DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS EM TEMPOS DE PANDEMIA: NECESSÁRIAS EQUAÇÕES ENTRE SEGURANÇA PÚBLICA E PRIVADA

Rogério Gesta Leal

Desembargador do Tribunal de Justiça do Estado do Rio Grande do Sul. Doutor em Direito. Professor Titular da Universidade de Santa Cruz do Sul (Santa Cruz do Sul, RS) e Fundação Escola Superior do Ministério Público (Porto Alegre, RS).

Resumo: O presente estudo tem como escopo analisar a relação entre direito fundamental social à segurança pública e direito fundamental individual à privacidade, com o intuito de responder ao seguinte problema de pesquisa: em que medida estes direitos podem e devem encontrar equilíbrios conjunturais em face do enfrentamento de emergências de saúde pública como esta da pandemia decorrente do corona vírus? A hipótese que vamos sustentar aqui é a de que, por vezes, o direito fundamental social à segurança e à saúde pública vai exigir, legitimamente e de forma controlada, a flexibilização ao direito fundamental individual a privacidade. O método de abordagem do presente trabalho foi o hipotético-dedutivo, partindo-se de reflexões sobre o tema alinhadas pela doutrina especializada. A técnica de pesquisa adotada foi a bibliográfica na elaboração do referencial teórico.

Palavras-chave: Direito fundamental social à segurança e à saúde pública. Direito fundamental individual à privacidade. Pandemia do corona vírus.

I Notas introdutórias

A adoção cada vez maior de medidas emergenciais (legislativas, de políticas e mesmo jurisdicionais) para o enfrentamento de riscos e ameaças ao direito fundamental de intimidade e privacidade, o que envolve o trado de dados privados, em todo o mundo, tem sido realidade inafastável, nomeadamente em face dos espaços virtuais nos quais muitas relações sociais e institucionais têm se dado, o que se agudizou sobremaneira diante dos trágicos à vida humana causados pela pandemia do corona vírus.

RBDFJ_43_MIOLO.indd 357 06/05/2021 14:02:19

Tais cenários, entretanto, reclamam atenção destacada do debate constitucional e infraconstitucional, pois exigem dos sistemas jurídicos que avaliem como lidar com comportamentos fundados, por vezes, na lógica da força e violência institucional legitima (monitoramento estatal de dados e informações privadas) e, ao mesmo tempo, que se mantenham compromissados com as categorias normativas que concretizam as conquistas civilizatórias dos direitos humanos e fundamentais.

Duas consequências diretas destes fenômenos são sentidas em termos de políticas públicas dos Estados de direito em regimes de exceção/emergências como estes impostos pela Covid-19: (i) a ampliação qualitativa e quantitativa de normas e políticas de prevenção contra aqueles riscos e ameaças; (ii) a adoção acelerada de medidas de contenção e gestão das consequências provocadas por situações pandêmicas como estas.

O problema é que mecanismos de gestão de crises imprevisíveis como a do corona vírus, para as quais inexistem protocolos fechados e testados de tratamento e evitação, levam o Estado de direito a desenvolver políticas de enfrentamento muitas vezes invasivas daqueles direitos individuais referidos, como é o caso do chamado sistema de controle inteligente para evitar aglomerações, utilizando o monitoramento indiscriminado de celulares das pessoas.[1]

Tais constatações atingem inúmeros direitos, entre outros, os da privacidade e intimidade das pessoas (físicas e jurídicas), razão pela qual o presente texto pretende abordar, num primeiro momento, como se tem tratado estes direitos fundamentais individuais no campo da doutrina e jurisprudência internacional e nacional, para em seguida cotejá-los com o direito fundamental social à segurança – nomeadamente da saúde pública –, verificando em que medida é possível e necessário equacionar interesses privados e públicos, muito especialmente para os fins de enfrentamento dos riscos e perigos que representam os contágios e suas consequências da Covid-19.

II Privacidades devassadas: riscos e perigos

Os ativistas virtuais – *cypherpunks* – Julian Assange, Jacob Appelbaum, Andy Müller e Jérémie Zimmermann, em obra coletiva de 2012, alertavam para o fato de

[1] Várias cidades brasileiras, através de seus governos, estabeleceram, com operadoras de telefonia móvel (Vivo, Claro, Oi e TIM), convênios de cooperação para receber dados de aglomeração a partir de número determinado de pessoas, o que implica invasão de privacidade induvidosa (Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/04/12/covid-19-iniciativas-usarao-monitoramento-e-geram-preocupacoes.htm. Acesso em: 3 jun. 2020).

RBDFJ_43_MIOLO.indd 358 06/05/2021 14:02:19

que os escândalos de acesso a dados pessoais não autorizados pelas forças de segurança dos Estados Unidos da América, divulgados pelos relatos do *Collateral Muder*, *War Logs* e *Cablegate*, evidenciam, de modo objetivo, a fragilidade dos direitos fundamentais de privacidade e intimidade que nos são assegurados por constituições em todo o Ocidente.[2] Neste texto, os autores deixam muito claro como nossa vida privada quotidiana passou a ser militarizada por sistemas complexos, públicos e privados, de controle de dados e informações, alguns dos quais sequer sabemos que existem.[3] Dizem os autores:

> The NSA warrantless domestic surveillance scandal is the most consequential case of mass surveillance in United States history. The US Foreign Intelligence Surveillance Act 1978 (FISA) made it illegal for US agencies to spy on US citizens without a warrant. After 9/11, the NSA began to engage in mass violations of FISA, authorized by a secret executive order of George W. Bush. The Bush administration claimed executive authority to do this under 2001 emergency legislation passed by Congress: The Authorization for the Use of Military Force (AUMF), and the PATRIOT ACT. The NSA's warrantless domestic spying program – which involved co-operation from private companies, including AT&T –remained secret until 2005, when it was exposed by the New York Times. See "Bush Lets U.S. Spy on Callers Without Courts," New York Times, December 16, 2005: http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all. Reporters for the New York Times had been contacted by an anonymous whistleblower who had leaked the existence of the warrantless surveillance program. In 2004 the then executive editor of the New York Times, Bill Keller, agreed on the request of the Bush administration to withhold the story for a year, until after Bush was reelected.[4]

[2] ASSANGE, Julian; APPELBAUM, Jacob; MÜLLER-MAGUHN, Andy; ZIMMERMANN, Jérémie. *Cypherpunks*: freedom and the future of the internet. New York: OR Books LLC, 2012. Para maiores informações sobre os relatos referidos, ver os *sites*: (i) http://wikiLeaks.org/irq; (ii) http://www.collateralmurder.com; (iii) http://wikiLeaks.org/cablegate.html.

