REVISTA NOVOS ESTUDOS JURÍDICOS - ELETRÔNICA, VOL. 28 - N. 1 - JAN-ABR 2023
Disponível em: periodicos.univali.br
DOI: https//:doi.org/10.14210/nej.v28n1.p71-93

LIMITES DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS EM FACE DA INSTRUÇÃO PROBATÓRIA NO PROCESSO PENAL

LIMITATIONS OF THE FUNDAMENTAL RIGHT TO DATA PROTECTION IN LIGHT OF THE PROBATORY INSTRUCTIONS IN CRIMINAL PROCEEDINGS

LIMITACIONES DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS ANTE LA INSTRUCCIÓN PROBATORIA EN EL PROCESO PENAL

Rogério Gesta Leal[1]

Universidade de Santa Cruz do Sul

https://orcid.org/0000-0002-4162-4907

RESUMO

Contextualização: Na sociedade moderna em que vivemos, caracterizada pelo constante e acelerado desenvolvimento tecnológico, compreender de que modo se pode tutelar adequadamente o direito à privacidade, intimidade e dados individuais, representa questão fundamental, nomeadamente quando inúmeras políticas públicas, em nome da segurança social, têm surgido colocando em risco aqueles direitos.

Objetivo: Avaliar como tem se constituído o debate doutrinário e casuístico das tensas equações entre o direito fundamental à proteção de dados da pessoa física, em face da persecução penal, nomeadamente no Brasil.

Metodologia: Utilizou-se, na pesquisa, o método dedutivo, testando as hipóteses com os fundamentos gerais a serem declinados e análise de alguns casos jurisprudenciais, bem como técnica de pesquisa com documentação indireta, nomeadamente bibliográfica.

Resultados: Enquanto resultados, sustenta-se que a requisição de dados pessoais

[1] Doutor em Direito pela Universidade Federal de Santa Catarina. Mestre em Desenvolvimento Regional pela Universidade de Santa Cruz do Sul. Professor titular da Universidade de Santa Cruz do Sul. e da Fundação Escola Superior do Ministério Público do Rio Grande do Sul - FMP, nos cursos de graduação, mestrado e doutorado em Direito. Desembargador do Tribunal de Justiça do Estado do Rio Grande do Sul. ORCID: https://orcid.org/0000-0003-1372-6348. Endereço eletrônico: gestaleal@gmail.com

armazenados por provedores de serviços de internet pode se dar desde que indicados os elementos previstos na Lei nº 12.965/2014, em seus Arts. 22 e 23, a saber: a) fundados indícios da ocorrência do ilícito; b) justificativa motivada da utilidade da requisição; e c) período ao qual se referem os registros, e que sua execução também se dê observados os ditames da adequação, necessidade e proporcionalidade em sentido estrito referidos.

Palavras-chave: Direito fundamental à proteção de dados; Direito fundamental à privacidade; Responsabilidade penal.

ABSTRACT

Contextualization: In the modern society we live, characterized by constant and accelerated technological development, understanding how the right to privacy, intimacy and individual data can be adequately protected is a fundamental issue, particularly when numerous public policies, in the name of social security, have emerged putting those rights at risk.

Objective: To evaluate how the doctrinal and casuistic debate on the tense equations between the fundamental right to personal data protection in the face of criminal prosecution, particularly in Brazil, has developed.

Methodology: It was used, in this research, the deductive method, testing the hypotheses with the general foundations to be outlined and analysis of some jurisprudential cases, as well as the research technique with indirect documentation, namely bibliography.

Results: As a result, it is proposed that the request for personal data stored by internet service providers can be given as long as the elements provided for in Law nº 12.965/2014, in articles 22 and 23, are indicated, namely: a) founded evidence of the occurrence of the offense; b) motivated justification of the usefulness of the request; and c) period to which the records refer, and that their execution also takes into account the dictates of adequacy, necessity and proportionality in a strict sense.

Keywords: Fundamental right to data protection; Fundamental right to privacy; Criminal responsibility.

RESUMEN

Contextualización: En la sociedad moderna en que vivimos, caracterizada por un constante y acelerado desarrollo tecnológico, entender cómo se puede proteger adecuadamente el derecho a la privacidad, la intimidad y los datos individuales es un tema fundamental, particularmente cuando numerosas políticas públicas, en nombre de la seguridad social, ha surgido poniendo en riesgo esos derechos.

Objetivo: Evaluar cómo se ha desarrollado el debate doctrinal y casuístico sobre las ecuaciones tensas entre el derecho fundamental a la protección de datos personales frente a la persecución penal, especialmente en Brasil.

Metodología: Se utilizo, en la investigación, el método deductivo, contrastando las hipótesis

con los fundamentos generales a declinar y análisis de algunos casos jurisprudenciales, así como la técnica de investigación con documentación indirecta, fundamentalmente la bibliografía.

Resultados: Se propone que la solicitud de datos personales almacenados por los proveedores de servicios de internet puede darse siempre que se indiquen los elementos previstos en la Ley nº 12.965/2014, en sus artículos 22 y 23, a saber: a) prueba fundada de la ocurrencia del delito; b) justificación motivada de la utilidad de la solicitud; y c) plazo a que se refieren las actas, y que su ejecución se produzca también con sujeción a los dictados de idoneidad, necesidad y proporcionalidad en el sentido estricto a que se refiere.

Palabras clave: Derecho fundamental a la protección de datos; Derecho fundamental a la intimidad; Responsabilidad penal.

INTRODUÇÃO

O objetivo geral deste trabalho é avaliar como tem se constituído o debate doutrinário e casuístico das tensas equações entre o direito fundamental a proteção de dados da pessoa física, em face da persecução penal, nomeadamente no Brasil.

Para tanto, o problema que pretendemos indagar é se podemos estabelecer, pela via judicial, modulações eventualmente restritivas do Direito Fundamental à Proteção de Dados – e com que critérios – diante da necessidade de persecução penal para apurar responsabilidades desta natureza.

Com base no problema levantado, a hipótese é no sentido de ser possível, observando critérios de adequação, necessidade e proporcionalidade, e pela via judicial, estabelecer, caso a caso, modulações restritivas à inviolabilidade de dados relacionados à privacidade e intimidade para fins de apuração da responsabilidade penal no Brasil.

O texto foi desenvolvido a partir dos seguintes objetivos específicos: (i) demarcar alguns contornos do debate sobre a proteção de dados na experiência internacional, tanto na perspectiva doutrinária, como na jurisprudencial; (ii) delimitar como está se desenvolvendo esta temática no Brasil, no âmbito doutrinário e casuístico; (iii) identificar como tem se dado as equações entre a proteção de dados – com alguns casos concretos – e a persecução penal no Brasil, propondo sugestões para o seu tratamento.

Utilizou-se, na pesquisa, o método dedutivo, testando as hipóteses com os fundamentos gerais a serem declinados e análise de alguns casos jurisprudenciais. Utiliza-se, para tanto, técnica de pesquisa com documentação indireta, nomeadamente bibliográfica.

1. A PROTEÇÃO DE DADOS NA EXPERIÊNCIA INTERNACIONAL

Na sociedade moderna em que vivemos, caracterizada pelo constante e acelerado desenvolvimento tecnológico, compreender de que modo se pode tutelar adequadamente o direito à privacidade, intimidade e dados individuais, representa questão fundamental. Em particular, a grande difusão de smartphones e das redes sociais tem proporcionado que se possa vir a acessar/conhecer informações do passado e do

presente, de aspectos importantes da vida das pessoas – físicas e jurídicas.

Evidente que esta espetacularização do privado recebe impulso quotidiano de auto exposições multifacetárias envolvendo opiniões, relações sociais, hábitos, experiências de trabalho, de relacionamentos, projetos de vida, etc. Provavelmente, e em certos aspectos também inconscientemente, estamos perdendo a concepção e o valor da tutela da própria privacidade, deixando de perceber como a proteção dos dados pessoais representa articulação fundamental em relação a outros direitos e seus exercícios.

Por conta disto, os ordenamentos jurídicos democráticos hodiernos têm cada vez mais adotado mecanismos emergenciais e de polícia para enfrentar ameaças à segurança dos cidadãos e de seus dados, tendo de revisar, por vezes, antigos institutos dogmáticos vigentes para atualizá-los – ou criar novos – a fim de dar conta destas demandas.

Por outro lado, também os níveis de criminalidade e violência em todos os países do globo tem aumentado assustadoramente (tráfico de drogas, pessoas, órgãos humanos, armas, lavagem de dinheiro, cibercriminalidade), colocando em estado de alerta sistemas de segurança pública nacionais e transnacionais, e fazendo com que ordenamentos jurídicos sejam revistos, tanto no aspecto preventivo como curativo, para tentar dar conta de modo mais efetivo a tais cenários.

Dentre as ações e reações institucionais que temos observado surgir por conta destas conjunturas são as de caráter penal e processual penal, as quais dá-se um destaque e, neste ponto, há certo consenso de que uma das primeiras respostas mais incisivas dada aos riscos e perigos sob comento foi a adotada pelos Estados Unidos da América – USA, a partir do *Patriot Act*, de 2001, impondo inúmeras restrições às liberdades individuais, e mesmo criando formas de duvidosa constitucionalidade e legalidade para lidar com o terrorismo, como a prisão de Guantanamo.[2]

Não bastasse isto, ainda temos o escândalo do chamado *Datagate*, de autoria de Edward Snowden, revelando detalhes de programas de vigilância global da NSA norte americana, notadamente através do programa PRISM, expondo políticas de invasão de privacidade do governo sem controle político ou social, tudo em nome da segurança contra o mesmo terrorismo.[3]

A partir do século XXI só aumentam os instrumentos de investigação do Estado em nome da segurança pública e para o enfrentamento de várias espécies de criminalidades, o que inexoravelmente atinge dados de pessoas físicas e jurídicas, colocando em risco vários e históricos direitos e garantias constitucionais.

O problema é que esta expressão segurança pública tem tido múltiplas designações conceituais, passando por segurança interna e externa, dependendo se se leva em conta

[2] Para ver melhores informações sobre esta política de segurança: https://www.justice.gov/archive/ll/highlights.htm. Acesso em: 12 mai. 2021.

