



## A HIPEREXPOSIÇÃO PESSOAL E O DIREITO AO ESQUECIMENTO E À EXTIMIDADE

Gustavo Noronha de Ávila<sup>1</sup>

Thaís Aline Mazetto Corazza<sup>2</sup>

**RESUMO:** Objetiva-se analisar o direito à privacidade na Sociedade da Informação, os riscos decorrentes da hiperexposição nas redes sociais e seus desdobramentos, em especial na área penal. A pesquisa parte de um raciocínio hipotético-dedutivo e será bibliográfica e documental, onde se buscará alcançar uma exata compreensão por meio de materiais como leis, sites oficiais e doutrina jurídica aplicável ao tema. Concluiu-se que a sociedade da informação atual trouxe mudanças de sentido no que se entende como direito à privacidade e seus desdobramentos onde se incluem o direito ao esquecimento e o direito à extimidade.

**PALAVRAS-CHAVE:** Privacidade; Sociedade da Informação; Hiperexposição Pessoal; Direito ao esquecimento; Direito à extimidade.

### PERSONAL HYPEREXPOSURE AND THE RIGHT TO OBLIGATION AND EXTIMITY

**ABSTRACT:** The objective is to analyze the right to privacy in the Information Society, the risks arising from overexposure in social networks and its consequences, especially in the penal area. The research starts from a hypothetical-deductive reasoning and will be bibliographic and documentary, in which an exact understanding will be sought through materials such as laws, official websites and legal doctrine applicable to the theme. It was concluded that the current information society has brought changes in the meaning of what's understood as the right to privacy and its consequences, which include the right to be forgotten and the right to extimacy.

**KEYWORDS:** Privacy; Information Society; Personal Hyperexposure; Right to be forgotten; Right to Extimacy.

## 1 INTRODUÇÃO

<sup>1</sup> Possui graduação em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul, Mestrado e Doutorado em Ciências Criminais pela Pontifícia Universidade Católica do Rio Grande do Sul. Realizou Estágio de Pós-Doutoramento, sob a supervisão da Profa. Dra. Lilian Milnitsky Stein, no Programa de Pós-Graduação em Psicologia da PUCRS. Professor da Pontifícia Universidade Católica do Paraná (Campus Maringá). Professor Permanente do Programa de Pós-Graduação, Mestrado e Doutorado, em Ciência Jurídica do Centro Universitário de Maringá. Também é Professor da Especialização em Ciências Penais da Universidade Estadual de Maringá, ABDConst, Universidade Ceuma, PUCPR, Univel, Universidade Feevale e Instituto Paranaense de Ensino. E-mail: gusnavila@gmail.com.

<sup>2</sup> Doutoranda e Pesquisadora Capes do Programa de Pós-Graduação, Doutorado, em Ciência Jurídica do Centro Universitário de Maringá. Mestre e graduada em Ciências Jurídicas pelo Centro Universitário de Maringá – UNICESUMAR. E-mail: thaiscorazza@hotmail.com.





O período atual histórico é conhecido como a Era Digital que se refere à realidade tecnológica como mediadora das relações humanas e do intercâmbio entre máquinas, essas cada vez mais autônomas. A Sociedade da Informação se compõe no contexto de aceitação global, na qual o incremento da tecnologia reconfigurou o modo de existir, de ser, de se relacionar e de agir das pessoas, propondo os modelos de comunicação vigentes. A tecnologia não pode ser separada da informação e isso vem sendo remodelado e institucionalizado com os progressos na área do conhecimento e das técnicas.

Nesse contexto, se verifica que o Direito, nos países adeptos ao *Civil Law*, padece com a realidade virtual, tendo dificuldade para garantir o seu fundamento, já que as mudanças por costumes acontecem subitamente. O Direito à intimidade e à privacidade fazem parte dos direitos da personalidade. Trata-se da proteção do modo de ser e do próprio ser do indivíduo. Porém, a maior parte das pessoas que cedem e informam seus dados, de forma voluntária ou não, não possuem ciência da destinação desses dados.

A hiperexposição decorrente do avanço da Era Digital pode gerar consequências e danos imensuráveis e de difícil reparação. Isso porque a privacidade se refere a coleta de informações e ao direito a ser deixado só, sendo que a exposição (involuntária ou não) demasiada culmina na impossibilidade do controle do uso das informações pessoais.

Objetiva-se com o presente artigo analisar o direito à privacidade dentro do contexto da Sociedade da Informação e os riscos decorrentes da hiperexposição pessoal nas redes sociais, sopesando seu desdobraimento como o direito à extimidade e ao esquecimento.

Com o aparecimento da internet e das redes sociais, tornou-se hábito que os cidadãos divulguem suas informações em redes sociais sem conhecimento da devida dimensão do impacto que essa excessiva exposição possa provocar. Costuma ser negligenciada a segurança na rede e a exposição exacerbada torna vulnerável a proteção da privacidade, tornado os sujeitos vulneráveis aos mecanismos de controle do Estado e do Mercado.

É um estudo teórico que utiliza a abordagem fenomenológica-hermenêutica, com a finalidade de, com sua lógica compreensiva-descritiva, fundir horizontes e ratificar a afirmação inicial. A pesquisa usa um raciocínio hipotético-dedutivo e será bibliográfica e documental, buscando alcançar uma exata compreensão através de materiais como leis, jurisprudências, sites oficiais e doutrina jurídica aplicável ao tema (teses, dissertações, livros, artigos científicos, entre outros), de âmbito nacional e internacional.



Para isso se fará um panorama do direito à privacidade e dos dados pessoais na Sociedade da Informação, após, se fará uma análise da hiperexposição na Era Digital e por fim se analisará o direito ao esquecimento e o direito à intimidade.

## 2 OS DADOS PESSOAIS E O DIREITO À PRIVACIDADE

O Direito Digital tem como maior desafio equilibrar a difícil relação existente entre os interesses criados pelos novos veículos de comunicação: a privacidade, o comercial, a responsabilidade e o anonimato (PINHEIRO, 2016). Ocorre que essa equação só se fundamenta se tiver de um lado a vigilância e do outro a punibilidade.

Fazem parte dos direitos da personalidade o direito à privacidade e à intimidade. É a proteção da pessoa, do ser e do modo de ser. Entretanto, a maior parte daqueles que cedem e informam seus dados, de forma voluntária ou não, não tem ciência da destinação dos mesmos.