[3] Eles citam os exemplos do caso NSA x AT&T, em que os agentes da National Security Agency coletavam milhões de informações de pessoas físicas e jurídicas que a gigante de telecomunicações AT&T lhes passava sem qualquer ordem judicial; assim como a experiência do modelo EAGLE, sistema que a empresa francesa Amesys vendeu à Líbia para que interceptasse simplesmente todas as comunicações realizadas no país (ASSANGE, Julian; APPELBAUM, Jacob; MÜLLER-MAGUHN, Andy; ZIMMERMANN, Jérémie. *Cypherpunks*: freedom and the future of the internet. New York: OR Books LLC, 2012. p. 54).

[4] ASSANGE, Julian; APPELBAUM, Jacob; MÜLLER-MAGUHN, Andy; ZIMMERMANN, Jérémie. *Cypherpunks*: freedom and the future of the internet. New York: OR Books LLC, 2012. p. 69.

RBDFJ_43_MIOLO.indd 359 06/05/2021 14:02:19

Para aprimorar todo este cenário de violação de direitos, os ataques terroristas do 11.9.2001, nos EUA, e os ocorridos no ambiente europeu (de Madrid e Londres, em 2002; Paris em 2015, e Bruxelas em 2016) provocaram reações instantâneas de ódio e vingança, tanto por parte dos governos como de segmentos massivos da cidadania, fomentados por campanhas midiáticas contra violência, sob o argumento da legítima defesa, abordada a partir de premissas absolutamente instintivas e de baixa racionalidade.[5]

Sem dúvidas que as tradicionais liberdades negativas – incluindo aqui a liberdade pessoal – são os primeiros direitos fundamentais a serem alvos potenciais das ações/reações públicas em nome deste símbolo igualmente fundamental e constitucional que é a segurança, isto porque a exigência de controles e prevenções alcançam as dimensões de tutela das liberdades fundamentais na forma de exercício mais clássica e tradicional, e em sua declinação na modalidade digital, com o emprego dos meios de comunicação virtual.

Lembremos dos incisivos atos de invasão da privacidade que foram adotados nos EUA a partir do conhecido *Patriot Act*, de 2001, associados aos mecanismos que incidiram – e alguns ainda incidem – sobre as liberdades constitucionais mais tradicionais. Da mesma forma o famoso escândalo *Datagete*, provocado por Edward Snowden, e que está relacionado a medidas ditas de segurança oriundas do mesmo gatilho que foi o 11 de setembro, consistindo na revelação da maciça atividade governamental dos EUA na coleta secreta de dados pessoais de cidadãos do mundo todo em nome da segurança nacional e internacional, a partir do acesso de inúmeros servidores de instituições gestoras e operadoras de banco de dados em solo americano (e até mesmo em áreas internacionais, pela via da espionagem).[6]

Ainda nos EUA podemos fazer referência ao chamado *Freedom Act*, aprovado em 2.6.2015, a nova e extremamente liberal lei que disciplina atividades de investigação por parte das autoridades federais, substituindo o *Patriot Act*, de 2001, aprovando ainda novo acordo com a Comunidade Europeia, adotado pela Comissão Europeia de 12.7.2016, substitutivo do *Safe Harbour*, definido como *Privacy Shield*.[7] Este novo ato restaura várias medidas do primeiro, entre as quais

[5] Ver o texto de VERGOTTINI, Giuseppe de. La difficile convivenza fra libertà e sicurezza. La risposta delle democrazie al terrorismo. *Boletín Mexicano de Derecho Comparado*, nueva serie, año XXXVII, n. 111, p. 1185-1211, sept./dic. 2004.

[6] Ver os textos de: (i) RUBINSTEIN, Ira. Big data: the end of privacy or a new beginning? *Public and Legal Theory Research Paper Series*, New York, n. 357, 2012; (ii) SCHWARTZ, Paul M.; SLOVE, Daniel J. The PII problem: privacy and a new concept of personally identifiable information. *New York University Law Review*, New York, v. 86, 2011.

[7] Veja-se a matéria do *New York Times*, dizendo que: "Breaking a long silence about a high-profile National Security Agency program that sifts records of Americans' telephone calls and text messages in search of

RBDFJ_43_MIOLO.indd 360 06/05/2021 14:02:19

as incontroláveis escutas telefônicas itinerantes, dando poder absoluto para as agências de segurança de controlar qualquer tipo de comunicação entre quaisquer pessoas – físicas e jurídicas –, desde que suspeitas de configurarem *risco à segurança nacional*.[8]

Nos últimos anos também os países europeus têm intervindo de modo mais incisivo na privacidade e intimidade das pessoas físicas e jurídicas, e em contextos caracterizados pelos mais elevados níveis de tecnologia e informação que oferecem novos desafios, seja à prevenção e ao controle, seja às limitações que devem ser demarcadas a estes.[9] O exemplo francês é muito paradigmático neste particular, limitando (entre outros direitos fundamentais) a liberdade de domicílio diante de perseguições domiciliares sem autorização judicial prévia no âmbito de atuação do *Estado de Urgência*, instalado em dezembro de 2015, por conta dos atentados *yihadistas* de Paris. Este Estado de Exceção foi prorrogado

terrorists, the Trump administration on Thursday acknowledged for the first time that the system has been indefinitely shut down — but asked Congress to extend its legal basis anyway. In a letter to Congress delivered on Thursday and obtained by The New York Times, the administration urged lawmakers to make permanent the legal authority for the National Security Agency to gain access to logs of Americans' domestic communications, the USA Freedom Act. The law, enacted after the intelligence contractor Edward J. Snowden revealed the existence of the program in 2013, is set to expire in December, but the Trump administration wants it made permanent" (matéria veiculada em 15.8.2019. Disponível em: https://www.nytimes.com/2019/08/15/us/politics/trump-nsa-call-records-program.html. Acesso em: 1º out. 2019. Grifos nossos).

8 Lembremos que muitos membros do Congresso norte-americano acreditavam que, após as divulgações de Snowden, a restauração da confiança do público exigiria mudanças legislativas severas, sendo que mais de 20 projetos de lei foram escritos desde o início das divulgações deste agente, com o objetivo de esclarecer os poderes de vigilância do governo. Naquela época, o congressista Jim Sensenbrenner, um dos grandes responsáveis pela introdução do *Patriot Act*, em 2001, após os ataques terroristas de 11 de setembro, declarou já em 2014 que estava na hora de encerrar o programa de metadados da NSA, eis que a comunidade de inteligência teria usurpado os poderes que lhes foram conferidos, indo muito além da intenção original do Congresso. A despeito disto, o governo Trump desejava reeditar aqueles poderes para as agências de inteligência, como mostra o jornal *Washington Post* (Disponível em: https://www.washingtonpost.com/world/national-security/white-house-has-signaled-it-may-seek-permanent-renewal-of-controversial-surveillance-power/2019/04/30/b4407af2-67a5-11e9-8985-4cf30147bdca_story.html. Acesso em: 1º out. 2019).