[3] Ver a interessante matéria do The Guardian no site: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/4. Acesso em: 12 mai. 2021. Isto se espalha também à Europa, até por conta dos atos terroristas que lá ocorrem, basta observar as normativas francesas relacionadas na chamada *assignation à résidence*, estabelecendo restrições de circulação a determinados sujeitos identificados como perigosos à ordem pública e segurança, ex vi a Lei nº 1501, de 20/11/2015, sobre o estado de urgência e seus poderes investigativos. Destaca-se o seguinte texto: GAZZETTA, Cristina. Sicurezza, terrorismo e cittadinanza: la nuova legislazione francese anti-terrorismo e l'impegno Internazionale contro i cd. *foreing fighters*. **Osservatório sulla normativa**. Ano V, nº 3, out. 2015.

a proveniência de ameaças a determinados grupos sociais; também se pode contrapor segurança individual à segurança coletiva; assim como podemos falar de segurança material (relacionada à incolumidade de bens e pessoas), e segurança formal (preservação de princípios e valores fundamentais dos ordenamentos jurídicos).[4]

Em qualquer destas perspectivas a segurança configura bem jurídico fundamental às relações sociais e interindividuais, e isto porque representa valor constitutivo de qualquer ordem pública contemporânea; indo além, Marco Rutuolo sustenta que o conceito de segurança está muito vinculado à proteção de bens constitucionais e infraconstitucionais permanentemente, e isto no sentido de que:

> la sicurezza sarebbe strettamente collegata alla rimozione degli ostacoli che si frappongano all'effettivo godimento dei diritti: e dunque si dovrebbe parlare più appropriatamente di «sicurezza dei diritti» piuttosto che di «diritto alla sicurezza» nella forma di Stato sociale.[5]

A par disto, a segurança configuraria *valor super primário*, no sentido de que não se presta a balanceamentos, mas deve sempre ser garantida em face de sua natureza contratualista matricial, inexoravelmente vinculada à dignidade da vida humana, à incolumidade física, patrimonial e extrapatrimonial das pessoas, seu bem-estar e qualidade de existência, ou seja, trata-se de direito fundamental indispensável à fruição de direitos os quais os indivíduos são titulares.[6]

Nos dias atuais, pela ocorrência de mutações significativas destes conceitos, eis que os ordenamentos jurídicos democráticos garantem níveis de segurança mais robustos em face a tempos pretéritos, para alcançar dimensões sociais indispensáveis à vida em comunidade.

Por isto, está na agenda atual do debate jurídico e político internacional como devemos nos situar entre o princípio *salus rei publicae suprema lex esto*, no sentido de que eventuais derrogações ou flexibilizações a direitos fundamentais individuais devem ser aceitas na medida em que efetivamente necessárias, adequadas e proporcionais à garantia de direitos fundamentais sociais – como a segurança pública.

Neste sentido, ganha relevo, a título exemplificativo, a decisão da Corte de Justiça da União Europeia de 21/12/2016, conhecida como Caso Tele2, na qual estabeleceu que os Estados membros não podem impor a fornecedores de serviços de comunicação eletrônica obrigação genérica e indiferenciada de conservação de dados relativos ao tráfego e à localização dos usuários, sem o consentimento destes. Autorizou a Corte,

---

[4] Estas são definições bastante amplas apresentadas pelo trabalho coordenado por COCCO, Giovanni. (a cura di). **I diversi volti della sicurezza**. Milano: Giuffrè, 2012.

[5] RUTUOLO, Marco. Diritto ala sicurezza e sicurezza dei diritti. **Osservatório sulla normativa.** Ano III, nº 2, 2013, p. 06. A Itália já conta com um Código de Proteção de Dados Pessoais, acessível pelo site: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9042678. Acesso em: 01 jun. 2021.

[6] Conforme a dicção de CERRINA FERONI, Ginevra e MOBIDELLI, Giuseppe. **La sicurezza: un valore superprimario**. In Percorsi Costituzionale. V.I, nº1/2008, p.39. No mesmo sentido FROSINI, Tomaso Edoardo. **Il diritto costituzionale alla sicurezza**. In Forum on line di Quaderni Costituzionali. Disponível em: https://www.forumcostituzionale.it/wordpress/wp-content/uploads/pre_2006/440.pdf. Acesso em: 26 mai. 2021. Diz este autor: *C'è un bisogno di sicurezza che si impone nella società odierna, che è sempre più una società del rischio: e la sicurezza si impone sia come attività statale per tutelare il cittadino da rischi e pericoli sociali, sia come diritto fondamentale, quale condizione "per l'esercizio delle libertà e per la riduzione delle disuguaglianze*".

somente a título preventivo, a conservação destes elementos voltada exclusivamente ao enfrentamento de graves fenômenos de criminalidade, limitando-se ao estritamente necessário para os que detém a categoria de dados a conservar.[7]

E o fez bem a Corte, porque os conceitos de privacidade e comunicação resultam indissociáveis da proteção dos dados pessoais, o que lhes dão enquadramento mais dinâmico do que estático em termos de configuração e aplicação no tempo e espaço – nomeadamente em face dos aspectos virtuais que lhes alcançam. E na medida em que resta considerada a *privacy* como ínsita à liberdade pessoal, isto de um lado implica certo tipo de liberdade negativa, no sentido de que ninguém pode se intrometer na esfera privada do titular de liberdade; em outro viés, liberdade positiva, tomada como possibilidade de atribuir ao titular de direito a autonomia de agir/reagir em face de comportamentos de outrem que possam ofender sua posição.[8]

Salienta-se que a Declaração Americana dos Direitos e Deveres do Homem, de 1948, deu proteção internacional à privacidade, em seu artigo 5º, dispondo que: *toda pessoa tem direito à proteção da lei contra os ataques abusivos a sua honra, a sua reputação e a sua vida privada e familiar*. Em 10 de dezembro do mesmo ano foi aprovada pela Assembleia Geral das Nações Unidas a Declaração Universal de Direitos do Homem, prevendo em seu Art. 12 que: ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou correspondência, nem de ataques à sua honra ou reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências ou ataques.

No plano doutrinário, ao término da 26ª *International Conference on Privacy and Personal Data Protection*, Stefano Rodotà sustentou que:

> La privacy si presenta come un elemento fondamentale della società dell'eguaglianza. Senza una forte tutela dei dati riguardanti le convinzioni politiche o l'appartenenza a partiti, sindacati, associazioni, i cittadini rischiano di essere esclusi dai processi democratici: così la privacy diventa una condizione essenziale per essere inclusi nella società della partecipazione. Senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo. Diventa così evidente che la privacy è uno strumento necessario per difendere la società della libertà, e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale.[9]

O problema é que determinados fenômenos criminais, como já anunciado, continuam a fazer vítimas em todo o mundo, levando Estados a buscarem novas formas de proteção e enfrentamento dos riscos e perigos que isto representa, dentre as quais políticas de acesso, armazenamento e manejo de dados de pessoas físicas e jurídicas para fins de prevenção e responsabilização por atos de violência e defraudação dos sistemas

[7] Ver a integra da decisão no site: https://privacyinternational.org/sites/default/files/2019-08/CELEX_62015CJ0203_EN_TXT.pdf. Acesso em: 24 fev. 2021. O Parlamento Europeu e o Conselho da Europa modificaram a Diretiva 2002/58/CE, através da Diretiva 2006/24/CE, que agora versa sobre a conservação de dados gerados ou tratados no âmbito do fornecimento de serviços de comunicações eletrônicas acessíveis ao público ou de redes públicas de comunicação.

[8] Ver no ponto o excelente texto: BALDASSARRE, Antonio. **Diritti della persona e valori costituzionale**. Torino: Giappichelli, 1997.

[9] RODOTÀ, Stefano. Privacy, libertà, dignità. **Garante per la protezione dei dati personali**, 2004. Disponível em: www.garanteprivacy.it. Acesso em: 12 mai. 2021.

normativos, e mesmo inéditos mecanismos de investigação e persecução criminal.

A tal ponto que o Reino Unido vai instituir o *investigatory powers bill*, medida de grande impacto sob a tutela da liberdade e privacidade das comunicações dos cidadãos em nome da segurança contra atos de terror, permitindo que as autoridades investigativas do Estado desenvolvam interceptações telefônicas e telemáticas sem que os fornecedores destes serviços possam descumprir tais determinações, e autorizando o acesso e conservação destes, mais as informações concernentes aos sítios web objetos de navegações, pelo prazo de um ano.[10]

Na Alemanha, desde 2016, vige lei de reforma dos poderes investigativos da agência para a segurança externa do país (BND), que prevê a possibilidade de interceptar comunicações telemáticas da internet de estrangeiros para fins de prevenção de potenciais e indiciários atos de terrorismo, introduzindo no ordenamento jurídico discutível diferenciação entre cidadãos tedescos e estrangeiros. A par disto, o Tribunal Constitucional Alemão, em sentença de 20/04/2016, decidiu que seriam necessários rígidos escrutínios de proporcionalidade à aplicação de várias disposições da lei federal sobre atividades de forças policiais – *Bundeskriminalamtgesetz (BKAG*) – que buscavam utilizar formas de vigilância oculta e o emprego de meios informáticos para adquirir dados remotos de investigados.[11]

A Corte de Cassação italiana, por sua vez, já teve oportunidade de reconhecer significativas restrições de liberdades fundamentais para fins de investigação criminal, admitindo que instrumentos de captação e invasão (trojan) informática, veiculados por e-mail na forma de vírus, mensagens ou download de aplicações da rede, fossem instalados, de forma remota, em aparelhos múltiplos (celulares, tablets, PCs) de pessoas investigadas ou suspeitas, por setores de investigação oficiais e com autorização judicial, para fins de obtenção de provas sobre crimes tentados, em execução ou consumados.[12] Como refere Albrecht:

> verifica-se na atualidade uma crescente tematização do que seria uma suposta tensão envolvendo a eficiência do processo penal e da política de segurança, de um lado, e a liberdade dos cidadãos, de outro. Os debates sobre essa relação conflituosa entre segurança, eficiência e liberdade vêm sendo marcados por um deslocamento da função atribuída ao Direito Penal, do qual se exigem mais e mais medidas garantidoras da segurança e pela ênfase dada a riscos excepcionais atribuídos à crimina- lidade organizada transnacional e, sobretudo, ao terrorismo internacional. Com isso, também o conceito de "segurança" ganha novos contornos, passando a ser entendido cada vez mais como segurança frente à criminalidade e sobretudo frente à

[10] Ver mais dados no sitio https://www.gov.uk/government/collections/investigatory-powers-bill. Acesso em: 16 jun. 2021.