Os direitos da personalidade se tratam de prerrogativas de toda pessoa humana pela sua própria condição, referentes aos seus predicados essenciais e suas extensões. São considerados direitos absolutos, implicando um dever geral de abstenção para seu amparo. De acordo com a melhor doutrina, bem como com o artigo 11 do Código Civil, são ainda indisponíveis, irrenunciáveis, intransmissíveis, de difícil estimação pecuniária, inatos (originários), imprescritíveis, extrapatrimoniais, necessários e oponíveis *erga omnes*, vitalícios e impenhoráveis (BITTAR, 2003, p. 11).

O direito à privacidade, como direito da personalidade, é um limite natural ao direito de informação, não podendo haver lesão ao direito sem o consentimento do sujeito. No entanto, nos dias atuais, por conta própria, as pessoas expõem sua privacidade e intimidade diariamente nas redes, se esquecendo da falta de segurança na rede virtual.

Essa hiperexposição pessoal, advinda do avanço da Era Digital, é capaz de gerar consequências/danos irreparáveis e imensuráveis. A privacidade se refere ao direito de ser deixado só e a coleta de informações (RODOTA, 2008) e a exposição (voluntária ou involuntária) de forma demasiada impossibilita o controle da utilização das informações pessoais. É por isso que as recentes extensões da coleta e do tratamento de informações propagam a súplica à privacidade, ao mesmo tempo que majoram a consciência da impossibilidade de romper e colocar limites nas novas questões que surgem no tradicional quadro institucional deste conceito (RODOTA, 2008).



O desenvolvimento do conceito de privacidade preencheu o seu conteúdo com a reserva do indivíduo em si e a garantia de isolamento, ao mesmo tempo que deu ao sujeito o poder de controlar a utilização de suas próprias informações. Por tal motivo, prevalece na sociedade da informação as definições funcionais da privacidade que dizem respeito à possibilidade de remeter, conhecer, obstruir e controlar o fluxo das informações a ele relacionadas (ALMEIDA, TEIXEIRA, & TEPEDINO, 2016), devendo-se considerar sempre que os dados pessoais protegem os indivíduos e todo grupo nele inserido.

Da sua tradicional definição como o direito a ser deixado só, o conceito de privacidade passou, influenciado pela tecnologia dos computadores, ao conceito do direito a controlar o uso que os outros façam das informações que lhe dizem respeito. Por fim, mais recentemente surgiu um outro tipo de definição, segundo a qual a privacidade diz respeito ao direito do indivíduo de escolher aquilo que está disposto a revelar aos outros (ALMEIDA, TEIXEIRA, & TEPEDINO, 2016, p. 286).

O maior desafio está no estabelecimento de parâmetros razoáveis, pois os dados pessoais são capturados automaticamente e compartilhados. O centro da gravidade da cultura solidificou a desvalorização do passado, considerado avesso à razão e à liberdade, desconstruindo a confiabilidade do futuro, pela prioridade do “aqui e agora”, em uma temporalidade dominada pelo precário e pelo transitório (LIPOVETSKY, 2004), dinâmica esta, com a qual o direito parece não conseguir lidar (ALMEIDA, TEIXEIRA, & TEPEDINO, 2016).

Mesmo que a intimidade e a privacidade estejam dispostas e garantidas nos diplomas legais como direito e garantia fundamental, danos podem ocorrer, tendo em vista que os direitos individuais tradicionais e os sociais são antinômicos no sentido de que a realização integral de uns impede a de outros e quanto mais aumenta os poderes do sujeito, mais diminuem as suas liberdades (BOBBIO, 1992).

Dá a necessidade de amparo dos direitos que individualizam a pessoa em si e socialmente, ocorrendo a troca do “Nunca estar sozinho” pela esperança de “Nunca mais vou ficar sozinho” (BAUMAN, 2013, p. 30)

Decidindo se conectar, a pessoa aceita (ainda que tacitamente) a socialização e compartilhamento dos seus dados, consentindo com a perda do controle das suas informações (PINHEIRO, 2016). Quando se aceita os termos de uso dos aplicativos que são instalados há o consentimento em repassar as informações pessoais para terceiros.



A maioria dos termos de uso dos serviços explicita que mesmo que o sujeito deixe de ser usuário, o que já foi compartilhado permanecerá sob o domínio da internet para sempre, cabendo apenas ao sujeito refletir, antes, sobre o legado de conteúdo que deseja deixar a seu respeito, já que tecnicamente ainda é difícil conseguir praticar o direito ao esquecimento (PINHEIRO, 2016).

A colheita dos dados pessoais aumentou exponencialmente nas últimas décadas, e no Brasil foram criados mecanismos para garantir a proteção dos parâmetros mínimos de privacidade dos usuários de internet. Todavia, não obstante a existência do Marco Civil da Internet (Lei 12.965/2014) e suas normas a respeito da necessidade do livre consentimento e esclarecimento como requisito para a coleta, armazenamento, uso, tratamento e proteção de dados pessoais, bem como a Lei Geral de Proteção de Dados, não é isso que se nota, de fato, na prática (LIMA; BARRETO JUNIOR, 2016).

O primeiro empecilho na aplicação tecnológica dos algoritmos e coleta de dados das pessoas é a garantia de sua privacidade. Os algoritmos têm acesso a dados provenientes de um número crescente de fontes (ainda que anônimos), sendo que a partir da combinação do cruzamento delas se poderia aferir algumas características sobre uma pessoa específica, ainda que o sujeito nunca tenha divulgado tal informação. Para minimizar o impacto sobre a privacidade algumas medidas podem ser tomadas, tais como a agregação de dados anônimos. O aumento de algoritmos para a tomada de decisões baseadas em dados supõe a procura da objetividade e da vontade de tomar decisões baseadas em evidências, minimizando ou eliminando a discriminação, a injustiça, a corrupção ou a ineficiência das quais as decisões humanas não escapam (MONTJOYE, 2017).

Por sua natureza, o direito à privacidade é minucioso e em uma sociedade democrática gera sua proteção como critério orientador da imprensa livre (DE LUCCA & SIMAO FILHO, 2000, p. 476). Isso porque *“na onda das ferramentas digitais, as pessoas surfam muitas vezes inocentemente sem dar-se conta do informar”* (ALMEIDA, TEIXEIRA, & TEPEDINO, 2016, p. 354).

