FLUXO DE DADOS, PROVA E PROCESSO PENAL

DATA FLOW, PROOF AND CRIMINAL PROCEDURE LAW

Daniela Dora Eilberg[1]
Pontifícia Universidade Católica do Rio Grande do Sul

Resumo:
A mudança paradigmática do procedimento probatório penal não deriva das propriedades da prova digital em si, mas do processamento massivo de dados, do protagonismo do setor privado em atividades tradicionalmente públicas e de competência de sujeito processual, bem como da reformulação da garantia de jurisdição em razão do caráter transnacional da prova digital. A partir do deslocamento do centro informativo do processo penal à investigação, o tratamento de dados em massa redireciona o foco da esfera privada à esfera da autodeterminação informacional, introduzindo discussões cruciais acerca do contexto da finalidade e transmissão de dados. Este artigo discute o fluxo de dados durante a investigação criminal e o procedimento probatório penal, a legitimidade do levantamento desses dados, o compartilhamento entre diferentes atores para diferentes finalidades, e o uso secundário de tais dados para a finalidade de produção probatória. A partir de revisão bibliográfica e análise jurisprudencial brasileira, o objetivo deste artigo é assentar premissas para uma dogmática de compartilhamento de dados no campo penal.
Palavras-chave:
Prova digital. Processo penal. Compartilhamento. Uso secundário. Proteção de dados.

Abstract:
The paradigmatic change in criminal evidentiary law is not an immediate outcome of the digital evidence properties itself, but from the massive processing of data, the leading role of the private sector in activities traditionally public, and the reformulation of jurisdiction due to the transnationality of digital evidence. By shifting the information center to the criminal investigation, the mass processing of data changes the focus from the private sphere to the informational self-determination sphere, introducing crucial discussions on the context of the purpose and data sharing. This article discusses the data flow during criminal investigation and procedural measures, the legitimacy of collecting such data, the data transferring and sharing between different actors for different purposes, and the secondary use of such data for criminal evidence purposes. Based on a bibliographic review and Brazilian case law analysis, the objective of this article is to establish premises for a theory on data sharing for the purposes of the criminal prevention, investigation, detection or prosecution of criminal offences.
Keywords: Digital evidence. Proof. Criminal procedure law. Data sharing. Secondary use. Data protection.

1 INTRODUÇÃO: FLUXO DE DADOS DURANTE A INVESTIGAÇÃO CRIMINAL E O PROCEDIMENTO PROBATÓRIO PENAL

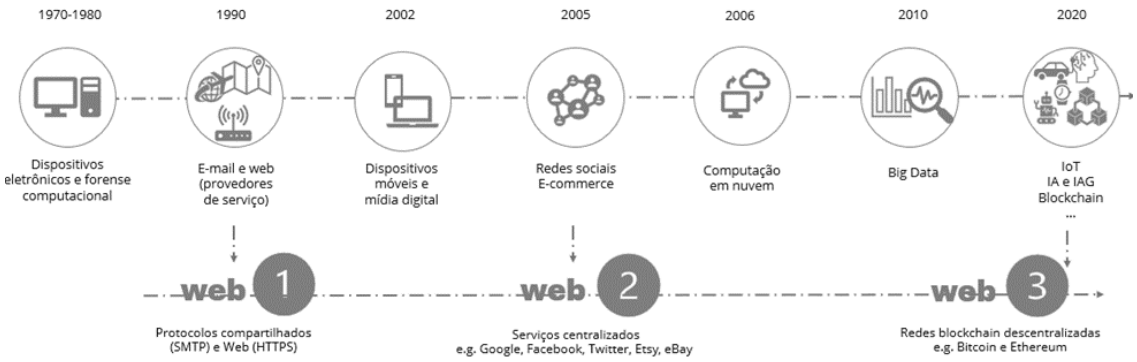
O "giro" tecnológico da investigação criminal e do procedimento probatório não deriva das propriedades da prova digital. O caráter volátil, frágil e imaterial define apenas os métodos e as ferramentas a serem utilizadas para o manejo do vestígio digital e a preservação de sua integridade e confiabilidade. Vestígios digitais utilizados para investigação criminal não são novidade restritas aos últimos anos. Se percorrermos um breve histórico de mais de sete décadas, observamos a transição das fontes tradicionais da forense digital (*e.g.* computador, laptop, celular,

[1] Doutora com Louvor e Mestra pelo Programa de Pós-Graduação em Ciências Criminais da Pontifícia Universidade Católica do Rio Grande do Sul - Bolsista CAPES. Visita Profissional na Corte Interamericana de Direitos Humanos. Especialista em Cibercrime e Prova Digital pela Universidade de Buenos Aires – UBA. Spring School Berkeley Law AI (Artificial Intelligence) Institute da University of California. Graduação em Direito com período sanduíche na Université Paris I – Panthéon-Sorbonne.

smartphone, tablet) aos novos desafios enfrentados, tais como a computação em nuvem, Internet das Coisas (*Internet of Things –IoT*), IA (Inteligência Artificial), IAG (IA Generativa), e redes descentralizadas de *Blockchain*. No entanto, os desafios e dilemas se impõem quando passamos a observar que certos marcos da transformação tecnológica começaram a provocar profundas mudanças nos métodos de investigação criminal no contexto global, principalmente no que diz respeito ao processamento e armazenamento de dados em massa, afetando específicas características da produção probatória digital.

A mudança paradigmática do sistema, portanto, está relacionado principalmente i) ao papel central que o setor privado assume no controle dos dados a serem utilizados pelas investigações; ii) à alteração do centro informativo do processo da instrução processual à investigação[2] ou às atividades securitárias, em decorrência da era digital[3] e à reformulação da garantia de jurisdição em razão do caráter transnacional da prova digital; e iii) ao deslocamento da esfera privada para o da autodeterminação informacional essencialmente por conta da era do Big Data e da algoritmização do direito e do processo (BARONA VILAR, 2021), introduzindo discussões e problemas cruciais acerca do contexto da finalidade e transmissão de dados.

Figura 1: Os marcos tecnológicos da investigação criminal e da produção probatória



Fonte: EILBERG (2024, p. 33)[4].

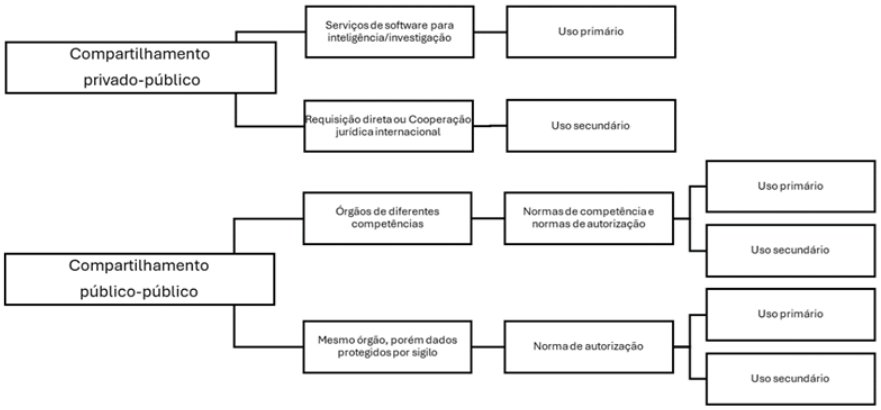
[2]Ao desenvolver como os maxiprocessos antecipam o local da resolução da lide para a investigação preliminar a partir da "produção antecipada de informação válida para julgamento antes de serem aplicáveis as garantias processuais", Antonio E. R. Santoro explora as lições de Ferrajoli sobre as características que acreditamos muito bem se adequarem não apenas aos maxiprocessos, mas a todos os demais processos que não possuem cobertura midiática massiva (2020, p. 88-90).

[3] Stanislaw Tosza explora como a natureza do capitalismo digital, que é baseada na produção massiva de dados, resulta na transformação da comunicação da era pré-internet (e-mail e mensagens instantâneas) pelo fato de os provedores de serviço coletarem cópias ou metadados que os correios não costumavam guardar com relação às cartas. (TOSZA, Stanislaw, 2023, p. 164).

[4] A imagem foi inspirada em diversas artes. Ver: a16z State of Crypto; Oxygen Forensics; Medium.

O fluxo de dados e sua transmissão em um contexto probatório brasileiro de hipermassificação (BAUDRILLARD, 2003; VIRILIO, 1999) [5] informativa evidencia as problemáticas da fusão informacional (ESTELLITA, 2022) entre órgãos de inteligência e órgãos de persecução penal, basicamente exercida através do compartilhamento de dados. [6] Essa transmissão se dá em três diferentes contextos: i) entre órgãos de setores privados e público (cujo uso será primário, isto é, dentro da finalidade que justificou a coleta, ou secundário,[7] qual seja, distinto do fim que legitimou a coleta); ii) entre órgãos do setor público com diferentes competências (e, portanto, cujo tratamento de dados possui diferente finalidade); iii) entre agentes de mesmos órgãos, porém compartilhamento automático de dados protegidos sob sigilo sem autorização prévia e com finalidade de tratamento diversa da que legitimou o seu levantamento.