9 Ver o interessante texto de LÓPEZ CARBALLO, Daniel. *Responsabilidades derivadas del tratamiento y explotación de los datos personales*. Disponível em: http://dlcarballo.com/2017/01/27/responsabilidades-derivadas-del-tratamiento-y-explotacion-de-los-datos-personales/. Acesso em: 23 jul. 2019. Lembremos, por outro lado, do ocorrido com a empresa Yahoo: "Los problemas de seguridad de Yahoo se agravan. La compañía tecnológica informó anoche en un comunicado difundido tras el cierre de Wall Street de que, en agosto de 2013, sufrió un nuevo asalto informático en el que le fueron robados datos de más de mil millones de usuarios en todo el mundo. El anuncio llega después de que la firma admitiese, en septiembre que, en 2014, registró *otro robo masivo que afectó a 500 millones de cuentas*, en el que ya se consideró el mayor caso de piratería informática de la historia a una empresa, ahora duplicado" Disponível em: https://elpais.com/tecnologia/2016/12/14/actualidad/1481753868_540005.html. Acesso em: 23 jul. 2019).

RBDFJ_43_MIOLO.indd 361 06/05/2021 14:02:19

diversas vezes, com apoio substantivo da Assembleia Nacional, até ser perenizado em lei aprovada pelo governo de Emmanuel Macron em outubro de 2017.[10]

Ou seja, já vivemos rel0ações e hábitos expostos, de alguma maneira, independente de nossa vontade, na medida em que boa parte de nossa vida passa e se dá – direta e indiretamente – por vias digitais, transmitindo dados e informações que não sabemos como são gerenciados; quiçá as ações domésticas mais comuns estão senso observadas por olhos estranhos, como faz referência Vecchi.[11]

Mas não é só o Estado que pode realizar interceptações telefônicas, telemáticas, instalação de sistemas de vigilância individual e ambiental, criando grandes bancos de dados, tudo em nome da segurança pública; também o mercado já faz isto de maneira radical, através, por exemplo, dos sistemas integrados de proteção ao crédito nacional e internacional (SPC, Serasa, Cadin, no Brasil), ou mesmo pela via do consumo global, através das informações coletadas pelos cartões de créditos nacionais e internacionais, os quais, muitas vezes, são utilizados inclusive para fins ilícitos, pois manipulados e vendidos como perfis de consumo para segmentos os mais diversos da economia.[12]

O *site* de tecnologia britânico The Register revelou a existência de novo pacote de dados virtuais vazados que já está sendo comercializado no submundo da internet. Os *sites* envolvidos são Dubsmash (162 milhões de contas), MyFitnessPal (151 milhões), MyHeritage (92 milhões), ShareThis (41 milhões), HauteLook (28 milhões), Animoto (25 milhões), EyeEm (22 milhões), 8fit (20

[10] Ver a excelente entrevista de Patrice Spinosi, advogado francês da Liga dos Direitos do Homem, intitulada *Etat d'urgence: Quel paradoxe pour la démocratie!*, publicada no *Le Parisien* (Disponível em: http://www.leparisien.fr/quel-paradoxe-pour-la-democratie-30-01-2016-5498313.php. Acesso em: 23 jul. 2019). Diz o autor: « L'état d'urgence renforce considérablement les pouvoirs de la police administrative en termes de perquisitions, d'assignations à résidence et d'interdictions de manifester. Ce qui est inquiétant c'est l'absence de tout contrôle judiciaire, seul garant des libertés dans une démocratie ».

[11] VECCHI, Benedetto. *La Democrazia blindata dei Big Data*. Disponível em: http://www.euronomade.info/?p=12085. Acesso em: 23 jul. 2019. Ver também o texto de BRENNER, Susan W. Cybercrime, cyberterrorism and cyberwarfare. *Revue Internationale de Droit Penal*, v. 77, p. 453-471, 2006/3. Disponível em: https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm. Acesso em: 6 ago. 2019.

[12] O Facebook dispõe dos dados que o usuário deposita voluntariamente nele, mas também faz inferências com base nas interações com pessoas e informações que transitam por lá, compartilha-as com terceiros e desenvolve perfis exclusivos que permitem determinar o que aparece no mural identitário de cada usuário, tanto por parte dos amigos como de anunciantes virtuais. Assim, todo "curtir" ou registro feito por meio do Facebook gera informações que são analisadas e classificadas por algoritmos, tanto para conhecer particularidades individuais dos usuários como de consumidores, desenvolvendo modelos sociais para agências de publicidade, o que gera milhões de dólares à empresa. O registro continua mesmo que tenhamos fechado a página; a não ser que saiamos manualmente, os *cookies* do Facebook continuam espionando tudo o que fazemos *online* (Disponível em: https://brasil.elpais.com/brasil/2015/06/12/tecnologia/1434103095_932305.html. Acesso em: 30 jul. 2019). Ver o texto de CASTRO, Catarina Sarmento e. *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina, 2005.

RBDFJ_43_MIOLO.indd 362 06/05/2021 14:02:19

milhões), Whitepages (18 milhões), Fotolog (16 milhões), 500px (15 milhões), Armor Games (11 milhões), BookMate (8 milhões), CoffeeMeetsBagel (6 milhões), Artsy (1 milhões) e DataCamp (700 mil). Os dados foram ofertados no Dream Market, um mercado negro acessível somente pela rede anônima Tor. O pagamento devia ser feito em *bitcoin*.[13]

Ou seja, a privacidade e sigilo de dados pessoais (de pessoas físicas e jurídicas) está em permanente risco que, por vezes, sequer é provocado, mas decorrência dos cenários que apontamos até aqui. Um destes cenários é o que envolve a promoção de políticas de segurança pública fundadas em razões de Estado, ou seja, embasadas no atendimento de demandas sociais indisponíveis cuja responsabilidade originária é das instituições estatais.

Agora, a Covid-19 tem imposto por todo o globo terrestre restrições de mobilidade humana – direito fundamental de ir e vir – para evitarmos os contágios que tanto ameaçam as vidas das pessoas, e isto com velocidades de ação/reação nunca antes vistas, fazendo com que os Estados tenham que criar protocolos, rotinas e políticas de distanciamento ora radicais, ora controlados; ora verticais, ora horizontais, e, para tanto, estão se valendo de decisões normativas e executivas igualmente emergenciais, as quais, em algumas oportunidades, de exceção, como o monitoramento de dados e informações de saúde, de trânsito, de atividades laborais e localização de indivíduos, medidas que podem colidir com direitos fundamentais individuais muito caros.

