V ENCONTRO INTERNACIONAL DO CONPEDI MONTEVIDÉU – URUGUAI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

ROSANE LEAL DA SILVA

MARCELO EDUARDO BAUZA REILLY

Copyright © 2016 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos.
Nenhuma parte deste livro poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Raymundo Juliano Feitosa – UNICAP
Vice-presidente Sul - Prof. Dr. Ingo Wolfgang Sarlet – PUC - RS
Vice-presidente Sudeste - Prof. Dr. João Marcelo de Lima Assafim – UCAM
Vice-presidente Nordeste - Profa. Dra. Maria dos Remédios Fontes Silva – UFRN
Vice-presidente Norte/Centro - Profa. Dra. Julia Maurmann Ximenes – IDP
Secretário Executivo - Prof. Dr. Orides Mezzaroba – UFSC
Secretário Adjunto - Prof. Dr. Felipe Chiarello de Souza Pinto – Mackenzie

Representante Discente – Doutoranda Vivian de Almeida Gregori Torres – USP

Conselho Fiscal:
Prof. Msc. Caio Augusto Souza Lara – ESDH
Prof. Dr. José Querino Tavares Neto – UFG/PUC PR
Profa. Dra. Samyra Haydêe Dal Farra Naspolini Sanches – UNINOVE
Prof. Dr. Lucas Gonçalves da Silva – UFS (suplente)
Prof. Dr. Fernando Antonio de Carvalho Dantas – UFG (suplente)

Secretarias:
Relações Institucionais – Ministro José Barroso Filho – IDP
Prof. Dr. Liton Lanes Pilau Sobrinho – UPF
Educação Jurídica – Prof. Dr. Horácio Wanderlei Rodrigues – IMED/ABEDi
Eventos – Prof. Dr. Antônio Carlos Diniz Murta – FUMEC
Prof. Dr. Jose Luiz Quadros de Magalhaes – UFMG
Profa. Dra. Monica Herman Salem Caggiano – USP
Prof. Dr. Valter Moura do Carmo – UNIMAR
Profa. Dra. Viviane Coêlho de Séllos Knoerr – UNICURITIBA
Comunicação – Prof. Dr. Matheus Felipe de Castro – UNOESC

D598

Direito, governança e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI/UdelaR/Unisinos/ URI/UFSM /Univali/UPF/FURG;

Coordenadores: Marcelo Eduardo Bauza Reilly, Rosane Leal Da Silva – Florianópolis: CONPEDI, 2016.

Inclui bibliografia
ISBN: 978-85-5505-251-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Instituciones y desarrollo en la hora actual de América Latina

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Interncionais. 2. Direito. 3. Governança. 4. Novas tecnologias. I. Encontro Internacional do CONPEDI (5. : 2016 : Montevidéu, URU).

CDU: 34

Conselho Nacional de Pesquisa e Pós-Graduação em Direito
Florianópolis – Santa Catarina – Brasil
www.conpedi.org.br

Universidad de la República
Montevideo – Uruguay
www.fder.edu.uy

V ENCONTRO INTERNACIONAL DO CONPEDI MONTEVIDÉU – URUGUAI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

Apresentação

Vive-se sob o impacto crescente do desenvolvimento tecnológico. Diariamente incontáveis produtos e serviços são projetados e disponibilizados no mercado global de consumo e a cada novo lançamento se renovam as promessas de mais qualidade de vida, redução de distâncias, maior conexão e felicidade.

A indústria desenvolvedora de tecnologia não mede esforços na criação de produtos e aplicativos mais dinâmicos e inteligentes e, amparados em poderosas campanhas de marketing, criam e/ou antecipam desejos de consumo. Novos lançamentos se sucedem num curto espaço de tempo, ditados mais pelo ritmo frenético da obsolescência programada do que por qualquer real necessidade dos usuários. No outro lado da cadeia de produção, consumidores ávidos por novidades não medem esforços para a aquisição de um novo dispositivo eletrônico e, cativados pelo discurso publicitário, apostam nas promessas mercadológicas como verdadeiras fórmulas garantidoras de uma vida plena e feliz.

Não é diferente no segmento das Tecnologias da Informação e Comunicação (TIC), cujos produtos, aplicativos e serviços seduzem milhares de usuários em todo o mundo. Em nenhum outro período histórico foi tão fácil e rápido obter informação e o acesso aos bens culturais como livros, músicas e filmes também experimentou relativa democratização.

Ao lado da pluralidade de fontes de consultas, a tecnologia alçou o consumidor, antes reduzido a um papel mais passivo, à condição de produtor de conteúdos, fato que se revela atrativo, especialmente para os internautas mais jovens, denominados nativos digitais. E as anunciadas vantagens não cessam no campo da informação, pois as experiências comunicativas também se renovam sob a promessa de conexão global.

Para permitir a comunicação instantânea e sem fronteiras são criados dispositivos móveis e variados aplicativos que tanto possibilitam contatos reservados entre um número limitado de atores, quanto interações mais amplas e públicas, ocorridas nos inúmeros sites de redes sociais. E o ato de comunicar ganha novos matizes, pois ao lado da palavra falada e escrita novos signos são incorporados, encontrando nas imagens e símbolos aliados para dar vazão à liberdade de expressão e comunicação.

Todas essas facilidades introduzem modos próprios de ser e estar no mundo, típicos da era digital, e incorporam ao vocabulário cotidiano verbos como “publicar”, “curtir” e “compartilhar”. Quando esses verbos se transformam em ações, experiências de vida tornam-se insumos de um mercado que não cessa de se expandir. Grande parte dessa expansão ocorre graças aos dados pessoais dos internautas, captados durante as interações on-line, momento em que os usuários das TIC abrem mão de sua privacidade em nome de experiências compartilhadas nos mais variados ambientes virtuais. Ao lado da disponibilização voluntária de informações também são utilizadas técnicas mais veladas de captura dos dados pessoais, tanto realizadas pelo mercado quanto pelos Estados.

Em grande medida essa foi a tônica das discussões que se realizaram no GT Direito, Governança e Novas Tecnologias, realizado no dia 09 de setembro de 2016, na Universidad de la República Oriental del Uruguay, em Montevidéu, aos auspícios do V Encontro Internacional do CONPEDI.

A seleção dos trabalhos que compõem a presente obra foi realizada após criteriosa avaliação (com dupla revisão cega por pares), o que resultou na qualidade dos dezesseis artigos apresentados nesta obra. Ainda que com enfoques distintos, os artigos guardam em comum a preocupação com os impactos produzidos pelo uso crescente das tecnologias da informação e comunicação, quer isso se revele como um desafio para a regulação da internet, nos efeitos que vai produzir na sua regulação, quer se manifeste nas relações entre os particulares.

Para dar maior coerência aos debates ao longo da apresentação, ocorrida no dia 09 de setembro de 2016, os trabalhos foram divididos em três eixos temáticos, assim distribuídos:

1) Temas mais gerais, que situam o leitor sobre os desafios impostos à sociedade e Estado em decorrência do uso das tecnologias da informação e comunicação, tanto pelo aspecto da governança, quanto em razão dos processos de regulação, o que pode ser encontrado nos artigos: A governança do endereçamento da rede: breve análise comparativa; A regulamentação da internet à luz da violação à liberdade de uso; Apartheid tecnológico ou tragédia dos comuns: a América Latina na sociedade da informação; Crimes de informática e cruzamento de informação a partir de dispositivos móveis; Os contratos eletrônicos e os deveres anexos: aspectos da boa-fé objetiva e as novas tecnologias.

2) Os potenciais das tecnologias da informação e comunicação como instrumento para atuação política, tema que foi objeto de atenção nos trabalhos: A influência das novas tecnologias no processo democrático; As novas tecnologias da informação e o e-gov como instrumento de participação social; Em tempos de comunicação digital a transparência e o

acesso à informação como condições indispensáveis para o exercício da cidadania democrática.

3) O terceiro eixo é composto por trabalhos que versam sobre novas formas de violação da privacidade e de dados pessoais, discutindo-se as estratégias para a sua proteção na sociedade em rede, temática que perpassa os trabalhos: A proteção de dados no e-processo: entre a publicidade do processo e a privacidade na era internet; A tutela da privacidade e a proteção à identidade pessoal no espaço virtual; A sociedade da informação como ambiente de transmissão de dados; Breves considerações sobre desafios à privacidade diante do big data na sociedade da informação; Os comunicadores instantâneos e o direito fundamental à privacidade nos ambientes corporativos; Privacidade e proteção de dados pessoais na era pós-Snowden: o Marco Civil da Internet mostra-se adequado e suficiente para proteger os internautas brasileiros em face da cibervigilância? Sociedade virtual do risco vs. Filosofia libertária criptoanarquista: livre manifestação do pensamento, anonimato e privacidade ou regulação, segurança e monitoramento da rede; Anotações sobre o marco civil da internet e o direito ao esquecimento.

