

A HIPEREXPOSIÇÃO PESSOAL E SEUS REFLEXOS NOS DIREITOS DA PERSONALIDADE: NECESSIDADE DE UMA TUTELA TRANSVERSAL DO DIREITO À PRIVACIDADE, COM ENFOQUE NO ÂMBITO PENAL

PERSONAL HYPEREXPOSITION AND ITS REFLECTIONS ON THE RIGHTS OF PERSONALITY: THE NEED FOR A CROSS-CUTTING OF THE RIGHT TO PRIVACY, WITH A FOCUS ON THE CRIMINAL SCOPE

Gustavo Noronha de Ávila¹

Thais Aline Mazetto Corazza²

RESUMO

Objetiva-se analisar o direito à privacidade na Sociedade da Informação e os riscos decorrentes da hiperexposição pessoal 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, nacional e internacional. Para tanto, 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 sua correlação com a segurança, e por fim, se demonstrar a necessidade da construção de uma tutela transversal da privacidade, nacional e internacional, com enfoque no âmbito penal e da segurança pública decorrentes da hiperexposição pessoal. Para colher todas as oportunidades do novo mundo que já se vivencia, são necessárias políticas públicas adequadas, instituições concebidas com a consciência de que as tecnologias suprimem a noção de espaço e tempo e, portanto, tornam vãs as proteções dentro das velhas regras e confins territoriais/nacionais. Está nascendo uma nova forma de cidadania que exige uma tutela transversal, mas deve nascer também conjuntamente uma nova ideia de soberania.

PALAVRAS-CHAVE:

Privacidade; Sociedade da Informação; Hiperexposição Pessoal; Direitos da Personalidade; Tutela Transversal.

¹ 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.

² 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.

ABSTRACT

The objective is to analyze the right to privacy in the Information Society and the risks arising from personal 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, national and international. To this end, an overview of the right to privacy and personal data in the Information Society will be provided, afterwards, an analysis of hyperexposure in the Digital Age and its correlation with security will be made, and finally, demonstrating the need to build cross-cutting protection for privacy, national and international, with a focus on the criminal sphere and public security resulting from personal overexposure. To reap all the opportunities of the new world that is already being experienced, are required adequate public policies, institutions designed with the awareness that technologies suppress the notion of space and time and, therefore, make the protections vain within the old rules and confines territorial / national. It's borning a new form of citizenship that requires transversal protection, but must also be born together a new idea of sovereignty.

KEYWORDS:

Privacy; Information Society; Personal overexposure; Personality Rights; Transversal Guardianship.

INTRODUÇÃO

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

Dentro desse contexto, verifica-se que o Direito, nos países adeptos ao *Civil Law*, padece com a realidade digital, tendo dificuldade para assegurar o seu fundamento, pois as mudanças por costumes acontecem subitamente. O Direito à privacidade e à intimidade fazem parte dos direitos da personalidade. Trata-se da proteção do ser, do modo de ser, da pessoa. No

entanto, a maioria das pessoas que cedem e informam seus dados, voluntária ou involuntariamente, não possuem ciência da destinação desses dados.

A hiperexposição decorrente do avanço da Era Digital pode trazer consequências e danos imensuráveis e irreparáveis. Isso porque a privacidade diz respeito a coleta de informações e ao direito a ser deixado só, sendo que a exposição (voluntária ou não) demasiada acaba impossibilitando o controle do uso das informações pessoais.

Assim, objetiva-se com o presente artigo analisar o direito à privacidade na Sociedade da Informação e os riscos decorrentes da hiperexposição pessoal nas redes sociais, analisando seu desdobramento como o direito à intimidade e ao esquecimento. Com o advento da internet e das redes sociais, tornou-se habitual que a maior parte dos cidadãos divulguem suas informações em redes sociais sem terem a devida dimensão do impacto que essa excessiva exposição possa provocar. A segurança na rede costuma ser negligenciada e a exposição exacerbada torna vulnerável a proteção da privacidade, tornado os indivíduos vulneráveis aos mecanismos de controle do Estado e do Mercado. Para essa finalidade, se faz necessária a construção de uma tutela transversal do direito à privacidade.

Trata-se de um estudo teórico. Utiliza-se a abordagem fenomenológica-hermenêutica, no intento de, com sua lógica compreensiva-descritiva, fundir horizontes e confirmar a afirmação inicial. A pesquisa parte de um raciocínio hipotético-dedutivo. A pesquisa será bibliográfica e documental, onde se buscará alcançar uma exata compreensão por meio de materiais como leis, sites oficiais, jurisprudência e doutrina jurídica aplicável ao tema (livros, artigos científicos, dissertações, teses, entre outros), nacional e internacional.

Para tanto, 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 sua correlação com a segurança, e por fim, se demonstrar a necessidade da construção de uma tutela transversal de privacidade, nacional e internacional.

1. UM PANORAMA DO DIREITO À PRIVACIDADE E DOS DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO

Muito embora o direito à privacidade tenha surgido da proteção à propriedade e à inviolabilidade do lar, posteriormente ocorreu uma migração para a inviolabilidade do domicílio, se revelando pela interferência não autorizada de terceiros na esfera pessoal do sujeito (PAESANI, 2009, p. 159). O direito à intimidade, por sua vez, engloba todos os direitos inerentes a pessoa, com suas limitações,

A intimidade esta afeta ao *right to be alone*, ou seja, o direito de estar só, no sentido de que todo o indivíduo tem o direito de estar só, (...) de reservar-se, de não tornar públicos aspectos da sua vida e de não permitir que terceiros tornem esses dados públicos, mesmo que esses sejam membros da família que vivam sob o mesmo teto (PAESANI L. M., 2009, p. 160).

O desafio do Direito Digital é trazer o equilíbrio para a difícil relação que existe entre os interesses gerados pelos novos veículos de comunicação, quais sejam, o comercial, a privacidade, a responsabilidade e o anonimato (PINHEIRO, 2016, p. 94). Fato é que essa equação só encontra fundamento se houve de um lado a vigilância e do outro a punibilidade.

A Era Digital é o período histórico atual. Costuma receber outras denominações, como Era da Informação ou Era Tecnológica, sendo também conhecida como Terceira Revolução Industrial e se refere à realidade tecnológica como mediadora das relações humanas e das interações entre máquinas, essas últimas cada vez mais autônomas. Uma das principais características dessa realidade é hiperconectividade, em outras palavras, o fato de estar todo mundo conectado o tempo todo. E a sociedade atual transita nessa realidade. Daí o termo Sociedade da Informação, surgido no século XX, no momento em que a tecnologia teve grandes avanços e se tornou essencial na determinação do sistema social e econômico (KOHN; MORAES, 2007, p. 2-4).

A Sociedade da Informação se estrutura no contexto de aceitação global, na qual o desenvolvimento da tecnologia reconfigurou o modo de existir, se relacionar, de ser e de agir das pessoas, propondo os modelos de comunicação vigentes. A informação não pode ser separada da tecnologia, e isso vem sendo remodelado e institucionalizado com os avanços na área do conhecimento e das técnicas. Nessa sociedade a informação é usada intensamente como

elemento da vida política, econômica, cultural e social, e depende de um meio tecnológico para que se propague. É por tal motivo que a sociedade marcha ao encontro da tecnologização, rumo à um processo de virtualização onde tudo acontece no interior de um universo virtual (KOHN; MORAES, 2007, p. 02-03).