Figura 2: Cenários de compartilhamento de dados no contexto penal



Fonte: EILBERG (2024, p. 34).

Na teoria geral da prova material da doutrina processual penal, a produção probatória terá suas fases distinguidas a partir da função que cada uma cumprirá nas etapas da investigação (BADARÓ; GOMES FILHO, 2007), proposição, admissão, produção, valoração (GOMES

[5] Chamaremos de hipermassificação informativa processual ao adotar ideias de Paul Virilio e Jean Baudrillard da "hipermassificação" e do "simulacro" em razão dos efeitos da internet.

[6] O art. 5º, inciso X da LGPD determina o compartilhamento de dados como uma operação de tratamento de dados de "comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados".

[7] A conceituação de "uso secundário" está diretamente relacionada ao princípio da finalidade. Nas palavras de Viktor Mayer-Schönberger e Kenneth Cukier "*The system takes information generated for one purpose and reuses it for another – in other words, the data moves from primary to secondary uses. This makes it much more valuable over time. (...) [The] sets of data find secondary uses – and new value – when they're applied to a completely different purpose. (...) In short, data's value needs to be considered in terms of all the possible ways it can be employed in the future*" (2014, p. 103). Daniel Solove buscou realizar uma taxonomia da privacidade, em que classificou quatro grupos de atividades prejudiciais: a coleta, o processamento, a disseminação e a invasão dos dados. O "uso secundário" seria um tipo de processamento de dados (2006, p. 519).

FILHO, 2008). Do ponto de vista técnico, a configuração da prova digital possui elementos tecnológicos que demandam a existência de protocolos que garantam integridade, autenticidade e auditabilidade "em contexto de apreensão, preservação, exame e emprego probatório desses elementos" (PRADO, 2008, p. 316-317), assim como materialização da proteção de dados nesses protocolos de preservação dos vestígios digitais. É no contexto de garantia dessa integridade e autenticidade "dos elementos informativos digitais obtidos durante a investigação criminal" (PRADO, 2008, p. 317) que a perícia forense digital assumirá um grande papel no processo digital. O que a atividade probatória digital exigirá para sua legalidade, contudo, provem não somente das principais características da forense digital, mas daquelas jurídicas: de relevância, suficiência, legalidade e confiabilidade (DI IORI et al, 2015, p. 23) – sendo confiável aquele vestígio digital justificável (pertinente), auditável, repetível e reproduzível.

Como em cada uma dessas fases o processamento massivo de dados poderá representar grave ingerência a direitos fundamentais, o processo penal deve ser concebido como verdadeira gestão de dados. Ou seja, pensar a forma de tratamento mais adequada em cada uma das etapas do ciclo de vida dos dados (acesso/coleta, processamento, análise, compartilhamento, armazenamento, reutilização e eliminação[8]) regulamentada (EILBERG; SALIBA; ZANATTA, 2021) para fins de segurança pública ou persecução penal ou, ainda, pelo contrário, identificar quando tal tratamento dos dados é inadequado. Joaquín Delgado Martin (2022. p. 34) desenvolve muito bem esse paralelo: a coleta do dado é o que condiciona a legitimidade da sua obtenção – que está diretamente ligada à (i)licitude da prova. É no tratamento desses dados que as questões relacionadas à suscetibilidade dos dados dos processos judiciais e à necessidade de cibersegurança[9] ganham foco. É, ainda, no processamento desses dados a partir das tecnologias emergentes de IA e *blockchain* – tanto para a resolução de conflito como para os meios de prova – que emergem novas contendas.

A gestão de dados do processo penal vem da compreensão também de que os órgãos de segurança pública e de persecução penal assumem um papel de controlador dos dados coletados para fins penais (COE, 2018). Portanto, como qualquer processamento de dados, a sua gestão estará suscetível à incorreta governança. No caso do campo penal brasileiro, tal gestão é

[8] Na doutrina, Ricardo Santana (2016, p. 116) resumiu o ciclo de vida em coleta, armazenamento, recuperação e descarte. No ordenamento pátrio, a previsão normativa do art. 5º, inciso X, da Lei Geral da Proteção de Dados dispõe: "X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

[9] No relatório da Comissão Interamericana de Direitos Humanos, "Libertad de Expresión e Internet", de 2013, da Relatoria de Liberdade de Expressão, a cibersegurança aparece como direito da sociedade e do indivíduo.

fortemente embasada em uma lógica securitária, herança de um processo penal autoritário cujos vieses escancaram, ao final, problemáticas estruturais do sistema brasileiro, tais como a filtragem racial. A determinação de quem, quando e como se pode acessar um dado está constantemente suscetível às mais variadas formas do vigilantismo digital; no entanto, a vigilância à qual toda a população está exposta é massivamente exercida para a finalidade penal sobre corpos específicos no cotidiano brasileiro.

Dentre todas as possibilidades de interpretação que se podem fazer sobre a coleta massiva e qualificada de dados no campo penal, é crucial diferenciar um mesmo dado que, a depender do contexto, pode configurar como fonte de prova, elemento probatório ou meramente um elemento informativo digital e, portanto, identificar o que legitimou a sua obtenção e os requisitos legais para o seu compartilhamento pelo controlador, operador ou co-controladores para terceiros. A determinação de como esse dado se configura é feita quando se observa a qual fase do procedimento probatório a finalidade do levantamento se refere, de modo que o controle processual e material serão ferramentas para conter as indevidas imbricações dos meios de inteligência, aos meios de investigação e aos meios de prova.

A vigilância refletida no combate à criminalidade organizada (FIGUEIREDO DIAS, 2008, p. 22-23) é acompanhada pela transmissão de dados em diferentes contextos: i) as representações cuja ordem judicial foi de sincronização automática das contas indicadas ou vinculadas ao IMEI informado de forma compulsória e velada ao usuário; ii) os e-mails trocados, objetos de interceptação conforme Lei n.º 9.296/96; ii) os dados armazenados na caixa de entrada, rascunho, lixeira e drive, objetos de quebra de sigilo; iii) os dados digitais retidos pelas empresas, objetos de cautelar probatória busca; iv) os casos de suspensão do WhatsApp por ausência de *backdoor* na criptografia; v) a necessidade de preservação rápida de dados digitais pelos provedores; vi) o dever de retenção dos provedores.

A produção massiva de dados em momento anterior às garantias processuais conhecidas no processo penal analógico gera a compreensão de que há deslocamento da produção probatória à investigação. Tal confusão é consequência da hipermassificação informativa processual, em parte identificada pela doutrina na discussão dos denominados maxiprocessos (FERRAJOLI, 2011). O escambo entre as funções investigativas com as securitárias é acompanhado pela "mutação substancial do modelo clássico penal" com o acréscimo dos meios de investigação (SANTORO, 2020, p. 88-90). Para além do *boom* da justiça negociada e os efeitos das Operações no Brasil para a transmutação dos maxiprocessos, temos a obtenção massivas de dados durante momentos pré-processuais, o que traz consigo questionamentos das exceções ao contraditório para as denominadas provas cautelares, não repetíveis e antecipadas ou, ainda, o que de fato constitui prova antecipada, cautelar e não repetível no contexto de investigação digital.

2 A LEGITIMIDADE DO LEVANTAMENTO DE DADOS

A alteração significativa dos métodos de policiamento e de investigação pelo uso de tecnologia reascende problemáticas antigas e evidencia novas. O ponto de partida está na diferenciação do desafio contemporâneo do campo probatório – cujas previsões dogmáticas e normativas atuais não dão conta de resolução – de um "velho novo" (SALT, 2016, p. 8) desafio – sobre os quais propostas de previsão legal já estão obsoletas – e do que se trata, de fato, de um desafio nada mais que tradicional, porém sofisticado pela tecnologia.

Antes de observar o embasamento do compartilhamento do dado em si, notamos a finalidade que legitimou a coleta do dado e seu uso para fins de investigação criminal. No ciclo de vida dos dados, temos em seu início da cadeia de etapas a coleta/levantamento. Pode ser que a base legal da coleta seja a mesma que a do uso (*e.g*. interceptação da comunicação, cuja finalidade é investigativa e probatória) ou pode ser que a finalidade seja diferente da finalidade que legitimou a coleta do dado (*e.g*. pedidos realizados aos prestadores de serviço de dados coletados para fins comerciais) e seja diferente da finalidade de investigar. Se a base legal da finalidade que legitimou a coleta do dado é diferente da finalidade de investigação/produção probatória/persecução penal, estamos falando de um "uso secundário".

