, Alexandre Libório Dias - O responsável pelo tratamento de dados segundo o Regulamento Geral de Proteção de Dados (RGPD). *Boletim da Faculdade de Direito da Universidade de Coimbra* [Em linha]. Vol. 95, n.º 2 (2019), p. 1161–1188. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://heinonline.org/HOL/Page?handle=hein.journals/boltfdiuc95&id=929&collection=journals&index=journals/boltfdiuc>. ISSN: 0303-9773.

PIERFELICI, Valeria - Relazioni. In GABRIELLI, ENRICO (Ed.) - *Il Diritto all'Oblio: Atti del Convegno di Studi del 17 maggio 1997.* Napoli : Edizioni Scientifiche Italiane, 1999. ISBN 88-8114-714-9. p. 55–95.

PINHEIRO, Alexandre Sousa - *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*. Lisboa : AAFDL, 2015. 907 p. ISBN 5606939008169.

PINHEIRO, Alexandre Sousa - Artigo 4o, 11). In PINHEIRO, ALEXANDRE SOUSA (Ed.) - *Comentário ao Regulamento Geral de Proteção de Dados*. Coimbra : Almedina, 2018. ISBN 978-972-40-7786-4. p. 166–173.

PINTO, Carlos Alberto Da Mota - *Teoria Geral do Direito Civil*. 4. ed., 2ª Reimp. Coimbra : Coimbra Editora, 2012. 687 p. ISBN 972-32-1325-7.

PINTO, Paulo Mota - O direito à reserva sobre a intimidade da vida privada. *Boletim da Faculdade de Direito: Universidade de Coimbra* [Em linha]. Vol. 69, (1993), p. 479–586. . [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://heinonline.org/HOL/Page?handle=hein.journals/boltfdiuc69&id=1&size=2&collection=journals&index=journals/boltfdiuc>. ISSN: 0303-9773.

POLITOU, Eugenia; ALEPIS, Efthimios; PATSAKIS, Constantinos - Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity* [Em linha]. Vol. 4, n.º 1 (2018), p. 1–20. [Consult. 28 Out. 2020]. Disponível em WWW:<URL: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056>. ISSN 2057-2093 doi: 10.1093/cybsec/tyy001.

PORNHUB - *Terms Of Service* [Em linha], 2020a. [Consult. 26 Set. 2020]. Disponível em WWW:<URL:https://pt.pornhub.com/information/terms>.

PORNHUB - *What is the difference between subscribers and friends?* [Em linha]. 2020b. [Consult. 26 Set. 2020]. Disponível em WWW:<URL:https://help.pornhub.com/hc/en-us/articles/360044327434-What-is-the-difference-between-subscribers-and-friends->.

POULLET, Yves - Data protection legislation: What is at stake for our society and democracy? *Computer Law & Security Review* [Em linha]. Vol. 25, n.º 3 (2009), p. 211–226. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://www.sciencedirect.com/science/article/pii/S0267364909000612>.
ISSN 0267-3649. DOI 10.1016/j.clsr.2009.03.008.

POULLET, Yves - About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In GUTWIRTH, SERGE; HERT, PAUL DE; POULLET, YVES (Eds.) - *Data Protection in a Profiled World*. Dordrecht : Springer, 2010. ISBN 978-90-481-8865-9. p. 3–30.

PROSSER, William - Privacy. California Law Review [Em linha]. Vol. 48, n.º 3 (1960), p. 383–423. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://www.jstor.org/stable/i276756 >. ISSN 0008-1221.

RAMASASTRY, Anita - Web sites change prices based on customers' habits. *CNN* [Em linha]. 24 jun. 2005. [Consult. 29 Out. 2020]. Disponível em WWW:<URL:http://edition.cnn.com/2005/LAW/06/24/ramasastry.website.prices/>.

RICCI, Annarita - I diritti dell'interessato. In FINOCCHIARO, GIUSELLA (Ed.) - *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali.* Bologna : Zanichelli, 2017. ISBN 978-8808521057. p. 179–250.

RICHARDS, Neil M. - Griswold v. Connecticut, 381 U.S. 479 (1965). In STAPLES, WILLIAM G. (Ed.) - *Encyclopedia of Privacy Vol. 1*. Westport e Londres : Greenwood Press, 2007. ISBN 0–313–33478–1 p. 261–266.