[11] BUNDESVERFASSUNGSGERICHT. **Headnotes to the Judgment of the First Senate of 20 April 2016.** Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2016/04/rs20160420_1bvr096609en.html. Acesso em: 16 jun. 2021.

[12] REDAZIONE GIURISPRUDENZA PENALE. **Intercettazioni su dispositivi elettronici mediante "captatore informatico": depositate le motivazioni delle Sezioni Unite (26889/2016).** 2 jul. 2016. Disponível em: https://www.giurisprudenzapenale.com/2016/07/02/intercettazioni-su-dispositivi-elettronici-mediante-captatore-informatico-depositate-le-motivazioni-delle-sezioni-unite-268892016/. Acesso em: 16 jun. 2021.

violência, convergindo nos conceitos de "segurança interna" e "segurança externa".[13]

Mesmo assim, parte da doutrina assente no argumento de que eventual aumento das condições de segurança vem sempre acompanhado do crescimento da sensação subjetiva de insegurança. Esse problema, em si já relevante, torna-se ainda maior quando lembramos que, frente a novas formas de criminalidade, os padrões convencionais de interpretação dos perigos tendem a se mostrar ineficazes, dado que esse tipo de medição tem por base prognósticos cujos pressupostos são normalmente controversos.

Neste sentido, políticas de segurança pública podem, em determinados contextos singulares, implicar/justificar ações de restrições de direitos e garantias individuais, mas isto também pode acarretar abusos de poder e desvios de finalidades se não avaliados e ponderados com direitos e garantias fundamentais individuais igualmente assegurados pelo constitucionalismo contemporâneo.

Daí porque os tribunais na União Europeia (EU) têm insistido com o argumento de que seja utilizado para aferir tais elementos – e a possibilidade ou não de se acessar, armazenar e manejar dados pessoais sem o consentimento dos seus titulares – severos testes de proporcionalidade entre os escopos perseguidos e bens tutelados, a partir do que tem evoluído a regulamentação destes temas; a título exemplificativo, tem-se documentos como: (i) o Tratado de Lisboa, de 2009, reconhecendo a proteção de dados pessoais enquanto direito fundamental; (ii) a edição da Diretiva (EU) 2016/680, do Parlamento Europeu e do Conselho, em 27/04/2016, relativa à proteção das pessoas singulares no que tange ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e a livre circulação destes dados, revogando a Decisão-Quadro 2008/977/JAI do Conselho.

Caso polêmico tratando deste tema na UE foi concluído em maio de 2021, com o julgamento do processo *Big Brother Watch and Others v. the United Kingdom*[14], pela Corte Europeia dos Direitos Humanos (CEDH), envolvendo Grã-Bretanha e Irlanda do Norte, por conta de violação ao Art. 34 da Convenção à Proteção dos Direitos Humanos e Liberdades Fundamentais, fundado em três requerimentos chegados a Corte (58170/13, 62322/14 e 24960/15).[15]

---

[13] ALBRECHT, Hans-Jörg. Direito Penal e Periculosidade: a politica criminal entre prevenção, combate a perigos e retribuição de culpa. In MACHADO, Marta R. de Assis e PÜSCHEL, Flavia Portella (org.). **Responsabilidade e Pena no Estado Democrático de Direito.** São Paulo: FGV, 2016, p.51. Ainda agrega o autor – e concordamos com ele: *O problema central consiste certamente na simples constatação de que a segurança em sentido amplo constitui necessariamente pressuposto da liberdade, de modo que, na realidade, não pode existir qualquer oposição entre esses dois valores. A liberdade apenas pode ser exercida se existirem condições sociais básicas de segurança que permitam a fruição desse Direito*.

[14] EUROPEAN COURT OF HUMAN RIGHTS. Case of Big Brother Watch and Others v. the United Kingdom. Disponível em: https://www.bailii.org/cgi-bin/format.cgi?doc=/eu/cases/ECHR/2021/439.html&query=(title:(+Big+))+AND+(title:(+Brother+))+AND+(title:(+Watch+))+AND+(title:(+Others+))+AND+(title:(+v+))+AND+(title:(+the+))+AND+(title:(+United+))+AND+(title:(+Kingdom+)). Acesso em: 14 jun. 2021. Ver também o caso *Google Spain, Data Retention e Teledue*, paradigmático nestes temas. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0131&from=PT. Acesso em: 11 out. 2022.

[15] Os postulantes destes requerimentos foram: Human Rights Watch, Access Now, Dutch Against, Plasterk, Center For Democracy & Technology, European Network of National Human Rights Institutions and the Equality and Human Rights Commission, the Helsinki Foundation For Human Rights, the International Commission of

Os requerimentos sustentam que se afigura ilegal o escopo e a magnitude dos programas de investigações eletrônicas operados pelo governo do Reino Unido. Em 04 de julho de 2017, a Câmara da Primeira Sessão, da CEDH, resolveu por agrupar todos os reclamantes e ouvi-los sobre suas petições, o que ocorreu em Strasbourg, na data de 07/11/2017. Os peticionantes apresentaram neste caso vários aspectos e abordagens de invasão de privacidade ilícita, mas também se referenciaram a partir das revelações feitas por Edward Snowden, atinentes aos programas de vigilância operados pelos serviços de inteligência dos Estados Unidos da América – EUA e da UK, sustentando que, devido a natureza das atividades monitoradas por estes programas, as suas comunicações eletrônicas tranquilamente poderiam ter sido interceptadas; ou mesmo obtidos por autoridades dos EUA e do Reino Unido de provedores de serviços de comunicação.[16]

As revelações de Edward Snowden, feitas em 2013, indicaram que o quartel general governamental de comunicações do serviço de inteligência britânico (GCHQ) estava operando um modelo global de vigilância e investigação secreta de dados e informações de pessoas físicas e jurídicas em nome da segurança nacional, denominado de *tempora*, o qual permitia acessar e armazenar milhões de dados extraídos de provedores, sendo que as autoridades deste país não confirmavam ou negavam a existência deste programa.[17]

Por mais que os sistemas e modelos de tratamento dos dados acessados e armazenados por estas ferramentas conseguissem constituir imensos acervos de informações, sempre foi impossível avaliar detidamente todos eles, razão pela qual foram criadas metodologias de abordagem e procedimentos, com seus respectivos protocolos, para selecionar quais elementos deveriam ser inspecionados com rigor (*complex queries*), advindo daí os seletores de dados e informações com base em perfis previamente demarcados por critérios e indicadores dos gestores destes sistemas de vigilância, o que, de qualquer sorte, não ameniza a gravidade da violação de privacidade e intimidade levada a cabo, e mais que isto, de forma secreta e sem prestação de contas. Para além disto, nenhuma informação segura existia sobre o modo de descarte dos dados/informações não considerados importantes, e quais as políticas de segurança na mantença daqueles selecionados como tais.[18]

Também a *National Security Agency (NSA)*, dos EUA, reconheceu, neste processo, a existência de duas operações globais voltadas a vigilância de dados e informações de pessoas físicas e jurídicas para fins de segurança nacional, a saber: (i) o programa PRISM,

---

Jurists, Open Society Justice Initiative, The Law Society of England and Wales and Project Moore, Center For Democracy & Technology, the Helsinki Foundation For Human Rights, the International Commission of Jurists, the National Union of Journalists and the Media Lawyers' Association, Electronic Privacy Information Center and to the Equality and Human Rights Commission.

[16] Os chamados *communications service providers* – CSPs.

[17] Ver no ponto a matéria publicada em 2013, por Philip Bump, no The Atlantic, disponível em: https://www.theatlantic.com/national/archive/2013/06/uk-tempora-program/313999/. Acesso em: 21 jun. 2021. Veja-se que somente em 2000 que a UK vai constituir sua *Regulation of Investigatory Power Act*, cujas informações podem ser obtidas através do site: https://justice.org.uk/regulation-investigatory-powers-act-2000/. Acesso em: 21 jun. 2021.

[18] Mais tarde a UK vai instituir seu *Interception of Communications Code of Practice*, regulamentando melhor esta matéria, como mostra o documento acessado pelo site: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf. Acesso em: 21 jun. 2021. Igualmente, cria o *Investigatory Power Tribunal – IPT*, órgão independente do governo que busca justamente julgar os abusos cometidos por autoridades em termos de violação do direito de privacidade e intimidade por meios tecnológicos. Disponível em: https://www.ipt-uk.com. Acesso em: 21 jun. 2021.

e o (ii) programa UPSTREAM. O primeiro visava obter comunicações através de provedores de serviços de internet (ISPs), estando regulado pelo *Foreign Intelligence Surveillance Act (FISA)*, sendo que o seu uso deveria ser aprovado pela *Foreign Intelligence Surveillance Court (FISC)*. Todavia, os documentos trazidos à tona por Snowden revelaram que o programa PRISM vinha sendo utilizado pelos EUA desde julho de 2010, gerando milhões de relatórios de inteligência, sem os devidos protocolos integrais de permissão e aprovação.[19]

A partir daí, as regulamentações foram se dando de forma fragmentada, nomeadamente pelos parlamentos dos Estados[20], o que não permitiu formatar base normativa nacional a fim de orientar a todos sobre a matéria, tanto que a *Federal Trade Comission (FTC)*, órgão público que responde pela supervisão do comércio nos EUA, em março de 2012, reconheceu que os níveis de tutela dos dados privados em seu território não eram adequadamente seguros, indicando ao Congresso a adoção de regulamentação nacional à proteção de dados.[21]