Com nossos votos de boa leitura!

Profa. Dra. Rosane Leal da Silva - UFSM/Brasil

Prof. Dr. Marcelo Eduardo Bauzá Reilly - UDELAR/Uruguay

A PROTEÇÃO DE DADOS NO E-PROCESSO: ENTRE A PUBLICIDADE DO PROCESSO E A PRIVACIDADE NA ERA INTERNET

THE DATA PROTECTION IN THE E-PROCEDURE: BETWEEN THE PUBLICITY OF PROCEDURE AND THE PRIVACY IN THE AGE OF INTERNET

Fernando Inglez de Souza Machado [1]
Sérgio Augusto da Costa Gillet [2]

Resumo

O presente artigo examina como ocorre a proteção de dados pessoais diante da virtualização do processo, em que o direito fundamental à publicidade do processo se perfaz por meio da rede mundial de computadores, resultando em aparente super-exposição do processo, podendo implicar em violação dos direitos fundamentais à privacidade e à proteção de dados pessoais. Deste modo, utilizando-se do método dedutivo de abordagem, foi possível determinar que o processo judicial eletrônico traz certa relativização da publicidade de seus atos de modo a compatibilizar-se com o direito fundamental à privacidade, no qual a proteção de dados pessoais ancora-se.

Palavras-chave: Proteção de dados, Processo judicial eletrônico, Direito fundamental à publicidade do processo, Direito fundamental à privacidade

Abstract/Resumen/Résumé

The present article exams how occurs the personal data protection before the procedure virtualization, in which the fundamental right to publicity of the procedure is materialized through the world wide web, resulting in apparent super-exposure of the procedure, possibly implying in violation of the fundamentals rights to privacy and to personal data protection. Thereby, using the deductive method of approach, it was possible to determine that the electronic judicial procedure brings some relativisation of the publicity of its acts in order to be compatible with the fundamental right to privacy, in which the personal data protection is grounded.

Keywords/Palabras-claves/Mots-clés: Data protection, Electronic judicial procedure, Fundamental right to procedure's publicity, Fundamental right to privacy

---

[1] Mestrando em Direito pela PUCRS. Bolsista CNPq. Advogado em Porto Alegre/RS.

[2] Mestrando em Direito pela PUCRS. Especialista em Direito Processual Civil pela PUCRS e em Direito Civil pela FADERGS. Bolsista CAPES/PROEX. Advogado em Belém/PA.

INTRODUÇÃO

O paradigma contemporâneo da Sociedade da Informação perpassa pela intensa transmissão e consumo de mídia, assim como pela virtualização das atividades humanas em contexto sócio-cultural, modificando vários aspectos da vida em sociedade. Nesta esteira, os impactos da popularização das tecnologias da informação e da comunicação (TICs) alcançam relevância jurídica, tendo em vista que o direito é um fenômeno cultural e, por esta razão, não está alheio às transformações advindas desta difusão de conexões e interações virtualizadas.

Todavia, com a realidade do uso das TICs cada vez mais difundido na Sociedade da Informação, o Estado passa, também, a utilizar-se de expedientes eletrônicos para a sua prestação jurisdicional. Notadamente com a virtualização do processo judicial, começa-se a implementar sistemas de tramitação eletrônica de autos judiciais e a usar ferramentas eletrônicas para garantir a efetividade do processo.

Para a devida prestação jurisdicional, a fim de garantir aos cidadãos a sua dignidade, o Poder Judiciário tem de coletar e tratar dados pessoais de seus jurisdicionados, o que demanda a devida ponderação entre o direito fundamental à publicidade dos atos processuais e o direito fundamental à privacidade, o qual guia a concessão do segredo de justiça.

No entanto, a experiência cibernética do processo judicial opera maiores considerações acerca da disposição das informações constantes em processos judiciais na rede mundial de computadores a clamar pela devida relativização do princípio da publicidade do processo face à exposição exagerada de seu conteúdo na Internet, cuidando, ainda, da segurança de eventuais dados pessoais.

Neste sentido, a presente pesquisa se apresenta com o objetivo de determinar de que modo a proteção de dados pessoais é alcançada no âmbito do processo judicial eletrônico. Para tanto, contrapõem-se a garantia da publicidade dos atos processuais e o direito à privacidade, a partir do problema da super-exposição e da segurança dos dados num processo em rede.

Partindo-se do método dedutivo de abordagem, buscou-se, dentro dos panoramas da proteção de dados pessoais e da virtualização do processo judicial, deduzir como os institutos analisados se confluem para a devida ponderação entre a publicidade e a privacidade. Deste modo, o presente artigo estruturou-se da seguinte maneira: primeiramente, analisou-se as configurações da proteção de dados pessoais; em seguida, da mesma maneira investigou-se a virtualização do processo judicial para, ao final, examinar como ocorre a proteção de dados pessoais no e-processo.

1 PANORAMA DA PROTEÇÃO DE DADOS PESSOAIS

A proteção de dados[1] pessoais[2] está inserida dentro do âmbito de proteção do direito à privacidade[3], mais especificamente no aspecto da privacidade informacional. Assim, os valores tutelados pela proteção de dados pessoais coincidem com aqueles tutelados pelo direito à privacidade, sendo válido o destaque daqueles mais relevantes e que justificam o enquadramento da ambos os direitos como direitos fundamentais.

Mais do que resguardar a esfera íntima da pessoa, ou a sua vida privada, o direito à privacidade está atrelado à própria noção de liberdade e, em última análise, de democracia (RUARO, 2015). Prova cabal de tal constatação é o fato de que, seja no âmbito literário – como o Grande Irmão do livro "1984", de Orwell –, seja no âmbito histórico-fático – por exemplo, os regimes fascistas de Hitler e Mussolini e o regime socialista de Stalin –, a supressão da privacidade era instrumento essencial de controle e de domínio da população nos regimes totalitaristas.

O fascínio de Foucault pelo panóptico de Bentham não era injustificado. De fato, a estrutura arquitetônica idealizada por Bentham incrementa significativamente o potencial de aplicação de disciplina e de controle ao impor a lógica da vigilância constante (FOUCAULT, 2002). Ainda que de forma menos extremada – quando comparada a sua aplicação a uma instituição prisional – a lógica adotada por Bentham também é válida no que concerne o livre desenvolvimento da personalidade.

O comportamento individual é sensível a influências externas; somente sob o resguardo do olhar alheio é que cada indivíduo adota a sua postura mais autêntica[4], uma vez que livre de

---

[1] Em que pese o reiterado uso indiscriminado dos termos dados e informações, eles não consistem em sinônimos. Dados seriam uma espécie de "pré-informação", ele consiste numa representação, via de regra indefinida. Assim, um dado pode ser uma informação *per si* ou depender de outros dados para ser dotado de um significado e, portanto, tornar-se uma informação. "A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição." (DONEDA, 2011, p. 94).

[2] Dado pessoal consiste em toda e qualquer informação (ou fragmento), independente de seu formato – som, texto, imagem, etc. –, que diga respeito a uma pessoa singular identificada ou identificável. Identificável, por sua vez, diz respeito ao indivíduo que, por meio de algum número de identificação, ou algum elemento inerente à sua identidade – seja físico, psíquico, econômico, social ou cultural –, pode ser identificado direta ou indiretamente, considerando-se o emprego de "meios susceptíveis de serem razoavelmente utilizados para efetuar essa identificação, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa." (Diretiva 95/46/CE).

[3] Adianta-se que, ao se falar em privacidade, compartilha-se do entendimento de Doneda (2006) que julga improdutiva a distinção entre intimidade, vida privada, sigilo e privacidade para fins de verificação do âmbito de tutela desses direitos, vez que, apesar de distintos, todos são esferas de proteção englobadas por uma maior que resolveu se chamar de direito à privacidade, sendo tal discriminação pertinente apenas para fins de quantificação da indenização por eventual violação.