RODOTÀ, Stefano - *Tecnologie e diritti*. Bologna : Il Mulino, 1995. 406 p. ISBN 88-15-04855-3.

RODOTÀ, Stefano - Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali. *Rivista Critica del Diritto Privato*. Vol. 15, (1997), p. 683–609. ISSN 1123-1025.

RODOTÀ, Stefano - Data Protection as a Fundamental Right. Em GUTWIRTH, SERGE et al. (Eds.) - *Reinventing Data Protection?* Dordrecht : Springer, 2009. ISBN 978-1-4020-9498-9. p. 77–82.

RODOTÀ, Stefano - *Il diritto di avere diritti*. Bari : Laterza, 2012. 433 p. ISBN 9788842096085.

RODRIGUES, Carla Estela Dos Santos; ARAÚJO, Erônides Câmara De - Leis civis e penais machistas do século xx e a obra Homens Traídos. *A Barriguda* [Em linha]. Vol. 6,

n,.º 2 (2016), p. 277–296. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: http://oasisbr.ibict.br/vufind/Record/CIPED-2_13c62488b76768f9787ee2c9685eb737>. ISSN 2236-6695.

ROPPO, Enzo - I diritti della personalità. Em ALPA, GUIDO; BESSONE, MARIO (Eds.) - *Banche dati telematica e diritti della persona*. Padova : CEDAM, 1984. ISBN 2560448237119. p. 61–87.

ROSENBLAT, Alex; KNEESE, Tamara; BOYD, Danah - Networked employment discrimination. Open Society Foundations' *Future of Work Commissioned Research Papers* [Em linha]. (2014), p. 1–17. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2543507>. DOI: 10.2139/ssrn.2543507.

ROTENBERG, Marc - Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get). *Stanford Technology Law Review* [Em linha]. (2001), p. 1–35. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://heinonline.org/HOL/Page?handle=hein.journals/stantlr2001&div=2&g_sent=1&casa_token=&collection=journals>. ISSN 1098-4267.

RUVALCABA, Yanet; EATON, Asia A. - Nonconsensual Pornography Among U.S. Adults: A Sexual Scripts Framework on Victimization, Perpetration, and Health Correlates for Women and Men. *Psychology of Violence* [Em linha]. Vol. 10, n.º 1 (2020), p. 68–78. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://www.researchgate.net/publication/330858398_Nonconsensual_Pornography_Among_US_Adults_A_Sexual_Scripts_Framework_on_Victimization_Perpetration_and_Health_Correlates_for_Women_and_Men >. ISSN 2152081X. DOI: 10.1037/vio0000233.

RYAN, David - European remedial coherence in the regulation of non-consensual disclosures of sexual images. *Computer Law & Security Review* [Em linha]. Vol. 34, n.º 5 (2018), 1053–1076. [Consult. 29 Out. 2020]. Disponível em WWW:<URL:

https://www.sciencedirect.com/science/article/pii/S0267364918300475 >. ISSN 0267-3649. DOI: 10.1016/j.clsr.2018.05.016.

S. G. P. - Torts: The Right to Privacy and the Pursuit of Happiness. *California Law Review* [Em linha]. Vol. 20, n.º1 (1931), p. 100–102. . [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://www.jstor.org/stable/3475941?seq=1#metadata_info_tab_contents>. ISSN 0008-1221 DOI: 10.2307/3475941.

SARTOR, Giovanni - Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms? *International Data Privacy Law* [Em linha]. Vol. 3, n.º 1 (2013), p. 3–12. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://academic.oup.com/idpl/article/3/1/3/643990>. ISSN 2044-4001 doi: 10.1093/idpl/ips034.

SCHREIBER, Anderson - *Direitos da Personalidade*. 2. ed. São Paulo : Atlas, 2013. 275p. ISBN 978-85-224-7895-8.

SINGLETON, Jennifer; SEIGNIOR, Bryony; SUZOR, Nicolas - Non-Consensual Porn and the Responsibilities of Online Intermediaries. *Melbourne University Law Review* [Em linha]. Vol. 40, n.º 3 (2017), p. 1057–1097. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://www.researchgate.net/publication/317754687_Non-consensual_porn_and_the_responsibilities_of_online_intermediaries>. ISSN 0025-8938.