Assim, o condicionamento dos acessos e usos dos dados pela autoridade policial precisa estar previsto em lei explicitamente a partir de requisitos materiais de causa e proporcionalidade ou autorização judicial. No entanto, há "falta de profundidade e clareza quanto aos princípios normativos subjacentes aos traços fundamentais da articulação entre privacidade e segurança no direito constitucional" (ABREU, 2022, p. 300) brasileiro. A privacidade e a segurança aparecem na jurisprudência constitucional (ABREU, 2022, p. 217) brasileira primordialmente em decisões sobre sigilo bancário, inviolabilidade do domicílio, sigilo de documentos e correspondência, sigilo profissional, sigilo das conversas orais privadas, sigilo de registros telefônicos, dados pessoais (dados cadastrais), dados pessoais sensíveis (DNA) e sigilo telemático.

Jacqueline Abreu elabora como os critérios de prerrogativa de acesso estabelecidos pelo processo penal, que desconsideram até mesmo o caráter dos dados sensíveis, precisam refinar os critérios da justa causa, além da própria regulação do tratamento de tais dados (SALT, 2016, p. 301-302). Seriam, portanto, esses padrões de justificação (de justa causa) que careceriam de mais bem fundamentadas razões decisórias para as quebras de sigilo. Com base nas reflexões de Daphne Renan (RENAN, 2016, p. 1052) a pesquisadora destaca a necessidade de "métrica individualizada das causas suficientes para acreditar que medidas de vigilância (que acarretam

obtenção de informações) sobre certas pessoas mostrarão elementos de prova de atividade criminosa" (ABREU, 2022, p. 308).

No Brasil, temos direitos e remédios constitucionais, garantias fundamentais e sanções previstas ao indevido tratamento de dados – sejam eles abarcados pelo princípio do sigilo da comunicação, seja pela proteção de dados. A previsão às dimensões das comunicações positivas (direito à liberdade de expressão, no inciso IV do art. 5º da CF) e negativa (direito à privacidade inciso IX do mesmo dispositivo, e direito ao sigilo no inciso XII, do mesmo artigo), no entanto, ainda enfrentam fragilidades como "as disputas interpretativas [...] [que] repercutem no grau de proteção que esses direitos garantem contra a vigilância indevida de autoridades do Estado sobre comunicações" (INTERNETLAB, 2020, p. 20).

Essa problemática se evidencia quando o objeto da proteção ao sigilo previsto constitucionalmente está em jogo. Disputas sobre o que estaria sob sigilo – o conteúdo em si ou o fluxo das informações comunicadas –, além das exceções previstas no dispositivo que permitem a quebra de sigilo (INTERNETLAB, 2020, p.20) exigem a valorização da privacidade mesmo de dados telemáticos cujo caráter é estático. A relativização da garantia constitucional é infundada, pois "falsa a noção de que o fluxo de comunicações só seria violável pelas comunicações telemáticas e telefônicas na forma da Lei nº 9.296/96" (INTERNETLAB, 2022, p. 301). É preciso também estender a noção de intimidade e vida privada que é dada às empresas quando tratam do sigilo bancário e quando analisamos o sigilo das comunicações.

O julgamento do Recurso Extraordinário nº 418.416/SC pelo STF em 2006 é exemplo de caso em que se fez uso do próprio direito fundamental (direito ao sigilo) para justificar a sua restrição. O processamento massivo de dados também adere à pauta da jurisprudência brasileira com outro importante caso de Repercussão Geral do Tema nº 1148,[10] cujo *Leading case* no STF é o RE nº 1.301.250. No julgamento pelo STF em 2006 do Recurso Extraordinário 418.416/SC, o Ministro Relator Sepúlveda Pertence fundamentou que o sigilo da proteção constitucional não se referiria às informações comunicadas, mas apenas ao fluxo delas. Em contrapartida, dentre as disputas existentes, a doutrina brasileira já admitiu a extensão da interceptação das comunicações à interceptação de dados, "em caráter excepcional, desde que o conteúdo não fique armazenado" (BADARÓ, 2010, p. 499) (pois então seria o caso de busca e apreensão do dispositivo), bem como a extensão para a compreensão do e-mail como uma forma de comunicação eletrônica, de modo a não se permitir sua interceptação, mas apenas apreensão. No entanto, o entendimento majoritário não estendeu o sigilo das comunicações pela telefonia para os fluxos de dados, comunicações

[10] Tema 1148 - Limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas.

telemáticas, ou cartas, o que deságua na exclusão da previsão constitucional quando se trata de dados de conteúdo e metadados (INTERNETLAB, 2022, p. 37).

A decisão acima mencionada teve seu entendimento reafirmado em um julgamento pelo STJ no ano de 2021, pela decisão sobre o Ag. Reg. no Ag. em Recurso Especial nº 1.910.871/RS, de Relatoria do Ministro Reynaldo Soares da Fonseca, e no ano de 2016, pelo Recurso em Habeas Corpus nº 75.800-PR, reforçando o entendimento do corpo jurisprudencial brasileiro de que dados armazenados não gozariam da mesma proteção do direito ao sigilo das comunicações (INTERNETLAB, 2022, p.29). Em contrapartida, o STF sobre o HC nº 168.052, de Relatoria do Min. Gilmar Mendes, enfrentou a doutrina da não extensão do sigilo aos dados armazenados e interpretou a partir da Lei nº 12.965/2014 e declarou a nulidade das provas obtidas mediante o acesso indevido ao celular sem autorização prévia. Além disso, declarou a ilicitude das provas derivadas do acesso indevido para observar conversas aplicativo WhatsApp, reafirmando o entendimento do HC n.º 91.867/PA.

O acesso a dados contidos nos celulares sem autorização judicial também possui outro importante *leading case,* ARE nº 1.042.075, cuja repercussão geral foi reconhecida pelo STF no Tema nº 977.[11] A busca e apreensão dos dados armazenado em dispositivo eletrônico ainda tema incontroverso e de repercussão geral no Tema nº 977 teve decisão em que se reconheceu a ilicitude da prova por violação do sigilo das comunicações em razão do acesso ao celular encontrado fortuitamente sem autorização judicial.

Em 2020, no que tange ao levantamento de dados pelos órgãos de inteligência (especificamente as atividades da Agência Brasileira de Inteligência – Abin), o STF interpretou o dispositivo 4º, parágrafo único da Lei nº 9.883/99 (Lei ABIN), no sentido de reforço à reserva jurisdicional, requerendo a remoção dos dados compartilhados entre os órgãos de inteligência e os órgãos de investigação. O caso sobre a formação de dossiês de funcionários públicos foi julgado pela ADPF nº 722, momento em que se ressaltou a inexistência de interesse legítimo da coleta de dados respaldado pelo art. 3º da Lei nº 9.883/1999, convocando-se a aplicação da LGPD por não se configurar nenhuma das exceções previstas no art. 4º, inciso III.

Fato é que, atualmente, o sigilo da comunicação em fluxo está devidamente regulamentado pela Lei de Interceptações a partir de rigorosos requisitos (e, portanto, o acesso aos dados de conteúdo é restringido conforme a sua sensibilidade reconhecida). Contudo, os debates entornam nas demais categorias de dados (metadados) como determinante para a definição da necessidade ou não de autorização judicial prévia como requisito para a coleta. A tradicional relação do grau

[11] Tema 977 - Aferição da licitude da prova produzida durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime.

de proteção às diferentes categorias (cadastrais, de tráfego, de conteúdo) para determinação da reserva jurisdicional proveniente da dogmática alemã possui respaldo na Convenção de Budapeste e, na perspectiva nacional, no Marco Civil da Internet, mas é uma concepção ultrapassada que não dá conta dos desafios atuais das novas tecnologias, dentre os quais destacamos dois.

Em primeiro lugar, adotar o entendimento de que inciso XII, art. 5º é apenas para fluxo de comunicações (e não informações comunicadas armazenados) significa "assumir que informações cadastrais e metadados são menos relevantes à privacidade" (INTERNETLAB, 2022, p. 26). A Comissão Interamericana de Direitos Humanos em seu relatório de 2016 "*Estandares para una internet libre, abierta e inlcluyente*" (OAS, 2020) já evidenciava que a inclusão dos "metadados" na esfera do direito enquanto parte integral das comunicações seria necessária, permeando os desafios da proteção de dados, vigilância, monitoramento e interceptação, a criptografia e o anonimato.

A segunda questão está relacionada ao fato de que, em certos casos, tem-se atribuído o grau de proteção de dados cadastrais aos metadados – como é o caso da "porta lógica" do IP, em razão de um IP de uso compartilhado – a fim de ter mais facilidade para relativizar balizas por meio de interpretações "extensivas de um dever de retenção geral" (INTERNETLAB, 2022, p. 45) e por mudanças legislativas que alteram a necessidade de ordem judicial para seu acesso. Além disso, discussões sobre o IP dinâmico ser considerado dados de comunicação ou metadados rompem barreiras mais fortes de proteção desses dados, uma vez que ao invés de exigir maiores requisitos específicos conforme a lei e estabelecidos constitucionalmente na ordem judicial, basta a autorização fundamentada.