Estes movimentos todos levaram este Congresso, por sua comissão antitruste, em julho de 2020, a realizar audiência pública com os CEOs da Amazon, Apple, Google e Facebook, para tratar de eventuais problemas de monopólio excessivo relacionado às suas posições dominantes no mercado da internet, o que envolve, por óbvio, o tema da proteção de dados privados e públicos.[22]

---

[19] O The Guardian, em 2013, publicou matéria sobre o tema dizendo: The National Security Agency has obtained direct access to the systems of Google, Facebook, Apple and other US internet giants, according to a top secret document obtained by the Guardian. The NSA access is part of a previously undisclosed program called Prism, which allows officials to collect material including search history, the content of emails, file transfers and live chats, the document says. Disponível em: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em: 21 jun. 2022. É preciso lembrar que nos Estados Unidos da América o tema da proteção de dados privados tem como base normativa fundamental a Quarta Emenda da sua Constituição – que trata justamente do Direito Fundamental à Privacidade – que se viu ampliada para além da privacidade em termos de espaços físicos e de interpretação jurisprudencial, dentre outros, a partir dos casos *Griswold vs. Connecticut*, de 1965*; Katz vs. United States*, de 1967; *United States vs. Antoine Jones*, de 23/01/2012, julgados pela Suprema Corte deste país. Disponível em: https://supreme.justia.com/cases/federal/us/381/479/. Acesso em: 14 abr. 2022. Disponível em: https://supreme.justia.com/cases/federal/us/389/347/. Acesso em: 14 abr. 2021. Ver igualmente o trabalho de MCNEIL, Sonia. Privacy and the modern grid. **Harvard Journal of Law & Technology.** v. 25, n.1, 2011. Em termos históricos ver também o texto classico de WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, vol. 4, nº 5., dez. 1890, pp.193-220. Disponível em: https://www.justice.gov/sites/default/files/osg/briefs/2011/01/01/2010-1259.mer.aa.pdf. Acesso em: 14 jun. 2022.

[20] Podemos citar aqui, como iniciativas inovadoras na proteção de dados privados, o *California Consumer Privacy Act (CCPA)*. Disponível em: https://oag.ca.gov/privacy/ccpa. Acesso em: 14 abr. 2022; e a *New York Stop Hacks and Improve Electronic Data Security Act (NY SHIELD)*. Disponível em: https://legislation.nysenate.gov/pdf/bills/2019/S5575B. Acesso em: 14 abr. 2022.

[21] FEDERAL TRADE COMISSION. **Protecting consumer privacy in an era of rapid change: recommendation for businesses and policymakers**, 2012. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. Acesso em: 14 abr. 2021. Por certo que existem outras agências que também tratam de proteção de dados, mas de forma setorializada, como por exemplo: *(i) Federal Communications Commission (FCC); (ii) Department of Health and Human Services (HHS); (iii) Consumer Financial Protection Bureau (CFPB); (iv) Securities and Exchange Commission (SEC)*.

[22] Ver matéria no site: https://www.nytimes.com/2020/10/06/technology/congress-big-tech-monopoly-power.html. Acesso em: 16 jun. 2022. As matérias jornalísticas dão conta de que só a Google tem o monopólio de 92% das ferramentas de pesquisas na internet, o que lhe dá condição de monopólio absoluto destes serviços, com todas suas implicações comerciais e de acesso a dados pessoais os mais distintos, pagando a

Na América Latina, a Argentina, já em 2002, obteve a aprovação europeia para receber dados pessoais de sua comunidade, tendo previsto na Constituição a proteção da dados pessoais, contando ainda com a regulamentação da Lei de Proteção de Dados Pessoais – LPDP – (nº 25.326/2000), e o Decreto Regulamentar nº 1.558/2001, e o fez tendo como base as normativas da Europa, ampliando-as por conta de ter contemplado também a proteção de dados das pessoas jurídicas.

Da mesma forma, o Uruguai regulamentou o tema, tendo sido considerado em 2010 como detentor de normas protetivas de dados adequadas para receber dados da União Europeia, a despeito de sua Constituição não prever o direito a esta proteção. O país reconheceu a proteção de dados privados como fundamental na Lei nº 18.331/2008, e por sua regulamentação através do Decreto nº 414/2009.

Também o Chile previu em Constituição o direito à vida privada, sendo que em 1999 aprovou a Lei nº 19.628, regulamentando de forma detalhada o disposto na Carta Política a este título, assim como editou o Decreto nº 779/2000, aprimorando ainda mais a tutela.[23] Já no ano de 2018 foi modificado o Art. 19, nº 4 da Constituição, justamente para constitucionalizar o direito à proteção de dados pessoais, incorporando-o ao catálogo de Direitos Fundamentais, encontrando-se o parlamento chileno discutindo mudanças nesta legislação.

O Peru, em 2011, aprovou legislação própria sobre proteção de dados (Lei nº 29.773), atendendo a tutela já existente que a Constituição dava a tais bens jurídicos, regulamentando-a pelo Decreto Supremo nº 003-2013-JUS. Da mesma maneira, o México, em 05 de julho de 2010, aprovou sua lei de proteção de dados pessoais, com o correspondente regulamento aprovado em dezembro de 2011. E a Colômbia seguiu o mesmo caminho, aprovando, em 2012, sua Lei (nº 1.581) de Proteção de Dados, regulamentada pelo Decreto Nacional nº 1.337/2013, e pelo Decreto nº 1.081/2015.[24] Todos estes dispositivos muito semelhantes às diretivas da União Europeia.

Cumpre agora avaliar como está posto o debate no Brasil sobre o tratamento da proteção de dados em face, em especial, da persecução penal, o que será feito adiante.

2. A PROTEÇÃO DE DADOS ENQUANTO DIREITO FUNDAMENTAL NO BRASIL

Falar de proteção de dados remete – como já referido – aos direitos fundamentais

Apple bilhões de dólares por ano para que esta mantenha a sua plataforma de busca como padrão em seus aparelhos – por certo implicando algum tipo de compartilhamento de dados – tudo a ser investigado pelo Congresso. Ver também a reportagem publicada no site da NBC News: https://www.nbcnews.com/tech/tech-news/big-tech-congress-squared-frustration-was-palpable-rcna507. Acesso em: 16 jun. 2022.

[23] Até pelo fato do Chile não tomar como referência expressa as normativas europeias para tratar do tema de proteção de dados em seu território, há várias criticas sobre alguns déficits destes marcos normativos, dentre os quais o silêncio sobre: (i) a relação direta entre a coleta e a utilização dos dados (princípio da finalidade); (ii) clareza sobre o responsável pelos dados privados; (iii) informação a ser dada para o processamento dos dados; (iv) sanções em caso de infração; (v) previsão sobre a autoridade de controle de proteção de dados. Ver no ponto o texto de CORTÉS, Raúl Arrieta. **El nuveo entorno regulatorio de la protección de datos personales en Chile**. Disponível em: https://iapp.org/news/a/el-nuevo-entorno-regulatorio-de-la-proteccion-de-datos-personales-en-chile/. Acesso em: 14 jun. 2022.

[24] COLÔMBIA. **Lei nº 1.581/2012.** Disponível em: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981. Acesso em: 14 abr. 2021.

REVISTA NOVOS ESTUDOS JURÍDICOS - ELETRÔNICA, VOL. 28 - N. 1 - JAN-ABR 2023
Disponível em: periodicos.univali.br
DOI: https//:doi.org/10.14210/nej.v28n1.p71-93

da pessoa humana, em especial relacionados com a intimidade e privacidade, e neste ponto, as reflexões de Robert Alexy precisam ser chamadas à colação, muito particularmente quando menciona em sua obra, Teoria dos Direitos Fundamentais, a *Teoria das Esferas*, pela qual é possível separar três esferas com decrescente intensidade de proteção dos sistemas jurídicos contemporâneos destes direitos, quais sejam: (i) **a esfera mais interna** (âmbito último intangível da liberdade humana), caracterizando-se por ser o núcleo mais íntimo e, conforme interpretação do Tribunal Constitucional alemão, campo absolutamente protegido da organização da vida privada, compreendendo os assuntos mais secretos que não devem chegar ao conhecimento dos outros devido a sua natureza extremamente reservada; (ii) a **esfera privada ampla**, que não pertença à esfera mais interna, incluindo assuntos que o indivíduo leva ao conhecimento de outra pessoa de sua confiança, ficando excluído o resto da comunidade; (iii) e a **esfera social**, que engloba tudo o que não for incluído na esfera privada ampla.[25]

Com o objetivo de encontrar esse âmbito mais íntimo e interno do indivíduo, bastaria indagar se existe comportamento de uma pessoa que, em nenhum aspecto, refira-se ou afete a esfera de outras, ou os interesses da vida em comunidade. Assim, determinadas situações e formas de comportamento conduziriam a prioridade absoluta do *princípio da liberdade negativa,* conjuntamente com o da dignidade da pessoa, frente a quaisquer princípios opostos concebíveis.

A Constituição Federal do Brasil, em seu Art. 5º, X, estabelece como princípio fundamental da República que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, *assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*. A reforçar tal disposição, recentemente foi aprovada a Emenda Constitucional nº 115, de 10/02/2022, que incluiu a proteção de dados pessoais, inclusive os disponíveis em meios digitais, na lista das garantias individuais da Constituição Federal.[26]

Ao mesmo tempo, o texto constitucional igualmente prevê, em seu Art. 5º, XXXV, o princípio da inafastabilidade do controle judicial; e no Art. 102, I, *a*, II, *a* e *b*, III, *a*, *b* e *c*, e Art. 103, § 2º, o princípio da constitucionalidade dos atos estatais ao dispor sobre os mecanismos assecuratórios da ordem normativa e seus remédios/instrumentos protetivos.

Por conta disto, temos que ter em conta a necessária leitura sistemática do ordenamento jurídico pátrio.[27] Ou seja, aqueles dois campos regulatórios reclamam sempre integração racional e ponderada dos bens jurídicos e interesses tutelados, daí porque – e já adiantando um pouco nossas percepções sobre o objeto proposto neste trabalho – direitos fundamentais individuais personalíssimos não podem configurar obstáculo impeditivo de acesso à informação qualificado, por exemplo, em face de investigações sobre cometimento de violações de normas cogentes. Vai na mesma direção o trabalho de Paulo José da Costa Jr., ao dizer que:

> Não pode o princípio la vie privée doi être murée ser interpretado como se, em torno da esfera privada a ser protegida, devesse ser erguida verdadeira

[25] ALEXY, Robert. **Teoria dos Direitos Fundamentais**. São Paulo: Atlas, 2010. p. 119.