III Segurança pública e direito fundamental à proteção de dados: sinergias necessárias em face da pandemia provocada pela Covid-19

Como lembra Alessandro Torre, a doutrina constitucional tem se ocupado desde há muito sobre definições de segurança e seus fundamentos políticos, sociais e institucionais.[14] Sem a pretensão de esgotar esta matéria, não é comum que em âmbito constitucional a ordem pública esteja associada a possível limite aos direitos de liberdades individuais, razão pela qual alguns doutrinadores

[13] Ver o *site* https://www.theregister.co.uk. Para a notícia referida, especialmente, a matéria publicada no *link*: https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/. Acesso em: 30 set. 2017, e nesta data há a notícia sugestiva de que: "It's official: Deploying Facebook's 'Like' button on your website makes you a joint data slurper".

[14] TORRE, Alessandro (A cura di). *Costituzioni e sicurezza dello Stato*. Rimini: Maggioli Editore, 2014. Ver nosso LEAL, Rogerio Gesta. *Déficits democráticos na sociedade de riscos e (des)caminhos dos protagonismos institucionais no Brasil*. São Paulo: Tirant lo Blanch, 2020.

RBDFJ_43_MIOLO.indd 363 06/05/2021 14:02:19

sustentam que seria mais adequado considerar a segurança como interesse coletivo do que direito fundamental – do que discordamos.[15]

É certo que a expressão *segurança*, em si, pode assumir diversas declinações sem qualquer natureza jurídica necessária, eis que podemos falar de *segurança externa*, ou de *segurança interna*, dependendo da referência que fazemos a determinado tipo de ameaça social; podemos opor a segurança individual à coletiva; ainda é possível avaliarmos a segurança material e a segurança ideal, tomada a primeira como tutela da incolumidade de determinados bens e pessoas, e a segunda como necessidade de preservar certos princípios e valores fundamentais de ordenamentos aí sim jurídicos.

Com relação aos fundamentos constitucionais da segurança, é possível fazermos referência àquelas duas perspectivas já referidas, de um lado, a que lhe outorga a condição de interesse coletivo, e, de outro, a que lhe reconhece a condição de direito fundamental individual. Estas posições, todavia, não são irreconciliáveis, e devem estar associadas, e isto porque as dimensões individuais e coletivas/sociais das relações humanas, hoje e cada vez mais, contam com intersecções integracionistas, basta vermos o que ocorre nas chamadas redes sociais (Facebook, Instagram, WhatsApp, YouTube, Twitter, LinkedIn, Pinterest, Google+); tudo e todos estão interligados.

Em face disto, temos que se impõem o reconhecimento de ter a segurança significado hodierno muito amplo, estendendo-se de modo intenso à proteção de bens jurídicos (constitucionais e infraconstitucionais, públicos e privados, de pessoas físicas e jurídicas) individuais, coletivos e difusos os mais diversos. Em tal perspectiva, a segurança reclama, ao mesmo tempo, função repressiva e promocional, pois exaltada como condição de possibilidade de fruição de direitos e garantias; mais, como forma de remoção dos obstáculos que se colocam no caminho do efetivo gozo de direitos, devendo-se falar, por conta disto, da segurança de direitos mais do que direito à segurança.[16]

Vai nesta direção Cerrina Feroni, ao sustentar a segurança como direito fundamental constitucional, eis que "un valore superprimario, un bene inscindibilmente legato alla vita, alla incolumità fisica, al benessere dell'uomo e alla qualità della sua esistenza, nonché alla dignità della persona".[17] A partir daqui, não estamos mais

[15] Ver a excelente coletânea coordenada por COCCO, Giovanni (A cura di). *I diversi volti della sicurezza* – Atti del convegno. Collana Università degli studi di Milano, 4 giugno 2009. Milano: Giuffrè, 2012.

[16] Ver no ponto o texto de TORRE, Alessandro (A cura di). *Costituzioni e sicurezza dello Stato*. Rimini: Maggioli Editore, 2014. p. 551, para quem: "*sicurezza pubblica e ordine pubblico* costituiscono non già concetti diversi tra loro ma i due lati della stessa medaglia, il primo soggettivo, il secondo oggettivo" (grifos nossos).

[17] FERONI, Cerrina. La sicurezza: un valore superprimario. *Percorsi constituzionali: quadrimestrale di diritti e libertà*, Roma, 2008. p. 22. Ver também o texto de BUTTARELLI, Giovanni. *Banche dati e tutela della riservatezza*: la privacy nella società dell'informazione. Milano: Giuffrè, 2007.

RBDFJ_43_MIOLO.indd 364 06/05/2021 14:02:19

falando de segurança tão somente como objeto de serviço público estatal à garantia da paz social (em algumas circunstâncias privada também), pois nos encontramos diante de um direito à existência digna protegida, indispensável à fruição dos demais direitos de que o indivíduo – e mesmo a coletividade – são titulares.

Estes elementos a que estamos nos referindo podem ser facilmente vislumbrados tanto nas constituições democráticas atuais como em políticas públicas de Estados democráticos, todos comprometidos com a equalização dos interesses individuais e coletivos/sociais, potencializando cenários de desenvolvimento e efetivação de direitos e garantias sem exclusão. Aqui não há a substituição de prerrogativas individuais, mas suas potencializações a fim de que possam ser fruídas de maneira integrada com a comunidade em que são exercidas, sob pena de criarmos tensões e conflitos insuperáveis – nomeadamente em conjunturas de riscos e perigos os quais já nos referimos.

Empregando definição de segurança de caráter restritivo, ou seja, limitada ao seu tradicional perfil preventivo e repressivo e, portanto, tomada no sentido de garantia da ordem pública, e dentro desta, a da saúde pública (para os efeitos de nossa reflexão), é possível concordarmos com o fato de que ela não se caracteriza tão somente assim, mas se coloca com o escopo que pode justificar meios restritivos de liberdade, configurando, pois, razões de limite de direitos reconhecidos pelo sistema normativo. Neste sentido, parece-nos mais adequado referirmo-nos ao tema da definição da relação entre segurança e direitos fundamentais em termos de ponderação e equilíbrio dos seus limites para perseguirmos os escopos postos.

Por outro lado, o direito à privacidade vem sendo cada vez mais ampliado na doutrina jurídica internacional, justamente em face do excesso de exposição que as relações sociais contemporâneas possuem com as novas tecnologias de comunicação e a realidade virtual.[18] Neste aspecto, toma relevo a tutela das liberdades pessoais conectadas à inviolabilidade de domicílio, dos dados pessoais, de saúde, de trabalho, de mobilidade, fiscais, financeiros, o segredo das comunicações, entre outros.[19]

[18] Ver o texto de CASTILLO JIMENEZ, Cinta. Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información. *Revista Derecho y Conocimiento*, v. 1, p. 35-48. ISSN 1578-8202. Disponível em: https://core.ac.uk/download/pdf/60634513.pdf. Acesso em: 20 ago. 2019. Na mesma direção ver o texto de PIZZETTI, Franco. *Privacy e il diritto europeo alla protezione dei dati personali*. Il Regolamento europeo 2016/679. Torino: Giappichelli, 2016. v. 2, quando refere na p. 32: "l'interesse alla riservatezza rappresenta infatti una vera e propria condizione necessaria perché la persona sia libera di svilupparsi autonomamente, il che non potrebbe avvenire se tutti gli aspetti della sua vita potessero essere noti al pubblico".