A segurança da informação sempre se deparou com um barreira natural na privacidade, questionando: *“se a monitoração e a vigilância são essenciais para prevenção de incidentes na Sociedade Digital, como fica a questão da privacidade neste mundo tão vigiado? Há quem*



*justifique o aumento da vigilância na Internet, que muitas vezes ultrapassa os limites da ética e da legitimidade e esbarra na espionagem digital” (PINHEIRO, 2016, p. 481).*

A transgressão da privacidade dos usuários da internet e a espionagem internacional e nacional são problemas mundiais e as normas regulamentadoras são ainda tímidas, já que não impõem limites drásticos aos governos, empresas e serviços de segurança. Muitos utilizam a internet para expressar anseios que na vida real (leia-se não virtual) tardariam a demonstrar, culminando em uma hiperexposição pessoal, sem considerar os riscos aos quais estão expostos. E simplesmente por se sentir feliz aceita o risco.

Ocorre que a vida virtual se difere, e muito, da real. Nas redes sociais não tem importância quem você é e o que faz, mas o que simula para a sociedade com suas postagens. A exposição excessiva não leva em conta o quanto isso pode ser prejudicial, e as consequências deste ato são proporcionais à sua exposição.

### 3 A HIPEREXPOSIÇÃO SOCIAL

O *Youtube* permitiu aos usuários comum fazer publicações e visualizar vídeos facilmente na internet, sem precisar de uma conexão direta entre as partes. A maioria da população não imaginava a migração e avanço tecnológico que estava prestes a acontecer, pois essas atividades que eram possíveis apenas por computadores de mesa passariam a serem feitas através dos Smartphones, especialmente com o desenvolvimento do sistema IOS e Androide. Houve com isso uma explosão de aplicativos, criados por plataformas, e as redes sociais passaram a conectar os usuários com a transferência de informações. Porém, de nada adianta excelentes softwares antivírus instalados e firewalls com boas configurações, se a pessoa que usa a rede clica em qualquer aplicativo que lhe é sugerido e informa dados sensíveis, sem ter a certificação do local e segurança daquilo (LIMA, 2016).

A hipótese de liberdade infinita e anárquica resguardada pela Internet conflita com a realidade atual onde há câmeras de vídeo para vigilância por todos os lados, a coleta dos rastros deixados pelo uso de cartão de crédito ou durante a navegação online, a venda de perfis pessoais cada vez mais detalhados, as possibilidades de interconexão entre os bancos de dados indicam a expansão progressiva de uma sociedade do controle, da vigilância e da classificação. Essa descrição das características da sociedade da informação intimida sombrear o aumento intenso dos bancos de dados mais tradicionais, ou seja, aqueles com finalidade de segurança que também sofrem modificações com a tecnologia. Em relação à União Europeia, verifica-se



claramente a multiplicação dos acordos e convenções de cooperação em matéria de justiça e segurança, o que leva a estruturação de grandes bancos de dados, como o caso do Acordo Schengen<sup>3</sup>, das convenções instituídas pela Europol<sup>4</sup> e do sistema alfandegário europeu, do regulamento Eurodac<sup>5</sup> (RODOTÀ, 2008).

Há bancos de dados em alguns países contendo DNA de indivíduos considerados perigosos. Ampliam-se as coletas de dados sobre a saúde. Ampliam-se as formas de controle com câmeras, já habituais em alguns setores como banco, e que controlam zonas consideradas perigosas. Há boas razões para sustentar a necessidade de utilização de todas as oportunidades oferecidas pelas novas tecnologias para proteger a sociedade dos crimes, fomentar a prevenção de doenças e proteger as pessoas dos riscos sociais em busca de justo equilíbrio entre uma visão individualista de privacidade e a satisfação das exigências sociais sempre. É justamente a necessidade do uso social das tecnologias que exige que sejam projetadas novas instituições de liberdade, capazes de evitar uma poluição da social e de garantir a defesa dos direitos fundamentais em um ambiente caracterizado pelo recurso às coletâneas de informações. Deve-se suspeitar do argumento de quem afirma que o cidadão honesto nada tem a temer com a disseminação das informações que lhe dizem respeito, pois o homem de vidro é uma metáfora totalitária, eis que nela se embasa a pretensão do Estado de saber de tudo, até mesmo dos aspectos mais íntimos da vida dos indivíduos (RODOTÀ, 2008).

As mídias sociais oferecem grande quantidade de informações sobre seus usuários, sendo tais dados usados para funções mais diversas, a exemplo, um recrutador de uma empresa pode examinar os costumes de um candidato; um criminoso pode buscar informações de suas próximas vítimas, entre outros. Neste último caso, a maneira como a maioria dos usuários se comportam, mostrando muitas informações pessoais em redes sociais causa grande preocupação, já que os criminosos, com uma simples visita a um perfil consegue descobrir

<sup>3</sup> O Acordo Schengen, firmado de 1995, elimina o controle do passaporte nas fronteiras de países europeus que fazem parte da “área Schengen”. No acordo houve a previsão de criação de um “Sistema d’Informazione Schengen (SIS)”, um banco de dados automatizado para a gestão e troca de informações entre os países aderentes à Convenção Europeia.

<sup>4</sup> Europol é a agência central de informações para cooperação na repressão à criminalidade na União Europeia.

<sup>5</sup> O Objetivo da Eurodac, conforme previsão do Regulamento (CE) n. 2725/2000 do Conselho, de 11.12.2000, foi a criação de um sistema para a comparação das impressões digitais de requerentes de asilo e de imigrantes clandestinos, a fim de facilitar a aplicação da Convenção de Dublin. O regulamento entrou em vigor e o Eurodac começou suas atividades em 15.01.2003.



nome de parentes, locais que a pessoa e seus familiares frequentam, e demais informações valiosas para criar seu plano de ataque (LIMA, 2016).

Esse problema não fica restrito as mídias sociais, sendo o mesmo de ordem comportamental. Houve grande aumento da hiperexposição pessoal nos últimos anos, seja para expor os bens e pertences, para expor suas práticas, entre outros. Essas inúmeras espécies de capturas de informações podem gerar ataques cibernéticos. Aproximadamente 300 horas de vídeos são publicados no *Youtube* por minuto, tornando-o a maior rede de vídeos mundial (LIMA, 2016), o que mostra a existência contínua da hiperexposição dos indivíduos e da ausência de fiscalização sobre tais publicações.