SMITH, H. Jeff - *Managing Privacy: Information Technology and Corporate America*. Chapel Hill : University of North Carolina Press, 1994. 297 p. ISBN 0-8078-4454-3.

SOLOVE, Daniel J. - *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven : Yale University Press, 2007. 247 p. ISBN 978-0-300-12498-9.

SOLOVE, Daniel J. - Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* [Em linha]. Vol. 126, n.º 7 (2013), p. 1880–1903. [Consult. 29 Out. 2020].

Disponível em WWW:<URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018>. ISSN 0017-811X.

SOUSA, Rabindranath V. A. Capelo De - *O Direito Geral de Personalidade*. Coimbra : Wolters Kluwer, 2011. 703p. ISBN 9723206773.

STEINFELD, Nili - "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior* [Em linha]. Vol. 55, (2016), p. 992–1000. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://www.sciencedirect.com/science/article/pii/S0747563215301692>. ISSN 0747-5632. doi: 10.1016/j.chb.2015.09.038.

SYKES, Charles J. - *The end of privacy*. New York : St. Martin's Press, 1999. 292 p. ISBN 0-312-20350-0.

TRUSTE - Consumers Have False Sense of Security About Online Privacy - Actions Inconsistent With Attitudes. *PR Newswire*. [Em linha]. 6 dez. 2006. [Consult. 29 Out. 2020]. Disponível em WWW:<URL:https://web.archive.org/web/20170316063146/http://www.prnewswire.com:80/news-releases/consumers-have-false-sense-of-security-about-online-privacy---actions-inconsistent-with-attitudes-55969467.html>.

TUROW, Joseph et al. - The FTC and Consumer Privacy In the Coming Decade. *Samuelson Law, Technology and Public Policy Clinic* [Em linha]. 8 nov. 2006. [Consult. 29 Out. 2020]. Disponível em WWW:< https://www.law.berkeley.edu/files/FTC_Consumer_Privacy.pdf >.

UNCULAR, Selen - The right to removal in the time of post-google Spain: myth or reality under general data protection regulation? *International Review of Law Computers & Technology* [Em linha]. Vol. 33, n.º 3 (2019), p. 309–329. . [Consult. 29 Out. 2020]. Disponível em WWW:<

https://www.tandfonline.com/doi/abs/10.1080/13600869.2018.1533752?journalCode=cirl20>. ISSN 13646885.

VALDÉS, Isabel - "Ya no puedo más". *El País* [Em linha]. 2 jun. 2019. [Consult. 27 Out. 2020]. Disponível em WWW:<URL:https://elpais.com/sociedad/2019/06/01/actualidad/1559383749_362348.html>.

VALENTE, Mariana Giorgetti et al. - *O Corpo é o Código* [Em linha]. São Paulo : InternetLab, 2016. 191 p. ISBN 978-85-92871-00-0. [Consult. 27 Out. 2020]. Disponível em WWW:<URL: https://www.internetlab.org.br/wp-content/uploads/2016/07/OCorpoOCodigo.pdf>.

VASCONCELOS, Pedro Pais De - Protecção de dados pessoais e direito à privacidade. In MELO, ALBERTO DE SÁ E; VICENTE, DÁRIO MOURA; ASCENSÃO, JOSÉ DE OLIVEIRA (Eds.) - *Direito da Sociedade da Informação Vol. I*. Coimbra : Coimbra Editora, 1999. ISBN 9723209160. p. 241–253.

VLACHOPOULOS, Spyridon - Freedom of expression in the internet: The example of the «Right to be Forgotten». *Revue Européenne de droit public*. Vol. 30, n.º 1 (2018), p. 113–120. ISSN 1105-1590.

WARREN, Samuel D.; BRANDEIS, Louis D. - The Right to Privacy. *Harvard Law Review*. Vol. 4, n.º 5 (1890), p. 193–220. ISSN 0017-811X.

WESTIN, Allan - *Privacy and Freedom*. New York : Atheneum, 1967. 487 p.