[19] Basta vermos as contribuições neste particular das principais cartas de direitos internacionais, como: (i) a Declaração Universal dos Direitos do Homem, de 1948, em seu art. 12; (ii) a Convenção Europeia dos Direitos do Homem, de 1950, em seu art. 8º; (iii) a Convenção nº 108, sobre proteção das pessoas no que tange ao tratamento automatizado de dados e caracteres pessoais, adotada pelo Conselho da Europa

RBDFJ_43_MIOLO.indd 365 06/05/2021 14:02:19

Nos dias atuais, os aspectos da tutela da privacidade e intimidade encontram-se muito integrados com a proteção de dados pessoais, pelo fato de que tais dados representam pressupostos irrenunciáveis ao desenvolvimento da pessoa humana e, ao mesmo tempo, estão conectados com demandas de mercado, pois alimentam infindáveis segmentos de atividades industriais e comerciais que pagam valores imensos por informações de seus consumidores, formatando-se, neste âmbito, zonas de potenciais conflitos entre interesses distintos.[20]

Em tais cenários, as mutações ocorrem inclusive sobre os objetos de tutela jurídica envolvendo o direito à privacidade e intimidade, pois, da tradicional liberdade negativa (livre de ingerência externa), passa a ser integrado como bem tutelado o direito de autodeterminação informativa relacionada ao indivíduo e sujeito de direito. Ou seja, passa-se a reconhecer a todo o cidadão a faculdade de escolher o que deseja fazer com os seus dados pessoais – e o que não deseja também.[21]

Esta expansão do conteúdo do direito à privacidade tem se dado, também, através do diálogo constante entre juízes e legisladores, evidenciando as repercussões de tutelas ampliadas e de multiníveis, como evidencia, provocada pelos atos de terrorismo e em sede internacional, a Diretiva 2016/681, da União Europeia, no tocante à aquisição e conservação do chamado *Passenger Name Record – PNR*, que consiste na formatação de enorme data-base que armazena dados de todos os indivíduos que usam voos no âmbito do território europeu. Tais dados referem-se aos itinerários da viagem, informações sobre os bilhetes de passagens, contatos fornecidos pelo viajante, bem como a modalidade de aquisição e pagamento da viagem e informações sobre sua bagagem.[22]

em 1981; (iv) a Carta dos Direitos Fundamentais da União Europeia, de 2000, em seus arts. 7 e 8; (v) o Tratado de Lisboa, em seu art. 16, de 2007; (vi) a Regulação Geral de Proteção de Dados (conhecida como GDPR – General Data Protection Regulation), que é a nova lei europeia de proteção de informações digitais, de 2018.

20 Ver o texto de SOLOVE, Daniel J. *The digital person*: technology and privacy in the information age. New York: New York University Press, 2004. No Brasil ver a coletânea de MARTINS, Guilherme Magalhães (Coord.). *Direito privado e internet*. São Paulo: Atlas, 2014.

21 Como nos lembra FERONI, Cerrina. La sicurezza: un valore superprimario. *Percorsi constituzionali: quadrimestrale di diritti e libertà*, Roma, 2008. p. 41: "Questo concetto di autodeterminazione informativa viene a trovare una sua dimensione concreta attraverso l'istituto del consenso al trattamento dei dati, come peraltro sancito anche dall'art.8 della Carta di Nizza. Il consenso potrebbe dunque costituire il presupposto principale per la tutela dei diritti, divenendo l'elemento centrale nella garanzia per l'effettività del diritto fondamentale". Ver também o texto de PIZZETTI, Franco. *Privacy e il diritto europeo alla protezione dei dati personali*. Il Regolamento europeo 2016/679. Torino: Giappichelli, 2016. v. 2.

22 Ver a matéria interessante publicada no *site* https://ec.europa.eu/home-affairs/news/security-union-new-rules-eu-passenger-name-record-data_en, com o título: *Security Union: New rules on EU Passenger Name Record data*, contextualizando bem o alcance e escopo desta iniciativa, referindo que: "The new rules strictly limit the use of PNR data for the purpose of prevention, detection, investigation and prosecution of serious crime and terrorism. Under those rules, each participating Member State is required to set up a

RBDFJ_43_MIOLO.indd 366 06/05/2021 14:02:19

Neste sentido, ao Corte de Justiça da União Europeia – UE emitiu pronunciamentos de impactos relevantes no que tange a políticas de segurança pública dos Estados-Membros, entre as quais se revela paradigmática a sentença no caso Google (Google Spain SL; Google Inc.) x Espanha (Agencia Espanhola de Proteção de Dados e Mario Costeja González), de 2014, eis que restou afirmada a importância de proteção de dados pessoais enquanto direito fundamental como premissa da ordem constitucional contemporânea, podendo sofrer aberturas diante de demandas de ordem pública previamente demarcadas por autoridades competentes e nos termos da lei permissiva.[23]

Em termos de Brasil e no momento em que escrevemos este texto (5.6.2020), o jornal *Folha de S.Paulo* anuncia que 1.473 mortes pela Covid-19 foram registradas no país, superando 34.000 mortes, isto 100 dias após ter sido diagnosticada pela primeira vez em nosso território, fazendo ir a óbito mais de um brasileiro a cada minuto.[24] Sem dúvidas que isto evidencia quadros de tragédias públicas insofismáveis, cujas causas não se resumem à pandemia em si, mas estão associados a problemas de gravidade similar envolvendo a inexistência de infraestrutura de saúde pública, logística, recursos humanos, orçamentários e de inteligência institucional adequada para lidar com tamanho desafio.

Por certo que não poderíamos exigir as providências das condições ideais necessárias para tal enfrentamento como algo ordinário, eis que a situação criada em velocidade sem precedentes é de exceção; mas o fato é que o Estado nacional como um todo está, de algum modo, colapsado diante das emergências que têm se apresentado, muitas delas relacionadas com perdas literais de vidas humanas.

Seria razoável o argumento de que, em tais contextos de urgências, medidas de evitação, contenção e cuidados reclamam políticas e ações de igual estatura e agilidade, sem estarem divorciadas totalmente do sistema normativo regedor destas matérias?

Entendemos que sim, em especial no que diz com a questão do acesso pelo poder público a dados e informações da vida privada das pessoas para os fins de criar políticas de enfrentamento da pandemia, basta atentarmos para os

legal and technical framework for the transfer, processing and exchange of PNR data provided by airlines". Mas perguntamos: quem controla o uso destes dados?