O serviço de pré-visualização e avaliação resultaria na falta de possibilidade econômica do serviço continuar a existir, sem falar nas inúmeras dificuldades para lidar em escala mundial com peculiaridades como identificar se tal conteúdo é ilícito em determinado país. Por exemplo, no direito brasileiro tal ação seria considerada censura prévia, ação esta que é vedada pela Constituição Federal (LIMA, 2016).

Buscando alcançar a liberdade de se expressão, se abre mão da segurança, ocorrendo uma troca da segurança para se atingir um ápice fictício de liberdade com a exposição. Porém, a liberdade de expressão acompanhada dos riscos relativos à redução da privacidade nos meios digitais pode culminar na hiperexposição, trazendo riscos pessoais presentes ou futuros, tanto para segurança quanto para reputação (GABRIEL, 2018).

No ano de 2010, o *Facebook* disponibilizou a funcionalidade de *check-in* para possibilitar que seus usuários compartilhassem suas informações sobre a localização na rede social. Após um mês, uma rede de assaltantes nos EUA roubou o equivalente a US\$ 100 mil em bens de 50 residências, levando em conta as pessoas que faziam *check-in* em lugares distantes de suas residências (GABRIEL, 2018).

Conscientemente ou não, os indivíduos passam suas informações à terceiros, e igualmente acontece no mundo não virtual, há diversos riscos na rede também. Em virtude da descontrolada hiperexposição, diversas pessoas acabam tendo sua reputação atingida, sendo que a única maneira de controlar isso seria por meio do uso racional do direito à privacidade, que permite revelar seletivamente os aspectos pessoais.



Ao interromper o controle sobre a privacidade pessoal, revelando suas informações pessoais *on-line*, os sujeitos acabam comprometendo sua própria reputação, pois as informações expostas na internet continuam eternamente no mundo virtual (GABRIEL, 2018).

Ressalta-se que todas as curtidas, bate-papo, comentários, *check-in*, fotos, etc., fazem parte da construção da reputação e se divide em pegadas, rastros e sombras. As pegadas ou *footprint* são informações pessoais compartilhadas ativa ou intencionalmente na internet, como *posts* e comentários nas mídias sociais, *check-ins*, fotos, entre outros. Os rastros ou *traces* são informações pessoais compartilhadas ativa ou intencionalmente na internet, como os dados que são disponibilizados nas navegações pela internet, como o IP, a configuração do computador, a localização, o *browser*, o IMEI do celular, entre outros. Finalmente, as sombras ou *shadows* são informações pessoais disponibilizadas por terceiros, como fotos menções, opiniões, depoimentos, etc. (GABRIEL, 2018).

Alguns rastros digitais são deixados tanto *on-line* quanto *off-line*, portanto, todos têm responsabilidade pelas ações e conteúdos compartilhados e pesquisados nas redes de internet. Uma simples brincadeira online para determinar com qual personagem você se parece em um filme confere informações sobre os traços de personalidade do indivíduo (GABRIEL, 2018). A preocupação que esses fatos trazem é que além de ser manipulativo, dificilmente pode ser detectado, acabando com a privacidade pessoal na internet.

Os rastros ligados as pegadas formam um rico dossiê a respeito das pessoas, possibilitando ao computador determinar sua personalidade de forma mais precisa do que um humano conseguiria fazer: gostos, preferências, reações, entre outros. Assim, o poder de exercer a privacidade está cada vez mais comprometido e limitado em decorrência do avanço tecnológico computacional inteligente, exigindo que se pense e se reconstrua as relações sociais (GABRIEL, 2018, p. 77).

O uso compulsivo das mídias sociais se liga diretamente à hiperexposição, que expõe a vida cotidiana, sem levar em consideração os riscos que tais atitudes podem causar, bem como a segurança das pessoas e da rede. Inicia-se o uso por um hábito de informar e acaba virando um vício em se expor. Entre as tecnologias digitais que estimulam esses hábitos o principal é o smartphone, pois converge a informação em tempo real, a exposição, o uso da tecnologia, a conexão e o *multitasking*, para um único dispositivo que está sempre ao alcance. Tanto é que depois da tempestade Sandy em 2012, em Nova Iorque, que provocou a ausência de energia



elétrica, inúmeros nova-iorquinos reportaram que suportaram crise de abstinência de celular (GABRIEL, 2018). O vício da exposição é tamanho que a preocupação das pessoas com a falta de energia elétrica está mais na ausência de carregamento dos celulares do que com própria segurança particular. As medidas em que a tecnologia digital permite conexão e exposição, as pessoas se exibem e passam mais tempo conectadas, porém continuam estranhamente mais sozinhas.

O que se nota é que a legitimidade de cada um está em ser visto pelo outro. Esse fenômeno tem se apassivado conforme as pessoas permanecem mais conectadas e com smartphones melhores, tanto é que a palavra *selfie* foi eleita a palavra de 2013 pelo *Oxford Dictionaries*. Além disso, as estatísticas demonstram que acidentes com *selfies* está matando mais do que tubarões, pois registrar e compartilhar a vida tem se tornado mais importante do que viver (GABRIEL, 2018).

Ao fazer a exposição de fatos relevantes da vida cotidiana, o sujeito se cerca de tecnologia, mas sente falta do toque humano. A exposição nas mídias alimenta o ego, expõe e deixa a pessoa vulnerável aos riscos e ainda gera a perda de segurança, causando danos à reputação. Ademais, pode ocorrer a perda da integridade quando, inexistindo a devida segurança, acontece a alteração de um tópico relevante que pode ser mudado pelos mais surpreendentes motivos (até mesmo intencionalmente) (DE LUCCA & SIMAO FILHO, 2000).

A confidencialidade é a segurança da rede. Se algumas informações forem vistas e copiadas por alguém que esteja utilizando a internet para praticar o mal, o ponto de segurança não está sendo observado. Hoje a sociedade da informação busca um equilíbrio entre a reserva da vida privada e a prestação da notícia (DE LUCCA & SIMAO FILHO, 2000), no entanto muitos expõem sua confidencialidade para serem notados na rede de internet.