[4] Nesse sentido, Maria Cláudia Cachapuz (2014) questiona até que ponto aquilo que se torna público – ou seja, aquilo que integra o chamado mundo das aparências – reflete, de fato, o que a pessoa extrai de seu espaço de reflexão individual, da sua própria essência, em uma realidade em que há uma tendência à autoexposição, marcada por "confissões públicas" e por uma repaginação do que é público e do que é privado.

julgamentos críticos dos outros. Destarte, percebe-se a necessidade de um âmbito privado – e, portanto, fora da ingerência de terceiros – que possibilite ao indivíduo um autoconhecimento imprescindível para a construção de seu caráter e para o desenvolvimento de sua personalidade[5].

Em suma, o próprio exercício do direito à privacidade se confunde com o exercício do direito à liberdade[6], vez que cabe ao indivíduo decidir o quanto pretende expor a terceiros de sua intimidade e de sua vida privada (VIEIRA, 2007). Porém, não se pode limitar a concepção de privacidade como um direito de ser deixado só (*right to be left alone*), sequer o fizeram Warren e Brandeis (1890) em seu artigo intitulado "Right to privacy" ao consagrar o aludido termo[7].

Tal concepção se limita à dimensão negativa do direito à privacidade, enquanto defesa da esfera privada contra ingerências externas, sendo insuficiente para dar respostas às problemáticas desse direito no atual contexto social. A lógica puramente individualista de tutela de direitos fundamentais deve ser superada num cenário em que apenas uma discussão mais ampla e de cunho coletivo pode compor interesses distintos. Forçoso asseverar que estamos inseridos numa realidade em que grupos econômicos são "[...] capazes de controlar o exercício dos poderes baseados na disponibilização de informação" (RUARO; RODRIGUEZ, 2011, p. 47).

Vivemos na chamada Sociedade da Informação[8], e esta alterou significativamente a estrutura do tecido social, inclusive no que toca à organização do poder. Nessa nova composição social, a infraestrutura informativa passa a figurar como um dos eixos fundamentais na concentração e manutenção do poder (RODOTÀ, 1995, *apud* DONEDA, 2006).

---

[5] "A presumida 'transparência de quem não tem nada a temer', deixa de fazer sentido dada a crescente complexidade das situações que tais arroubos podem desencadear. Uma esfera privada, na qual a pessoa tenha condições de desenvolvimento da própria personalidade, livre de ingerências externas, ganha hoje ainda mais em importância; passa a ser um pressuposto para que ela não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cerceiam sua autonomia privada [...] e, em última análise, inviabilizariam o livre desenvolvimento de sua personalidade." (DONEDA, 2006, p. 142).

[6] Se evidencia a íntima relação entre privacidade e liberdade, a ponto de se afirmar que ambas consistem em "duas faces de uma mesma moeda" (VIEIRA, 2007, p. 27). A privacidade, então, surge como pressuposto indispensável ao exercício do direito à liberdade ao garantir uma autodeterminação livre de ingerências externas indevidas. Por sua vez, o simples exercício do direito à privacidade pressupõe a existência de liberdade, consoante já referido acerca dos regimes totalitários (VIEIRA, 2007).

[7] No aludido artigo intitulado "Right to privacy", os autores trabalharam o chamado *right to be left alone*, enquanto apenas um dos aspectos da privacidade, o qual não esgotaria o âmbito de proteção desse direito (WARREN; BRANDEIS, 1890).

[8] Apesar da existência de outros termos para definir o contexto social atual como sociedade da hiperinformação; sociedade de vigilância; sociedade de rede; e modernidade líquida; utilizaremos a expressão sociedade da informação.

Nunca antes, a assertiva "informação é poder"[9] fora tão evidente. A informação sobre terceiros aparece não só como mecanismo de controle, mas como mecanismo de discriminação. A partir dela, é possível identificar, analisar e classificar os indivíduos com base em critérios preestabelecidos para gestão do risco[10].

Tal alteração parece bastante clara ao se analisar o comportamento jurídico dos anos 1970 em diante, quando o meio jurídico passou a dar maior atenção aos bancos de dados, confrontando o tratamento de informações pessoais com o direito à privacidade[11]. Percebeu-se que esse direito não se resumia a manutenção do sigilo de determinados aspectos da vida de uma pessoa, passando a englobar, também, o direito de se saber quais informações pessoais são coletadas, por quem são utilizadas e se elas estão corretas (DONEDA, 2006).

É a partir dessa preocupação que se constrói o direito à proteção de dados pessoais, como instrumento imprescindível a tutela do direito à privacidade em uma realidade cada vez mais complexa. Com base nesse direito, busca-se dar resposta às novas problemáticas da privacidade oriundas das inovações tecnológicas no âmbito informacional.

1.1 A autodeterminação informativa

A questão central acerca da proteção de dados pessoais recai no chamado direito à autodeterminação informativa. Tal termo, por sua vez, foi consagrado pelo Tribunal Constitucional Federal Alemão no chamado caso da Lei do Censo de 1983 (*Volkszählungsgesetz*), tido, até hoje, como um dos *leading cases* no enfrentamento da temática[12].

---

[9] A partir do conceito weberiano (clássico) de poder e do conceito de Diogo Moreira – "poder é um fenômeno social no qual uma vontade, individual ou coletiva, se manifesta com capacidade de estabelecer uma relação da qual resulta a produção de efeitos desejados, que de outra maneira não ocorreriam espontaneamente" (MOREIRA, 1996, *apud* SILVEIRA, 2000, p. 80) – Henrique da Silveira (2000) percebe que não só informação é poder, mas também é pressuposto, fator multiplicador e meio de mensuração deste.

[10] A partir de análises estatísticas os riscos passam a ser calculáveis, previsíveis e, portanto, passíveis de serem evitados. Tal lógica é largamente aplicada, seja a situações fáticas como a seres humanos, criando-se as chamadas categorias de risco – ou seja, aquelas em que o risco existente não é aceitável. É a partir de tal classificação que se inicia um processo de exclusão e marginalização de indivíduos na sociedade, seja por meio de uma perseguição estatal ou pela própria privação de sua participação na sociedade (MACHADO, 2005).

[11] Consoante se constata, a atenção do poder judiciário sobre a proteção de dados pessoais é anterior ao surgimento do computador e dos meios eletrônicos em si. Não só a defesa da intimidade, mas o próprio direito à proteção de dados pessoais são noções "pré-informática", a automação surge, nesse aspecto, apenas como instrumento potencializador do tratamento de dados pessoais, dando margem a inúmeras aplicações a estes dados (RUARO; RODRIGUEZ, 2010).

[12] A Lei do Censo alemão promulgada em 1982 previa, para 1983, o recenseamento da população alemã, estabelecendo questionários informações profissionais, de moradia, dentre outros aspectos. O texto legal previa, ainda, o cruzamento, a transmissão e a comparação dos dados obtidos com outros bancos de dados públicos, bem como instituía sanções aos que se recusassem a responder o censo (SCHWABE; MARTINS, 2005). O resultado foi temor de um "Estado superinformado", plausível ao se falar em Alemanha pós-nazismo,

A partir do julgado do TCF Alemão, o direito à autodeterminação informativa fora concebido como um direito fundamental, decorrente do direito geral de personalidade, que garante ao titular o poder de decidir quais, com quem e de que forma ele pretende compartilhar suas informações de cunho pessoal. Porém, de grande valia a ressalva feita por Doneda (2006) de que tal controle não importa numa patrimonialização desses dados e dessas informações pessoais.

Tal tratamento configuraria, *per si*, uma violação ao direito à privacidade enquanto um direito de personalidade[13], extrapolando os limites deste direito, do qual se desdobra a autodeterminação informativa. Em se tratando de desdobramento do direito à privacidade, é inadmissível que a autodeterminação informativa pudesse violar tal direito, porquanto estaria ferindo sua própria essência (RUARO, 2015).

Em que pese no Brasil não se tenha reconhecido de forma expressa um direito geral de personalidade – diferentemente do que ocorre na Alemanha –, é inquestionável a existência de um grupo de direitos que se enquadrem na categoria de direitos da personalidade. Ainda, seguindo uma corrente naturalista[14], a existência ou não de positivação desses direitos não afasta a sua aplicação ou existência[15].