Dentro desse contexto, verifica-se que o Direito, nos países adeptos ao *Civil Law*, padece com a realidade digital, tendo dificuldade para assegurar o seu fundamento, pois as mudanças por costumes acontecem subitamente. Os Direitos da Personalidade foram resguardados pela Declaração Universal dos Direitos Humanos em 1948, bem como pelo Código Civil de 2002 e pela Constituição Federal, no seu artigo 5º, inciso X, no entanto, o conceito de privacidade, trazido por esses diplomas legais, sofreu modificações e está em constante evolução, a fim de abarcar todas as modificações sociais sofridas, principalmente no que diz respeito à privacidade na Sociedade da Informação. Isso porque, com o advento da era tecnológica e com as novas possibilidades abertas à invasão da intimidade, tornou-se mais premente a necessidade de uma tutela jurídica da vida privada. Em primeira análise, a tecnologia destina-se ao desenvolvimento da personalidade humana, à ampliação da capacidade de domínio sobre a natureza, escavação do conhecimento e derramamento da riqueza, mostrando e gerando novos rumos de ingresso ao conforto. Todavia, seus efeitos alastram-se das mais indesejadas e variadas maneiras (SCARZELLI, 1997, p. 23)

O Direito à privacidade e à intimidade fazem parte dos direitos da personalidade. Trata-se da proteção do ser, do modo de ser, da pessoa. No entanto, a maioria das pessoas que cedem e informam seus dados, voluntária ou involuntariamente, não possuem ciência da destinação desses dados. Os direitos da personalidade são prerrogativas de toda pessoa humana pela sua própria condição, alusivos aos seus atributos essenciais em suas emanações e prolongamentos, são considerados direitos absolutos, que implicam em um dever geral de abstenção para a sua defesa e amparo, são indisponíveis, intransmissíveis, irrenunciáveis e de difícil estimação pecuniária. São também inatos (originários), absolutos, extrapatrimoniais, imprescritíveis, impenhoráveis, vitalícios, necessários e oponíveis *erga omnes*, de acordo a melhor doutrina e o artigo 11 do Código Civil (BITTAR, 2003, p. 11).

É notório que o direito à privacidade é um limite natural ao direito de informação, de modo que não pode haver lesão ao direito, sem o consentimento do indivíduo. Ocorre que

atualmente as pessoas por conta própria expõe sua privacidade e intimidade diariamente nas redes, olvidando-se da ausência de segurança virtual.

A hiperexposição decorrente do avanço da Era Digital pode trazer consequências e danos imensuráveis e irreparáveis. Isso porque a privacidade diz respeito a coleta de informações e ao direito a ser deixado só (RODOTA, 2008, p. 24), sendo que a exposição (voluntária ou não) demasiada acaba impossibilitando o controle do uso das informações pessoais. Nesse sentido, as recentes dimensões da coleta e do tratamento de informações culminam na propagação de súplica à privacidade, ao mesmo tempo que aumentam a consciência da impossibilidade de romper e limitar as novas questões surgidas no tradicional quadro institucional deste conceito (RODOTA, 2008, p. 23).

A evolução do conceito de privacidade preencheu o seu conteúdo com a garantia de isolamento e reserva do indivíduo em si, ao mesmo tempo que deu a ele o poder de controlar o uso de suas próprias informações. Por isso, na sociedade da informação prevalece as definições funcionais da privacidade que se referem à possibilidade da pessoa conhecer, remeter, controlar e obstruir o fluxo das informações a ele relacionadas (ALMEIDA, TEIXEIRA, & TEPEDINO, 2016, p. 255), levando-se em consideração sempre que os dados pessoais agasalham os indivíduos e todo grupo nele inserido. Sobre o tema, o estudioso Rodotà assevera que:

De sua tradicional definição como — direito a ser deixado só passa-se, justamente pela influência da tecnologia dos computadores, àquela que constituirá um constante ponto de referência na discussão: —direito a controlar o uso que os outros façam das informações que me digam respeito. Em fase mais recente surge um outro tipo de definição, segundo a qual a privacidade se consubstancia no — direito do indivíduo de escolher aquilo que está disposto a revelar aos outros (ALMEIDA, TEIXEIRA, & TEPEDINO, 2016, p. 286).

O desafio maior está em estabelecer parâmetros razoáveis, já que os dados pessoais que são capturados automaticamente são compartilhados. O centro da gravidade da cultura consolidou a desvalorização do passado, considerado contrário à razão e à liberdade, desconstruindo a credibilidade do futuro, pela primazia do “aqui e agora”, em uma temporalidade dominada pelo precário e pelo efêmero (LIPOVETSKY, 2004), dinâmica esta, com a qual o direito, ainda analógico, parece não conseguir lidar (ALMEIDA, TEIXEIRA, & TEPEDINO, 2016, p. 334).

Ainda que a privacidade e a intimidade estejam declaradas e garantidas nos diplomas legais como direito e garantia fundamental, os danos podem ocorrer, tendo em vista que:

Todas as declarações recentes dos direitos do homem compreendem, além dos direitos individuais tradicionais, que consistem em liberdades, também chamados direitos sociais, que constituem em poderes (...) São antinômicos no sentido de que o desenvolvimento deles não pode proceder paralelamente; as realizações integrais de uns impedem a realização integral de outros. Quanto mais aumenta os poderes dos indivíduos, tanto mais diminuem as liberdades dos mesmos indivíduos (BOBBIO, 1992, p. 21).

Evidente assim a necessidade de proteção a esses direitos que individualizam a pessoa em si e na sociedade a qual pertence, ocorrendo a troca do pesadelo paróico de “Nunca estar sozinho” pela esperança de “Nunca mais vou ficar sozinho” (BAUMAN, 2013, p. 30)

A pessoa que decide se conectar aceita, ainda que de forma tácita, a socialização dos seus dados, ou melhor dizendo, consente com a perda do controle das suas informações (PINHEIRO, 2016, p. 100). Ao aceitar os termos de uso dos aplicativos que são instalados, ocorre o consentimento em repassar as informações pessoais para terceiros.

Alerta Patrícia Peck Pinheiro que a maior parte dos termos de uso dos serviços deixa claro que ainda que o sujeito deixe de ser usuário, o que já foi compartilhado ficará sob o domínio da internet eternamente, cabendo apenas à ele mesmo refletir, antes, sobre o legado de conteúdo que deseja deixar a seu respeito, já que:

Hoje a maior parte dos termos de uso destes serviços deixa muito claro que, por mais que a pessoa deixe de ser usuária, o que ela compartilhou por ali fica lá na galáxia da Internet para sempre, e cabe apenas a ela a responsabilidade de refletir antes sobre qual legado de conteúdo quer deixar a seu respeito, já que tecnicamente ainda é bem difícil conseguir praticar o direito ao esquecimento (PINHEIRO, 2016, p. 101).

A captação dos dados pessoais cresceu exponencialmente nas últimas décadas, sendo criados, no Brasil, mecanismos para garantir a proteção dos parâmetros mínimos de privacidade dos usuários de tecnologias. No entanto, não obstante a existência do Marco Civil da Internet (Lei 12.965/2014) e suas determinações normativas quanto à necessidade do livre esclarecimento e consentimento como requisito para a coleta, uso, armazenamento, tratamento e proteção de dados pessoais, bem como a Lei Geral de Proteção de Dados, não é isso que de fato se nota na prática (LIMA; BARRETO JUNIOR, p. 241).

O primeiro obstáculo na aplicação tecnológica dos algoritmos e coleta de dados pessoais é a garantia da privacidade dos indivíduos. Isso porque os algoritmos têm acesso a dados provenientes de um número crescente de fontes (ainda que esses dados sejam anônimos), sendo que a partir de seu cruzamento e combinação poderia se aferir algumas características sobre

uma pessoa em específico, ainda que tal informação nunca tenha sido divulgada pelo sujeito. Para minimizar ou eliminar o impacto sobre a privacidade, felizmente, algumas medidas podem ser tomadas, tais como a agregação de dados anônimos. O incremento de algoritmos para a tomada de decisões baseadas em dados conjectura a procura da objetividade e da vontade de tomar decisões com base em evidências, eliminando ou minimizando a discriminação, a corrupção, a injustiça ou a ineficiência das quais não escapam as decisões humanas. (MONTJOYE, 2017).