[26] Em face disto, o art. 5º, da Constituição Federal, conta com o inciso LXXIX, que diz: *é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais*. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=515&pagina=2&data=11/02/2022. Acesso em: 29 set. 2022.

[27] A partir de CANARIS, Wilhelm Canaris. **Pensamento sistemático e conceito de sistema na ciência do direito**. Lisboa: Fundação Calouste Gulbenkian, 1996. p. 83.

REVISTA NOVOS ESTUDOS JURÍDICOS - ELETRÔNICA, VOL. 28 - N. 1 - JAN-ABR 2023
Disponível em: periodicos.univali.br
DOI: https//:doi.org/10.14210/nej.v28n1.p71-93

> muralha. Pelo contrário, os limites da proteção legal deverão dispor de suficiente elasticidade. O homem, enquanto individuo que integra a coletividade, precisa aceitar delimitações que lhe são impostas pelas exigências da vida em comum. E as delimitações de sua esfera privada deverão ser toleradas tanto pelas necessidades impostas pelo Estado, quanto pelas esferas pessoais dos demais concidadãos, que poderão perfeitamente conflitar ou penetrar por ela.
> Hipóteses se configuram em que o interesse do individuo é superado pelo interesse publico, justificando-se o sacrifício da intimidade.[28]

Por mais que a norma constitucional – e o sistema jurídico como um todo – estabeleça catálogos de direitos e garantias constitucionais como autoaplicáveis, e disto não se tem dúvidas, o fenômeno de efetivação concretizante destes sempre contará com graus/medidas passíveis de mensuração, e estas, definitivamente não estão dadas de modo absoluto pela Carta Política, demandando do intérprete/aplicador atribuição de sentido racional e material às suas reivindicações, caso por caso (que inclusive pode tratar de interesse coletivo, difuso ou individual homogêneo), levando em conta o universo de variáveis que convergem a ele.

O Novo Código Civil brasileiro regulamentou ainda mais o tema sob comento, destacando, dentre outras coisas: (a) que toda a pessoa tem direito ao nome, nele compreendidos o prenome e o sobrenome (Art. 16); (b) que, salvo se autorizadas, *ou se necessárias à administração da justiça*, ou manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização de imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se destinarem a fins comerciais (Art. 20); (c) ao fato de que a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma (Art. 21).

Em outras palavras, há determinadas qualidades que caracterizam a dignidade da pessoa, dentre elas, o respeito dos concidadãos (honra subjetiva e objetiva), o bom nome, a imagem e a reputação, e por tal razão devem ser preservadas.[29] Pérez Luño lembra, neste particular, que se tratavam destas questões como o direito das pessoas à fama e reputação, bem como direito à tranquilidade do espírito e à solidão.[30]

O direito de privacidade, entretanto, não se confunde com o de intimidade, representando este o núcleo mais reservado e indevassável da vida de determinada pessoa, em nada interessando à opinião pública o que faz ou deixa de fazer, pensar, sentir, fruir, etc., desde que não interferindo de forma invasiva na vida de outrem, e que não represente risco/perigo, atual ou iminente, à ordem jurídica e segurança pública.[31]

---

[28] COSTA JUNIOR, Paulo José da. **O Direito de estar só – tutela penal da intimidade**. São Paulo: Revista dos Tribunais, 2007. p. 51.

[29] CARVALHO, Márcia Haidée Porto de. **A defesa da honra e o direito à informação**. Florianópolis: Letras Contemporâneas, 2002. p. 94.

[30] LUÑO, Antonio Henrique Pérez. **Derechos Humanos, Estado de Derecho y Constitución**. Madrid: Tecnos Ltda, 1999. p. 335.

[31] No Brasil ver os textos já clássicos de PONTES DE MIRANDA, Francisco Cavalcanti. **Tratado de Direito Privado. Direito de Personalidade. Direito de Família.** Rio de Janeiro: Borsoi, 1955; GOMES, Orlando. **Introdução ao Direito Civil**. Rio de Janeiro: Forense, 2000; FRANÇA, Rubens Limongi. **Instituições de Direito Civil**. São Paulo: Saraiva, 1999.

Disponível em: periodicos.univali.br
DOI: https//:doi.org/10.14210/nej.v28n1.p71-93

A nova legislação sobre proteção de dados no Brasil, Lei nº 13.709/2018, que versa sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, avançou mais nos níveis de proteção destes bens sobre os quais estamos tratando, atribuindo várias responsabilidades aos gestores e usuários de dados.

Em seu Art. 4º, inciso III, a mesma norma faz referência ao acesso a dados 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, evidenciando a preocupação acertada com o enfrentamento da criminalidade que, muitas vezes, se oculta em situações de aparente legalidade ou através de estratagemas complexos e sofisticados, como a lavagem de dinheiro, gestão fraudulenta e evasão de dívidas.

Registre-se que o tratamento de dados pessoais previsto neste inciso 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...".[32] 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, matéria a ser aferida pelo devido processo legal e decisão judicial.[33]

Recentemente, o Supremo Tribunal Federal (STF), no julgamento das Ações Declaratórias de Inconstitucionalidade nº 6.387, 6.388, 6.389, 6.390 e 6.393, reconheceu a proteção de dados pessoais como categoria autônoma no catálogo de direitos fundamentais, com conteúdo independente do direito ao sigilo de informações, o que se projeta para o âmbito dos critérios de identificação da licitude da prova produzida em investigações criminais.[34] E mais, ratificou a Corte o entendimento de que configura decorrência dos direitos da personalidade o respeito à privacidade e à autodeterminação informativa, eis que positivados no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.[35]

Entendeu a Corte que a relativização da proteção constitucional referida somente

---

[32] BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD), Art. 4º, § 1º.** Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 29 set. 2022.

[33] Por exemplo, no caso do artigo 13-B, do Código de Processo Penal brasileiro, incluído pela Lei nº 13.344/2016 (Lei do Tráfico de Pessoas), nomeadamente em seu § 4º, temos delicada, mas necessária, cláusula de quebra da reserva de jurisdição para a requisição, às empresas prestadoras de serviço de telecomunicações, de informações sobre aparelhos que utilizam antena de torres de celular que permitam a localização da vítima ou dos suspeitos de delito em curso, quando não houver manifestação judicial no prazo de 12 horas a contar do pedido para tal do Ministério Público ou Delegado de Polícia.

[34] Estas ADIs foram interpostas contra a Medida Provisória nº 954/2020, que dispôs sobre o compartilhamento de dados cadastrais de usuários por prestadores de serviço de telecomunicações com o IBGE, durante a emergência sanitária da COVID-19. Maiores informações no site do STF: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902. Acesso em: 06 out. 2022.

[35] Em face disto conclui a decisão que: "ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não oferece condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. Desatende, assim, a garantia do devido processo legal (art. 5º, LIV, da Lei Maior), em sua dimensão substantiva".

pode se dar em caráter excepcional, condicionado ao atendimento dos seguintes critérios: (i) finalidade e amplitude específicas; (ii) acesso permitido na extensão mínima comprovadamente necessária ao atendimento do objetivo estabelecido; (iii) e adoção de procedimentos de segurança adequados para prevenção de danos, como vazamentos acidentais e utilização indevida.

E tal posição jurisdicional ganha ainda mais relevo quando sabemos que, na persecução penal, a mineração de dados, por exemplo, constitui ferramenta de grande relevância na investigação de crimes de alta complexidade, praticados por organizações criminosas. E ainda outras formas de investigação penal – e produção de prova – podem ser avaliadas a partir dos elementos trazidos até aqui, o que se passa a fazer.

3. A PERSECUÇÃO PENAL E A TUTELA DE DADOS

Ressalta-se que, historicamente, o poder requisitório dos órgãos de persecução penal encontra fundamento, de um lado, no sistema jurídico nacional, e também na chamada teoria dos poderes implícitos[36], destacando-se, nomeadamente, as normas específicas autorizadoras de acesso e coleta de dados e informações voltadas a investigação e responsabilização penal, inclusive de modo direto – independentemente de autorização judicial, como as contidas na lei de lavagem de dinheiro, do crime organizado e do tráfico de pessoas.[37]

Ou seja, desde o inquérito policial e seus meios de investigação, procura-se, na apuração penal, elementos informativos os mais diversos possíveis de indicar fontes de prova associados ao suposto fato penalmente típico, ilícito, culpável e punível, o que se estende para o processo penal judicializado (aí já com os meios de prova constituídos dialeticamente entre todos os envolvidos), até a decisão final transitada em julgado. Para tanto, vale-se o sistema jurídico nacional de meios e procedimentos técnicos previamente regulados em lei (oitiva de pessoas, monitoramentos, interceptações, infiltrações, vigilâncias, buscas e apreensões), de forma exemplificativa para as investigações policiais, e de modo mais exaustivo a produção da prova no processo penal.

Em termos específicos de dados pessoais, interessante notar o que tem ocorrido com o uso da imagem na seara penal no Brasil, e a forma deficitária com que a legislação nacional tem regulado a matéria, considerando que o reconhecimento pessoal é cada vez mais fundamental neste âmbito, sendo, por vezes, a única possível. Por outro lado, as tecnologias têm sido importantes na formatação desta prova, desde os vetustos álbuns de fotos de investigados, réus e condenados, das delegacias de polícia brasileiras, até a

[36] Entenda-se como tal a ideia de que, quando o sistema normativo outorga competência explícita a determinado órgão estatal, pode-se interpretar, a partir de critérios e contextos de razoabilidade e proporcionalidade, que a esse mesmo órgão tenham sido dados os meios necessários para a efetiva e completa realização dos fins atribuídos. Ver no ponto a pesquisa de HODUN, Milozs. **Doctrine of implied powers as a judicial tool to build federal polities – comparative study on the doctrine of implied power in the European Union and the United States of America**. Islândia: Reykjavik University, 2015. Disponível em: https://opinvisindi.is/bitstream/handle/20.500.11815/2479/Doctrine%20of%20implied%20powers%20as%20a%20judicial....pdf?sequence=1&isAllowed=y. Acesso em: 06 out. 2022.