Desta feita, independentemente de haver, ou não, uma previsão expressa do direito "à autodeterminação informativa"[16], deve-se reconhecer a sua existência diante da relevância dos valores que tutela[17]. Outrossim, a própria caracterização desse direito demanda não só sua

---

despertando grande insegurança da população alemã frente às imposições da lei (RUARO, 2015). Consequentemente, o caso foi submetido ao apreço do Tribunal Constitucional Federal (TCF) Alemão que, no enfrentamento do mérito, declarou nulo diversos dispositivos da aludida lei, em especial aqueles que versavam sobre o tratamento de dados pessoais – comparação, transmissão e cruzamento de dados. Na ocasião, o TCF "[...] reconheceu o direito do cidadão germânico de negar informações de caráter pessoal, entendendo como uma faculdade individual consentir, ou não, na coleta, no armazenamento e no compartilhamento de dados pessoais." (SCHWABE; MARTINS, 2005, p. 44).

[13] Em se tratando de direito de personalidade, o direito à privacidade e, por consequência, o direito à autodeterminação informativa são dotados das características típicas deste instituto, ou seja, são direitos intransmissíveis, irrenunciáveis e não são passíveis de limitação voluntária (*vide* artigo 11 do Código Civil de 2002).

[14] Segundo essa corrente, os direitos de personalidade são direitos inatos ao ser humano e condição essencial a manutenção da dignidade deste. Assim, tratam-se de direitos naturais do ser humano que independem de reconhecimento pelo Estado, vez que anteriores à própria noção de Estado. A este, caberia, apenas, a regulamentação e defesa de tais direitos como meio de dotá-los de maior efetividade (BITTAR, 2015).

[15] No Brasil, inexiste uma regulação específica acerca da proteção de dados pessoais, havendo apenas leis esparsas que abordam o tema como questão de segundo plano, sendo a construção desse direito no âmbito jurídico nacional praticamente jurisprudencial e doutrinária, ou seja, sem uma base legal.

[16] Segundo o Tribunal Constitucional Federal Alemão, "A autodeterminação é uma condição elementar de funcionamento de uma comunidade democrática fundada sobre capacidade de agir conjuntamente de seus cidadãos. [...] A informação, ainda quando relacionada a pessoa, apresenta uma figuração da realidade social, a qual não pode ser exclusivamente subordinada ao afetado (CACHAPUZ, 2014, p. 828).

[17] Mais do que ao controle das próprias informações, a autodeterminação informativa está atrelada ao próprio ser humano. Ou seja, "expressão 'autodeterminação informacional' significa, mais que o controle do indivíduo sobre as informações e dados produzidos sobre si, uma (necessária, mas insignificante) pré-condição para que

aplicação independente de previsão legal, mas coíbe sua limitação de forma arbitrária. Tal direito só pode ser restringido face a interesse predominante da coletividade, lastreado em base legal de ordem constitucional, ou dela decorrente, sempre em observância ao princípio da proporcionalidade (SCHWABE; MARTINS, 2005).

Não obstante, o interesse da coletividade ou interesse público – que figuram como limitadores típicos de direitos fundamentais individuais – consistem num conceito extremamente vago e, portanto, de difícil mensuração quando não tratado a partir de um caso concreto. Sua compatibilização com o valor de dignidade da pessoa humana e de liberdade, questão central da autodeterminação informativa, demanda, destarte, a existência de parâmetros que norteiem o intérprete. Somente a partir desses é que poder-se-á afirmar com maior propriedade qual desses interesses conflitantes deve preponderar.

Estes parâmetros que norteiam a discussão da autodeterminação informativa se confundem com aqueles que pautam os clássicos conflitos que envolvem os direitos de personalidade, a exemplo do choque entre direito à privacidade e o direito à informação; o direito à honra e o direito à liberdade de expressão, dentre outros. Nesse sentido a relevância da situação para a população; a pessoa a quem se refere o fato – se pessoa pública ou não –; a natureza do fato – de cunho íntimo, particular ou público – são exemplos de parâmetros a serem ponderados quando da análise do caso concreto, porém não esgotam a questão[18].

Em que pese ter espaço de destaque na proteção de dados pessoais, a autodeterminação informativa não esgota a problemática. Questões como a proteção de dados sensíveis e a segurança no tratamento de dados são de sua importância para uma tutela efetiva da proteção de dados e, não obstante, fogem do âmbito da autodeterminação informativa. Nesse sentido, é preciso enfrentar questões próprias desse direito, que abarca tantos aspectos da privacidade, como da informação (DONEDA, 2006).

1.2 Princípios inerentes ao tratamento de dados pessoais

A falta de uma abordagem coesa do direito à proteção de dados pessoais[19], fundada principalmente na falta de legislação específica do tema no direito brasileiro, torna mais enfática

---

ele viva uma existência que pode ser dita como autodeterminada" (ROUVROY; POULLET, 2009, *apud* RUARO, 2015, p. 45-46).

[18] Em que pese a relevância desses parâmetros para o presente trabalho, a identificação desses foge ao objeto ora estudado. Tal questão demanda pesquisa específica em razão de sua complexidade, que, para fins de completude, demanda um fôlego que extrapola os limites deste artigo.

[19] O sistema jurídico pátrio adota uma abordagem complexa desse direito, carecendo de uma estrutura consolidada – por exemplo o CDC (Lei n. 8.078/1990) e o Marco Civil da Internet (Lei n. 12.965/2014) que abordam a

a necessidade de se buscar elementos que deem maior concretude ao mesmo na legislação e na doutrina estrangeira. Prova de tal situação é a adoção quase unânime do modelo europeu de proteção de dados pessoais como parâmetro a ser estudado, adaptado e, então, implementado à realidade brasileira.[20]

No entanto, como bem ensina Humberto Ávila (2015), a norma nasce da interpretação do texto, mas também não advém exclusivamente deste. Disso se depreende que a análise dos institutos do direito há sempre de revelar normas ainda que não oriundas de texto, e que podem ser flexíveis e orientadoras quando da aplicação desses institutos, sendo essas as características, segundo o jurista, dos princípios, pois "[...] instituem o dever de adotar comportamentos necessários à realização de um determinado estado de coisas. [...]." (ÁVILA, 2015, p. 161).

Sendo assim, cumpre traçar breves considerações sobre os principais princípios que norteiam a proteção de dados no Brasil, firmados pela doutrina nacional, notadamente por Danilo Doneda (2006) e Tatiana Vieira (2007), virtualização do processo judicial, sem a pretensão de esgotamento do tema[21]:

O *princípio da publicidade* consiste na obrigatoriedade de se informar o público quanto à existência de um banco de dados e a finalidade do tratamento dos dados pessoais ali constantes. Segundo a Diretiva 95/46/CE, é obrigatória a notificação para autoridade de controle da existência de bancos de dados com informações pessoais, bem como sua existência deve ser de conhecimento público.

Pelo *princípio da exatidão* (ou *veracidade*), os dados armazenados devem ser verdadeiros, ou seja, corresponderem à realidade. Nesse sentido, depreendem-se desse princípio a necessidade de cuidado e correção na coleta e tratamento de dados pessoais, bem como a realização de atualizações periódicas destes dados conforme a necessidade da manutenção desses. É com base neste princípio (e no princípio seguinte) que ganha destaque a figura do *habeas data* no que toca proteção de dados pessoais.

---

matéria em seus respectivos âmbitos de incidência. Nesse sentido, é possível extrair, do ordenamento jurídico brasileiro, apenas disposições esparsas acerca desse direito, enquanto desdobramento dos direitos à vida privada e à intimidade, bem como de alguns dispositivos legais que abordam a questão de forma superficial.

[20] O próprio projeto de lei sobre a proteção de dados pessoais (Projeto de Lei do Senado n. 330/2013) é amplamente inspirado na Diretiva 95/46/CE que aborda a temática da proteção de dados pessoais e deveria ser aprovado em conjunto com o Marco Civil da Internet (que inclusive faz alusão a este projeto), porém até hoje aguarda a apreciação pelo senado.

[21] Em que pese a multiplicidade de leis existentes no âmbito estrangeiro acerca da proteção de dados, inclusive a ponto de se falar em gerações de leis de proteção de dados pessoais, "é possível reagrupar materialmente seus objetivos e linhas de atuação principais em torno de alguns princípios comuns, presentes em diversos graus em ordenamentos vários – no que podemos verificar uma forte manifestação da convergência das soluções legislativas quanto à matéria em diversos países, bem como uma tendência sempre mais marcada rumo à consolidação de certos princípios básicos e sua vinculação sempre mais estreita com a proteção da pessoa e com os direitos fundamentais" (DONEDA, 2011, p. 98).

Pelo *princípio do livre acesso*, o indivíduo tem o direito de acesso aos bancos de dados que contenham informações pessoais suas, inclusive lhe sendo facultado a solicitação de cópias desses registros, a fim de garantir seu controle sobre as suas informações.