WILLIAMS, Robert W. - Politics and self in the age of digital (re)producibility. *Fast Capitalism* [Em linha]. Vol. 1, n.º 1 (2005), p. 104–121. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://www.researchgate.net/publication/331243366_Politics_and_Self_in_the_Age_of_Digital_Reproducibility>. ISSN 1930-014X. DOI: 10.32855/fcapital.200501.008.

WONG, Rebecca - Social networking: a conceptual analysis of a data controller. *Communications Law* [Em linha]. Vol. 14, n.º5 (2009), p. 142–149. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1529738 >. ISSN 17467616.

XVIDEOS - *Terms of Service.* [Em linha], 2020. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://info.xvideos.com/legal/tos>.

YOUPORN - *YouPorn Terms Of Service*. 2016. [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://www.youporn.com/information/#terms>.

ZENO-ZENCOVICH, Vincenzo; RESTA, Giorgio - Volontà e consenso nella fruizione dei servizi in rete. *Rivista Trimestrale di Diritto e Procedura Civile* [Em linha]. n.º 2 (2018), p. 411–440. . [Consult. 29 Out. 2020]. Disponível em WWW:<URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213551>. ISSN 2499-2836.

JURISPRUDÊNCIA

Tribunal de Justiça da União Europeia

Acórdão do Tribunal De Justiça. 20 de Maio de 2003, C-465/00, C-138/01 e C-139/01 *Österreichischer Rundfunk e o.,* ECLI:EU:C:2003:294.

Acórdão do Tribunal de Justiça. 6 de novembro de 2003, C-101/01, *Lindqvist*, ECLI:EU:C:2003:596.

Acórdão do Tribunal de Primeira Instância (Terceira Secção). 8 de Novembro de 2007, T-194/04, Bavarian Lager/Comissão, ECLI:EU:T:2007:334.

Acórdão do Tribunal De Justiça (Grande Secção). 29 de junho de 2010, C-28/08 P, Comissão/Bavarian Lager, ECLI:EU:C:2010:378.

Acórdão do Tribunal De Justiça (Grande Secção). 13 de maio de 2014, C-131/12, *Google Spain e Google*, ECLI:EU:C:2014:317.

Acórdão do Tribunal De Justiça (Quarta Secção). 11 de dezembro de 2014, C-212/13, *Ryneš*, ECLI:EU:C:2014:2428.

Acórdão do Tribunal De Justiça (Grande Secção). 5 de junho de 2018, C-210/16, *Wirtschaftsakademie Schleswig-Holstein,* ECLI:EU:C:2018:388.

Acórdão do Tribunal De Justiça (Grande Secção). 10 de julho de 2018, C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551.

Acórdão do Tribunal De Justiça (Segunda Secção). 14 de fevereiro de 2019, C-345/17, *Buivids*, ECLI:EU:C:2019:122.

Tribunal Europeu dos Direitos do Homem

Acórdão do Tribunal Europeu dos Direitos do Homem. 31 de janeiro de 1995. *Friedl v. Austria*, ECLI:CE:ECHR:1995:0131JUD001522589.

Comissão Europeia dos Direitos do Homem

Applications 32200/96 e 32201/96. Decision of 14 January 1998. *Pierre Herbecq and the Association 'Ligue des droits de l'homme' v Belgium*.

Corte di Cassazione (Itália)

Cassazione, terza sez. civile – sentenza 09 aprile 1998, n. 3679.

Cassazione., terza sez. civile – sentenza 5 aprile 2012, n. 5525

Cassazione, sez. III Penale, sentenza 17 dicembre 2013, 3 febbraio 2014, n. 5107

Audiencia Nacional (Espanha)

Audiencia Nacional. Sala de lo Contencioso. 29 de diciembre de 2014. Sentencia SAN 5252/2014 - ECLI: ES:AN:2014:5252.

Supreme Court of the United States (Estados Unidos da América)

Griswold v. Connecticut. 381 U.S. 479 (more) 85 S. Ct. 1678; 14 L. Ed. 2d 510; 1965 U.S. LEXIS 2282

Eisenstadt v. Baird 405 U.S. 438 (more) 92 S. Ct. 1029; 31 L. Ed. 2d 349; 1972 U.S. LEXIS 145

United States Court of Appeals

U.S. Court of Appeals for the Second Circuit - 113 F.2d 806 (2d Cir. 1940) July 22, 1940