Nesse caso, o levantamento de dados pela polícia para identificação de pessoas que utilizaram buscador com termos específicos (quebra de sigilo de pesquisas de internet), bem como a massiva coleta de dados de geolocalização com individualização e identificação de todas as pessoas em um certo horário e local. O julgamento do STJ que teria determinado ao Google o fornecimento da lista de usuários que pesquisaram combinações de palavras relacionadas à vereadora Marielle Franco na semana anterior ao seu assassinato nos coloca mais uma vez diante da necessidade de pensarmos em limites ao levantamento e compartilhamento de dados de pessoas insuspeitas (ESTELLITA; GLEIZER, 2020) bem como a produção probatória baseada em dados de informação não necessariamente provenientes da comunicação entre pessoas-alvo de investigação. Ainda sobre o tema de sigilo das comunicações telefônicas, destacamos o ARE nº 1.042.075, abordado anteriormente, em que se discute a repercussão geral da possibilidade de acessar a agenda telefônica e o registro de chamadas do celular sem ordem judicial.

3 COMPARTILHAMENTO DE DADOS

Uma das fases do ciclo de vida dos dados é a de compartilhamento de dados, entendida normativamente no ordenamento brasileiro como a "comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais" (art. 5º, inciso XVI da LGPD).

3.1 Compartilhamento de dados entre setor privado e público

O compartilhamento de dados do setor privado com o público traz implicações legais de diferentes cenários e perspectivas. O primeiro cenário diz respeito ao uso secundário dos dados levantados pelas *Big Techs*, cuja grande maioria de investigações se pautam. A princípio estamos falando de legitimidade do levantamento de dado para finalidade comercial, por exemplo, mas o problema aparece com seu uso para fins penais. Se anteriormente a tecnologia era restringida aos aparelhos eletrônicos, hoje os menores detalhes do cotidiano inerentes ao socializar de alguma forma envolvem coleta de dados e o subsequente armazenamento em alguma base de dados.

Ao serem bases de dados de serviços prestados pelo setor privado, o cenário de compartilhamento de dados tem os provedores de serviço com papel central em um contexto de atividade do poder público (investigar/processar). Os dados processados em massa pelas grandes corporações resultam na incorporação da cooperação do setor público-privado[12] como realidade (não regulada na maioria dos países) à investigação e, portanto, à produção probatória digital. Assim, as questões jurídicas que se sobressaem desse cenário envolvem tanto a necessidade de cooperação jurídica internacional ou não frente aos pedidos de auxílio direto (questionando-se o tradicional sistema de acordo de cooperação mútua em matéria penal) como o dever de retenção e preservação (e, portanto, os serviços que envolvem criptografia e a necessidade ou não de existir um *backdoor).*[13]

O segundo cenário concerne às empresas privadas de forense digital que estão coletando e processando os dados com base no uso primário que é justamente a investigação ou inteligência. Essa vigilância privada realizada em nome do Estado, porém pautada por políticas de interesses

[12] O que, no entanto, não é novidade. Nilo Batista aponta a ilusão de que a "concentração do poder penal que implica a construção de pena pública jamais se exerce sem a participação privada das classes sociais dominantes" (BATISTA, 2002, p. 88). Quanto ao ponto, reflexão trazida por Geraldo Prado (2024), os trinômios "crime-punição-controle social" e "verdade-prova-prova digital" são verdadeiros "subterfúgios retóricos do Poder e a tendência dos juristas de camuflarem a tensão política subjacente à incriminação de condutas e punições de agentes".

[13] Na computação, o conceito de "backdoor" (porta dos fundos) refere-se ao método de transpassar a autenticação tradicional e, na criptografia, refere-se à possibilidade de ter acesso à informação encriptada sem possuir as corretas credenciais. (STANFORD, 2020).

econômicos, pode (re)configurar o espectro de vigilância massiva,[14] razão pela qual a legitimidade da coleta para essa finalidade precisa estar regulamentada e ser periodicamente fiscalizada. Além disso, a própria LGPD no dispositivo em que excetua o tratamento para fins de segurança pública e investigação criminal, dispõe no §4º, art. 4º que "[e]m nenhum caso a totalidade dos dados pessoais de banco de dados de que trata [as exceções] do artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público".

Assim como outras indústrias possuem certificação para fornecer serviços (ainda que na capacidade privada) de interesse público, a indústria da forense digital utilizada para atividades de inteligência ou de investigação também deveria passar por regulamentação. Por isso, entendemos as avaliações de impacto regulatório (de vigilância) (BIONI; EILBERG; CUNHA; SALIBA; VERGILI, 2020, p. 10-12) que instrui o processo legislativo como necessariamente produzidas pela Autoridade Nacional da Proteção de Dados ou o Conselho Nacional de Justiça ou, ainda, em uma perspectiva de inovação regulatória, como proposto pela Associação Data Privacy Brasil de Pesquisa, de um "Conselho Nacional de Proteção de Dados de Segurança Pública" (BIONI; EILBERG; CUNHA; SALIBA; VERGILI, 2020, p. 25-26), o qual deveria ser um conselho multissetorial inspirado no art. 58-A da Lei Geral de Proteção de Dados para atuar com atribuições consultivas, deliberativas e de fiscalização.

Somado à avaliação de vigilância (produzida pelos legisladores) estão os relatórios de impacto (produzidos pelos controladores e apresentados à Autoridade Nacional de Proteção de Dados). Adicionar informações sobre a confiabilidade dos dados coletados quando os algoritmos do *software* não são auditáveis, por conta do segredo comercial ou industrial (*black box*[15]), seria uma forma de compensar as assimetrias informacionais quanto aos relatórios de impacto de vigilância de *softwares* utilizados para inteligência e investigação, já que o contraditório da prova digital dependerá de questões principalmente relacionados à confiabilidade no sentido jurídico e não da forense digital (STOYKOVA, 2023).

3.1.1 Cooperação jurídica internacional: acordo de cooperação mútua em matéria penal (MLAT) ou requisição direta

[14] Não apenas a vigilância massiva, mas a espionagem estatal, que abandona os motivos meramente políticos e/ou de segurança nacional/pública e se direciona aos ganhos comerciais da exploração de dados por meio de parcerias entre Estado e empresas, o que exige limites. In: WATT (2021, p. 775).

[15] O conceito de inteligência artificial *Black Box* refere-se opacidade das tecnologias dos modelos de inteligência artificial, as quais não fornecem informação acerca de como os sistemas decidem ou tomam resultados, isto é, de como os algoritmos são alimentados.

"A primeira e mais importante restrição imposta pelo direito internacional a um Estado é que [...] a jurisdição é certamente territorial; não pode ser exercido por um Estado fora do seu território, exceto em virtude de [...] convenção"[16] – assim estabelecia o emblemático caso Lótus no Tribunal Penal Internacional, em 1927. Esse princípio da territorialidade, como entendido pela corte internacional, hoje enfrenta dificuldades de concretização no mundo digital transfronteiriço. Vale ressaltar que o acesso transfronteiriço a dados traz consigo o diálogo de jurisdições cujas tradições jurídico-penais foram construídas e consolidadas a partir de premissas que se diferem, razão pela qual indevidas analogias e paralelismos são feitos.

Na reconfiguração tecnológica promovida pela inovação, as plataformas tecnológicas tornam-se novos mundos que redesenham configurações completamente diferente, como é o caso do setor de serviços de computação em nuvem, em que a maioria dos serviços não pertencem apenas às empresas que os prestam, mas são fornecidos por outras empresas que o desenvolvem. Atualmente, na "guerra das nuvens" a *Amazon AWS, Microsoft Azure* e *Google Cloud* (A16Z, 2022)[17] ocupam mais de dois terços do mercado.[18] Além de noticiar cada vez mais uma maior substituição de dispositivos por softwares de nuvens, a contratação de provedores de serviço também anuncia o velório do princípio da territorialidade. À medida em que as nossas socializações do cotidiano são atravessadas pelo uso de plataformas e serviços prestados por empresas que estão localizadas em um país e, por vezes, armazenam os dados em um terceiro país. E mais, servidores (servidores, cabos submarinos e provedores de acesso) que estão nos mais variados países podem ser utilizadas de acordo com as necessidades de cada empresa.

É nesse cenário do mundo virtual de crise identitária do princípio da territorialidade que se intensificam os desafios quando temos os sistemas de computação em nuvem (RAMALHO, 2014, pp. 95-122) e de prestação de serviços de *softwares* – que refletem importantes consequências na cooperação jurídica internacional em matéria penal (SALT, 2016). O caso da prestação dos serviços em nuvens recai sobre a questão de arquivos armazenados em nuvens em uma jurisdição, cujo serviço prestado é fornecido por empresas de outra jurisdição, e que, por vezes, podem ter a custódia de controle dos dados por uma terceira jurisdição (SALT, 2016, p. 9), provocando a tradicional cooperação jurídica internacional. Também trata dos casos em que não há *backup* no dispositivo, e, portanto, estão essencialmente armazenados na nuvem (em estranha

[16] No original: "*The first and foremost restriction imposed by international law upon a State is that – failing existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State.* ***In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention***". S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) N. 10 (Sept. 7). (Grifo nosso).

[17] Entrevistado: Michael Dell. Entrevistadores: Marc Andreessen, Martin Casado e Sonal Choksh.