Com o *princípio da finalidade*, os dados pessoais só podem ser utilizados para a finalidade a que se destinou a sua coleta, situação que importa na proibição da transferência destes dados para terceiros, bem como garante a possibilidade de aplicação do princípio da proporcionalidade.

O *princípio da proporcionalidade* afasta o tratamento de informações não pertinentes ao fim almejado pela coleta. É por este princípio que se protege o titular dos dados contra coletas abusivas ou excessivas.

O *princípio da segurança no tratamento* visa à adoção de medidas técnicas e administrativas que protejam bancos de dados para que as informações pessoais neles contidas não sejam objeto de acesso não autorizado (*sigilo*), de alteração (*integridade*), e de destruição (*disponibilidade*). Por meio de tal princípio é que se evidencia o caráter de atividade de risco do tratamento de dados pessoais.

O *princípio do consentimento* (*esclarecido*): consiste na concordância prévia do titular dos dados em relação a sua coleta e seu tratamento. Porém, para que este consentimento seja válido é dever do responsável pela coleta e pelo tratamento informar ao titular – de forma que este o compreenda – quais dados serão coletados, para qual finalidade, quem terá acesso a esses dados, como se dará o tratamento e como é a segurança do banco de dados. Tal princípio aproxima-se do direito à autodeterminação informativa.[22]

Por fim, pelo *princípio da proibição de tratamento de dados sensíveis*, há uma regra geral de proibição dos dados sensíveis. Os dados sensíveis são aqueles que dão maior margem a discriminação – por exemplo, orientação sexual ou inclinação religiosa –, ou que digam respeito à uma esfera mais íntima do indivíduo (esfera confidencial) o que dependerá, invariavelmente, do caso concreto. Assim, a proibição do tratamento de dados sensíveis busca coibir o tratamento e coleta desses dados sempre que possível e, quando estas atividades forem imprescindíveis, elas demandam maior rigor na sua proteção.

[22] Em sentido semelhante na eleição e definição dos princípios mais relevantes no tratamento de dados pessoais, DONEDA (2006, 2011) e VIEIRA (2007).

2 PANORAMA DA VIRTUALIZAÇÃO DO PROCESSO JUDICIAL

Como bem explicitado no tópico 1 deste artigo, a sociedade da informação em que se vive é intrínseca e inexoravelmente em rede, significando que todas as esferas da sociedade estão conectadas, notadamente, pela rede mundial de computadores. É de se dizer, portanto, que se vive numa sociedade cujas bases estão sendo fundidas com as TICs de tal modo que suas forças produtivas dependam da rede de comunicação na qual se insere a Internet para a transmissão de informação, inclusive o Poder Público (GILLES, 2008).

É com base nessa premissa que o Poder Judiciário, igualmente, integra-se neste movimento de utilização das TICs com a manutenção de sítios eletrônicos a conter informações e serviços, como, por exemplo, pesquisas de jurisprudência ou consulta a processos, ou de perfis ou páginas em redes sociais para a divulgação de informações e julgados importantes[23] (RIGHI; HOCH, 2015).

No entanto, verifica-se que a maior integração do Poder Judiciário na sociedade da informação é a virtualização do processo judicial[24], pela qual o processo, enquanto ferramenta do exercício da jurisdição, tramita em ambiente eletrônico capaz de proporcionar a feitura e a comunicação dos atos processuais pela Internet, utilizando-se de sistemas de e-processo para tanto (MADALENA; OLIVEIRA, 2008).

A primeira experiência[25] nesse sentido foi em julho de 2003 nos Juizados Especiais Federais (JEFs) do Tribunal Regional Federal da 4ª Região (TRF4) com a implementação do e-Proc para a tramitação eletrônica de seus processos. Dado o aparente sucesso da medida e a possibilidade de se utilizar das TICs para a virtualização dos autos, a Lei n. 11.419/2006 (Lei do e-Processo) foi promulgada com o intuito de se tornar o marco regulatório para a prática de atos processuais em meio eletrônico com a informatização do processo judicial (ATHENIENSE, 2010).

---

[23] A título de exemplo, veja-se o sítio eletrônico do Supremo Tribunal Federal: <http://www.stf.jus.br/>, e a sua respectiva página no Twitter: <https://twitter.com/stf_oficial>, demonstrando como a suprema corte do país mantém-se ativa na Internet.

[24] Ainda que a expressão comumente usada seja "processo eletrônico" ou "processo judicial eletrônico", não se trata de terceira espécie de processo como o são o de conhecimento e o de execução (ALMEIDA FILHO, 2015), razão pela qual opta-se por tratar como "virtualização do processo judicial" ou ainda de "e-processo", pela utilização da partícula "e", do termo inglês "electronic", a denotarem ambas as expressões que o processo se desenvolve em ambiente virtual e utiliza-se das TICs.

[25] Diga-se a primeira experiência em implementação de sistema de tramitação eletrônica para toda a fase de conhecimento do processo, pois já haviam sido editadas outras normas a prever a utilização de meios telemáticos no processo, como a Lei do Fax (Lei n. 9.800/1999) e a Lei da Penhora *Online* (Lei n. 11.382/2006).

Todavia, a utilização das TICs para a materialização do processo não se revela como mera transposição de meio: do físico, em papel, para o digital, em *bits*[26], mas pela aplicação da lógica informacional ao processo, significando que este assume outras nuances que não seriam obtidas com a sua tramitação física, introduzindo um novo pensar sobre o processo enquanto uma rede de informações (CHAVES JÚNIOR, 2010), por ser capaz de alterar a percepção que se tem do conteúdo do processo senão porque depende, para o seu sucesso, de uma mudança de comportamento sobre como a informação contida no processo judicial passa a ser consumida pelos agentes processuais (ABRÃO, 2015).

Em suma, é o mesmo processo judicial regulado pelo ordenamento processual, contudo, seus procedimentos são operados em meio eletrônico hábil a garantir-lhes a eficácia, de tal modo que o e-processo se revela como expoente da modernização do Poder Judiciário por trazer para dentro do processo judicial a lógica da sociedade da informação em que se vive no Século XXI (ABRÃO, 2015). Igualmente, é possível considerar que democratiza a atuação do Poder Judiciário, pois o processo judicial tem o seu acesso disponível *online* na rede mundial de computadores, o meio ambiente virtual para todos (FIORILLO, 2012).

2.1 Atos e-processuais

Para a devida transposição do meio físico para o meio eletrônico de tramitação, aplica-se o *princípio da equivalência instrumental ao papel*, preceito desenvolvido por Augusto Tavares Rosa Marcacini (2013). Nesse sentido, não há porque se falar em novos institutos processuais a serem acrescentados como condições da ação ou pressupostos processuais de existência ou validade, apenas a conformação e adaptação dos já existentes ao meio eletrônico, já que sempre haverá uma equivalência de modo que, quando necessário, recorrer-se-á ao papel, como, por exemplo, a citação ou intimação daqueles que não têm cadastro no sistema eletrônico pela via postal ou outra estipulada em lei (MENDONÇA, 2008).

Outrossim, a comunicação dos atos processuais também é possível pelo meio eletrônico de tal sorte que as partes, seja pessoalmente ou por seus patronos, mediante prévio cadastro, poderão receber em seus endereços eletrônicos notificações de cada andamento processual, bem como das citações e intimações. Ademais, caso exista um Diário da Justiça eletrônico naquele tribunal, preconizado pela Lei do e-Processo, este será alimentado com as publicações dos atos

[26] Unidade de informação, sendo que 8 *bits* (8b) formam 1 *byte* (1B).

nos processos eletrônicos de modo a dar-lhes a devida publicidade que a lei exige, como é possível perceber nos artigos 4º a 7º da referida lei (MENDONÇA, 2008).

Não obstante, a citada lei também prevê a encriptação dos dados para que haja segurança na transmissão e certificação de que aquele ato praticado corresponde ao seu autor, bem como que apenas os envolvidos nos processos em segredo de justiça tenham acesso. Para tanto, é prevista a atuação de Autoridade Certificadora credenciada, ou criação sistema de cadastramento próprio de cada Tribunal, de modo a garantir a pretendida segurança (KRUEL, 2009). A assinatura digital é o mais seguro por usar da criptografia assimétrica[27], método de encriptação e decriptação de mensagem que garante sua autenticidade, além da possibilidade se gerar uma certificação digital, a qual será prestada por uma Autoridade Certificadora a integrar uma Infraestrutura de Chaves Públicas – ICP (FONSECA; BIRCHAL, 2008).