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

Adverte Patrícia Peck Pinheiro que a segurança da informação sempre se deparou com um obstáculo 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 violação da privacidade dos usuários da internet e a espionagem nacional e internacional digital são problemas mundiais. Veja-se que as normas regulamentadoras são ainda tímidas, não impondo limites drásticos aos governos, empresas e serviços de segurança. Muitos indivíduos utilizam a internet para expressar desejos que na vida real (leia-se não virtual) demorariam a demonstrar, o que acaba causando uma hiperexposição pessoal, sem levar em conta os riscos que estão expostos, simplesmente por se sentir feliz aceita-se o risco. Observa-se que a maioria das pessoas que se relacionam com o mundo virtual não buscam a problematização de sua vida, o autoconhecimento, mas a confirmação de suas convicções e ser objeto do olhar alheio.

Fato é que a vida virtual se difere, em muito, da real. Nas redes sociais não importa quem você é e o que faz, mas o que representa para a sociedade com suas postagens. Quem se

expõe excessivamente não leva em consideração o quanto isso pode ser prejudicial, sendo as consequências de tais atos proporcionais à sua exposição.

2. A HIPEREXPOSIÇÃO DA ERA DIGITAL E A SEGURANÇA

A criação do *Youtube* permitiu aos usuários comum realizar publicações e visualizar vídeos na internet com facilidade, sem necessitar de uma conexão direta entre as partes (feitas através de computadores de mesa). A maior parte da população não imaginava a migração tecnológica que estava prestes a acontecer, vez que as atividades que eram possíveis apenas por computadores de mesa passariam a serem feitas por meio dos Smartphones, em especial, com a evolução do sistema Androide e o IOS. Com isso veio a explosão de aplicativos, criados por plataformas, e as redes sociais que passou a conectar os usuários, transferindo informações. Porém, *“de nada adianta formidáveis softwares antivírus instalados e firewalls bem configurados se aquele que utiliza a rede clica em qualquer aplicativo sugerido ou informa dados sensíveis, sem se certificar do local onde se encontra”* (LIMA, 2016, p. 73).

Veja-se que a hipótese de liberdade infinita e anárquica resguardada pela Internet entra em conflito com outra realidade que está diante dos olhos de todos: câmeras de vídeo para vigilância, a coleta dos rastros deixados pelo uso de cartão de crédito ou durante a navegação na internet, a produção e venda de perfis pessoais cada vez mais detalhados, as possibilidades de interconexão entre os mais diversos 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 ameaça sombrear o crescimento também intenso dos bancos de dados mais tradicionais, ou seja, aqueles com finalidade de segurança que também sofrem modificações com a tecnologia e com a realidade de um mundo sem fronteiras. Em relação à União Europeia, verifica-se de forma clara a multiplicação dos acordos e convenções de cooperação em matéria de segurança e justiça, o que leva a estruturação de grandes bancos de

dados, como o caso do Acordo Schengen³, das convenções instituídas pela Europol⁴ e do sistema alfandegário europeu, do regulamento Eurodac⁵, mas são outros os casos que fornecem mais prontamente as dimensões e perspectivas das coletâneas de informações para finalidade de segurança (RODOTÀ, 2008, P. 145-146).

Em alguns países existem bancos de dados contendo DNA de indivíduos considerados perigosos. Ampliam-se as coletas de dados sobre a saúde. Aumenta-se as formas de controle com câmeras de vídeo, já habituais em setores como banco, estações e supermercados, e que controlam zonas consideradas perigosas. Fato é que existem evidentemente boas razões para sustentar a necessidade de usar todas as oportunidades oferecidas pelas novas tecnologias para proteger a sociedade dos crimes, fomentar a prevenção de doenças e proteger os mais vulneráveis dos riscos sociais, devendo-se buscar sempre um justo equilíbrio entre uma visão individualista de privacidade e a satisfação das exigências sociais. é justamente a necessidade de um uso social das tecnologias a exigir que sejam projetadas novas instituições de liberdade, capazes de evitar uma poluição da sociedade e de garantir a defesa dos direitos fundamentais em um ambiente caracterizado pelo recurso maciço às coletâneas de informações. Deve-se suspeitar do argumento de quem salienta 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, já que nela se baseia a pretensão do Estado de saber de tudo, até mesmo dos aspectos mais íntimos da vida dos cidadãos (RODOTÀ, 2008, p. 147-148).

As mídias sociais podem prover grande apanhado de informações sobre seus usuários, sendo esses dados usados para diversas funções. Exemplificando: um recrutador de uma empresa pode examinar os costumes de um candidato; um pretendente pode tentar descobrir mais sobre seu parceiro amoroso; um criminoso pode buscar informações de suas próximas vítimas. Veja-se que, no último caso, traz preocupação a maneira como a maioria dos usuários se comportam, escancarando muitas informações, e os criminosos, em uma simples visita a um

³ 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.

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

⁵ 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.

perfil, conseguem descobrir nome de parentes, locais que a pessoa frequenta (por exemplo, nome da escola dos filhos) e outras informações valiosas a fim de criar um plano de ataque (LIMA, 2016, p. 127). O citado problema não se restringe as mídias sociais, trata-se de um problema comportamental. A hiperexposição pessoal aumentou muito nos últimos anos, seja para expor os bens e pertences, seja para expor suas práticas, entre outros. Essas diversas espécies de capturas de informações podem gerar ataques cibernéticos. Cerca de 300 horas de vídeos são publicados no *Youtube* por minuto, tornando-o a maior rede de vídeos no mundo (LIMA, 2016, p. 129). Isto evidencia a hiperexposição dos indivíduos e a ausência de fiscalização sobre tais publicações. Ainda:

A existência do serviço de prévia visualização e avaliação resultaria na impossibilidade econômica de existência do serviço, sem falar nas incontáveis dificuldades para lidar em escala mundiais com peculiaridades como, por exemplo, identificar se determinado conteúdo é considerado ilícito em determinado país. No caso do direito brasileiro, por exemplo, se trataria caso de censura prévia, ação proibida pela Carta Magna (LIMA, 2016, p. 130).

Em busca da liberdade de se expressão, abre-se mão da segurança. Há uma troca da segurança para se atingir um ápice fictício de liberdade e exposição. No entanto, a liberdade de expressão acompanhada dos riscos relativos à diminuição da privacidade nos ambientes digitais pode trazer uma hiperexposição, gerando riscos pessoais presentes ou futuros, tanto da segurança quanto de reputação (GABRIEL, 2018, p. 69). Exemplificando,

Em 2010, o Facebook disponibilizou a funcionalidade de check-in, para permitir que seus usuários compartilhassem suas informações de localização na rede social. Um mês após o lançamento dessa funcionalidade, uma rede de assaltantes nos Estados Unidos roubou equivalente a US\$ 100 mil em bens de 50 casas, mirando nas pessoas que faziam check-in em lugares longe de suas residências (GABRIEL, 2018, p. 69).

De forma consciente ou não, as pessoas repassam suas informações à terceiros, e da mesma forma que acontece no mundo não virtual, há diversos riscos na rede também. Em decorrência da hiperexposição descontrolada, muitos acabam tendo sua reputação atingida e a única maneira de controlar isso é através do uso racional do direito à privacidade, que permite revelar seletivamente os aspectos pessoais.

Ao parar de exercer o controle sobre a privacidade pessoal, revelando suas informações pessoais *on-line*, as pessoas acabam por comprometer sua reputação, já que as informações expostas na internet permanecem para sempre no mundo virtual (GABRIEL, 2018, p. 72).

Salienta-se que todas os comentários, curtidas, bate papo, fotos, *check-in*, fazem partes da construção da reputação e se divide em pegadas, rastros e sombras. As pegadas ou *footprint* são as informações pessoais que são compartilhadas ativa ou intencionalmente na internet, como os *posts* e comentários nas mídias sociais, *check-ins*, fotos, entre outros. Os rastros ou *traces* são também informações pessoais compartilhadas ativa ou intencionalmente na internet, como os dados que são disponibilizados nas navegações pela rede, como o IP, a localização, a configuração do computador, o *browser*, o IMEI do celular, hábitos de *e-mail*, preferências por diferentes assuntos, entre outros. E, por fim, sombras ou *shadows* são as informações pessoais que são compartilhadas por terceiros, como fotos menções, depoimentos, opiniões, etc. (GABRIEL, 2018, p. 74).