[37] É dever da autoridade policial coletar informações e dados sobre o evento criminoso investigado, nos termos do art. 6º, do CPP. Para além disto, em determinadas situações, tais coletas podem se dar sem autorização judicial prévia, consoante nas disposições expressas: (i) do artigo 17-B, da Lei nº 9.613/1998, incluído pela Lei nº 12.683/2012; (ii) do artigo 15, da Lei nº 12.850/2013; (iii) e do artigo 13-A, do CPP, incluído pela Lei nº 13.344/2016.

captação de imagens feitas por câmeras de vídeo e monitoramento privadas e públicas.[38]

Mas quais os critérios e limites de utilização deste dado informacional imagético na esfera penal e processual penal? Esta pergunta é importante na medida em que outros países com mais dados sobre este tema do que o Brasil, como os EUA, em pesquisa tópica, tem evidenciado que a cada dez condenações de inocentes, sete deveram-se a reconhecimento falso de imagem.[39]

O CPP, em seu Art. 226, estabelece forma adequada para se dar o reconhecimento de pessoa, indicando procedimentos próprios[40], havendo inclusive a possibilidade de que isto ocorra por videoconferência, nos termos do Art. 185, § 8º, do mesmo estatuto[41], sendo que os Tribunais têm minimizado a importância desta modalidade de prova quando houver outros elementos que possam fundamentar o veredito.

O STF, em 22/02/2022, absolveu réu condenado pelo crime de roubo tendo como prova tão somente o reconhecimento fotográfico feito, inicialmente, por WhatsApp. O órgão colegiado entendeu que o reconhecimento fotográfico realizado na fase do inquérito policial, para fins de gerar édito condenatório, deve estar lastreado em outros elementos de prova que indiquem com segurança a autoria do fato, o que não ocorreu no caso.[42] Ou seja, a tecnologia pode e deve ser utilizada também para fins de segurança pública e persecução penal, todavia, isto deve se dar atentando-se para os direitos e garantias fundamentais, dentre eles o devido processo legal, sob pena de comprometer-se a fiabilidade da prova produzida ilicitamente.

Também o Superior Tribunal de Justiça (STJ), depois de sustentar que o reconhecimento por fotografia é válido e suficiente para fundamentar a condenação,

---

[38] Interessante estudo da Defensoria Pública do Rio de Janeiro, no ano de 2021, deu conta de que o tempo médio perdido nas prisões do Estado por conta de reconhecimento fotográfico equivocado em delegacias foi de um ano e dois meses, sendo que nos 242 casos analisados (envolvendo 342 pessoas), 30% dos réus foram absolvidos. Entre eles, mais de 80% (54 pessoas) tiveram sua prisão preventiva decretada e há quem tenha passado quase seis anos encarcerado preventivamente até a absolvição. DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO. **O reconhecimento fotográfico nos processos criminais no Rio de Janeiro.** 04 mai. 2022. Disponível em: https://static.poder360.com.br/2022/05/reconhecimento-fotografico-processos-criminais-mai-2022.pdf. Acesso em: 03 out. 2022.

[39] Dados colhidos pela pesquisa pelo *Innocence Project, conforme dados divulgados pelo site:* https://innocenceproject.org/eyewitness-identification-reform/. *Acesso em: 11 out. 2022. Refere a pesquisa que: "Mistaken eyewitness identifications contributed to approximately 69% of the more than 375 wrongful convictions in the United States overturned by post-conviction DNA evidence".*

[40] Sendo imperioso que a pessoa que tiver de fazer o reconhecimento descreva aquela que deva ser reconhecida; e que o suspeito seja colocado, se possível, ao lado de outras que com ele tiverem qualquer semelhança, convidando-se quem tiver de fazer o reconhecimento a apontá-la.

[41] Lembrando que tal possibilidade pode ocorrer nos termos do § 2º, do mesmo artigo (excepcionalmente, o juiz, por decisão fundamentada, de ofício ou a requerimento das partes, poderá realizar o interrogatório do réu preso por sistema de videoconferência ou outro recurso tecnológico de transmissão de sons e imagens em tempo real), desde que a medida seja necessária para atender uma das finalidades descritas nos incisos I a IV, deste parágrafo.

[42] Recurso em Habeas Corpus nº 206846, Segunda Turma do STF, Relator Min. Gilmar Mendes, julgado em 22/02/2022, por maioria. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=482230&ori=1. Acesso em: 03 out. 2022. O caso tratava de roubo e, segundo a narrativa dos autos, uma hora após o crime o recorrente foi abordado por policiais que o fotografaram, enviando a imagem por WhatsApp para outro policial, que estava com a vítima, a qual, por sua vez, teria reconhecido o suspeito.

desde que repetido em juízo, com contraditório e ampla defesa[43], mais recentemente decidiu, por sua 5ª Turma, absolver indivíduo condenado com base no reconhecimento feito por meio de foto em sede policial. No ponto, o Tribunal expressamente referiu que:

> O reconhecimento de pessoa, presencialmente ou por fotografia, realizado na fase do inquérito policial, apenas é apto, para identificar o réu e fixar a autoria delitiva, quando observadas as formalidades previstas no art. 226 do Código de Processo Penal e quando corroborado por outras provas colhidas na fase judicial, sob o crivo do contraditório e da ampla defesa.[44]

Em outra decisão paradigmática mais antiga o STJ já reconhecia, inclusive, que são comuns as falhas e os equívocos que podem advir da memória humana e da capacidade de armazenamento de informações. O valor probatório do reconhecimento, portanto, possui considerável grau de subjetivismo, a potencializar falhas e distorções do ato e, consequentemente, causar erros judiciários de efeitos deletérios e muitas vezes irreversíveis.[45]

A mesma lógica, entretanto, e de modo equivocado, não tem sido aplicada para fundamentar decreto de prisão preventiva, haja vista que esta reclama apenas indícios suficientes de autoria do crime, assim como de perigo gerado pelo estado de liberdade do imputado, nos termos do Art. 312 do CPP. Nestes casos, o STJ já denegou ordem de habeas corpus impetrado por indivíduo acusado de latrocínio tentado, cuja preventiva fora determinada após reconhecimento feito por fotografia pelas vítimas. A questão é que esta fotografia seria datada de 2013, enquanto o crime teria ocorrido em 2020, entendendo o relator do caso, Min. Antonio Saldanha Palheiro, que a imagem identificada como sendo do autor atendeu os ditames do Art. 226 do CPP, tendo o conjunto de outras provas evidenciado indícios suficientes para autorizar a segregação extraordinária.[46]

E por que isto é importante debater? Pelo simples fato de existir alto índice de condenados nomeadamente por conta dos chamados *catálogos de suspeitos* (acervo de

---

[43] Como na decisão indicada no Jurisprudência em teses, nº 105, de 2018. Disponível em: www.stj.jus.br/internet_docs/jurisprudencia/jurisprudenciaemteses/Jurisprudência%20em%20teses%20105%20-%20Provas%20no%20Processo%20Penal%20-%20I.pdf. Acesso em: 11 out. 2022.

[44] Habeas Corpus nº 652284, Relator Min. Reynaldo Soares da Fonseca, julgado em 27/04/2021, a unanimidade, Dje 03/05/2021. Ainda teve oportunidade o julgado de destacar outros elementos importantes destes cenários que são: "Tampouco o reconhecimento pessoal em sede policial pode ser reputado confiável se, além de ter sido efetuado um ano depois do evento com a apresentação apenas do réu, a descrição do delito demonstra que ele durou poucos minutos, que a vítima não reteve características marcantes da fisionomia ou da compleição física do réu e teve suas lembranças influenciadas tanto pelo decurso do tempo quanto pelo trauma que afirma ter sofrido com o assalto. Tendo a autoria do delito sido estabelecida com base unicamente em questionável reconhecimento fotográfico e pessoal feito pela vítima, deve o réu ser absolvido". Da mesma forma, a 6ª Turma do STJ assim decidiu, nos autos do HC nº 598.886, Rel. Min. Rogério Schietti Cruz, DJe de 18/12/2020.

[45] HC nº 598.886/SC, julgado pela 6ª Turma do STJ, relator Min. Rogério Schietti Cruz, em 27/10/2020, Dje de 18/12/2020. Aduz a Corte ainda que: "O reconhecimento de pessoa por meio fotográfico é ainda mais problemático, máxime quando se realiza por simples exibição ao reconhecedor de fotos do conjecturado suspeito extraídas de álbuns policiais ou de redes sociais, já previamente selecionadas pela autoridade policial. E, mesmo quando se procura seguir, com adaptações, o procedimento indicado no Código de Processo Penal para o reconhecimento presencial, não há como ignorar que o caráter estático, a qualidade da foto, a ausência de expressões e trejeitos corporais e a quase sempre visualização apenas do busto do suspeito podem comprometer a idoneidade e a confiabilidade do ato". O mesmo ocorre no HC nº 768881/RJ, 6ª Turma do STJ, relator Min. Antonio Saldanha Palheiro, julgado em 04/10/2022.