Pelo exposto, mostra-se plenamente cabível a utilização do meio eletrônico para o trâmite de um processo judicial, pois os pressupostos processuais de validade e existência continuam a ser preenchidos em face das tecnologias disponíveis, como a encriptação dos dados, a equivalência instrumental ao papel e a comunicação dos atos de maneira escorreita. Destarte, o que se vislumbra é que os atos virtuais mantêm a identidade com os atos físicos, porquanto conservem a validade e a existência que haveriam de ter (ALMEIDA FILHO, 2015).

Verifica-se, portanto, uma imaterialidade dos autos, cuja intangibilidade não favorece aos acontecimentos eventuais do processo físico, já que este pode ter os autos tocados, manuseados, folheados, rabiscados, dobrados, amassados, rasgados, arrancados, queimados, arremessados, pisados, manchados, além de poderem ser esquecidos em algum arquivo, sendo este último a pior coisa a se acontecer com um processo judicial.

2.2 Princípios inerentes à virtualização do processo

Cumpre, neste momento, remeter-se à lição de Humberto Ávila (2015) já exposta no subtópico 1.2 para, igualmente, demonstrar a construção de princípios a nortearem a virtualização do processo judicial, sendo o principal expoente desta manifestação José Eduardo de Resende Chaves Júnior (2010) a identificar os principais fenômenos inerentes ao e-processo.

[27] A criptografia assimétrica se entende como o uso de duas chaves: uma pública, pela qual é possível tomar conhecimento da transmissão de determinado dado; e uma privada, que dá acesso ao conteúdo do dado transmitido. O dado, por sua vez, é transmitido com duas "fechaduras": quem tem a chave pública abre a fechadura pública para ver a sua transmissão e quem tem a chave privada específica abre a fechadura privada específica para ver o seu conteúdo (SOARES, 2010).

O *princípio da instantaneidade* advém de o e-processo tratar-se de um processo em rede, pois "a instantaneidade é mais viva e interativa que o surrado e ineficiente princípio da celeridade do processo de papel" (CHAVES JÚNIOR, 2010, p. 35), logo torna mais célere o desenvolvimento de um processo judicial, já que há a disposição dos autos e seu trâmite a qualquer tempo a garantir maior agilidade na tramitação dos processos de modo a assegurar maior celeridade (BAIOCCO, 2013).

O *princípio da imaterialidade* "[...] enfatiza a corrente instrumentalista do processo, ao desmaterializar os formalismos a bem de uma adequação social dos direitos materiais" (CHAVES JÚNIOR 2010, p. 26), portanto, traz imensa economia processual pela instrumentalidade das formas[28], de modo que sejam poupados recursos (humanos, financeiros e jurídicos) no desenvolvimento regular de um processo judicial (BAIOCCO, 2013).

O *princípio da interação* deve ser havido como uma releitura do princípio do contraditório, uma vez que este pode se mostrar como um desserviço ao processo em razão da procrastinação processual e da desvirtuação dos fatos que carrega (CHAVES JÚNIOR, 2010). Assim, em sede de processo eletrônico, o contraditório a que as partes se submetem tem contornos de interação entre si e entre eles e o juízo.

Na outra ponta, o *princípio da conexão* aborda precipuamente que o processo eletrônico se encontra na rede e, assim, conectado aos agentes processuais e estes entre si em razão da rede que o e-processo forma. No segundo plano desse princípio, pelo fato de essa rede ser virtual, conecta o processo ao mundo virtual como um todo. O que está na rede e no mundo virtual, está no processo eletrônico (CHAVES JÚNIOR, 2010).

O *princípio da intermidialidade* trata que o processo eletrônico é capaz de ofertar a comunicação dos atos e a produção de provas em vários formatos de mídia eletrônica (imagem, áudio e vídeo), de modo que, por estar em *bytes*, o processo virtual torna o conhecimento do conteúdo da comunicação ou da prova intermídia instantâneo (GILLET; FINCATO, 2015) e aumenta a possibilidade de se aferir uma verdade processual mais próxima da verdade real, além de contribuir para a deformalização do processo (CHAVES JÚNIOR 2010).

Na outra ponta, o *princípio da hiper-realidade* preceitua que a realidade a ser trazida para os autos virtuais transcende o que se documenta em papel, uma vez que é demonstrada através de imagens, sons e vídeos, além de textos (CHAVES JÚNIOR, 2010). Os fatos, então, são hiper-realizados, pois são apresentados como realmente ocorreram no mundo material ao mundo virtual em que o processo eletrônico se desenvolve (GILLET; FINCATO, 2015).

[28] Compreende-se como modelos para aproveitamento dos atos processuais, desprendendo-se da forma quando se alcança o fim sem prejuízo às partes (PORTANOVA, 2013).

Por fim, o *princípio da desterritorialização* aponta que o processo eletrônico, por estar desmaterializado, também está desterritorializado em razão de seu alcance em qualquer lugar onde se possa ter acesso ao sistema. Isto corrobora para a noção consolidada de a jurisdição ser una e ubíqua, desfazendo os limites que a distribuição de competência faz impor com o processo físico e, quiçá, fomentando a cooperação jurídica nacional (CHAVES JÚNIOR, 2010).

Apresentam-se, portanto, princípios idealizadores, cujas observâncias levam em conta todas as possibilidades no uso do meio eletrônico voltado para a prestação jurisdicional, além de mostrar a precariedade de possibilidades do papel, corroborando a ideia de que o processo eletrônico se aproxima de um processo judicial ideal (BAIOCCO, 2013). Os princípios específicos do processo eletrônico por ora elencados decerto demonstram a racionalização e otimização da prestação jurisdicional do Estado.

3 PROTEÇÃO DE DADOS NO e-PROCESSO

Neste ponto da presente pesquisa, o que se pretende realizar é discutir a necessária ponderação entre a tutela do Estado na proteção de dados como concretização do direito à privacidade e a publicidade do processo potencializada com a sua virtualização, vislumbrando-se mais um embate entre os interesses privados e o interesse público.

Assim, para evitar o lugar-comum de o interesse público sempre prevalecer sobre os interesses privados, cumpre debater a natureza, o fim e os limites da consagração do direito fundamental à publicidade do processo estampado nos artigos 5º, inciso LX, e 93, inciso IX, da CRFB, com a sua devida relativização diante do uso de novas tecnologias e da proteção de dados pessoais como garantia ao direito fundamental à privacidade esculpido no artigo 5º, inciso X, da CRFB (PAULA, 2009).

3.1 Natureza e fim do princípio da publicidade no processso

A natureza pública do processo reclama por igual publicidade dos atos processuais, notadamente as decisões judiciais, como consagram os artigos 5º, inciso LX, e 93, inciso IX, da CRFB. Neste sentido, a compreensão do processo como espaço em que o autor demanda a tutela de seu direito; o réu, a sua defesa diante da demanda; e o juiz, na figura do Estado, é o agente que dirá o direito existente e ordenará o seu cumprimento, há de incutir a noção de publicidade necessária para que a sociedade possa conhecer o que e como se decide (PORTANOVA, 2013).

Em complementação a este pensamento, é salutar que o Estado, notadamente o Estado Democrático de Direito, seja transparente na condução da coisa pública, o que perpassa pelo exercício da jurisdição enquanto demonstração tanto de força do Estado como de tutela efetiva de direitos em lesão ou em ameaça lesão (TESHEINER; THAMAY, 2015).

Isto significa dizer, portanto, que o Estado tem o poder de dizer o direito, e que isto repercute no surgimento do direito do jurisdicionado de que este exercício ocorra de modo transparente para que ele possa ter conhecimento e, assim, poder insurgir-se diante de eventual injustiça neste exercício, pelo que a publicidade dos atos processuais, neste contexto, assume o caráter de controle popular da atuação estatal no processo (PORTO; USTÁRROZ, 2009).

A extensão da publicidade dos atos processuais alcança todos os que adquirem esta natureza, ou seja, todos os atos processuais praticados por todos os agentes processuais: partes, juízes, advogados, promotores, defensores, serventuários, peritos etc. Isto demonstra que a publicidade não apenas se conecta ao controle dos atos, mas igualmente ao exercício do contraditório – ainda que diferido em sede de tutela provisória, por exemplo – e, em última análise, ao devido processo legal (TESHEINER; THAMAY, 2015).