Os rastros digitais, denominados de sombras, são deixados tanto *on-line* quanto *off-line*, portanto, todos possuem responsabilidade pelas ações e conteúdos compartilhados e pesquisados nas mídias sociais. Uma simples brincadeira na internet para determinar com qual personagem você se parece em um filme concede informações sobre os traços de personalidade do indivíduo (GABRIEL, 2018, p. 76). A preocupação que isso traz é que além de ser manipulativo, dificilmente pode ser detectado, excluindo a privacidade na internet.

Os rastros aliados as pegadas acabar por formar um rico dossiê a respeito das pessoas, permitindo aos sistemas computacionais determinar sua personalidade de forma mais precisa do que um humano conseguiria fazer: preferências, fobias, reações, entre outros. Assim, o poder de exercer a privacidade encontra-se cada vez mais limitado e comprometido em razão do avanço da tecnologia computacional inteligente, o que exige que se pense e se reconstrua as relações sociais (GABRIEL, 2018, p. 77).

A hiperexposição está ligada ao uso compulsivo das mídias sociais, expondo a vida cotidiana, sem levar em conta os riscos que podem causar, bem como a segurança da rede. Inicia-se o uso por um hábito de informar e acaba por um vício em se expor. Entre as tecnologias digitais que impulsionam os hábitos descritos anteriormente, o smartphone é a principal, vez que converge a informação em tempo real, a exposição, a conexão, o uso da tecnologia e o *multitasking*, para um único dispositivo que está sempre ao alcance. Tanto é que após a tempestade Sandy em 2012, em Nova Iorque, que provocou a falta de energia elétrica, diversos nova-iorquinos reportaram que sofreram crise de abstinência de celular (GABRIEL, 2018, p. 87). O vício da exposição é tão grande, que a preocupação das pessoas com a falta de energia

elétrica liga-se mais a ausência de carregamento dos celulares do que com própria segurança. A medidas em que a tecnologia digital permite conexão e exposição, as pessoas se expõem e passam mais tempo conectadas, mas estranhamente mais sozinhas.

O que se percebe é que a validade de cada um está em ser visto pelo outro. Esse fenômeno tem se intensificado conforme as pessoas ficam mais conectadas e com smartphones melhores, tanto que a palavra *selfie* foi eleita a palavra de 2013 pelo *Oxford Dictionaries*. Ademais, estatísticas demonstram que acidentes com *selfies* têm matado mais do que tubarões, isso porque registrar e compartilhar a vida tem se tornado mais importante do que viver (GABRIEL, 2018, p. 91).

Ao expor fatos importantes da vida cotidiana, o indivíduo cerca-se de tecnologia, mas sente falta do toque humano. A exposição nas mídias alimenta o ego, deixa vulnerável aos riscos e ainda culmina na perda de segurança, com danos à reputação. Ainda, ocorre a perda da integridade quando, inexistindo a devida segurança, ocorre a alteração de um tópico importante, que pode ser modificado pelos mais surpreendentes motivos, até mesmo intencionalmente (DE LUCCA & SIMAO FILHO, 2000, p. 133).

A segurança da rede é a confidencialidade. Se algumas informações forem vistas e copiadas por um indivíduo que esteja usando a internet para praticar o mal, o ponto segurança não está sendo observado. Atualmente a sociedade da informação busca um equilíbrio entre a reserva da vida privada e a prestação da notícia (DE LUCCA & SIMAO FILHO, 2000, p. 469), porém muitos expõem sua confidencialidade para se fazerem notáveis na rede.

Muito embora possa parecer excessivo e perigoso afirmar que “*nós somos nossos dados*”, fato é que a representação social de cada indivíduo está cada vez mais adstrita às informações disseminadas nos diversos bancos de dados e aos perfis e simulações construídas por tais meios. O sujeito torna-se cada vez mais conhecido como público ou privado através dos dados que lhe dizem respeito, o que acaba por incidir sobre a liberdade de comunicação, sobre o princípio de igualdade, de expressão ou de circulação, sobre o direito à saúde, sobre a condição de trabalhar, entre outros. E transformando-se em entidades desencarnadas, surge a necessidade de tutelar o seu “*corpo eletrônico*”, ou seja, tutelar os seus dados pessoais tanto contra a expansão do monitoramento estatal, quanto contra a utilização sem discriminação de dados por empresas de diversos segmentos (SILVA, 2016).

A sociedade da informação hodierna acarretou diversas mudanças de sentido no que se entende como direito à privacidade e seus possíveis desdobramentos como intimidade e vida privada, onde se incluem o “*direito ao esquecimento*” e o “*direito à intimidade*”⁶.

A expressão norteamericana “*right to be let alone*”, trazida por Samuel Warren e Louis Brandeis para a configuração do direito de ser deixado em paz/só, iniciou o reconhecimento do direito à privacidade (no sentido atual do termo). Ocorre que essa expressão, não raras as vezes, é utilizada como sinônimo de um direito ao esquecimento (FORTES, 2015, p. 157), sendo que a adequada conceituação para direito ao esquecimento seria “*right to be forgotten*”, uma vez que ultrapassa a simples proteção da vida privada, possibilitando que um usuário apague dados e informações pessoais na internet (BERNAL, 2014). Não é à toa que, em conferência na *New York University*, Eric Schmidt disse que um dos grandes desafios do futuro da internet é a elaboração de um “*botão delete*”, oportunizando as pessoas a apagarem publicações relacionadas a atos feitos no passado que não desejam mais que sejam exibidos os resultados de busca ou de páginas indexadas na web (FORTES, 2016, p. 158).

Para Sarlet, o direito ao esquecimento pressupõe a necessidade de reconhecimento e proteção em face do Estado e de terceiros em um plano social ampliado, ou seja, de não sofrer permanentemente e indeterminadamente as repercussões geralmente negativas associadas a fatos ocorridos do passado, o que é importante para uma vida pessoal saudável física e psiquicamente, bem como para a integração do indivíduo na sociedade (SARLET, 2020, p.70).

O termo “*direito ao esquecimento*” foi utilizado primeiramente pelo Tribunal Constitucional da Alemanha. O Caso Lebach (STF, 2018, p. 7-8), decidido em 5 de junho de 1973, foi um dos julgados de notoriedade daquele país, onde se discutia a colisão entre o direito de liberdade de imprensa e os direitos da personalidade. Em suma, tratava-se de um pedido liminar feito por um reclamante que, juntamente com outros dois sujeitos, se envolveram em crime que culminou na morte quatro soldados, deixando outro gravemente ferido. O fato ocorreu à noite, quando os soldados protegiam um depósito de munições que foram roubadas (MARTINEZ, 2014, p. 90). Os dois principais acusados foram condenados à prisão perpétua em agosto de 1970 e um terceiro partícipe (que auxiliou na preparação do crime) foi condenado

⁶ Frise-se que, 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.

a seis anos de reclusão. Um pouco antes de ganhar a liberdade através de livramento condicional, a ZDF (*Zwites Deutsches Fernsehen* ou Segundo Canal Alemão), levando em consideração o interesse da opinião pública, fez um documentário sobre o caso, e, apesar de tentar impedir a sua exibição, o programa foi ao ar, já que o pedido foi negado pelos tribunais ordinários (o Tribunal Estadual de Mainz e o Tribunal Superior de Koblenz), seguindo o entendimento de que havia interesse público na divulgação das informações. Porém, foi procedente a Reclamação Constitucional junto ao Tribunal Constitucional, onde os julgadores entenderam que ocorreu a violação ao direito de desenvolvimento da personalidade (MARTINEZ, 2014, p. 90), sendo importante ressaltar que a reprodução dos fatos citou os nomes e mostrou fotos dos acusados, descrevendo minuciosamente a relação entre eles, inclusive suas relações homossexuais (MARTINS, 2014, p. 06). Nesse sentido, acertada foi a decisão daquele Tribunal Constitucional, visto que a exposição de questões de foro íntimo dos acusados não possuía relevante interesse público.