Embora pareça excessivo e perigoso afirmar que “*nós somos nossos dados*”, é fato que a representação social de cada indivíduo está cada vez mais restrita às informações disseminadas nos diversos bancos de dados e as simulações construídas por tais meios. O sujeito torna-se cada vez mais conhecido como público ou privado por meio dos dados que lhe dizem respeito, acabando por incidir sobre a liberdade de comunicação, sobre o princípio de igualdade, de expressão ou de circulação, sobre a condição de trabalhar, entre outros. E se transformando em entidades desencarnadas, surge o imperativo de resguardar o seu “*corpo eletrônico*” (seus



dados pessoais) tanto contra a expansão do monitoramento estatal, quanto contra o seu sem discriminação de dados por empresas de diversos segmentos (SILVA, 2016).

#### 4 O DIREITO AO ESQUECIMENTO E À EXTIMIDADE

Como já dito anteriormente, a sociedade da informação atual trouxe mudanças de sentido no que se entende como direito à privacidade e seus desdobramentos como intimidade e vida privada (onde se incluem o “direito ao esquecimento” e o “direito à extimidade”)<sup>6</sup>.

O reconhecimento do direito à privacidade no sentido atual do termo teve início com a expressão norte-americana “*right to be let alone*”, apresentada por Samuel Warren e Louis Brandeis para a configuração do direito de ser deixado em paz/só. No entanto, a referida expressão, não raras as vezes, é usada como sinônimo do direito ao esquecimento (FORTES, 2015, p. 157), quando a adequada conceituação para o direito ao esquecimento seria “*right to be forgotten*”, vez que ultrapassa a simples proteção da vida privada, permitindo que um usuário apague dados e informações pessoais na internet (BERNAL, 2014).

Nesse contexto, em conferência na *New York University*, Eric Schmidt afirmou que um dos grandes desafios futuros da internet é elaborar um “botão delete”, dando oportunidade para as pessoas apagarem publicações relacionadas a atos feitos no passado que não querem mais que sejam expostos nos resultados de busca ou de páginas indexadas na web (FORTES, 2016).

O direito ao esquecimento pressupõe a necessidade de reconhecimento e amparo em face do Estado e de terceiros em um plano social ampliado, ou seja, de não sofrer de forma permanente e indeterminada as repercussões geralmente negativas conexas a fatos ocorridos do passado, fato que é essencial para uma vida pessoal saudável física e psicologicamente, auxiliando inclusive na integração do indivíduo na sociedade (SARLET, 2020).

A primeira vez que se utilizou o termo “direito ao esquecimento” foi pelo Tribunal Constitucional da Alemanha no Caso Lebach (STF, 2018), decidido em 5 de junho de 1973. Foi um dos julgados de popularidade daquele país, onde se debatia a colisão do direito de liberdade de imprensa e dos direitos da personalidade. Em resumo, tratava-se de um pedido liminar realizado por um reclamante que, junto com outros dois indivíduos, se envolveram em crime que gerou a morte quatro soldados, deixando outro gravemente ferido. O fato ocorreu à

---

<sup>6</sup> No ordenamento brasileiro, não há consenso sobre a possibilidade de denominação desses como “novos” direitos fundamentais, que ainda se apresentam como propostas interpretativas sobre o direito à privacidade e o princípio da dignidade da pessoa humana, sem a existência de uma norma prévia que os regulamente.



noite, quando os soldados resguardavam um depósito de munições que foram roubadas (MARTINEZ, 2014).

Em agosto de 1970, os dois principais acusados foram condenados à prisão perpétua e um terceiro partícipe foi condenado a seis anos de reclusão. Um pouco antes de ganhar a liberdade por meio do livramento condicional, a ZDF (*Zwites Deutsches Fernsehen* ou Segundo Canal Alemão), considerando o interesse da opinião pública, fez um documentário sobre o caso, e, em que pese tenha tentado impedir a sua exibição, o programa foi ao ar, pois o pedido foi negado pelos tribunais ordinários (o Tribunal Estadual de Mainz e o Tribunal Superior de Koblenz) que entenderam que havia interesse público na divulgação das informações. Entretanto, a Reclamação Constitucional junto ao Tribunal Constitucional foi procedente, onde os julgadores acharam que ocorreu a violação ao direito de desenvolvimento da personalidade (MARTINEZ, 2014).

Importante frisar que a reprodução dos fatos citou os nomes e mostrou as fotos dos acusados, descrevendo de maneira minuciosa a relação entre eles, inclusive suas relações homossexuais (MARTINS, 2014). Nesse sentido, parece acertada a decisão daquele Tribunal Constitucional, visto que a exposição de questões de foro íntimo dos acusados não tinha relevante interesse público.

Na Espanha, um dos julgamentos que ganhou destaque ocorreu em outubro de 1986, no âmbito do Tribunal Constitucional, em relação a demanda movida por Isabel Pantoja contra a comercialização de um vídeo que reproduzia a agonia do seu esposo e toureiro Paquirri. O referido tribunal anulou a decisão anterior do Tribunal Supremo que entendeu que o falecimento do toureiro não se tratava de sua esfera íntima. O Tribunal Constitucional advertiu que as cenas vividas dentro da enfermaria não tinham conexão com o espetáculo público taurino (PÉREZ LUÑO, 2012).

No âmbito internacional, o termo “direito ao esquecimento” foi utilizado pelo Tribunal de Justiça da União Europeia (TJUE) em 2013, ao exigir dos mecanismos de busca que cessassem a exposição de determinados resultados. Como em grande parte do ocidente, na Europa a proteção de dados tem grande relevância e o “*derecho al olvido*” é considerado tradicional (STF, 2018).

Outro caso de destaque foi a decisão do TJUE referente ao Processo no C-131/12, onde são partes a “*Google Spain SL*” e a “*Google Inc.*” em face da *Agência Espanhola de Protección*



*de Datos* (AEPD) e Mario Costeja González (STF, 2018). Neste caso algumas informações de Mario Costeja González foram divulgadas por um jornal espanhol, em duas de suas edições impressas, no ano de 1998 e após também foram republicadas em sua versão eletrônica. A partir de então, quando se pesquisava o nome do autor da ação nos mecanismos de busca, aquela informação aparecia e era acessada. Não obtendo êxito no requerimento junto à “*Google Spain*”, Mario Costeja González reclamou à *Agência Espanhola de Protección de Datos* (AEPD) pleiteando que fosse exigida a eliminação ou a modificação da publicação, deixando seus dados de serem exibidos (UNIÃO EUROPEIA, 2014).