3.2 Relativização da publicidade no processo: físico e eletrônico

A publicidade dos atos processuais não é absoluta, havendo várias exceções, notadamente, na CRFB em seus incisos retrocitados e na Lei n. 13.105/2015 (Código de Processo Civil – CPC), em seu artigo 188, a estipular os momentos e as pessoas às quais haverá a restrição ao acesso ao conteúdo dos atos. Deste modo, é possível definir que as partes e seus advogados sempre terão acesso ao conteúdo dos autos, ao passo que terceiros somente terão acesso quando a lei ou o juiz não atribuir segredo de justiça (TESHEINER; THAMAY, 2015).

O segredo de justiça pode ser definido como o instrumento pelo qual o conteúdo dos atos processuais fica restrito somente às partes e seus procuradores em razão da defesa da intimidade ou do interesse social (artigo 5º, inciso LX, da CRFB e artigo 188, incisos I e III, do CPC), ou ainda em ações de família ou que envolva arbitragem (artigo 188, incisos II e IV, do CPC) (PORTANOVA, 2013). Todavia, o segredo de justiça pode ser relativizado caso prejudique o interesse público à informação (artigo 93, inciso IX, *in fine*, da CRFB).

Pelo exposto, a aplicação do segredo de justiça pode ser legal, aplicando-se desde logo às ações de família ou que versem sobre arbitragem com cláusula de confidencialidade, ou judicial, pelo que o juiz decidirá conforme o caso em defesa da intimidade ou pelo interesse social (TESHEINER; THAMAY, 2015), excluindo-se desta categoria os momentos em que a

publicidade não é simultânea para ambas as partes, mas diferida para o devido alcance da efetividade do processo (PORTANOVA, 2013).

Entretanto, a concretização da publicidade ganha nuances diferentes no processo convencional e no e-processo: enquanto que no processo físico é necessário dirigir-se ao foro para ter conhecimento do teor dos autos; no e-processo, está disponível na rede mundial de computadores (CHAVES JUNIOR, 2010). Esta mera facilidade de acesso aos autos eletrônicos, bastando conexão, faz relativizar ainda mais a publicidade do processo, pois é como se estivesse numa vitrine quando em ambiente virtual, ao passo que se encontra inacessível quando numa estante, sendo necessário que um funcionário do foro ache e entregue os autos para consulta (PAULA, 2009).

Com a realidade dos autos eletrônicos, o que se tem nos mais variados sistemas de tramitação eletrônica é a visualização da movimentação processual, com entradas referentes a cada ato processual efetuado sem que, necessariamente, seja mostrado o seu conteúdo. Esta é a visualização padrão para terceiros alheios ao processo, que porventura podem ter acesso ao conteúdo de eventuais pronunciamentos do juiz ou dos serventuários da justiça (ATHENIENSE, 2009). Para as partes e seus procuradores, no entanto, a visualização de seus processos é plena, bem como para os serventuários e o juiz da causa, tendo acesso ao conteúdo de todos os atos, ressalvados os casos em que a publicidade é diferida (PAULA, 2009).

O que se verifica, portanto, é que a publicidade dos atos processuais em ambiente virtual há de depender da posição do indivíduo no processo: (a) se juiz, escrivão ou serventuário ligados diretamente a determinado processo em razão do foro, terão acesso a todo o conteúdo; (b) se parte ou procuradores dentro do próprio processo, terão acesso conforme a postergação da publicidade necessária para a efetividade do processo, mas em algum momento terão acesso pleno a todo o conteúdo; (c) se outro agente processual, como terceiro interventor ou membro do Ministério Público, terão acesso conforme a necessidade de conhecimento do conteúdo dos atos; e (d) se terceiro alheio, terá acesso somente à movimentação processual e conteúdo de pronunciamentos judiciais, ressalvado o segredo de justiça.

3.3 (Im)Pessoalidade e segurança dos dados no e-processo

Tem-se na automação dos mecanismos de tratamento de dados pessoais o principal fator que desencadeou uma discussão acerca da proteção desses dados, em especial quando se fala em meios virtuais (DONEDA, 2006). Nesse sentido, a virtualização do processo judicial evidencia a pertinência de se trabalhar a questão da proteção de dados pessoais nesse âmbito.

Necessário reconhecer que o processo judicial pressupõe o tratamento de dados pessoais, seja na identificação das partes, na produção de provas, ou em outro momento processual. Destarte, cabe verificar quando se está lidando com dados pessoais e de que forma deve se dar a proteção destes.

Para identificação dos dados pessoais, nos valemos do conceito elaborado pelo Tribunal Europeu de Direitos Humanos (TEDH) no sentido de que dados pessoais seriam "[...] qualquer informação relativa a um indivíduo identificado ou identificável [...]", ainda que não digam respeito à vida privada do indivíduo, mas que, de alguma forma, interfiram no desenvolvimento de sua personalidade (RUARO; RODRIGUEZ, 2010). Isto posto, tanto atos puramente processuais[29] como informações atinentes a produtos ou bens[30] não se enquadram nesta definição, sendo passíveis de publicização.

Soma-se a essa problemática, também, a questão da prova emprestada. Quando seu conteúdo é alheio a questão dos dados pessoais, não se verifica maiores empecilhos na operacionalização desse meio de produção de prova, porém a questão toma outros contornos quando o conteúdo dessa prova tiver caráter pessoal.

Sobre este último aspecto, poder-se-ia trabalhar com duas possibilidades. A primeira seria a anonimização[31] dos dados pessoais, ou seja, fazer com que esses dados não sejam relativos a pessoa identificada ou identificável[32]. Tal situação enseja, por sua vez, dois problemas: a verificação de uma anonimização efetiva[33]; e a impossibilidade de se desvincular a pessoa da prova a ser produzida.

Quanto a segunda possibilidade, esta consistiria em se requerer ao titular do dado a autorização da utilização deste para fins de produção de prova. Com isso, o tratamento do dado pessoal atenderia aos princípios especificados no item 1.2 deste artigo, em especial o princípio do consentimento esclarecido e o da finalidade, não implicando em violação ao direito à proteção de dados pessoais.

---

[29] Consoante referido anteriormente, os atos processuais são acessíveis ao público em geral, sendo resguardado, apenas, o conteúdo daqueles que envolvam aspectos referentes às partes que compõem a lide.

[30] Ou seja, questões ligadas a fato do produto ou do serviço, ou relativas a algum bem material.

[31] Um exemplo recorrente de anonimização de dados pessoais no âmbito do judiciário é a inserção apenas das iniciais das partes em vez de seus nomes completos nas decisões judiciais para fins de publicação das mesmas sem a identificação dos envolvidos na lide.

[32] Segundo o Manual da legislação europeia de proteção de dados (2014), a pessoa é identificável quando, a partir da obtenção de informações adicionais ou não, for viável a identificação do titular dos dados sem que para isso seja necessário um esforço desproporcional ou que tal identificação demande uma expertise incomum.

[33] Existem diversas críticas acerca da possibilidade de anonimização de fato dos dados pessoais, vez que existem diversos meios de identificação das pessoas que – ao menos teoricamente – tiveram seus dados anonimizados (TEIXEIRA, 2015).

Outra questão pertinente a essa temática é a segurança no tratamento de dados no âmbito do e-processo, em especial no que toca os dados sensíveis. Consoante já explicitado no tópico 2.1 deste artigo, a utilização de criptografia é um dos meios mais eficazes de garantir a restrição do acesso as informações constantes no processo apenas às pessoas autorizadas. A utilização de cadastros com senhas para acesso do conteúdo serve como primeira barreia imposta ao acesso não autorizado, sendo a criptografia um mecanismo de segurança complementar[34].

No que toca a utilização de dados sensíveis no âmbito do e-processo, entende-se que há uma necessidade de um trâmite processual sob segredo de justiça ou, ao menos, que haja uma anonimização desses dados. Via de regra, há uma presunção de proibição do tratamento de dados pessoais sensíveis, e, sendo tal tratamento imprescindível ao processo, esta demanda uma segurança mais rígida do que aquela atribuída ao tratamento de dados pessoais não sensíveis (DONEDA, 2006). Ou seja, o acesso a esses dados deve ser mais restrito e controle sobre eles deve ser mais rigoroso.

CONSIDERAÇÕES FINAIS

Do exposto, percebe-se a nítida influência que os avanços tecnológicos, em especial no âmbito das TICs, exercem sobre o corpo social e, inclusive, no que toca a atuação e estruturação do próprio Estado. Notadamente, a virtualização do processo surge como resposta a inúmeros problemas típicos do processo físico, não só ao ampliar as possibilidades e recursos na formação do processo – por exemplo, a produção de provas nos mais variados formatos de mídia eletrônica –, bem como ao proporcionar mecanismos mais eficientes e sustentáveis que permitem uma resposta jurisdicional mais célere e, portanto, com mais chances de ser tempestiva.