Na Espanha, uma das decisões que ganhou destaque ocorreu em outubro de 1986 no âmbito do Tribunal Constitucional em relação a ação movida por Isabel Pantoja em face da comercialização de um vídeo que reproduzia a agonia do seu marido e toureiro Paquirri. O citado tribunal anulou a decisão anterior do Tribunal Supremo que entendeu que a morte do toureiro não se tratava de sua esfera íntima. O Tribunal Constitucional ressaltou que as cenas vividas dentro da enfermaria não diziam respeito ao espetáculo público taurino (PÉREZ LUÑO, 2012, p. 102).

No âmbito internacional, o termo “*direito ao esquecimento*” foi usado pelo Tribunal de Justiça da União Europeia (TJUE) em 2013, ao entender ser exigível dos mecanismos de busca que parassem de mostrar determinados resultados. Na Europa, como em grande parte do ocidente, a proteção de dados tem grande importância e o “*derecho al olvido*” é considerado tradicional (STF, 2018, p. 5-6).

Merece destaque aqui a decisão do TJUE referente ao Processo no C-131/12, do qual 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, p. 5-6). No citado caso, algumas informações de Mario Costeja González foram publicadas por um jornal espanhol, em duas de suas edições impressas, no ano de 1998 e posteriormente foram republicadas em sua versão eletrônica. Desde então, quando se pesquisava o nome do autor nos mecanismos de busca,

aquela informação aparecia e era acessada. Sendo inexitoso o requerimento junto à “Google Spain”, Mario Costeja González fez uma reclamação à Agência Espanhola de Protección de Datos (AEPD), onde pleiteou que fosse exigida a eliminação ou a modificação da publicação deixando seus dados de serem exibidos (UNIÃO EUROPEIA, 2014). O processo foi juntado em 13 de maio de 2014, onde se garantindo ao cidadão europeu o direito ao esquecimento, reconhecendo a responsabilidade das ferramentas de busca pelo processamento de dados pessoais exibidos nos resultados, devendo prevalecer o direito ao esquecimento sobre o direito do público de conhecer e de ter fácil acesso à informação. No caso, a informação excluída foi considerada irrelevante e ultrapassada, não sendo necessária sua preservação, porém tal fato deve ser analisada de acordo com o contexto de cada caso em concreto (MARTINS, 2014, p. 08).

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

Porém, em fevereiro de 2021, foi julgado pelo Supremo Tribunal Federal o Recurso Extraordinário 1.010.606/RJ sobre o caso Aida Curi, tendo prevalecido, por maioria, o voto do Ministro Dias Tóffoli, que, após histórico da matéria, das controvérsias que a cercam e da apreciação do caso Aida Curi, considerou 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 deixa claro que tal decisão, embora abranja tanto a mídia tradicional quanto a Internet, não alcança os pedidos de desindexação, que, de acordo com a fundamentação, não se confunde com o direito ao esquecimento. Nesse sentido, hipóteses como a do famoso caso Google Spain já citado, não serão abrangidas pela Tese 786 no Brasil. Desindexar é assinalar o URL (*Uniform Resource Locator* - o endereço de uma página na web), para que ele não conste dos resultados nas procuras dos buscadores normais, ou seja, quando o usuário digita o conteúdo a ser buscado em um campo de busca, ainda que ele esteja público, não será mostrado na lista dos resultados. Assim, ao desindexar um conteúdo de um mecanismo de busca normal, ocorre significativa diminuição do potencial de disseminação desse conteúdo, e conseqüentemente diminui o dano que eventualmente venha a ser causado ao envolvido com a sua disseminação (VIOLA, 2016, p. 366).

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

Outro instituto que surgiu, trata-se da construção teórica desenvolvida por Jacques Lacan, chamada de “*direito à extimidade*”, que devido aos estudos de Serge Tisseron, se tornou acessível a outras áreas do conhecimento. O termo “*extimidade*” se refere a maneira como determinadas questões atinentes à intimidade são disponibilizadas aos outros, com a finalidade de serem validadas ou não, culminando na reapropriação daquelas formulações, em uma nova perspectiva (TISSERON, 2011, p. 84-85).

Assim, ao contrário do defendido por Luiz Flávio Gomes⁷, “*extimidade*” não pode ser entendida como o oposto de intimidade (GOMES, 2002). A 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 deseja ser revelado pelo sujeito (TISSERON, 2011, p. 84-85). Em outras palavras, significa lançar ao público algo da privacidade (não indicando o seu oposto), ou seja, trata-se da exteriorização de forma explícita da liberdade de expressão. Por conseguinte, os conceitos de “*extimidade*” e de intimidade não são antagônicas, trata-se da mesma matéria com destinação

⁷ Para quem “*extimidade*” é lançar ao público algo da privacidade.

diversa. No mesmo sentido, Jacques-Alain Miller afirma 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).

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

Tais novidades são utilizadas especialmente em âmbito virtual, em que se misturam o público e o privado. Deste modo, nas questões de proteção *online* questiona-se qual a dimensão pública e/ou privada da internet atualmente, ou seja, ela deve ser considerada um espaço privado ou público? A resposta a essa indagação é complexa e pressupõe o questionamento a respeito do que é internet e ciberespaço. Para aqueles que defendem que a internet é propriedade pública, existe a possibilidade efetiva de os usuários reivindicarem seus direitos e tê-los respeitados. No entanto, indaga-se qual parte da internet deve ser considerada privada e/ou pública e quais direitos poderá gozar o indivíduo que utiliza cada uma dessas partes. A resposta mais adequada a essa questão me parece a que todos os espaços da internet deveriam ser públicos, exceto haja razão conveniente para o contrário.

Uma mudança de modelo, em favor da natureza mista, é defendida por Paul Bernal, ou seja, no espaço privado os sujeitos teriam controle sobre as suas próprias configurações de privacidade e no espaço público solicitariam a proteção através de direitos de privacidade. Nessa visão, a regra seria a proteção da privacidade e aqueles que quisessem monitorar pessoas ou coletar, utilizar, armazenar dados pessoais necessitariam justificar os motivos para a vigilância (BERNAL, 2014).

Dentro dessa perspectiva, a ideia do privado migra para o “pessoal”, onde se tutela as informações pessoais e não necessariamente as privadas. Assim, se antes a ordem lógica era “*pessoa-informação-sigilo*”, na atualidade fala-se em “*pessoa-informação-circulação-controle-gestão*”, em outras palavras, o indivíduo não tem apenas o direito de obstruir uma informação de sua privacidade que tenha escapado, mas também pode controlar sua circulação ativa e passivamente (RODOTÁ, 2008, p. 93).

Fato é que a internet acabou com os binômios “*não visível/privado*” e “*visível/invisível*” e transformou o espaço público-privado no que Dominique Cardon chamou de cenário de um “*jogo de luz e sombras*”. Em outras palavras, o espaço público-privado se tornou um degrade, estando nos extremos a alta e a baixa visibilidade, e no meio as zonas de interação (CARDON, 2012, p. 49). Essa mistura entre o público e o privado na internet é uma nova maneira de interpretar esses espaços, vez que entre essa nova zona de baixa e alta visibilidade aparece um espaço intermediário surge um espaço intermediário, que não é nem privado, nem público, mas mais ou menos visível.

Na obra intitulada “*Les tyrannies de la visibilité*”⁸ que trata da tirania da visibilidade e da necessidade de tornar-se visível para realmente existir, as francesas Nicole Aubert e Claudine Haroche analisaram temas em torno dessa questão e concluíram que o termo “*visibilidade*” gera profunda ambivalência, já que nela se misturam dois polos antagônicos: o indesejável e o desejável (AUBERT; HAROCHE, 2011). Serge Tisseron, seguindo o mesmo raciocínio, argumenta que os relacionamentos considerados “*significativos*” passaram da intimidade para “*extimidade*” (TISSERON, 2011). Essa questão também é tratada por Zygmunt Bauman ao se referir ao analista do trajeto histórico do indivíduo moderno, Alain Ehrenberg, que escolhe um acontecimento da década de 1980, no qual Vivianne (uma “*francesa comum*”), declara num “*talk show*” de TV que, em decorrência de seu marido ter ejaculação precoce, ela nunca teria tido orgasmo (EHRENBERT apud BAUMAN, 2012). Chamaram a atenção de Alain Ehrenberg que os atos essencialmente privados foram revelados e foram abertos ao público sem controle (BAUMAN, 2012, p. 227).