[46] Autos do HC nº 651.595, julgado pela 6ª Turma do STJ, Rel. Min. Antonio Saldanha Palheiro, julgado em 17/08/2021, Dje 25/08/2021.

fotografias de pessoas retiradas, na grande maioria, de redes sociais, ou compondo álbum de fotos físicas antigas de delegacias de polícia), conforme demonstra a pesquisa levada a cabo pelo Colégio Nacional dos Defensores Públicos Gerais e pela Defensoria Pública do Rio de Janeiro, no período de 2012 a 2020, avaliando aproximadamente 90 (noventa) prisões levada a efeito, fundamentalmente, por meio destes tipos de reconhecimento fotográfico.[47]

Saindo desta experiência mais antiga, podemos passar para os casos de utilização nas investigações penais da chamada técnica *geo-fencing*, entendida como medida que permite a anunciantes e empresas atingir usuários da internet a partir de *cercas virtuais*, com parâmetros como geolocalização, termos de busca ou histórico de navegação, entre outros. No campo específico da investigação criminal, ela pode identificar quem esteve no local de um crime durante determinado horário, a partir dos dados de celulares conectados à internet.[48]

Aliás, em termos de acesso à agenda telefônica e registro de chamadas sem autorização judicial, no Brasil, o STF está discutindo a matéria no âmbito da Repercussão Geral nº 977, oriunda do Recurso Extraordinário com Agravo nº 1042075/RJ, relatoria do Min. Dias Toffoli. O relator propôs em seu voto dar provimento ao recurso, apresentando a seguinte proposta de tese: *É lícita a prova obtida pela autoridade policial, sem autorização judicial, mediante acesso a registro telefônico ou agenda de contatos de celular apreendido ato contínuo no local do crime atribuído ao acusado, não configurando esse acesso ofensa ao sigilo das comunicações, à intimidade ou à privacidade do indivíduo (CF, art. 5º, incisos X e XII)*.

Entretanto, os Ministros Gilmar Mendes e Edson Fachin propuseram negar provimento ao recurso, constituindo a seguinte tese: *O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos (CF, art. 5º, X e XX)*.[49]

Mas temos o caso Marielle Franco, no Brasil – vereadora do Rio de Janeiro que foi assassinada a tiros, junto com seu motorista, em 14/03/2018 – que até hoje não está totalmente solucionado em termos do mandante do crime, e tem sido paradigmático no tratamento jurisdicional destas questões, isto porque o Ministério Público do caso solicitou ao Judiciário fluminense – que deferiu – que o Google fornecesse: (i) os dados estáticos dos *IPs* ou *Device IDs* de usuários que tenham aberto o Google Maps, ou Waze, entre 10 e 14 de março de 2018, para pesquisar o endereço de rua em que a vereadora Marielle estaria participando de evento na noite em que foi executada; (ii) a identificação de quem, no mesmo período, pesquisou termos relacionados ao nome da vereadora e sua

[47] CONDEGE. **Relatórios indicam prisões injustas após reconhecimento fotográfico.** 19 abr. 2021. Disponível em: http://condege.org.br/arquivos/1029. Acesso em: 11 out. 2022.

[48] HARVARD LAW REVIEW. **Geofence warrants and the Fourth Amendment**. 134 Harvard Law Review nº 2508, mai. 2021. Disponível em: https://harvardlawreview.org/2021/05/geofence-warrants-and-the-fourth-amendment/. Acesso em: 03 out. 2022. Ver também matéria no U.S. News, intitulada *Cellphone dragnet used to find bank robbery suspect was unconstitutional, judge says*. 07 jul. 2022. Disponível em: https://www.nbcnews.com/news/us-news/geofence-warrants-help-police-find-suspects-using-google-ruling-could-n1291098. Acesso em: 03 out. 2022.

[49] Conforme informações prestadas no site do STF. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898. Acesso em: 04 out. 2022.

agenda. Em outros pedidos igualmente deferidos pelo magistrado, foram solicitadas informações e acessos ainda mais privados como: mídias (fotos e vídeos), e-mails, agenda, agenda de contatos, aplicativos instalados, backups contidos nos serviços de driver, mensagens instantâneas.[50]

O Google, em defesa, apontou que a medida atingiria número indeterminado de pessoas, pois abrangeria locais de amplo acesso público, fazendo referências ainda a óbices tecnológicos capazes de gerar resultados com baixa confiabilidade, podendo indicar usuários que não estiveram no local, ou mesmo excluir pessoas que por ali passaram, sustentando a configuração, em tal expediente, de pesca probatória (*fishing expedition*). [51] Além do que, sustentou que a quebra do sigilo de dados tem que obrigatoriamente indicar as pessoas suspeitas que serão investigadas e o objeto da medida invasiva, exigência do Art. 5º, X, XII, e 93, IX, ambos da CF/88, regulamentados pelo Art. 2º da Lei nº 9.296/96, e pela Resolução CNJ nº 59/2008, combinados com o Art. 22 do Marco Civil da Internet (Lei nº 12.965/14)[52], e Art. 11, do Decreto-Federal nº 8.771/2016.

O STJ manteve o deferimento das medidas deferidas pelo judiciário do Rio de Janeiro, em vários recursos interpostos e decididos por suas turmas criminais, até chegar a Terceira Seção, que ultimou o entendimento da matéria, ratificando a decisão tomada no primeiro grau.[53]

O argumento do relator Min. Rogério Schietti, no caso, é que a Corte deveria fazer distinção entre os **dados** (estáticos) que a investigação criminal queria acessar, entendidos como conjunto de fatos registrados no formato de declarações textuais, de modo a permitir seu compartilhamento ou análise por conjunto indefinido de observadores, a partir do qual pode ser obtida alguma informação dirigida a determinado propósito; e **conteúdos** (dinâmicos), enquanto produto do fluxo ou das formas de comunicação, as quais se imbricam com a proteção constitucional à intimidade, tendo como objeto de tutela, de um lado, a liberdade de manifestação do pensamento, de outro, o segredo como expressão do direito à intimidade.[54]

---

[50] Como referido expressamente no Acórdão do Agravo Regimental no Recurso em Mandado de Segurança nº 64.941/RJ, 3ª Seção, relator Min. Rogério Schietti Cruz, julgado em 03/08/2021, DJe 13/08/2021, fl.06.

[51] Modo geral a pescaria probatória é tida como a procura especulativa, no ambiente físico ou digital, sem causa provável ou mesmo de alvo definido, de elementos capazes de atribuir responsabilidade penal. Para melhor abordagem do tema ver o trabalho: ROSA, Alexandre Morais da; DA SILVA, Viviane Ghizoni; SILVA, Philipe Benoni Melo e. ***Fishing Expedition* e encontro fortuito na busca e na apreensão: um dilema oculto do processo penal.** Florianópolis: EMais, 2022.

[52] Lembrando que o Marco Civil da Internet não prevê, dentre os requisitos que estabelece para a quebra de sigilo, que a decisão judicial especifique previamente as pessoas objeto da investigação, ou que a prova da infração (ou da autoria) possa ser realizada facilmente por outros meios (arts. 22 e 23).

[53] Agr. Reg. RMS nº 64.941/RJ, acima citado. Veja-se que, a partir dai, esta Corte já deferiu medidas similares a vários outros casos menos complexos: (i) uso do *geo-fencing* para apurar roubo e estupro de uma vítima (RMS 66.668); (ii) roubo de joias e bens avaliados em R$1 milhão efetuado em joalheria (RMS 66.563); (iii) 84 furtos de "airbags" cometidos desde 2018, em especial de veículos Honda/Civic (RMS 65.064); (iv) sequestro seguido de homicídio de criança de nove anos de idade (RMS 65.412); (v) prática de associação para o tráfico e homicídios (RMS 61.419); (vi) homicídio qualificado (RMS 64.603); (vii) furtos em imóvel residencial no qual foram subtraídas joias, bebidas e outros bens móveis (RMS 65.242).

[54] Aliás, o que vai ao encontro de decisão já tomada pelo STF, quando assentou que não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados, nos termos do HC nº 91.867/PA, Rel. Ministro Gilmar Mendes, DJe 20/9/2012. Em outra decisão o STJ também já assentava o mesmo entendimento, no sentido de que a proteção contida no artigo 5º, inciso XII, da CF/88, restringe-se ao sigilo das

REVISTA NOVOS ESTUDOS JURÍDICOS - ELETRÔNICA, VOL. 28 - N. 1 - JAN-ABR 2023
Disponível em: periodicos.univali.br
DOI: https//:doi.org/10.14210/nej.v28n1.p71-93

CONSIDERAÇÕES FINAIS

A aceleração de crescimento do crime organizado no mundo tem se mostrado inversamente proporcional à capacitação e eficiência das forças de segurança pública, o que é possível ser dessumido dos indicadores de delinquência global que temos no campo do tráfico de drogas, de armas, de pessoas, de órgãos humanos, cibercriminalidade, lavagem de dinheiro, e tantos outros.[55] Mas não é só no campo da microcriminalidade que isto ocorre; também na microcriminalidade há organização, basta observar os fenômenos das milícias, das facções de menor porte, dos crimes contra a Administração Pública em geral.

Mesmo no caso referido envolvendo a vereadora Marielle Franco, o primeiro delegado que começou a investigar o tema, Giniton Lages, reconheceu os altos níveis de profissionalismo dos executores assassinos, tanto que, ao longo do primeiro ano das investigações policiais, as equipes ouviram 230 pessoas, analisaram mais de 33 mil linhas telefônicas, e interceptaram outras 318, com ordem judicial. Desde então, outros quatro delegados passaram pela investigação, sem chegar à resposta sobre os mandantes.[56]

A despeito disto, não podemos esquecer que o direito à proteção de dados já é uma realidade no país, e ele se conecta diretamente com vários elementos, dentre os quais, nos termos do Art. 2º, IV, da Lei nº 13.709/2018, à proteção da inviolabilidade da intimidade, honra e imagem – a despeito de não se aplicar ao tratamento de dados realizado para fins exclusivos de atividades investigativas à repressão de infrações penais (Art. 4º, III, d).

Mas, de qualquer sorte, por contarem aqueles direitos com tutela constitucional, eles se impõem inclusive à persecução penal, com modulações, como demonstrou já o STF, ao reconhecer que intimidade e privacidade, enquanto garantias públicas asseguradas, não tem caráter absoluto, inexistindo no sistema jurídico brasileiro bens que se revistam desta forma, mesmo porque *razões de relevante interesse público ou exigências derivadas do princípio de convivência das liberdades legitimam, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição*.[57]

Ou seja, sob o ponto de vista da argumentação jurídica que estamos adotando

comunicações telefônicas e telemáticas, não abrangendo os dados já armazenados em dispositivos eletrônicos. (HC nº 167.720/SP, Rel. Ministro Luiz Fux, DJe 14/4/2019).