Em 13 de maio de 2014 o processo foi julgado, onde foi garantido ao cidadão europeu o direito ao esquecimento, reconhecendo a responsabilidade das ferramentas de busca pelo processamento de dados pessoais exibidos nos resultados. Entendeu-se que deve prevalecer o direito ao esquecimento sobre o direito do público de conhecer e de ter fácil acesso à informação. No citado caso, a informação excluída foi avaliada como sem relevância e ultrapassada, não sendo imperiosa sua preservação, porém se deve analisar o contexto de cada situação em concreto (MARTINS, 2014).

No âmbito nacional, a jurisprudência já citou a expressão “direito ao esquecimento” em vários casos, em especial após a edição dos Enunciados nos 531 e 576 do Conselho de Justiça Federal. No primeiro aparece que “*a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento*” (BRASIL, 2013) e no segundo se afirmou que “*o direito ao esquecimento pode ser assegurado por tutela inibitória*” (BRASIL, 2015). Assim, vários tribunais vinham usando tais Enunciados para tomar suas decisões, seja aplicando ou não o citado direito.

Contudo, em fevereiro de 2021, foi apreciado pelo Supremo Tribunal Federal o Recurso Extraordinário 1.010.606/RJ sobre o caso Aida Curi, prevalecendo, por maioria, o voto do Ministro Dias Tóffoli, que, depois do histórico da matéria, das controvérsias que a cercam e da análise do caso, sopesou a proposta de tese de repercussão geral, aprovada por maioria de nove votos a um, a saber,

Tema 786 - É incompatível com a Constituição a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e lícitamente obtidos e publicados em meios de comunicação social analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais - especialmente os relativos à proteção da



honra, da imagem, da privacidade e da personalidade em geral - e as expressas e específicas previsões legais nos âmbitos penal e cível (BRASIL, STF, 2021).

O voto explicita que tal decisão, muito embora abranja tanto a mídia tradicional quanto a Internet, não alcança os pedidos de desindexação, que, conforme fundamentação, não se confunde com o direito ao esquecimento. Nesse sentido, hipóteses como a do famoso caso citado do Google Spain não serão abrangidas pela Tese 786 no Brasil. Desindexar significa assinalar o URL (*Uniform Resource Locator* - o endereço de uma página na web) - para que ele não apareça nos resultados dos buscadores normais, ou seja, quando o usuário digita o conteúdo a ser buscado no campo de busca, ainda que ele esteja público, não aparecerá na lista dos resultados. Portanto, ao desindexar um teor de um mecanismo de busca normal, ocorre grande diminuição do potencial de disseminação desse conteúdo, diminuindo também o dano que eventualmente venha a ser causado ao envolvido com a sua disseminação (VIOLA, 2016).

Assim sendo, na visão da maioria do STF, prevaleceram os direitos à memória e à liberdade de informação e de expressão, sendo invocado ainda no voto do relator o artigo 4º II, a da Lei Geral de Proteção de Dados Pessoais, que afirma que não se aplica o tratamento de dados àquilo feito para fins exclusivamente jornalísticos e artísticos. Deste modo, a regra é a liberdade e as exceções devem ser expressas.

Outro instituto resultante do desdobramento do direito à privacidade e intimidade foi a construção teórica desenvolvida por Jacques Lacan chamada de “*direito à extimidade*”, que em razão dos estudos de Serge Tisseron, se tornou acessível a outras áreas do conhecimento. O termo “*extimidade*” faz referência a forma como determinadas questões atinentes à intimidade são disponibilizadas aos outros, com o objetivo de serem validadas ou não, resultando na reapropriação daquelas formulações, em uma nova perspectiva (TISSERON, 2011).

Contrariamente ao defendido por Luiz Flávio Gomes (para quem “*extimidade*” é lançar ao público algo da privacidade), “*extimidade*” não pode ser entendida como o oposto de intimidade (GOMES, 2002). A citada expressão se refere a um desvio do segredo interno, que parte de uma linha tênue entre um local natural e íntimo para um local externo e que almeja ser revelado pelo sujeito (TISSERON, 2011). Ou seja, significa lançar ao público algo da privacidade (não indicando o seu oposto), é a exteriorização de forma explícita da liberdade de expressão. Assim, não são antagônicos os conceitos de “*extimidade*” e de intimidade, tratando-se da mesma matéria com destinação diversa. Nesse sentido Jacques-Alain Miller assevera que



“*extimidade*” é a exteriorização da intimidade, e não sendo o oposto da intimidade, a noção de uma complementa a outra (MILLER, 2011, p. 14).

Já é utilizada a expressão “*direito à extimidade*” por alguns estudiosos como Iuri Bolesina, que a conceitua como o direito de gozar ativamente da intimidade, por meio da exposição, voluntária, de informações da intimidade em face de terceiros. Assim sendo, a intimidade que o sujeito expõe na internet deixa de ser íntima, tornando-se “extima”, o que não significa pública (BOLESINA, 2015).

Essas novidades são usadas, em especial, no âmbito virtual onde se misturam o público e o privado. Deste modo, nas questões de proteção *online* se questiona qual a dimensão pública e/ou privada da internet hoje, ou seja, ela deve ser considerada um espaço público ou privado?

A resposta desse questionamento é complexa e pressupõe outro questionamento a respeito do que é internet e ciberespaço. Para os que defendem que a internet é propriedade pública, existe a possibilidade efetiva dos usuários reivindicarem seus direitos e tê-los respeitados. Porém, se indaga qual parte da internet deve ser considerada privada ou/e pública e quais direitos poderá gozar o sujeito que usa cada uma dessas partes? A resposta mais adequada a essa questão seria que todos os espaços da internet deveriam ser públicos, com exceção de haver razão conveniente para o contrário.

Uma modificação de modelo, em favor da natureza mista, é defendida por Paul Bernal, assim, no espaço privado os indivíduos teriam controle sobre as suas próprias configurações de privacidade e no espaço público requereriam a proteção através de direitos de privacidade. Nesse entender, a regra seria a proteção da privacidade e aqueles que almejassem monitorar pessoas ou coletar, usar, armazenar dados pessoais necessitariam justificar os motivos para a vigilância (BERNAL, 2014).

Nessa perspectiva, a ideia do privado migra para o “pessoal”, onde se resguarda as informações pessoais e não necessariamente as privadas. Portanto, se antes a ordem lógica era “pessoa-informação-sigilo”, hoje se fala em “pessoa-informação-circulação-controle-gestão”, ou seja, a pessoa não possui apenas o direito de obstruir uma informação de sua privacidade que tenha escapado, mas pode também controlar sua circulação de forma ativa e passiva (RODOTÁ, 2008).