Portanto, a barreira entre as esferas pública e privada foi eliminada, já que se vive hoje uma “*sociedade confessional*” que até então era desconhecida, com microfones instalados dentro de confessionários, onde a partir de então os segredos mais íntimos podem ser revelados (BAUMAN, 2012, p. 228). Bauman entende que ocorreu o fim da privacidade, pois não importa mais a possibilidade de violação da privacidade, e sim o oposto, ou seja, que se fechem as portas de saída da privacidade.

Antes do atentado ocorrido em 11 de setembro 2001, por razões de exigências do mercado e da tendência de montagem de banco de dados cada vez maiores para controlar

⁸ A tirania da visibilidade (tradução nossa). Ser visível para existir? Consultar livro em sua versão francesa (AUBERT; HAROCHE, 2011).

comportamentos, o fim da privacidade já era comentado, e percebendo o modo como o mundo está mudando emerge 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 ainda a ser frequentemente considerada como um obstáculo à segurança, sendo superada por legislações de emergência (RODOTÁ, 2008, p. 14).

3. A NECESSIDADE DE CONSTRUÇÃO DE UMA TUTELA TRANSVERSAL DO DIREITO À PRIVACIDADE

Importante destacar aqui que não se objetiva traçar a evolução dos direitos da personalidade, mas produzir indagações ao redor do termo e de como ele se relaciona com as novas tecnologias (NASCIMENTO, 2017, p. 266-267), e em especial, com o direito penal, surgindo a necessidade de uma tutela transversal da privacidade, em nível nacional e internacional, e de dimensões verticais e complementares, vez que a sociedade da informação hodierna acarretou diversas mudanças de sentido no que se entende como direito à privacidade e seus possíveis desdobramentos como intimidade e vida privada.

O avanço do conhecimento científico e dos saberes possibilita nas confluências e combinações se levando em consideração a constituição das disciplinas tradicionais. Ao se proclamar a autonomia de uma disciplina, corre-se o risco de equívocos (PAVIANI, 2007, p. 143). A transdisciplinaridade e a complexidade se entrelaçam e ajudam a enfrentar os grandes problemas, por isso se faz necessário aceitar a aventura do pensamento complexo, pois este dá instrumentos para ligar os conhecimentos (MORIN, 2007, p.28). Para a transdisciplinaridade é necessário um pensamento organizador e complexo. Uma visão que dá conta da dimensão planetária dos conflitos atuais poderá fazer frente à complexidade do mundo e ao desafio atual de autodestruição espiritual e material das sociedades (GAUER, 2013, p. 537).

A transversalidade e a interdisciplinaridade são modos de se estudar o conhecimento que procuram uma reintegração de aspectos que ficaram isolados uns dos outros pelo tratamento disciplinar, buscando, assim, uma visão adequada e ampla da realidade, que não raras as vezes

está fragmentada pelos meios disponíveis para conhecê-la e não porque o seja em si mesma (GARCIA, 2007).

Com a interdisciplinaridade questiona-se essa divisão em segmentos dos diferentes campos de conhecimento, buscando os pontos de convergência entre as várias áreas e a sua abordagem conjunta, de modo a fornecer uma relação epistemológica entre as disciplinas e aproximando os fenômenos naturais e sociais, que são normalmente complexos e irreduzíveis ao conhecimento obtido quando estudados através de uma única disciplina. Há também temas, cujo estudo exige uma abordagem particularmente ampla e diversificada, sendo alguns deles inseridos nos parâmetros curriculares nacionais e denominados de “Temas Transversais”, pois

"tratam de processos que estão sendo intensamente vividos pela sociedade, pelas comunidades, pelas famílias, pelos alunos e educadores em seu cotidiano. São debatidos em diferentes espaços sociais, em busca de soluções e de alternativas, confrontando posicionamentos diversos tanto em relação a intervenção no âmbito social mais amplo quanto a atuação pessoal. São questões urgentes que interrogam sobre a vida humana, sobre a realidade que está sendo construída e que demandam transformações macrossociais e também de atitudes pessoais, exigindo, portanto, ensino e aprendizagem de conteúdos relativos a essas duas dimensões"(GARCIA, 2007).

Aqui entra o direito à privacidade no âmbito penal e da segurança pública decorrentes da hiperexposição pessoal como tema transversal. Os temas transversais englobam o aprender sobre a realidade, na realidade e da realidade, intervindo também na realidade para modificá-la e a transversalidade é o modo adequado para o tratamento destes temas. A Interdisciplinaridade e transversalidade alimentam-se mutuamente, vez que ao trabalhar os temas transversais de forma adequada não se pode ter um ponto de vista disciplinar rígido, devendo o referido tema l ser um eixo unificador das disciplinas que o estuda. A interação entre as disciplinas faz recuperar a realidade, superando a fragmentação e tendo a visão do todo (GARCIA, 2007).

Vive-se um tempo de contradição das questões relacionadas à proteção de dados pessoais, pois ao mesmo tempo que tem aumentado a consciência da importância da proteção de dados das vidas privadas dos indivíduos, aumenta-se também a própria liberdade desses sujeitos. Tal constatação se reflete em inúmeros documentos nacionais e internacionais, em especial na Carta de Direitos Fundamentais da Comunidade Europeia que reconhece a proteção de dados como um direito fundamental autônomo. Ainda assim, torna-se cada vez mais difícil respeitar essa presunção geral, já que as exigências de segurança interna e internacional,

reorganização da administração pública e interesses de mercado estão levando à diminuição ou desaparecimento de garantias essenciais (RODOTÁ, 2008, p. 13).

A realidade se distancia cada vez mais da estrutura dos direitos fundamentais por três razões básicas: a primeira, porque depois do atentado de 11 de setembro diversos critérios de referência mudaram e as reduziram-se as garantias em todo o mundo; a segunda, porque a tendência de reduzir as garantias se estendeu a setores que tentam se beneficiar com as mudanças, como o mundo dos negócios; e terceiro, porque as novas tecnologias tornam disponíveis continuamente novas ferramentas para classificar, selecionar, triar e controlar os indivíduos, resultando em uma maré tecnológica que as autoridades nacionais e internacionais nem sempre poderão controlar de forma adequada. Com isso, alguns princípios do sistema de proteção de dados estão sendo pouco usados, e dados que foram coletados para um propósito são disponibilizados para propósitos diversos, considerados tão importante quanto aqueles que motivou a coleta, e ainda, dados processados por uma determinada agência são disponibilizados para outra, tornando o indivíduo cada vez mais transparente e os órgãos públicos cada vez mais fora de qualquer controle político e legal, implicando uma nova distribuição de poderes políticos e sociais (RODOTÁ, 2008, p. 14-15).

Atualmente, a privacidade é projetada para além de sua definição tradicional como “*direito a ser deixado só*”, apresentando-se como indispensável à liberdade existencial, como “*tutela das escolhas de vida contra toda forma de controle público e de estigmatização social*”. Não se trata mais apenas do direito de excluir os outros da possibilidade de conhecer ou divulgar as informações que me dizem respeito, sendo agora o direito de controlar o uso dessas informações em qualquer momento e em qualquer lugar (direito à autodeterminação informativa). Nesse sentido, a privacidade transforma-se em um poder social, o de controlar diretamente os sujeitos públicos e privados que tratam os dados pessoais, e, em uma sociedade na qual as informações tornam a riqueza mais importante, a tutela da privacidade contribui decisivamente para o equilíbrio dos poderes. Daí o porquê o fim da privacidade não representaria somente um risco para as liberdades individuais, podendo efetivamente conduzir ao fim da democracia (RODOTÁ, 2008, p. 144).