[23] Ver a decisão no sítio https://www.osservatoriosullefonti.it/archivio-rubriche-2014/fonti-dellunione-europea-e-internazionali/986-ue-corte-di-giustizia-causa-c-13112-google-spain. Acesso em: 10 set. 2019. Na mesma direção ver importante decisão dessa Corte na sentença da Grande Sessão de 8.4.2014, envolvendo a Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e a. (C-594/12).

[24] Conforme *site* https://www1.folha.uol.com.br/equilibrioesaude/2020/06/coronavirus-mata-mais-de-uma-pessoa-por-minuto-no-brasil.shtml. Acesso em: 5 jun. 2020. Temos até o dia de hoje o registro de 614.941 casos de contaminação pelo Ministério da Saúde.

RBDFJ_43_MIOLO.indd 367 06/05/2021 14:02:19

termos da Lei nº 13.709/2018, que visa proteger os direitos fundamentais de liberdade e de privacidade, e que avança nos níveis de proteção destes bens, atribuindo várias responsabilidades aos gestores e usuários de dados que dão maior segurança às pessoas físicas e jurídicas no país.

Ao mesmo tempo, em seu art. 4º, inc. III, a norma autorizou a flexibilização daqueles direitos para os fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais, sendo que o tratamento de dados pessoais previsto neste inc. III será regido por legislação específica, "que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei".[25] Por certo que aqui já temos outros desafios que é o de densificar materialmente – e no caso concreto – os níveis e possibilidades das *medidas proporcionais e estritamente necessárias* ao escopo da norma e diante de cenários os mais particulares existentes – como o da segurança da saúde pública na pandemia.

E isto se torna necessário quando vemos que, na China, ponto inicial da pandemia provocada pelo corona vírus, foram e são utilizados, até agora, *drones*, tecnologia de reconhecimento facial, *scanners* infravermelhos, além da implementação de aplicativo para classificar as pessoas de acordo com o risco de contágio, sendo tal informação transmitida às autoridades competentes. A Coreia do Sul, por sua vez, tem rastreado os celulares dos usuários para criar mapas que ficam disponíveis publicamente para que todos os cidadãos possam consultar por onde passaram as pessoas infectadas.[26] Diversas outras medidas de monitoramento, em maior ou menor grau das acima narradas, já foram adotadas também no Irã, Israel, Taiwan, Áustria, Polônia, Bélgica, Alemanha e Itália.[27]

No Brasil já estamos usando a tecnologia de utilizar dados de celulares para identificar aglomerações, em várias cidades, como nos faz saber matéria

[25] Art. 4º, §1º.

[26] Para além disto, a Coreia do Sul usa imagens de câmeras de vigilância, dados de geolocalização individualizados e até compras de cartão para identificar o trajeto das pessoas infectadas e quebrar a cadeia de contágio. Ver a excelente matéria no *site*: https://epoca.globo.com/mundo/as-licoes-da-coreia-do-sul-no-combate-ao-coronavirus-1-24315715. Acesso em: 10 jun. 2020.

[27] Conforme o texto de MOURA, Raíssa; FERRAZ, Lara. *Meios de controle à pandemia da Covid-19 e a inviolabilidade da privacidade*. Disponível em: https://content.inloco.com.br. Acesso em: 8 jun. 2020. O governo chinês adotou uma série de ferramentas, com base em GPS, antenas de celular, aplicativos e QR Code, entre outros, para identificar a localização de alguém infectado dias antes da confirmação do diagnóstico, contatar e por vezes isolar quem estava no mesmo vagão de metrô, e não no veículo inteiro, por exemplo. A medida serve também para proibir pessoas de entrarem em prédios ou transportes públicos ou identificar se alguém em quarentena desrespeitou a medida de isolamento imposta. Ver notícia completa no *site*: https://www.bbc.com/portuguese/brasil-52154128. Acesso em: 3 jun. 2020.

RBDFJ_43_MIOLO.indd 368 06/05/2021 14:02:19

do *G1*, tudo funcionando através da triangulação das antenas de celular, o que inevitavelmente invade a privacidade das pessoas usuárias destes aparelhos.[28]

IV Notas conclusivas

Segurança e privacidade são temas que se confrontam desde há muito, ganhando tensionalidades novas nestes tempos de realidades, comunicações e exposições virtuais exageradas. Diante do advento de inéditas modalidades de riscos e perigos – como este da pandemia do corona vírus –, a privacidade e a intimidade, enquanto direitos fundamentais individuais, reclamam adequação conformativa em face de outros direitos fundamentais sociais, como a saúde pública, fazendo com que se potencializem instrumentos de prevenção e controle de interesses indisponíveis da comunidade por parte de autoridades públicas competentes.[29]

No particular, o direito à privacidade e intimidade continua sendo fundamental à pessoa humana, sempre, todavia, temos que, em determinadas situações autorizadas por lei e de emergência imprevisível, como o caso da periclitação da saúde pública a que estamos submetidos, podemos ter autorizações controladas de acesso, por autoridades competentes, a dados e informações pessoais para fins específicos, durante prazo certo e determinado.

Qualquer interferência, física ou virtual, nos espaços privados da vida humana, constituem invasão a direito fundamental; esta premissa é inafastável, notadamente quando revelam a outrem informações sobre localização, conduta, opiniões e sentimentos, em tese, indevassáveis. Todavia, como vimos, há determinadas situações/condições normativas e fáticas que autorizam o Estado – e somente ele – a realizar ou permitir aquela invasão, nomeadamente para tutelar determinados valores e bens jurídicos indisponíveis, como a saúde pública ameaçada pela Covid-19.

E aqui está a natureza também política deste problema, pois a linha demarcatória entre liberdade dos cidadãos e a possibilidade de sua defraudação legítima em face do exercício autorizado da força coativa do Estado deve ser

[28] Conforme *site*: https://g1.globo.com/jornal-nacional/noticia/2020/04/08/governo-de-sp-usa-dados-de-celulares-para-localizar-aglomeracoes.ghtml. Acesso em: 10 jun. 2020.

[29] Esta a posição de FERONI, Cerrina. La sicurezza: un valore superprimario. *Percorsi constituzionali: quadrimestrale di diritti e libertà*, Roma, 2008. p. 31, com quem concordamos: "Diritto alla privacy e interesse collettivo alla sicurezza pari non sono dal punto di vista della dimensione costituzionale, e allora è necessario commisurare il loro rapporto in termini di ragionevolezza e proporzionalità, essendo il limite al diritto certamente giustificato in ossequio ad un interesse collettivo, ma senza che esso si possa mai estendere oltre la compressione del nucleo essenziale del diritto".

RBDFJ_43_MIOLO.indd 369 06/05/2021 14:02:19

constituída por instrumentos legítimos, em regra,[30] pelo Parlamento (lócus privilegiado do debate público inclusivo), como órgão representativo da soberania popular nas democracias representativas.