De fato, a internet rompeu com os binômios “não visível/privado” e “visível/invisível” e modificou o espaço público-privado no que o estudioso Dominique Cardon chamou de cenário de um “jogo de luz e sombras”. Ou seja, o espaço público-privado se tornou um degrade, estando nos extremos a baixa e a alta visibilidade, e no meio as zonas de interação (CARDON, 2012). Essa mistura entre o público e o privado na internet é uma forma nova de interpretar esses espaços, já que entre essa nova zona de alta e baixa visibilidade surge um espaço intermediário que não é nem privado, nem público, mas mais ou menos visível.

Na obra *Les tyrannies de la visibilité*<sup>7</sup> (que fala da tirania da visibilidade e da necessidade de se tornar visível para realmente existir) as francesas Claudine Haroche e Nicole Aubert ponderaram temas em torno dessa questão e chegaram a conclusão que o termo “visibilidade” gera profunda ambivalência, já que nela se misturam dois polos contrários: o desejável e o indesejável (AUBERT; HAROCHE, 2011).

Seguindo esse raciocínio, Tisseron explica que os relacionamentos considerados significativos passaram da intimidade para *extimidade* (TISSERON, 2011). Esse tema também é tratado por Zygmunt Bauman ao se referir ao analista do trajeto histórico do sujeito moderno, Alain Ehrenberg, que escolhe um acontecimento da década de 1980 no qual Vivianne (pessoa comum) declara num *talk show* de TV que, em razão de seu esposo ter ejaculação precoce, ela nunca teria tido orgasmo (EHRENBERT apud BAUMAN, 2012). Chamaram a atenção de Alain Ehrenberg que os atos essencialmente privados foram expostos ao público sem controle (BAUMAN, 2012).

Dessa forma, o impedimento entre as esferas pública e privada foi eliminada, pois atualmente se vivencia uma “sociedade confessional” que até então era desconhecida, com microfones alojados dentro de confessionários, onde a partir de então os segredos mais íntimos podem ser expostos (BAUMAN, 2012, p. 228). Bauman entende que houve o fim da privacidade, vez que não importa mais a possibilidade de transgressão da privacidade, e sim o oposto: que se fechem as portas de saída da privacidade.

Por razões de exigências do mercado e da tendência de montar banco de dados cada vez maiores para controlar comportamentos, o fim da privacidade, antes do atentado de 11 de setembro, já era comentado, e percebendo o modo como o mundo está em mudança emerge

---

<sup>7</sup> A tirania da visibilidade (tradução nossa). Ser visível para existir? Consultar livro em sua versão francesa (AUBERT; HAROCHE, 2011).



essa questão de forma mais radical (RODOTÁ, 2008, p. 13). Após esse episódio, a privacidade além de não ser mais vista como um direito fundamental passou a ser frequentemente considerada como um obstáculo à segurança, sendo superada por legislações de emergência (RODOTÁ, 2008).

## 5 CONSIDERAÇÕES FINAIS

Na atual sociedade da informação se multiplicam interações humanas em conjunto com uma serie de ferramentas, especialmente as digitais, com resultados que são nem sempre benéficos. De qualquer maneira, todas as modificações estão sendo assimilada pelo ordenamento jurídico brasileiro, sendo inegável a evolução que passou a ter o direito digital no judiciário.

Existe também o problema da hiperexposição, involuntário ou não, que possibilita que terceiros de má-fé utilizam os dados sensíveis desses sujeitos para usos totalmente indevidos.

A Internet, de fato, foi uma das mais relevantes invenções da história da humanidade e transformou definitivamente os rumos de sociedade que, como rede global, exige uma tutela transversal, de alcance internacional e nacional.

A sociedade da informação atual trouxe mudanças de sentido no que se entende como direito à privacidade e seus desdobramentos como intimidade e vida privada (onde se incluem o “direito ao esquecimento” e o “direito à extimidade”).

A barreira entre as esferas pública e privada foi eliminada e hoje a privacidade além de não ser mais vista como um direito fundamental passou a ser frequentemente considerada como um obstáculo à segurança, sendo superada por legislações de emergência.

## REFERÊNCIAS

ALMEIDA, Vitor; TEIXEIRA, Ana Carolina Brochado; TEPEDINO, Gustavo (coords.). **O Direito Civil entre o sujeito e a pessoa: estudos em homenagem ao professor Stefano Rodotá**. Belo Horizonte: fórum, 2016.

AUBERT, Nicole; HAROCHE, Claudine. **Les tyrannies de la visibilité: être visible pour exister?**. Toulouse: Érès, 2011.

BARRETO JUNIOR, Irineu Francisco. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman





e Manuel Castells. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; DE LIMA; Cintia Rosa Pereira. (Org.). **Direito & Internet III**. São Paulo: Quartier Latin, 2015, p. 100-127.

BAUMAN, Zygmunt. **Isto não é um diário**. Rio de Janeiro: Zahar, 2012.

BAUMAN, Zygmunt. **Vigilância líquida: diálogos com David Lyon/Zygmunt Bauman**, RJ: Zahar, 2013.

BERNAL, Paul. **Internet privacy rights: rights to protect autonomy**. Cambridge: Cambridge University, 2014.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. Rio de Janeiro: Forense, 2003.

BOLESINA, Iuri. Direito à extimidade no ciberespaço e a transformação do binômio público-privado. *In:* Mostra de pesquisa de direito civil constitucionalizado. 3., 2015, Rio Grande do Sul. **Anais eletrônicos**. Rio Grande do Sul: Unisc, 2015. Disponível em: <http://online.unisc.br/acadnet/anais/index.php/ecc/article/view/14341/2783> . Acesso em: 8 mar. 2022.

BRANDEIS, Louis D.; WARREN, Samuel D. The right to privacy. **Harvard Law Review**, Cambridge, v. IV, n. 5, 15 dec. 1890. Disponível em: <http://readingnewengland.org/app/books/righttoprivacy/?l=righttoprivacy> . Acesso em: 18 mar. 2022.

BRASIL. Conselho da Justiça Federal. **Enunciado no 531**. Disponível em: <http://www.cjf.jus.br/enunciados/enunciado/142> . Acesso em: 10 mar. 2022.