Portanto, a privacidade, neste seu significado mais amplo, constitui um elemento fundamental da cidadania atual, ou seja, da “*cidadania eletrônica*”, e a sociedade da informação

requer novos instrumentos e um novo quadro institucional. De fato, há anos, fala-se da necessidade de um *Information Bill of Rights*.

A construção de uma tutela da privacidade, em nível nacional e internacional é relativamente recente na sociedade marcada pelo desenvolvimento das novas tecnologias. O juiz Frank Easterbrook, em 1996, questionou a necessidade de um direito direcionado ao estudo do ciberespaço, asseverando que a afirmando que o estudo seria tão útil quanto um “*direito do cavalo*”⁹. Argumentava ainda no texto intitulado “*Cyberspace and the Law of the horse*”, que em vez de os operadores jurídicos tratarem o “*ciberdireito*”, seriam mais bem servidos se dominassem princípios jurídicos fundamentais e após os aplicassem a novos fatos que surgissem (EASTERBROOK, 1996).

Stéfano Rodotá destacou esta posição no momento em que o meio jurídico considerou inserir como aulas extravagantes o curso de “*Tecnologias e direito*”. Afirmou que pareciam ser questões marginais, que tinham pouco a ver com o direito, ao passo que atualmente sabe-se que a bioética e a informática são temas capitais para a pesquisa jurídica e que transformam profundamente a maneira como o jurista olha a realidade, tornando obrigatória a revisão de categorias como o corpo e a pessoa, ou seja, tais categorias estavam fora da atenção do jurista (RODOTÁ, 2008, p. 04-05).

Após, diversos pesquisadores da área contestaram a tese de Frank Esterbrook. Destaca-se a tese de doutorado em direito defendida no Brasil, no ano de 2015, por Vinícius Borges Fortes, que cita Lawrence Lessig para responder explicitamente à teoria mencionada, salientando que as regras jurídicas, as percepções e o ambiente do ciberespaço precisam evoluir, se desenvolver e ser ampliado. Assim, mais importante do que a regulação do espaço real, a tutela do ciberespaço representa uma troca no paradigma de regulação, com a necessária definição de mudanças na formação e desenvolvimento de princípios que auxiliem, no âmbito real e virtual, os novos caminhos do direito, em especial, no âmbito penal (*apud* FORTES, 2015, p. 51).

A construção de um *Internet Bill of Rights* começou a ser notada na primeira edição do Internet Governance Forum (IGF), da ONU, em 2006, onde surgiu uma coalizão dinâmica

⁹ Assim, a expressão “direito do cavalo” foi um termo constantemente usado em meados da década de 1990, relativamente ao estágio embrionário em que se encontrava a internet.

chamada “*Internet Bill of Rights*”¹⁰”. Entre a primeira e a segunda edição do IGF, o governo da Itália promoveu o primeiro *Dialogue Forum on Internet Rights*, em Roma, no dia 27 de setembro de 2007. A abertura do evento foi realizada por Rodotà, que lançou as diretrizes para o debate sobre uma carta de direitos para a Internet. A segunda edição do IGF, que ocorreu em 2007 no Rio de Janeiro, solidificou uma junção de forças entre brasileiros e italianos em prol de uma carta de direitos para a Internet, sendo o ponto de partida para os trabalhos desenvolvidos em nível nacional nos dois países posteriormente, a saber, o Marco Civil da Internet brasileiro, aprovado em 2014 e a Declaração italiana sobre direitos na Internet, aprovada em 2015 (SOUZA, 2017). E a mais recente Lei Geral de Proteção de Dados (Lei nº 13.709, de 2018), aprovada em 2018 com entrada em vigor em 18 de agosto de 2020.

Contudo, continua grande o desnível de poderes entre os cidadãos e os grandes coletores de informações, públicos e privados. Para enfrentar de maneira correta esse problema fundamental, é oportuno considerar três questões significativas: o anonimato na rede, o papel da lógica do mercado e a função e os limites do direito. Isso porque o desenvolvimento da internet sempre esteve acompanhado de uma demanda pelo anonimato e da consequente possibilidade de assumir na rede múltiplas identidades, surgindo como uma condição indissociável da própria natureza da internet, vista como um espaço irreduzível de liberdade. Um lugar onde a convivência de interesses e liberdades diversas pode propiciar o surgimento de conflitos, como aquele entre a privacidade/anonimato de quem difunde notícias e a privacidade/reserva de quem é objeto delas, fazendo-se indispensável encontrar instrumentos para a resolução de tais conflitos (RODOTÀ, 2008, p. 150).

Esse conflito, contudo, deve ser analisado sob uma ótica mais ampla, levando-se em conta os modelos existentes: um modelo liberal, contrário à regulação legislativa e favorável à auto-regulamentação (modelo norte-americano) e um modelo europeu baseado na lei e no proibicionismo. Se considerar-se mais analiticamente a situação norte-americana, nota-se um crescente recurso ao instrumento legislativo, onde todos os anos os Estados aprovam dezenas de lei em matéria de privacidade e as associações norte-americanas de consumidores se referem cada vez mais ao modelo europeu, enquanto na Europa cresce uma orientação liberal acerca da criptografia. Assim, o conjunto desses fatos mostra como o problema de proteção de dados não

¹⁰ Esse grupo, consistente de atores de diversos setores, objetivava debater a oportunidade e o conteúdo de uma Carta de Direitos para a Internet (um Internet Bill of Rights).

pode mais ser analisado segundo o esquema que contrapõe a lei à auto-regulamentação (RODOTÀ, 2008, p. 150-151). Fala-se agora em um desenvolvimento geral de uma *lex informatica*, que imitaria o modelo da *lex mercatoria* (REIDENBERG, 1998, P. 553).

Fato é que a disciplina das matérias abrangidas pelas tecnologias da informação e da comunicação é atualmente confiada a uma miríade de fontes, diversas em conteúdo e forma, todas porém relevantes para fins de regulamentação, como tratados, convenções, acordos internacionais e supranacionais, disciplinas regionais, leis nacionais, normas estatais, direito jurisprudencial, regras provenientes das autoridades independentes supranacionais ou nacionais, diretrizes provenientes de organismos internacionais, códigos de conduta internacionais e nacionais, modelos contratuais uniformes, standards técnicos, garantias tecnológicas eventualmente impostas para a comercialização de determinados produtos ou para o desenvolvimento de atividades específicas, entre outros. Esse elenco, incompleto, demonstra que se está diante de uma multiplicidade de fontes que refletem a presença de uma pluralidade de atores e uma variedade de instrumentos, exigindo uma estratégia jurídica integrada e compositiva (RODOTÀ, 2008, p. 151-152).

A recusa ao paternalismo legislativo e a reafirmação de uma liberdade na rede, identificada com a ausência de qualquer regra, convertem-se em um ulterior crescimento da lógica do mercado sobre toda a dinâmica da rede com efeitos negativos graves, que podem ser evitados com uma disciplina legislativa sóbria e objetiva. Também as novas formas de auto-regulamentação e sua integração no sistema jurídico, podem ser consideradas como instrumentos aptos a favorecer soluções eficazes socialmente, que podem ser experimentadas inclusive como ponto de partida para posteriores e eventuais intervenções legislativas. Tendo em vistas tais aspectos, podem ser melhor avaliadas as razões das propostas americanas e de algumas dinâmicas que estão sendo verificadas na Europa. A proposta de considerar os dados como propriedade do interessado mostra uma tutela insuficiente justamente pelo perfil do direito fundamental à privacidade vez que a possibilidade de negociar uma contrapartida econômica se apresenta como o único instrumento capaz de atribuir um real poder de controle ao interessado sobre os seus próprios dados, que, de outra maneira, poderiam ser coletados sem seu consentimento ou conhecimento. Esta situação dos Estados Unidos foi superada pela Europa com a Diretiva 95/46/CE e pelo conjunto das normativas de todos os países da União, que mantem a privacidade no âmbito dos direitos fundamentais e, portanto, a consideram um

elemento da nova cidadania (RODOTÀ, 2008, p. 153-154). Veja-se que uma tutela forte não deve passar necessariamente pela transformação dos dados pessoais em objeto de propriedade, já que a relação entre o indivíduo e suas próprias informações insere-se no quadro dos direitos da personalidade, o que significa que o princípio básico é constituído pelo consentimento do interessado e que este não perde o direito de controlar os seus próprios dados pessoais mesmo se em poder de terceiros, sejam entes públicos ou privados.