Por certo que o abuso ou insuficiência das políticas aqui sempre estarão sob o crivo de aferição dos controles internos e externos da Administração Pública, entre eles o jurisdicional, mas como guardiães do cumprimento das regras da democracia, e não protagonistas neurais com superpoderes.

Abstract: The present study will look for to analyze the relationship between Fundamental Social Law to Public Security and Individual Fundamental Law to Privacy, in order to answer the following research problem: To what extent these Rights can and should find cyclical equilibrium in the face of coping with public health emergencies like this of the pandemic due to the corona virus? The hypothesis that we are going to maintain here is that, sometimes, the Fundamental Social Right to Security and Public Health will demand, legitimately and in a controlled way, the flexibility to the Individual Fundamental Right to Privacy. The method of approach of the present work was the hypothetical-deductive, starting from reflections on the theme aligned with the specialized doctrine. The research technique adopted was the bibliography in the elaboration of the theoretical framework.

Keywords: Fundamental social right to security and public health. Individual fundamental right to privacy. Corona virus pandemic.

Referências

ASSANGE, Julian; APPELBAUM, Jacob; MÜLLER-MAGUHN, Andy; ZIMMERMANN, Jérémie. *Cypherpunks*: freedom and the future of the internet. New York: OR Books LLC, 2012.

BALDASSARRE, Antonio. *Privacy e costituzione*: l'esperienza statunitense. Roma: Bulzoni, 1974.

BALDUCCI, Paola. *Le garanzie nelle intercettazioni tra Costituzione e Legge ordinária*. Milano: Giuffrè, 2002.

BRENNER, Susan W. Cybercrime, cyberterrorism and cyberwarfare. *Revue Internationale de Droit Penal*, v. 77, p. 453-471, 2006/3. Disponível em: https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm. Acesso em: 6 ago. 2019.

[30] Admitamos aqui, nomeadamente em estados de emergência como os que exsurgem da pandemia provocada pelo corona vírus, que mecanismos mais ágeis e eficientes de decisão de políticas públicas adequadas para o enfrentamento desta tragédia humana possam ser eleitos, como medidas provisórias e decretos-leis, desde que submetidos igualmente ao devido processo legal.

RBDFJ_43_MIOLO.indd 370 06/05/2021 14:02:19

BRICOLA, Franco. Prospettive e limiti della tutela penale della riservatezza. *Rivista Internazionale de Diritto e Processo Penale*, v. 43, 1967.

BUTTARELLI, Giovanni. *Banche dati e tutela della riservatezza*: la privacy nella società dell'informazione. Milano: Giuffrè, 2007.

CALIFANO, Licia. *Privacy*: affermazione e pratica di un diritto fondamentale. Collana Crispel. Napoli: Editoriale Scientifica, 2016.

CAMON, Alberto. *Le intercettazioni del processo penale*. Bologna: Giuffrè, 1996.

CAPONE, Arturo. Intercettazioni e costituzione – Problemi vecchi e nuovi. *Rivista Cassazione Penale*, Roma, n. 3, marzo 2017.

CASTILLO JIMENEZ, Cinta. Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información. *Revista Derecho y Conocimiento*, v. 1, p. 35-48. ISSN 1578-8202. Disponível em: https://core.ac.uk/download/pdf/60634513.pdf. Acesso em: 20 ago. 2019.

CASTRO, Catarina Sarmento e. *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina, 2005.

COCCO, Giovanni (A cura di). *I diversi volti della sicurezza* – Atti del convegno. Collana Università degli studi di Milano, 4 giugno 2009. Milano: Giuffrè, 2012.

COSA, Roberto. Il caso Datagate e la realtà italiana. *Rivista Sicurezza e Giustizia*. Disponível em: https://www.sicurezzaegiustizia.com/wp-content/uploads/2013/10/SeG_III_MMXIII_TRE.pdf. Acesso em: 3 set. 2019.

Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62014CJ0362&from=EN. Acesso em: 24 set. 2019.

Disponível em: http://wikiLeaks.org/cablegate.html. Acesso em: 27 fev. 2020.

Disponível em: http://wikiLeaks.org/irq. Acesso em: 27 fev. 2020.

Disponível em: http://www.archiviopenale.it/intercettazioni–cass-sez-un-1-luglio-2016-(cc-28-aprile-2016)-scurato/contenuti/6142. Acesso em: 15 out. 2019.

Disponível em: http://www.collateralmurder.com. Acesso em: 27 fev. 2020.

Disponível em: http://www.leparisien.fr/quel-paradoxe-pour-la-democratie-30-01-2016-5498313.php. Acesso em: 23 jul. 2019.

Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=431123&caixaBusca=N. Acesso em: 27 fev. 2020.

Disponível em: https://brasil.elpais.com/brasil/2015/06/12/tecnologia/1434103095_932305.html. Acesso em: 30 jul. 2019.

Disponível em: https://ec.europa.eu/home-affairs/news/security-union-new-rules-eu-passenger-name-record-data_en. Acesso em: 27 fev. 2020.

Disponível em: https://elpais.com/tecnologia/2016/12/14/actualidad/1481753868_540005.html. Acesso em: 23 jul. 2019.

Disponível em: https://eur-lex.europa.eu/oj/direct-access.html?locale=pt. Acesso em: 25 out. 2019.

Disponível em: https://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html. Acesso em: 8 out. 2019.

RBDFJ_43_MIOLO.indd 371 06/05/2021 14:02:19

Disponível em: https://online.norwich.edu/academic-programs/masters/information-security-assurance/resources/infographics/deep-web-crime-requires-new-forensic-approaches. Acesso em: 30 jul. 2019.

Disponível em: https://www.apple.com/customer-letter/. Acesso em: 8 out. 2019.

Disponível em: https://www.cnbc.com/2019/12/19/schrems-vs-facebook-legal-advisor-to-eu-supreme-court-gives-opinion.html. Acesso em: 26 fev. 2020.

Disponível em: https://www.cnil.fr/fr/publication-de-lavis-sur-le-projet-de-loi-relatif-au-renseignement. Acesso em: 3 set. 2019.

Disponível em: https://www.latimes.com/politics/la-na-pol-fbi-iphone-san-bernardino-20180327-story.html. Acesso em: 8 out. 2019.

Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318345&categorieLien=id. Acesso em: 3 set. 2019.

Disponível em: https://www.lemonde.fr/les-decodeurs/visuel/2016/01/08/un-an-apres-le-recit-detaille-des-attentats-de-janvier2015_4843963_4355770.html#introduction. Acesso em: 3 set. 2019.

Disponível em: https://www.libertyhumanrights.org.uk/human-rights/privacy/snoopers-charter. Acesso em: 3 set. 2019.

Disponível em: https://www.nytimes.com/2019/08/15/us/politics/trump-nsa-call-records-program.html. Acesso em: 1º out. 2019.

Disponível em: https://www.osservatoriosullefonti.it/archivio-rubriche-2014/fonti-dellunione-europea-e-internazionali/986-ue-corte-di-giustizia-causa-c-13112-google-spain. Acesso em: 10 set. 2019.