[18] Disponível em: https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues . Acesso em 10 out. 2022

jurisdição) e a (im)possibilidade dos *first responders,*[19] acessarem tais dados diretamente sem cooperação jurídica internacional.

Acionar a prática jurídica das novas realidades, à medida em que os elementos de prova digitais – basicamente os dados – começam a substituir, de alguma maneira, os elementos físicos, exige voltar às mudanças e percebê-las dentro de uma compreensão de desterritorialização do poder punitivo para reafirmar um lugar que não necessariamente é geográfico, mas de autoritarismos. Não fosse esse o terreno, não estaríamos discutindo formas de mitigar os danos do sistema em termos de controle da (i)legalidade de uma prova no processo penal.

Quando verificamos casos em que o compartilhamento de provas é feito de um país de *common law* a outro de tradição *civil law* evidenciamos que o procedimento probatório foi postulado, adquirido e produzido em um terreno cuja compreensão fundamental da culpabilidade se dá por meio do pressuposto de um elemento mental extremamente afundado na "febre subjetivista" [20] e que descontextualizam as bases fundantes do processo penal brasileiro, percebemos que a tecnologia tem a capacidade de corte transversal e de promover uma verdadeira tensão cuja solução ampara-se na aproximação efetiva das dogmáticas da proteção de dados, penal material e processual penal.

Algumas iniciativas internacionais preveem tal compartilhamento. O princípio da territorialidade já vem sendo discutido pela comunidade internacional, como no Segundo Protocolo da Convenção de Budapeste, bem como as iniciativas do "Pacote *E-Evidence*" no contexto europeu – que apostam em tentativas de harmonização dos pedidos de produção e preservação da prova digital envolvendo prestadores de serviços independentemente de onde estiverem localizados. Com a vigência das duas importantes normativas para a coleta de prova digital em processos penais transnacionais, quais sejam o Regulamento nº 2023/1543 do Parlamento Europeu e do Conselho da União Europeia[21] e a Diretiva nº 2023/1544 do Parlamento Europeu e do Conselho, [22] "dois elementos de design regulatório" de tais normativas são considerados de "impacto regulatório revolucionários" (TOSZA, p. 169): a aposta em uma alternativa à tradicional concepção de soberania, com redefinição da natureza do conceito de territorialidade, e a reformulação da cooperação transnacional baseada no reconhecimento mútuo.

[19] Primeiros agentes investigativos a entrarem em contato com a cena do crime e com os dispositivos digitais. "O termo *first responders* refere-se às primeiras pessoas (usualmente profissionais de segurança pública) que atendem ao local de crime. Optou-se nesta tradução, pela manutenção do termo original" (UNODC, 2010).
[20] Nos anos 80, Ashworth traz a crítica de como os juristas estão afetados pela "febre subjetivista" por meio da elasticidade da *mens rea* (ASHWORTH, 1981. p. 45).
[21] Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho de 12 de julho de 2023, "relativo às ordens europeias de produção e às ordens europeias de conservação para efeitos de prova eletrónica em processos penais e para efeitos de execução de penas privativas de liberdade na sequência de processos penais".
[22] Diretiva (UE) 2023/1544 do Parlamento Europeu e do Conselho, de 12 de julho de 2023 "estabelece regras harmonizadas aplicáveis à designação de estabelecimentos designados e à nomeação de representantes legais para efeitos de recolha de prova eletrónica em processos penais".

A comunidade internacional também possui outras iniciativas globais de regulação do cibercrime e da prova digital, como a Convenção da ONU que vem sendo elaborada pelo Comitê *Ad Hoc* liderado pelo Escritório das Nações Unidas de Drogas e Crimes (UNODC).

Como Stanislaw Tosza acentua, devido à grande tendência dos agentes de *law enforcement* recorrerem à "cooperação voluntária" (requisição direta de dados) – e dada a ausência de regulação no campo – as empresas assumem funções tidas como públicas e passam a, de fato, analisar a proporcionalidade e a legitimidade dos pedidos (TOSZA, 2023, p.166) de acesso a dados; assim, configurada uma certa forma de privatização do *enforcement* (JØRGENSEN, 2019, p. 176) e da confiança mútua na área da justiça criminal" (MITSILEGAS, 2018, p. 263-265) no contexto global por meio do denominado processo de "externalização da investigação" (PRADO, 2019, p. 191-206). Ao assumirem papel protagonista na retenção e preservação de dados – vez que coletam, armazenam e tratam os dados ao qual as autoridades pretendem alcançar –, as grandes corporações digitais passam a realizar diligências de investigação e até mesmo monopolizam a *expertise* necessária para o tratamento de tais dados (PRADO, 2020) a partir da consequentemente elaboração do relatório de análise criminal (constante o laudo pericial ou não). Por essa razão, a regulamentação dessas empresas como sujeitos processuais (PRADO, 2020) é de notória necessidade.

Em razão da ausência de regulação, uma série de acordos de grandes empresas com as polícias e o Ministério Público, além da possibilidade dos *Law Enforcement Online Requests*, culminam em discussões jurídicas acerca das obrigações das Big Techs. Se observarmos o Portal de Transparência da Meta,[23] por exemplo, as estatísticas relacionadas ao Brasil, de janeiro a dezembro de 2023, são de 45.603 pedidos, dos quais aproximadamente 80,21% tiveram dados produzidos. Dentre os pedidos, 5.594 foram considerados solicitações de emergência por agentes de órgãos de persecução penal. O Portal de Transparência da Google, na mesma época, indica 33.062 pedidos, 2.094 solicitações de divulgação de emergência, e 1570 pedidos de preservação de dados.[24] No primeiro semestre de 2023, 71% das solicitações resultaram no fornecimento de dados e na segunda 75%. Por fim, a Apple, em seu Portal de Transparência,[25] a partir de estatísticas que no momento deste trabalho indicavam apenas o primeiro semestre de 2023,[26]

[23] Ver: https://transparency.meta.com/reports/government-data-requests/country/BR/.
[24] Não indica, contudo, os tipos de pedidos, classificando como "outros tipos de pedidos".
[25] O portal da Apple classifica os pedidos em i) dispositivos (pedidos que buscam dados de clientes relacionados com identificadores do dispositivo, como o número de série ou número IMEI); ii) identificador financeiro (pedidos relacionados aos identificadores financeiros como cartão de crédito ou cartão-presente); iii) conta (pedidos relacionados aos identificadores de conta, como ID Apple ou endereço de e-mail); iv) push token (pedidos relacionados com tokens de serviço Apple Push Notification; v) Emergência: pedidos de dados em casos de emergência.
[26] Até a data de entrega deste artigo, não havia dados disponíveis com relação aos pedidos de julho a dezembro de 2023.

recebeu 5813 pedidos relacionados aos dispositivos com 17673 identificadores, dentre os quais 77% dos dados foram fornecidos; 18 pedidos com 121 identificadores financeiros, dos quais 78% foram concedidos, 3200 pedidos com 14584 dados de contas, dos quais 72% foram concedidos, e 82 pedidos de emergência, dos quais 74% foram concedidos.

Tais números exemplificam como funções tipicamente públicas, que Stanislaw Tosza (2023, p. 166) destaca – como a verificação da proporcionalidade e legitimidade de intervenção de direitos fundamentais –, passaram a ser exercidas pelas prestadoras de serviço, de modo que a maioria das autoridades de persecução penal vão tentar fazer uso da via de cooperação voluntária ao invés de partir à cooperação jurídica internacional – sem, no entanto, haver mecanismos de fiscalização[27] ou parametrização.

No campo da atividade probatória, as tensões se evidenciam quando um sistema reconhece a possibilidade de inclusão de qualquer prova, independentemente se legal ou ilegalmente obtida, como foi feito pela Corte Suprema do Canadá (POLYVIO,1981, p. 228). No caso da Lava Jato e das mensagens trocadas pelos aparelhos da *Blackberry*, qual o juízo de obtenção dos dados que deveria ter sido aplicado, o da lei do local onde ocorreu a coleta ou o da lei da sede do provedor de serviço? E nos auxílios diretos, como promovemos uma harmonização que garanta segurança jurídica? Para além dos problemas da atipicidade, que são resultado e causalidade no país que recebe a prova, o país que a transmitiu não possui concepção da categoria de *tipo*. Quais os conflitos que se desdobram desse diálogo de jurisdições? E quais as alternativas aos acordos de cooperação mútua (lentos e obsoletos) frente à dinâmica da prova digital se ausente previsão em tratado internacional?