Considerando que o artigo trata do direito à privacidade no âmbito penal e da segurança pública decorrentes da hiperexposição pessoal como tema transversal a privacidade, e este pertence aos direitos da personalidade, devem se estender à Internet as regras tradicionalmente aplicadas para garantir a liberdade de comunicação, o que implica na possibilidade de escolher as modalidades de comunicação, recorrendo, por exemplo, à criptografia (escolha severamente limitada nos Estados Unidos e aceita na Europa como instrumento capaz de aumentar o valor democrático da Internet). Tais formas de tutela jurídica são acompanhadas, nacional e internacionalmente, de indicações relacionadas à segurança física e lógica dos dados coletados, ao mesmo tempo em que se desenvolvem políticas de privacidade com vistas a informar aos usuários da Internet as garantias previstas para os seus dados¹¹. O conjunto de tutelas oferecidas aos cidadãos tende a se estender dos dados “em saída” àqueles “em entrada”, atribuindo especial importância ao “direito de não saber”, que no caso concreto se traduz no direito de não receber comunicações indesejadas ou para as quais, de qualquer forma, não foi dado o consentimento preventivo (RODOTÀ, 2008, p. 154-155).

Esse conjunto de garantias reduzem a pressão das lógicas de mercado que podem se traduzir em violações da esfera privada. Para evitar que a coleta de informações se transforme em violação da dignidade das pessoas são previstas formas de indisponibilidade ou inalienabilidade de certas categorias de dados, como o caso, em especial, dos dados sensíveis (relativos à opinião, raça, saúde., vida sexual), cujo tratamento não é suficiente nem mesmo a autorização por escrito do interessado. Por fim, é necessário evitar ainda a transformação em mercadoria dos aspectos mais íntimos da vida privada, fato especialmente importante para os dados genéticos utilizados para fins criminais, como aconteceu na Islândia, onde suscitou polêmicas e preocupações a lei que concedeu a uma empresa privada o direito de utilizar, com

¹¹ Isso ocorre também através da ação de sujeitos que certificam um determinado site e, recorrendo às *privacy enhancing Technologies (PET)*, buscam criar um ambiente informativo onde tecnologias ‘limpas’ substituam as tradicionais tecnologias ‘sujas’, as quais permitem seguir cada rastro deixado pelos frequentadores da rede.

exclusividade, durante doze anos, os dados referentes ao patrimônio genético da população (RODOTÀ, 2008, p. 156).

4. CONSIDERAÇÕES FINAIS

Na sociedade atual da informação, multiplicam-se interações humanas em conjunto com uma série de ferramentas, em especial as digitais, com resultados nem sempre benéficos. De qualquer forma, todas as mudanças estão sendo assimiladas pelo ordenamento jurídico, sendo inegável a evolução que passou a ter o direito digital no judiciário brasileiro.

Ainda, há o problema da hiperexposição, voluntário ou não, que acaba permitindo que terceiros de má-fé usem os dados sensíveis desses cidadãos para usos totalmente indevidos.

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

A sociedade da informação propõe novos desafios à própria democracia, oferecendo a ela a possibilidade de coletar qualquer informação sobre os cidadãos, com argumento de que tudo pode se revelar útil para a tutela da segurança, da saúde, entre outros, mas a democracia é também sobriedade, até mesmo renúncia, quando pode existir risco para a liberdade dos cidadãos.

Assim, o tema da tutela da privacidade, em especial no âmbito penal e da segurança pública decorrentes da hiperexposição pessoal deve ser tratado como um tema transversal. Para colher todas as oportunidades do novo mundo que já se vivencia, são necessárias políticas públicas adequadas, instituições concebidas com a consciência de que as tecnologias suprimem a noção de espaço e tempo e, portanto, tornam vãs as proteções dentro das velhas regras e confins territoriais/nacionais. Está nascendo uma nova forma de cidadania que exige uma tutela transversal, mas deve nascer também conjuntamente uma nova ideia de soberania.

REFERÊNCIAS BIBLIOGRÁFICAS

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 intimidade 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: 08/03/2021.

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: 18/03/2021.

BRASIL. Conselho da Justiça Federal. *Enunciado no 531*. Disponível em: <http://www.cjf.jus.br/enunciados/enunciado/142> . Acesso em: 10/03/2021.

BRASIL. Conselho da Justiça Federal. *Enunciado no 576*. Disponível em: <http://www.cjf.jus.br/enunciados/enunciado/821> . Acesso em: 10/03/2021.

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 : 04/03/2021.

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: Édípro, 2000.

EASTERBROOK, Frank. Cyberspace and the law of the horse. *Chicago Unbound*, n. 1, p. 207-216, 1996.

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 . Acesso em 08/03/2021.

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

GARCIA, Lenise Aparecida Martins. *Transversalidade e interdisciplinaridade*. Rio de Janeiro: 2007. Disponível em: <http://smeduquedecaxias.rj.gov.br/nead/Biblioteca/Forma%C3%A7%C3%A3o%20Continuada/Artigos%20Diversos/garcia-transversalidade-print.pdf> . Acesso em 26/03/2021.

GAUER, Ruth M. Chittó. Interdisciplinaridade e pesquisa. *Civitas -Revista de Ciências Sociais*, v. 13, n. 3, p. 536-543, 2013. Disponível em: https://www.scielo.br/scielo.php?pid=S1519-60892013000300009&script=sci_arttext&tlng=pt . Acesso em: 26/03/2021.

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: 18/03/2021.

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 expresso 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.

LIMA, Marco Antônio. BARRETO JUNIOR, Irineu Francisco. Marco Civil da Internet: limites da previsão legal de consentimento expresso 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. *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 . Acesso em: 27/03/2021.

MORIN, Edgar. *A cabeça bem feita: repensar a reformar, reformar o pensamento*. 15. ed. Rio de Janeiro: Bertrand Brasil, 2008.

MORIN, Edgar. Desafios da transdisciplinaridade e da complexidade. *Inovação e interdisciplinaridade na universidade*. Porto Alegre: EDIPUCRS, p. 22-28, 2007. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=nvAowfuBM2MC&oi=fnd&pg=PA22&dq=interdisciplinaridade+edgar+morin&ots=JZzNeY6pj3&sig=UTt3OBTxGWzpBATyqz9LrEqszo#v=onepage&q=interdisciplinaridade%20edgar%20morin&f=false> . Acesso em: 26/03/2021.

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. Acesso em: 10/02/2021.

PAESANI, Liliana Minardi. *O Direito na Sociedade da Informação II*. São Paulo: Atlas, 2009.

PAVIANI, Jaime. Interdisciplinaridade na universidade. *Inovação e interdisciplinaridade na universidade*. Porto Alegre: EDIPUCRS, p. 139-146, 2007. Disponível em: AUDI, JLN; MOROSINI, MC (Orgs.), p. 139-156, 2007. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=nvAowfuBM2MC&oi=fnd&pg=PA139&dq=interdisciplinaridade+cancelli&ots=JZzNeY6rp7&sig=u1RzrhJsnLOMe4OC6xFRa7eI158#v=onepage&q=interdisciplinaridade%20cancelli&f=false> . Acesso em: 26/03/2021.

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

REIDENBERG, J. R. Lex Informatica: The formulation of information policy rules through technology. *Texas Law Reviw*, n. 76, 1998.

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 10/03/2021.

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.

SCARZELLI, Patrícia. *A Comunidade Cibernética e o Direito*. Rio de Janeiro: Lumen Juris, 1997.

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/BJI5DIREITOAQUESQUECIMENTO.pdf>. Acesso em: 04/03/2021.

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.

Data de Submissão: 14/04/2021

Data de Aceite: 23/04/2022