BRASIL. Conselho da Justiça Federal. **Enunciado no 576**. Disponível em: <http://www.cjf.jus.br/enunciados/enunciado/821> . Acesso em: 10 mar. 2022.

BRASIL. STF. RE 1010606. **Tema 786** - Aplicabilidade do direito ao esquecimento na esfera civil quando for invocado pela própria vítima ou pelos seus familiares. Relator: MIN. DIAS TOFFOLI. Disponível em: <http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroTema=786> . Acesso em: 04 mar. 22.

CARDON, Dominique. **A democracia internet: promessas e limites**. Rio de Janeiro: Forense, 2012.



DE LUCCA, Newton; SIMÃO FILHO, Adalberto (coords.). **Direito e Internet: aspectos jurídicos relevantes**. Bauru, SP: Édipro, 2000.

EUROPEIA. Tribunal de Justiça da União Europeia. **Acórdão no C-131/12**. Curia, Luxemburgo, 13 maio 2014.

FORTES, Vinícius Borges. **O direito fundamental à privacidade: uma proposta conceitual para a regulação da proteção dos dados pessoais na internet no Brasil**. Rio de Janeiro: Universidade Estácio de Sá, 2015. Disponível em: [https://www.academia.edu/17425692/O\\_direito\\_fundamental\\_%C3%A0\\_privacidade\\_uma\\_proposta\\_conceitual\\_para\\_a\\_regulamenta%C3%A7%C3%A3o\\_da\\_prote%C3%A7%C3%A3o\\_dos\\_dados\\_pessoais\\_na\\_internet\\_no\\_Brasil](https://www.academia.edu/17425692/O_direito_fundamental_%C3%A0_privacidade_uma_proposta_conceitual_para_a_regulamenta%C3%A7%C3%A3o_da_prote%C3%A7%C3%A3o_dos_dados_pessoais_na_internet_no_Brasil). Acesso em 8 abr. 2022.

GABRIEL, Martha. **Você, eu e os robôs: pequeno manual do mundo digital**. São Paulo: Atlas, 2018.

KOHN, Karen; MORAES, Cláudia Herte de. O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade da Informação e da Sociedade Digital. Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação. **XXX Congresso Brasileiro de Ciências da Comunicação**, Santos, 29 de agosto a 2 de setembro de 2007. Disponível em: <http://www.intercom.org.br/papers/nacionais/2007/resumos/R1533-1.pdf>. Acesso em: 14 abr. 2022.

LIMA, Glaydson de Farias. **Manual de Direito Digital: fundamentos, legislação e jurisprudência**. 1.ed. – Curitiba: Appris, 2016.

LIMA, Marco Antônio. BARRETO JUNIOR, Irineu Francisco. Marco Civil da Internet: limites da previsão legal de consentimento expreso e inequívoco como proteção jurídica dos dados pessoais na internet. **Revista de Direito, Governança e Novas Tecnologias**. Brasília v. 1 | n. 2 | p. 241 -260 Jan/Jun. 2016.

LIPOVETSKY, G. **Os tempos hipermodernos**. São Paulo-SP: Barcarolla, 2004.

MARTINEZ, Pablo Domingues. **Direito ao esquecimento: a proteção da memória individual na sociedade da informação**. Rio de Janeiro: Lumem Juris, 2014.

MARTINS, Guilherme Magalhães. Nota do coordenador. *In: Direito privado e internet*. São Paulo: Atlas, 2014.





MILLER, Jacques-Alain. **Extimidad**: los cursos psicanalíticos de Jacques-Alain Miller. Buenos Aires: Paidós, 2011.

MONTJOYE, Yves Alexandre de. Big Data': antídoto contra a corrupção? Disponível em: [https://brasil.elpais.com/brasil/2017/03/24/ciencia/1490358953\\_071638.html](https://brasil.elpais.com/brasil/2017/03/24/ciencia/1490358953_071638.html). Acesso em: 27 mar. 2022.

NASCIMENTO, Valéria Ribas do. Direitos fundamentais da personalidade na era da sociedade da informação: transversalidade da tutela à privacidade. **Revista de Informação Legislativa: RIL**, v. 54, n. 213, p. 265-288, jan./mar. 2017. Disponível em: [http://www12.senado.leg.br/ril/edicoes/54/213/ril\\_v54\\_n213\\_p265](http://www12.senado.leg.br/ril/edicoes/54/213/ril_v54_n213_p265). Acesso em: 10 abr. 2022.

PINHEIRO, Patrícia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016.

ROCHA, Luiz Augusto Castello Branco de Lacerda Marca da; FILPO, Klever Paulo Leal. **Proteção do direito à vida privada na sociedade da hiperexposição**: paradoxos e limitações empíricas. a. 7, n. 1, 2018, p. 1-31. Disponível em: <http://civilistica.com/wp-content/uploads1/2018/05/Rocha-e-Filpo-civilistica.com-a.7.n.1.2018-2.pdf>. Acesso em 06 mar. 2022.

RODOTÀ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Tradução Danilo Doneda e Luciana Cabral Doneda, Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. Notas acerca do assim chamado direito ao esquecimento na jurisprudência do Superior Tribunal de Justiça brasileiro. *In*: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Boas. **Lei Geral de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2020.

SILVA, Francisco Vieira da. A constituição do sujeito celebridade no site ego: (re) configurações da intimidade em tempos de hiperexposição midiática. 2016. 212 f. **Tese (Doutorado em Linguística)** - Universidade Federal da Paraíba, João Pessoa, 2016.

STF. **Boletim de Jurisprudência Internacional**. Direito ao esquecimento. 5. ed. STF: Supremo Tribunal Federal, Dez/2018. Disponível em: <http://www.stf.jus.br/arquivo/cms/jurisprudenciaInternacional/anexo/BJI5DIREITOAESQUECIMENTO.pdf>. Acesso em: 04 mar. 2022.

TISSERON, Serge. **Intimité et extimité**. *Communication*, v. 88, n. 1, p. 83-91, 2011.



VIOLA, Mario; DONEDA, Danilo; CÓRDOVA, Yasodara; ITAGIBA, Gabriel. Entre privacidade e liberdade de informação e expressão: existe um direito ao esquecimento no Brasil? *In*: TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor. **O Direito Civil entre o sujeito e a pessoa: estudos em homenagem ao professor Stefano Rodotà.** Belo Horizonte: Fórum, 2016.