Sobrevieram inúmeras vezes durante as Operações realizadas no Brasil os acordos de cooperação jurídica internacional, principalmente em razão de crimes transnacionais que exigem uma prestação de informações jurídico-legais sobre dados telemáticos e informáticos ao Poder Judiciário Brasileiro envolvendo tratados internacionais e acordos em matéria penal. Por exemplo, nos casos de pessoas que vivem nos Estados Unidos (EUA), em que essas informações deveriam ser prestadas através do Acordo de Assistência Judiciária em Matéria Penal (*Mutual Legal Assistance Treaty* – MLAT), nos termos do Decreto nº 3.810, de 02 de maio de 2001, e não por meio de informações oferecidas pelo grupo econômico ou representante sediado no Brasil. Nos Estados Unidos os e-mails e as respectivas contas supostamente utilizadas para a preparação dos delitos vindicam um mandado judicial. Para casos envolvendo residentes nos Estados Unidos e, portanto, sob a proteção da Quarta Emenda, as autoridades necessitam realizar um pedido de

[27] Quanto ao ponto, Geraldo Prado explorou anteriormente como o auxílio direto tem "atalhado o caminho das cartas rogatórias, lentas e ineficientes" uma harmonização com as expectativas do Estado do direito por meio de mecanismos de fiscalização do devido processo legal. In: PRADO, 2013.

cooperação jurídica do Brasil por meio do Departamento de Justiça dos Estados Unidos das Américas (*Department of Justice – DoJ*), que determina se a demanda está de acordo com o corpo legislativo vigente, no intuito de expedir mandado judicial nos EUA para, então, acessar o e-mail das pessoas investigadas.

O procedimento nos EUA para a quebra de sigilo telemático possui inúmeras exigências legais e isso se dá principalmente pelo fato de o levantamento do sigilo de informações eletrônicas representar uma grande afronta à Quarta Emenda – a qual dispõe que nenhum mandado judicial será expedido face à ausência de causa provável, apoiado por juramento ou afirmação. Como requisitos do DoJ, além dos constantes no formulário padrão disponibilizado pelo Ministério da Justiça e Segurança Pública,[28] são exigidos: i) a concisão e a clareza dos fatos apresentados, com o nexo de causalidade (*probable cause*) demonstrado; ii) a transcrição integral dos dispositivos legais vigentes no Brasil; iii) a descrição da assistência solicitada e os objetivos da autoridade requerente; iv) os documentos que embasam o pedido, tais como a cópia da denúncia ou a decisão judicial; v) a tradução e a assinatura de todos os documentos; e, por fim, vi) a confidencialidade do pedido. Ainda, determina-se a necessidade da descrição do local ou coisa a ser apreendida e revistada, bem como a descrição da conclusão sobre a origem das provas solicitadas para a sua justificação.

A morosidade do processo MLAT costuma ser alegada pelo Poder Judiciário brasileiro como um empecilho para se seguir tal procedimento. Contudo, o próprio site do Ministério da Justiça e Segurança Pública descreve a possibilidade de as autoridades requerentes solicitarem a preservação dos dados de e-mail ao Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do MJSP (DRCI)[29] antes de formular o pedido formal de cooperação jurídica. Com efeito, o que se observa é que a maioria dos pedidos brasileiros é negada devido à ausência de indícios suficientes para embasar as investigações,[30] uma vez que a legislação americana (*Stored Communication Act*) é devidamente rigorosa quando se trata de violação do direito fundamental à privacidade.

A temática de fornecimento de dados digitais não é de simples resolução e isso se evidencia com o ajuizamento da Ação Declaratória de Constitucionalidade – ADC nº 51 pela Federação das Associações das Empresas de Tecnologia da Informação (Assespro Nacional), que

[28] No art. 2º do Decreto, dispõe-se o Ministério da Justiça e Segurança Pública, à época denominado Ministério da Justiça, como Autoridade Central para as solicitações de cooperação jurídica em matéria penal.
[29] O artigo 12, IV, do Decreto nº 9.150 de 04 de setembro de 2017 determina que compete ao Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional articular, instruir e coordenar a execução da cooperação jurídica como autoridade central.
[30] Ofício n. 965/2018/CGRA-DRCI-SNJ-MJ. Assunto: Cooperação Jurídica Internacional em Matéria Penal entre Brasil e EUA para fins de afastamento de sigilo telemático. Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América (Decreto nº 3.810, de 02 de maio de 2001).

discutia justamente a (im)possibilidade de fornecimento direto de informações telemáticas por parte de empresas no Brasil que sejam parte de grupo econômico dos EUA face à utilização do Marco Civil da Internet – MCI (Lei nº 12.965, de 23 de abril de 2014). A decisão da Suprema Corte no Brasil, no entanto, em 23 de fevereiro de 2023, foi com fundamento no art. 18 da Convenção de Budapeste e do art. 11 do MCI, decidindo pelo fenômeno da "territorialização" do ciberespaço e que, pelo fato de as empresas terem representação no Brasil, as normas de requisição direta de dados e comunicações eletrônicas às empresas do MCI seriam prevalentes, sem a realização de MLAT.

3.1.2 O dever de retenção e preservação frente aos desafios da criptografia

Há ou não há um "dever jurídico de ter habilidade de quebrar sigilo para empresas de tecnologia e internet"? (ABREU, 2017, p. 25-43). Além da tendência de protocolos de cooperação entre empresas privadas para requisição de auxílio direto ou cooperação jurídica internacional para preservação de dados, as relações com o setor privado também demonstram desafios quando observamos o tema das retenções de dados de comunicação (EILBERG; MOSCATELLI, 2020, p. 4) ou, ainda, de preservação dos dados para posterior acesso aos dados.

Há previsão normativa nos termos do i) art. 17 da Lei das Organizações Criminosas, em que se determina o prazo de 5 anos para guardar os "registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas"; conforme o disposto no ii) art. 13 do Marco Civil da Internet (MCI), com o prazo de 1 ano prorrogável (por cautelar probatória prevista no art. 13 §2º) para a retenção dos registros de conexão sob sigilo pelo provedor de conexão; e nos termos do iii) art. 15 do MCI, em que o prazo de retenção é de 6 meses. Também temos as resoluções nº 426/05, 477/07 e 614/13 da Agência Nacional de Telecomunicações (ANATEL), com a determinação do prazo de 1 ano para os dados referentes às conexões de internet pelos prestadores de serviços de telefonia e 5 anos para os dados relativos à prestação do serviço.

No que diz respeito ao acesso aos dados cadastrais, a Lei das Organizações Criminosas dispõe no art. 15, assim como a Lei de prevenção à Lavagem de Dinheiro no seu art. 17-B. Não há, ainda, previsão legal quanto aos metadados das chamadas, como os dados de geolocalização (utilizada para fins de triangularização de dados), sendo necessária ordem judicial para a produção de tal prova penal (EILBERG; MOSCATELLI, 2020, p. 5). O MCI, em seu dispositivo 10, §3º, também permite o fornecimento dos dados cadastrais quando autoridade competente requerer, e, conforme a previsão do art. 22, quando houver registros de conexão à internet e aplicativos por meio de ordem judicial acerca de justificativa motivada da utilidade dos registros solicitados para

fins de investigação ou instrução probatória; fundados indícios da ocorrência do ilícito; período ao qual se referem os registros (p. 4).

Em primeiro lugar, quanto à preservação de dados para posterior acesso por meio de busca, merece atenção o acórdão paradigmático do HC n. 222.141 AgR/PR, de relatoria do Min. Ricardo Lewandowski e HC 91.867/PA de relatoria do Min. Gilmar Mendes, cujas teses, respectivamente, dispõe da nulidade dos elementos obtidos a partir de dados preservados em contas da internet através de pedido de preservação direto pelo Ministério Público sem a prévia autorização judicial, bem como da previsão de que o sigilo das comunicações armazenadas é tutelado pela previsão constitucional do inciso X do art. 5º da Constituição Federal.

Ademais, quanto ao "dever de retenção", merece destaque a decisão do STF sobre o HC nº 168.052, de Relatoria do Min. Gilmar Mendes, que declarou a nulidade das provas obtidas mediante o acesso indevido ao aplicativo WhatsApp e à residência do paciente, com o reconhecimento da ilicitude das provas dele decorrente e, portanto, o reconhecimento pela nulidade do processo. O referido julgado faz menção ao caso Miranda vs. Arizona para a necessidade de desenvolver uma "fórmula de garantia dos direitos das pessoas investigadas cuja inobservância leve à nulidade dos atos de investigação e coleta de provas, mesmo que durante o inquérito policial".

Em termos jurisprudenciais, os Tribunais Superiores do Brasil avançam no caminho constitucional da proteção dos dados no campo penal. Na Ação Direta de Inconstitucionalidade (ADI) nº 5527 os dispositivos questionados foram os arts. 10, §2º, e 12, incisos III e IV, do Marco Civil da Internet, o que gerou a suspensão do serviço do WhatsApp. O fundamento seria o descumprimento das ordens judiciais que determinem a quebra de sigilo das comunicações. A Ministra Rosa Weber entendeu que a determinação da disponibilização do conteúdo das comunicações só poderia ocorrer quando houvesse ordem judicial, trazendo em questão o equilíbrio da proteção da privacidade com a atuação do Estado e não estendendo o dever de guarda de metadados (art. 15 do MCI) ao de conteúdo.