Disponível em: https://www.theregister.co.uk.

Disponível em: https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/. Acesso em: 30 set. 2019.

Disponível em: https://www.washingtonpost.com/world/national-security/white-house-has-signaled-it-may-seek-permanent-renewal-of-controversial-surveillance-power/2019/04/30/b4407af2-67a5-11e9-8985-4cf30147bdca_story.html. Acesso em: 1º out. 2019.

Disponível em: https://www.zdnet.com/article/national-security-letters-everything-you-need-to-know/. Acesso em: 27 fev. 2020.

Disponível em: https://www1.folha.uol.com.br/poder/2020/01/google-e-promotoria-brigam-na-justica-por-dados-de-usuarios-em-caso-marielle.shtml. Acesso em: 27 fev. 2020.

Disponível em: www.bundesverfassungsgericht.de. Acesso em: 10 set. 2019.

Disponível em: www.echr.coe.int/pages. Acesso em: 1º out. 2019.

FERONI, Cerrina. La sicurezza: un valore superprimario. *Percorsi constituzionali: quadrimestrale di diritti e libertà*, Roma, 2008.

FINOCCHIARO, Giusella. La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems. *Diritto dell'informazione e dell'informatica*, v. 31, n. 4-5, 2015.

FROSINI, Tommaso Edoardo. Il diritto costituzionale alla sicurezza. *Forum on line di Quaderni costituzionali*. Acesso em: http://www.forumcostituzionale.it/wordpress/wp-content/uploads/pre_2006/440.pdf. Acesso em: 6 ago. 2019.

GERMAN, Christiano. *As novas leis de segurança na Alemanha e nos Estados Unidos*: os efeitos para a comunicação local e global. Disponível em: https://www2.mppa.mp.br/sistemas/gcsubsites/upload/60/as%20novas%20leis%20de%20%20seguranÃ§a%20na%20alemanha%20e%20nos%20eua.pdf. Acesso em: 10 set. 2019.

RBDFJ_43_MIOLO.indd 372 06/05/2021 14:02:19

HALL, Matthew; HEARN, Jeff. *Revenge pornography* – Gender, sexualities and motivations. New York: Routledge, 2018.

LANA, Alice de Perdigão. *Mulheres expostas*: revenge porn, gênero e o Marco Civil da Internet. Curitiba: Gedai/UFPR, 2019.

LEAL, Rogério Gesta. O acesso a informação no processo penal enquanto condição de possibilidade do devido processo legal e do amplo direito de defesa: a sutil distinção entre provas documentadas e provas documentadas analisadas. *In*: LEAL, Rogério Gesta; GAVIÃO FILHO, Anizio Pires (Org.). *IV Seminário Nacional Tutelas à Efetivação de Direitos Indisponíveis*. Porto Alegre: FMP, 2018.

LEAL, Rogério Gesta. *Responsabilidade penal do patrimônio ilícito como ferramenta de enfrentamento da criminalidade*. Porto Alegre: FMP, 2017. Disponível em: http://www.fmp.edu.br/servicos/285/publicacoes/.

LÓPEZ CARBALLO, Daniel. *Responsabilidades derivadas del tratamiento y explotación de los datos personales*. Disponível em: http://dlcarballo.com/2017/01/27/responsabilidades-derivadas-del-tratamiento-y-explotacion-de-los-datos-personales/. Acesso em: 23 jul. 2019.

MALFATTI, Elena. *I "livelli" di tutela dei diritti fondamentali nella dimensione europea*. Torino: Giappichelli, 2018.

MARINELLI, Claudio. *Intercettazioni processuali e nuovi mezzi di ricerca della prova*. Roma: Giappichelli, 2007.

MARTINS, Guilherme Magalhães (Coord.). *Direito privado e internet*. São Paulo: Atlas, 2014.

NICOLICCHIA, Fabio. Il principio de proporzionalità nell'era del controlo tecnologico e le sue implicazioni processual rispetto ai nuovi mezzi di ricerca dela prova. *Diritto Penale Contemporaneo*. Disponível em: https://www.penalecontemporaneo.it/d/5784-il-principio-di-proporzionalita-nell-era-del-controllo-tecnologico-e-le-sue-implicazioni-processual. Acesso em: 22 out. 2019.

PIZZETTI, Franco. *Privacy e il diritto europeo alla protezione dei dati personali*. Il Regolamento europeo 2016/679. Torino: Giappichelli, 2016. v. 2.

RUBINSTEIN, Ira. Big data: the end of privacy or a new beginning? *Public and Legal Theory Research Paper Series*, New York, n. 357, 2012.

SCHWARTZ, Paul M.; SLOVE, Daniel J. The PII problem: privacy and a new concept of personally identifiable information. *New York University Law Review*, New York, v. 86, 2011.

SOLOVE, Daniel J. *The digital person*: technology and privacy in the information age. New York: New York University Press, 2004.

TORRE, Alessandro (A cura di). *Costituzioni e sicurezza dello Stato*. Rimini: Maggioli Editore, 2014.

UGHELINI, Denis. *Intercettazioni*: caratteri, limiti e prospettive di una controversa materia. Padova: Università degli Studi di Padova, 2014.

VACIAGO, Giuseppe; RAMALHO, David Silva. Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings. *Digital evidence and eletronic signature Law Review*, n. 13, 2016.

VECCHI, Benedetto. *La Democrazia blindata dei Big Data*. Disponível em: http://www.euronomade.info/?p=12085. Acesso em: 23 jul. 2019.

VERGOTTINI, Giuseppe de. La difficile convivenza fra libertà e sicurezza. La risposta delle democrazie al terrorismo. *Boletín Mexicano de Derecho Comparado*, nueva serie, año XXXVII, n. 111, p. 1185-1211, sept./dic. 2004.

RBDFJ_43_MIOLO.indd 373 06/05/2021 14:02:20

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 15 dez. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 27 set. 2019.

ZENO-ZENCOVICH, Vincenzo. Intorno ala decisione nel caso Schrems: la sovranità digitale e il governo Internazionale delle reti di telecomunicazione. *Rivista Diritto dell'informazione e dell'informatica*, v. 31, n. 4-5, 2015.

ZICCARDI, Giovanni. *Trasparenza, sorveglianza e segreto nell'era tecnologica*. Milano: Raffaelo Cortina Editore, 2015.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

LEAL, Rogério Gesta. Direito fundamental à proteção de dados em tempos de pandemia: necessárias equações entre segurança pública e privada. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 14, n. 43, p. 357-374, jul./dez. 2020.

Recebido em: 18.06.2020
Pareceres: 15.08.2020, 27.08.2020
Aprovado em: 18.09.2020

RBDFJ_43_MIOLO.indd 374 06/05/2021 14:02:20