[55] E cada país tem suas particularidades no âmbito desta criminalidade, pois na Itália a criminalidade organizada é comumente identificada com a máfia ou outras organizações similares; em Portugal, está associada aos crimes contra o mercado financeiro; na Alemanha caracteriza-se basicamente pela lavagem de dinheiro e corrupção, enquanto na Espanha tem uma identidade mais acentuada com o terrorismo, conforme relato de SCHOUCAIR, João Paulo Santos; CAIRES, Luciana Matutino. Ação controlada e sua análise no combate ao crime organizado. In PAULINO, Galtiênio da Cruz *et al* (Org.). **Técnicas avançadas de investigação.** Brasília: ESMPU, 2021, p. 95.

[56] Ver excelente matéria e entrevista do Delegado no site da The Intercept Brasil. CASTRO, Carol. ENTREVISTA: 'ALGUÉM DAVA INFORMAÇÃO PRIVILEGIADA AOS CRIMINOSOS', DIZ PRIMEIRO DELEGADO DO CASO MARIELLE. **The Intercept Brasil**, 27 abr. 2022. Disponível em: https://theintercept.com/2022/04/27/entrevista-marielle-giniton-lages-alguem-dava-informacao-privilegiada/. Acesso em: 04 out. 2022. Também o livro publicado sobre o tema: LAGES, Giniton; RAMOS, Carlos. **Quem matou Marielle?** São Paulo: Matrix, 2022.

[57] MS nº 23.452/RJ, Segunda Turma, Rel. Min. Celso de Mello, DJe de 15/5/2000.

aqui, afigura-se mais do que possível, mas recomendado, no âmbito da ponderação e do balanceamento de normas em face do caso concreto, elaborar certa ***ordem hierárquica conjuntural*** entre os princípios que se encontram em tensão na casuística, tutelando assim valor importante ao sistema jurídico que é a certeza do direito; entretanto, ele não é o único que demanda realização, pois ao seu lado está o valor de caráter pragmático relativo à eficiência social da prestação jurídica, igualmente importante e cuja realização pode eventualmente mitigar a realização do ideal de completude do ordenamento – como é o caso da condição hierárquica conjuntural superior da segurança pública perseguida pela responsabilização penal.[58]

Partilha-se, no ponto, do entendimento do Min. Rogério Schietti, no sentido de que quando o:

> direito à segurança pública e à preservação e restauração da ordem pública tem algum resvalo no direito ao sigilo de dados –, nota-se a realização da proporcionalidade em suas três diretrizes essenciais. Ela é adequada, na medida em que serve como meio auxiliar na elucidação dos delitos, cuja investigação se arrasta por dois anos, sem que haja uma conclusão definitiva. É necessária, diante da gravidade e complexidade do caso e da inexistência de outros meios menos gravosos para se alcançar os legítimos fins investigativos. E, por fim, é proporcional em sentido estrito, porque a restrição aos direitos fundamentais que dela redundam não ensejam gravame as pessoas afetadas, as quais não terão seu sigilo de dados registrais publicizados, certo, ainda, se não constatada sua conexão com o fato investigado, serão descartados.[59]

Agora o STF está apreciando o tema de repercussão geral nº 1148, envolvendo controvérsia relativa aos limites e ao alcance de decisões judiciais de quebra de sigilo de dados pessoais, nas quais determinado o fornecimento de registros de acesso à internet e de IPs, circunscritos a lapso temporal demarcado, sem, contudo, a indicação de qualquer elemento concreto apto a identificar os usuários, atinente, na origem, ao mesmo caso Marielle Franco.[60] Esta decisão será paradigmática para os fins de demarcarmos com mais segurança os parâmetros que deverão ser utilizados no país para medidas judiciais desta natureza, providência necessária a compatibilizar os interesses públicos e privados envolvidos.

Até que isto se resolva, tem-se que a requisição de dados pessoais armazenados por provedores de serviços de internet pode se dar, desde que indicados os elementos previstos na Lei nº 12.965/2014, em seus Arts. 22 e 23, a saber: a) fundados indícios da ocorrência do ilícito; b) justificativa motivada da utilidade da requisição; e c) período ao qual se referem os registros, e que sua execução também se dê observados os ditames da adequação, necessidade e proporcionalidade em sentido estrito referidos.

---

[58] Como nos ensina ALEXY, Robert. **The Construction of Constitutional Rights.** In Law & ethics of Human Rights, vol. 4, issue 1. article 2. Berkeley: Berkeley Electronic Press, 2010.

[59] Agr. Reg. RMS nº 64.941/RJ, citado, p.21.

[60] A presente Repercussão Geral se constituiu a partir do Recurso Extraordinário nº 1301250/RJ, relatoria da Min. Rosa Weber, tendo como recorrente Google Brasil Internet Ltda. e Google Inc., estando concluso à relatora desde 15/09/2022, conforme site do STJ (https://portal.stf.jus.br/processos/detalhe.asp?incidente=6059876, acesso em 04/10/2022). Ao lado desta Repercussão Geral, o STF também está debatendo, no âmbito da ADI nº5.527/DF, ADPF nº403/SE, o mesmo tema da proteção de dados em face do Marco Civil da Internet – Lei nº12.965/2014.

REFERÊNCIA DAS FONTES CITADAS

ALBRECHT, Hans-Jörg. *Direito* **Penal e Periculosidade: a politica criminal entre prevenção, combate a perigos e retribuição de culpa**. In MACHADO, Marta R. de Assis e PÜSCHEL, Flavia Portella (org.). Reponsabilidade e Pena no Estado Democrático de Direito. São Paulo: FGV, 2016.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. São Paulo: Atlas, 2010.
----. **The Construction of Constitutional Rights**. In Law & ethics of Human Rights, Volume 4, Issue 1. Article 2. Berkeley: Berkeley Electronic Press, 2010.

BALDASSARRE, Antonio. **Diritti della persona e valori costituzionale**. Torino: Giappichelli, 1997.

CANARIS, Wilhelm Canaris. **Pensamento sistemático e conceito de sistema na ciência do direito**. Lisboa: Fundação Calouste Gulbenkian, 1996.

CARVALHO, Márcia Haidée Porto de. **A defesa da honra e o direito à informação**. Florianópolis: Letras Contemporâneas, 2002.

CERRINA FERONI, Ginevra e MOBIDELLI, Giuseppe. **La sicurezza: un valore superprimari**o. In Percorsi Costituzionale. V.I, n°1/2008, p.39.

COCCO, Giovanni. (a cura di). **I diversi volti della sicurezza**. Milano: Giuffrè, 2012.

CORTÉS, Raúl Arrieta. **El nuevo entorno regulatorio de la protección de datos personales en Chile**. Publicado no site https://iapp.org/news/a/el-nuevo-entorno-regulatorio-de-la-proteccion-de-datos-personales-en-chile/, acesso em 14/06/2022.

COSTA Jr., Paulo José da. **O Direito de estar só – tutela penal da intimidade**. São Paulo: Revista dos Tribunais, 2007.

FEDERAL TRADE COMISSION - FTC. **Protecting consumer privacy in an era of rapid change: recommendation for businesses and policymakers**, 2012. Acesso pelo site https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, acesso em 14/04/2021.

FRANÇA, Rubens Limongi. **Instituições de Direito Civil**. São Paulo: Saraiva, 1999.

FROSINI, Tomaso Edoardo. **Il diritto costituzionale alla sicurezza**. In Forum online di Quaderni Costituzionali, acessado pelo site: https://www.forumcostituzionale.it/wordpress/wpcontent/uploads/pre_2006/440.pdf. Acesso em: 26/05/2021.

GAZZETTA, Cristina. **Sicurezza, terrorismo e cittadinanza: la nuova legislazione francese anti-terrorismo e l'impegno Internazionale contro i cd. foreing fighters**. In Osservatório sulla normativa, anno V, n°3, 2015.

GOMES, Orlando. **Introdução ao Direito Civil**. Rio de Janeiro: Forense, 2000.

HODUN, Milozs. **Doctrine of implied powers as a judicial tool to build federal polities – comparative study on the doctrine of implied power in the European Union and the United States of America**. Islândia: Reykjavik University, 2015, acesso pelo site: https://opinvisindi.is/bitstream/handle/20.500.11815/2479/Doctrine%20of%20implied%20powers%20as%20a%20judicial....pdf?sequence=1&isAllowed=y, acesso em 06/10/2022. 12/05/2021.

LAGES, Giniton e RAMOS, Carlos. **Quem matou Marielle?** São Paulo: Matrix, 2022.

LUÑO, Antonio Henrique Pérez. **Derechos Humanos, Estado de Derecho y Constitució*n***. Madrid: Tecnos Ltda, 1999.

MCNEIL, Sonia. **Privacy and the modern grid**. In Harvard Journal of Law & Technology.V.25 n.1, 2011.
PONTES DE MIRANDA, Francisco Cavalcanti. **Tratado de Direito Privado**. Direito de Personalidade. Direito de Família. Rio de Janeiro: Borsoi, 1955.

RODOTÀ, Stefano. **Privacy, libertà, dignità**. In www.garanteprivacy.it, 2004, acesso em 20/08/2022.

ROSA, Alexandre Morais da; DA SILVA, Viviane Ghizoni, e SILVA, Philipe Benoni Melo e. ***Fishing Expedition* e encontro fortuito na busca e na apreensão – Um dilema oculto do processo penal**. Florianópolis: EMais, 2022.

RUTUOLO, Marco. **Diritto ala sicurezza e sicurezza dei diritti**. In Osservatório sulla normativa, anno III, n°2, 2013.

SCHOUCAIR, João Paulo Santos e CAIRES, Luciana Matutino. **Ação controlada e sua análise no combate ao crime organizado**. In PAULINO, Galtiênio da Cruz, e outros (Org.). Técnicas avançadas de investigação. Brasília: ESMPU, 2021.

WARREN, Samuel D. & BRANDEIS, Louis D. *The Right to Privacy*. In Harvard Law Review, vol.4, n°5. December 15, 1890.
www.stj.jus.br/internet_docs/jurisprudencia/jurisprudenciaemteses/Jurisprudência%20em%20teses%20105%20-%20Provas%20no%20Processo%20Penal%20-%20I.pdf, acesso em 11/10/2022.

Recebido em: 15/10/2022
Aprovado em: 20/02/2023