Por fim, ressaltamos novamente o RE nº 1.301.250/RJ sobre a validade constitucional do decreto judicial genérico da quebra de sigilo telemáticos para divulgação de informações pessoais de usuários indeterminados sem a respectiva identificação. Neste caso, a Ministra Rosa Weber entendeu que "o art. 22 do MCI não ampara ordem judicial genérica e não individualizada de fornecimento dos registros de conexão e de acesso dos usuários que, em lapso temporal demarcado, tenham pesquisado vocábulos ou expressões específicas em provedores de aplicação". No campo jurisprudencial brasileiro, a via adotada prevalecente tem sido a de supressão de cooperação internacional, ao se decidir sobre o dever de fornecimento dos dados pelos provedores de serviço das plataformas (INTERNETLAB, 2022, p.82).

3.2 Compartilhamento de dados entre órgãos ou agentes do setor público

Duas são as situações que despertam desafios legais abordados por este trabalho referente ao compartilhamento de dados entre órgãos ou agentes do setor público: o primeiro diz respeito ao contexto de compartilhamento de dados entre diferentes órgãos do setor público – em que observamos tanto os compartilhamento de dados entre órgãos de inteligência com persecução penal como as tendências de interoperabilidade de dados obtidos para fins de exercício de cidadania compartilhadas com órgãos de persecução penal ou inteligência. O segundo está relacionado ao contexto de compartilhamento entre agentes de mesmo órgão, porém de dados que estão ancorados na reserva jurisdicional e cuja prévia autorização judicial não incluía a sua transmissão, configurando uso secundário de dado sem autorização judicial.

3.2.1 Compartilhamento entre órgãos de diferentes competências

Em termos de previsão normativa e compartilhamento de dados, merece destaque a decisão da repercussão geral do Recurso Extraordinário n. 1.055.941 acerca da constitucionalidade do compartilhamento de dados sigilosos sem autorização judicial para finalidade criminal, embasado no art. 15 da Lei 9.613/98 contraposta à Lei Complementar n.º 105/2001, cuja amplitude e intensidade com a qual o COAF realizou esse tratamento de dados desafiam a crença em um assentamento dos princípios da legalidade e da proteção de dados (ESTELLITA, 2021, p. 631). Tal entendimento do STF pela desnecessidade de autorização judicial prévia ao compartilhamento de Relatórios de Inteligência Financeira (RIF) pelo Conselho de Controle de Atividades Financeiras (COAF) para fins penais, ainda que grande parte dos dados pessoais tratados sejam sensíveis e sigilosos,[31] levou ao assentamento do Tema 990 em torno das representações fiscais para fins penais.[32] Recentemente, em sentido contrário, o STJ julgou o RHC nº 187.335, anulando as provas obtidas pelo MP por entender o compartilhamento ilícito devido à ausência de investigação formalizada. Isso porque a notícia de fato e a verificação preliminar de informações (VPI) seriam procedimentos prévios à investigação.[33]

[31] A extensão danosa do tratamento de dados está disposta em uma série de normativas do COAF, do Bacen e da CVM. Ver: ESTELLITA, 2021, p. 618.
[32] Tema 990 - Possibilidade de compartilhamento com o Ministério Público, para fins penais, dos dados bancários e fiscais do contribuinte, obtidos pela Receita Federal no legítimo exercício de seu dever de fiscalizar, sem autorização prévia do Poder Judiciário.
[33] "Se Ministério Público não pode, em notícia de fato, fazer requisições [com base na Resolução do Conselho Nacional do Ministério Público CNMP nº 147/2017], a polícia também não pode, em sede de VPI, requisitar informações ao Coaf" conforme Ministro Reynaldo Soares Fonseca, Relator do caso acompanhado por maioria pelos Ministros Joel Ilan Paciornik e Daniela Teixeira.

Outro caso que merece atenção é o HC nº 149.250/SP e a decisão do Superior Tribunal de Justiça ressaltando as atribuições do *modus operandi* da ABIN e sua impossibilidade de investigar crimes (sobre a Operação Satiagraha), bem como o HC nº 147.837- RJ, em que o Min. Gilmar Mendes evidenciou a ilicitude dos atos de infiltração de agente em razão da inexistência de autorização judicial e configuração de coleta de elementos informativos a partir de "tarefas de inteligência e prevenção genérica".

A proteção de dados em outro contexto semelhante já havia sido examinada pela Ministra Rosa Weber na ADI 6.387,[34] caso em que se decidiu sobre o compartilhamento massivo de dados pessoais com o Instituto Brasileiro de Geografia e Estatística (IBGE). A ADI nº 5.527 e a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403 de Relatoria do Ministro Edson Fachin tiveram decisão proferida no dia 02 de outubro de 2023.

A questão da interconexão e compartilhamento de dados em bancos nacionais é exemplificada pela transmissão de dados biométricos coletados para fins de exercício de cidadania (como a biometria digital para a Justiça Eleitoral) sendo transmitidos com diferentes agências governamentais e utilizados para as finalidades de investigação criminal – sem qualquer transparência, controle público ou medidas de segurança, representando uma violação substancial do princípio da legalidade (ADC, 2019, p. 18). O dado biométrico desperta ainda maiores complexidades quando relacionado aos vieses do reconhecimento facial, com campanhas internacionais pelo seu banimento.[35]

3.2.2 Compartilhamento de dados protegidos por sigilo entre agentes de mesma competência

O segundo caso é ilustrado pelo compartilhamento dos dados protegidos por sigilo fiscal obtidos durante a Lava Jato para os Ministérios Públicos Estaduais, previsto na Portaria Conjunta PGR/MPF-CMPF nº 1/2021.[36] A partir do princípio da unidade institucional, justificaram o

[34] Neste precedente, julgado em 07 de maio de 2020, o STF reconheceu a autonomia do direito fundamental à proteção de dados e o atribuiu *status* constitucional, sendo imprescindível no processo de consolidação da proteção de dados e privacidade no Brasil. Tratava-se de caso sobre a Medida Provisória nº 954/2020 concernente ao compartilhamento de dados pessoais das prestadoras de serviço de telefonia fixa com o IBGE. A Ministra Rosa Weber entendeu a violação do princípio da proporcionalidade pela MPv, além da ausência de determinação de finalidade e necessidade de tratamento. O entendimento foi de que a proteção de dados estaria galgada no art. 5º, *caput,* X, XII e que o seu tratamento deveria ser limitado pelo devido processo informacional (art. 5º, LIV).

[35] No entanto, o *Euopean Act of AI* não regulamentou o banimento do reconhecimento massivo, desapontando a sociedade civil com a expectativa da prevenção de danos massivos à sociedade. A respeito, ver: https://www.amnesty.org/en/latest/news/2023/12/eu-blocs-decision-to-not-ban-public-mass-surveillance-in-ai-act-sets-a-devastating-global-precedent/.

[36] A Portaria Conjunta regula o recebimento, o armazenamento e o compartilhamento entre os membros da instituição dos dados eletrônicos e digitalizados obtidos no exercício das funções.

compartilhamento de dados para uso secundário à finalidade que havia legitimado a autoridade judicial.

O compartilhamento de dados protegidos por sigilo entre agentes do mesmo órgão do setor público deve ser pautado por "normas legais de autorização veiculadas de forma clara" (ROGALL, 1985, p. 6-7 apud ESTELLITA, 2022). O uso primário dos dados coletados a partir de requisição de diligência investigatória era pautado na finalidade específica que legitimou a autorização judicial do levantamento de sigilo: uma ação penal pública específica. Isso não gera, necessariamente, o direito ao compartilhamento dos dados, justamente em razão da necessidade de "autorização parlamentar prévia", que exige a base legal para o uso secundário em razão da gravidade da ingerência de direitos fundamentais.

No âmbito da dogmática material penal, reiteramos a distinção da norma de competência, isto é, "reserva legal" – disposição das atribuições dos agentes e órgãos estatais – da norma autorizativa, qual seja, "reserva parlamentar" – a partir de "autorização judicial" permite atuação dos agentes conforme a sua atribuição. Ou seja, do ponto de vista processual penal, o princípio geral da reserva de lei determina que quando há ingerência de um direito fundamental, não basta a previsão de lei no sentido formal, mas a reserva parlamentar, uma vez que a norma de autorização não deriva automaticamente da norma de competência (GRECO, 2018. p. 37).

No mesmo sentido, dispõe a dogmática processual penal acerca do princípio da especialidade da prova. Há vinculação causal da prova do requerimento à finalidade da investigação específica em curso e à autoridade competente quando houver relativização de direito fundamental (como é o caso do levantamento de sigilo de comunicações, sigilo bancário ou sigilo fiscal). Assim, a admissão de tal prova poderia ser apenas *starter* investigativo (LOPES JR, 2019, p. 671).