Não obstante, a exemplo das demais inovações de cunho tecnológico, o e-processo trouxe novas problemáticas a serem enfrentadas pelos juristas: a publicidade dos atos processuais em um processo acessível via internet vislumbra uma super-exposição do mesmo, o que, por sua vez, implica em uma ameaça ao direito fundamental à privacidade em seu aspecto

[34] A criptografia serve para tornar ilegível o conteúdo de uma mensagem quando esta for interceptada ou acessada de alguma forma por pessoa não autorizada. Tal mecanismo codifica a mensagem de forma que apenas a pessoa que possui o código pode decifrar a mensagem e ver seu real conteúdo. Em que pese não um mecanismo que garanta de forma absoluta a proteção do conteúdo da mensagem, apenas hackers muito experientes são capazes de desencriptar uma mensagem sem o código e podem demorar um longo período dependendo da complexidade do sistema criptográfico adotado.

da proteção de dados pessoais. Desta feita, faz-se necessária uma nova releitura da publicidade dos atos processuais contraposta com a proteção de dados pessoais.

Nesse sentido, percebe-se que essa maior exposição do processo eletrônico em relação ao físico faz com que apenas os atos processuais em si – e não seu conteúdo – sejam acessíveis ao público em geral, com exceção de alguns pronunciamentos do juiz ou de serventuários da justiça. Nesta perspectiva, a extensão da publicidade do processo virtual varia consoante a posição do indivíduo frente ao mesmo.

Ademais, é necessário a devida cautela na definição de quais dados são, de fato, dados pessoais, sob pena de se dar proteção mais rígida a informações que não demandam tamanho rigor. Tal situação repercute não só na questão da publicidade no processo, mas em outros casos como o do instituto da prova emprestada, a qual demanda a observância da proteção de dados pessoais quando estes constituírem parte da prova que se pretende utilizar.

Em virtude do mencionado, conclui-se que a construção de um e-processo importa num significativo avanço para fins de prestação jurisdicional. Quanto aos problemas que essa virtualização do processo implica, constata-se que, a partir de uma análise sistemática, é possível solucioná-los com base na ponderação entre direitos que entram em conflito quando contextualizados numa sociedade da informação, marcada pelos avanços no âmbito da informática e das TICs em geral.

REFERÊNCIAS BIBLIOGRÁFICAS

ABRÃO, Carlos Henrique. *Processo eletrônico*: processo digital. 4. ed. rev., atual. e ampl. São Paulo: Atlas, 2015.

ALMEIDA FILHO, José Carlos de Araújo. *Processo judicial eletrônico e teoria geral do processo judicial eletrônico*: a informatização judicial no Brasil. 5. ed. Rio de Janeiro: Forense, 2015.

ATHENIENSE, Alexandre. *Comentários à Lei 11. 419/06 e as práticas processuais por meio eletrônico nos Tribunais brasileiros*. Curitiba: Juruá, 2010.

ÁVILA, Humberto. *Teoria dos princípios*: da definição à aplicação dos princípios jurídicos. 16. ed. São Paulo: Malheiros, 2015.

BAIOCCO, Elton. Princípios processuais: uma visão remodelada a partir das novas tecnologias da informação. *In*: SERBENA, César Antônio (coord.). *e-Justiça e processo eletrônico*: anais do 1º Congresso de e-Justiça da UFPR. Curitiba: Juruá, 2013. p. 171-188.

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

CACHAPUZ, Maria Cláudia Mércio. Privacidade, proteção de dados e autodeterminação informativa. *Revista Jurídica da Presidência*, Brasília, v. 15, n. 107, p. 823-848, out./jan. 2014.

CHAVES JÚNIOR, José Eduardo de Resende. O processo em rede. *In*: _____ (coord.). *Comentários à lei do processo eletrônico*. São Paulo: LTr, 2010. p. 15-38.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

_____. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

FIORILLO, Celso Antônio Pacheco. *Princípios do direito processual ambiental*. 5. ed. rev. e ampl. São Paulo: Saraiva, 2012.

FONSECA, Fernando Daniel de Moura; BIRCHAL, Leonardo de Abreu. Algumas considerações sobre os atos processuais em meio eletrônico: da Lei 9.800/99 à Lei 11.419/2006. *Revista de Processo*, São Paulo, v. 33, n. 166, jan., 2008. p. 131.

FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão. Tradução de Raquel Ramalhete. 26. ed. Petrópolis: Vozes, 2002.

GILLES, Peter. Electronic civil procedure (some remarks to general aspects in concern of civil court proceedings, teletechnology and e-procedural law). *Revista de Processo*, São Paulo, v. 33, n. 158, p. 185-200, abr. 2008.

GILLET, Sérgio Augusto da Costa; FINCATO, Denise Pires. Do papel à tela: conexões entre o direito à produção probatória e a aplicação dos princípios da intermidialidade e da hiper-realidade no processo judicial eletrônico. *In*: FINCATO, Denise Pires (org.). *Novas tecnologias, processo e relações de trabalho*. Porto Alegre: Sapiens, 2015. p. 647-659.

KRUEL, Eduardo. *Processo judicial eletrônico e certificação digital na advocacia*. Brasília: OAB, 2009.

MACHADO, Marta Rodriguez de Assis. *Sociedade do risco e direito penal*: uma avaliação de novas tendências político-criminais. São Paulo: IBCCRIM, 2005.

MADALENA, Pedro; OLIVEIRA, Álvaro Borges de. *Organização e informática no Poder Judiciário*: sentenças programadas em processo virtual. 2. ed. Curitiba: Juruá, 2008.

MANUAL DA LEGISLAÇÃO EUROPEIA SOBRE PROTEÇÃO DE DADOS. Luxemburgo: Serviço das Publicações da União Europeia, 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 27 maio 2016.

MARCACINI, Augusto Tavares Rosa. *Processo e tecnologia*: garantias processuais, efetividade e informatização processual. São Paulo: A. Marcacini, 2013.

MENDONÇA, Henrique Guelber. A informatização do processo judicial sem traumas. *Revista de Processo*, São Paulo, v. 33, n. 166, dez., 2008. p. 122.

PAULA, Wesley Roberto de. *Publicidade no processo judicial eletrônico*: busca da indispensável relativização. São Paulo: LTr, 2009.

PORTANOVA, Rui. *Princípios do processo civil*. 8. ed. Porto Alegre: Livraria do Advogado, 2013.

PORTO, Sérgio Gilberto; USTÁRROZ, Daniel. *Lições de direitos fundamentais no processo civil*: o conteúdo processual da Constituição Federal. Porto Alegre: Livraria do Advogado, 2009.

RIGHI, Lucas Martins; HOCH, Patrícia Adriani Hoch. A utilização de redes sociais pelo poder judiciário: contribuições para uma "esfera pública" virtual?. *In*: SILVA, Rosane Leal da (org.). *O Poder Judiciário na sociedade em rede*: jurisdição, informação e transparência. Curitiba: Multideia, 2015. p. 119-138.

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

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

_____; _____. O direito à proteção de dados pessoais e a privacidade. *Revista da Faculdade de Direito – UFPR*, Curitiba, n. 53, p. 45-66, 2011.

SCHWABE, Jürgen; MARTINS, Leonardo (orgs.). *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Berlim: Konrad-Adenauer-Stifung E.V., 2005. Disponível em: <http://www.kas.de/wf/doc/kas_7738-544-4-30.pdf>. Acesso em: 02 maio 2016.

SILVEIRA, Henrique Flávio Rodrigues da. Um estudo do poder na sociedade da informação. *Ciência da Informação*, Brasília, v. 29, n. 3, p. 79-90, set./dez. 2000.

TEIXEIRA, Lucas. Teoricamente impossível: problemas com a anonimização de dados pessoais. *Oficina Antivigilânica*, [s./l.], 08 maio 2015. Disponível em: <https://antivigilancia.org/pt/2015/05/anonimizacao-dados-pessoais>. Acesso em: 28 maio 2016.

TESHEINER, José Maria Rosa; THAMAY, Rennan Faria Krüger. *Teoria geral do processo*: em conformidade com o novo CPC. Rio de Janeiro: Forense, 2015.

VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sérgio Antônio Fabris, 2007.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, dez. 1890. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 30 abr. 2016.