4 CONSIDERAÇÕES FINAIS

O impacto da hipermassificação informativa processual aos institutos jurídicos pensados na era analógica enfrentam a obsolescência das previsões técnico-legais no anonimato na navegação a partir de *softwares* como o ToR (*software* livre de código aberto), na encriptação de arquivos, na criptografia utilizada para navegação e aplicativos (VPN que oculta IP e criptografa conexão), no monitoramento de redes P2P (*peer-to-peer*), na descentralização de plataformas em *blockchain*, no armazenamento em nuvem (*cloud computing*) e nos IPs dinâmicos, entre outros desafios. Tendências como o uso de *malware* e técnicas de acesso remoto a dados, a raspagem de dados, a geolocalização, os *drones*, as aplicações de inteligência artificial (IA) para o tratamento de dados coletados ou para a raspagem de dados abertos por técnicas de OSINT (*Open Source*

Intelligence) incrementam a potência da coleta massiva de dados e reconfiguram as práticas ditas investigativas, porém imbricadas também às atividades securitárias. Destacamos também tal problemáticas no contexto de postulação à produção probatória de atividades de prevenção e de inteligência fundidas às investigações.

Dividimos o artigo em três seções. Na primeira parte, observamos as abordagens das cortes supremas do Judiciário brasileiro com relação ao levantamento de dados e a necessária base legal para a interceptação ou busca, compreendidos os sigilos e a proteção de dados. Entendemos a legitimidade do levantamento dos dados como questão anterior que definirá o uso primário de tais dados, o que inclui seu eventual compartilhamento dentro do espectro primário ou secundário – o que deve considerar a existência de base legal. Na segunda, exploramos o compartilhamento de dados do setor privado ao público, cujas implicações legais trazem, de um lado, desafios legais quanto à cooperação jurídica internacional (quando observada a realidade de pedidos diretos) e, de outro, a existência ou não de um dever de auxílio das provedoras de serviço frente aos desafios da criptografia. A ausência de auditorias ou análise de impacto das empresas privadas de *software* de forense digital (para inteligência ou investigação) em razão dos segredos comerciais também é também discussão importante na esfera do uso primário. Na terceira seção, trabalhamos as implicações legais do compartilhamento de dados no setor público compartimentadas a depender do cenário: entre órgãos de inteligência e órgãos de persecução penal e de dados sob proteção de sigilo automaticamente compartilhado entre agentes de um mesmo órgão para uso secundário.

A autodeterminação informativa, assim, será compreendida como "princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado de dados" e "[o] risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados tratados" (MENDES, 2020, p. 11). Assim, abstrai-se da concepção de instrumentos procedimentais para a sua proteção (p. 13) e rompe-se com a tradicional concepção de enfoque na esfera privada/íntima que embasa a intrusão escalonada da categoria tripartite (de dados cadastrais, dados de tráfego e dados de conteúdo) para justificar (des)necessidade de autorização judicial. Isso também implicará compreender que muito mais importante que a privacidade serão o contexto da atividade-fim (finalidade) e da transmissão (base legal e a quem se transmite) somados à rastreabilidade dos dados para se diferenciar o meio de prova digital do meio de investigação na era de processamento massivo de dados.

REFERÊNCIAS

A16Z, **Cloud Wars and Company Wars:** Play Nice But Win. California, 07 Set. 2022. Disponível em: https://podcasts.apple.com/. Acesso em: 12 dez. 2022.

ABREU, Jacqueline de Souza. **Passado, presente e futuro da criptografia forte:** desenvolvimento tecnológico e regulação. Revista Brasileira de Políticas Públicas, v.7, n. 3, 2017, p. 25-43.

ABREU, Jacqueline de Souza. **Privacidade, segurança e tecnologia.** 2022. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2022 (No prelo).

ADC. Tu y yo digital. **Descubriendo las narrativas sobre identidad y biometría en América Latina**: los casos de Argentina, Brasil, Colombia y México, 2019, p. 18.

ASHWORTH, J. **The elasticity of mens rea**. In: Crime, proof and punishment. Essays in Memory of Sir Rupert Cross, 1981.

BADARÓ, Gustavo. **Interceptação de Comunicações telefônicas e telemáticas:** limites ante o avanço das tecnologias. In: LIMA, Joel Corrêa; CASARA, Rubens R. Temas para uma Perspectiva Crítica do Direito, Homenagem ao Professor Geraldo Prado. Rio de Janeiro, 2010, p. 499.

BARONA VILAR, Silvia. **Algoritmización del Derecho y de la Justicia.** De la inteligencia artificial a la Smart Justice. València: Tirant lo Blanch, 2021.

BATISTA, Nilo. **Matrizes ibéricas do Sistema Penal Brasileiro.** 2ª Ed. Rio de Janeiro: Ed. Revan, Instituto Carioca de Criminologia, 2002.

BAUDRILLARD, Jean. Tela total: mito-ironias do virtual e da imagem. 3. ed. Porto Alegre: Sulina, 2003; VIRILIO, Paul. **A bomba informática.** São Paulo: Estação Liberdade, 1999.

BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. **Proteção de dados no campo penal e de segurança pública:** nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020, p. 10-12.

CONSELHO DA EUROPA, **Practical guide on the use of personal data in the police sector**. Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data. 2018.

DELGADO MARTIN, Joaquín. **Judicial-Tech, el proceso digital y la transformación tecnológica de la justicia.** Obtención, tratamiento y protección de datos en la jurisprudencia. Madrid: Wolters Kluwer, 2022. p. 34.

DI IORI, Ana Haydée [et al.]. **Guía Integral de Empleo de la Informática Forense en el Proceso Penal**. 1a ed. Mar del Plata: Universidad FASTA, 2015.p. 23. Aprovado pela Resolución de la Procuración General de la Suprema Corte de Justicia de la prov. de Buenos Aires (Res. 483/16). Disponível em: https://www.mpba.gov.ar/files/documents/483-16.zip Acesso em: 10 mai. 2022.

EILBERG, Daniela Dora. **Ciclo de vida dos dados da prova penal digital:** Considerações para uma teoria geral da prova digital além da gestão de caráter securitário, 2024, 229p. Tese (Doutorado) – Programa de Pós-Graduação em Ciências Criminais, PUCRS.

EILBERG, Daniela; MOSCATELLI, Livia. **Comunicações telemáticas, avanços tecnológicos e vigilância no contexto dos maxiprocessos**. In: Anais do 11º Congresso Internacional de Ciências Criminais, 2020, p.4.

EILBERG, Daniela; SALIBA, Pedro; ZANATTA, Rafael. **Uma questão de justeza procedimental:** regulamentação do reconhecimento fotográfico e ciclo de vida dos dados. Ensaio sobre o ciclo de vida dos dados na procedimentalização do reconhecimento fotográfico, 2021. Disponível em: https://www.dataprivacybr.org/uma-questao-de-justeza-procedimental/. Acesso em: 20 mai 2022.

ESTELLITA, Heloisa Estellita. **O acesso do MP a dados protegidos por sigilo fiscal e a decisão do STJ**. CONJUR. Disponível em: https://www.conjur.com.br/2022-fev-17/estellita-acesso-mp-dados-sigilo-fiscal-stj/. Acesso em: 20 de mai. 2022.

ESTELLITA, Heloisa. **O RE 1.055.941:** um Pretexto para Explorar Alguns Limites à Transmissão, Distribuição, Comunicação, Transferência e Difusão de Dados Pessoais pelo COAF. Dossiê – Privacidade e Proteção de Dados Pessoais na Segurança Pública e no Processo Penal. RDP, Brasília, v.18, n. 100, 606-636, out./dez. 2021.

ESTELLITA, Heloisa; GLEIZER, Orlandino. **A investigação penal de insuspeitos.** STJ fere direitos ao exigir coleta massiva de dados. Disponível em: 12 set. 2020. Disponível em: https://www1.folha.uol.com.br/opiniao/2020/09/a-investigacao-penal-de-insuspeitos.shtml. Acesso em: 10 out. 2021.

FERRAJOLI, Luigi. **Por uma teoria dos direitos e dos bens fundamentais.** Tradução Alexandre Salim, Alfredo Copetti Neto, Daniela Cademartori, Hermes Zaneti Júnior, Sérgio Cademartori. Porto Alegre: Livraria do Advogado, 2011.

FIGUEIREDO DIAS, Jorge de. **A criminalidade organizada do fenômeno ao conceito jurídico-penal**. Revista Brasileira de Ciências Criminais, n. 71, 2008, p. 22-23.

GASCÓN INCHAUSTI, Fernando. **Desafíos para el proceso penal en la era digital:** externalización, sumisión pericial e inteligencia artificial. In: CONDE FUENTES, Jesús; SERRANO HOYO, Gregorio (dir.). **La justicia digital en España y la Unión Europea**: situación actual y perspectivas de futuro. Barcelona: Atelier Libros Jurídicos, 2019, p. 191-206.

GOMES FILHO, Antônio Magalhães. *Provas*. In: MOURA, Maria Thereza Rocha de Assis. **As reformas no processo penal:** as novas leis de 2008 e os projetos de reforma. São Paulo: Editora Revista dos Tribunais, 2008.

GOMES FILHO, Antonio; BADARÓ, Gustavo. *Prova e sucedâneos de prova no processo penal brasileiro.* **Revista Brasileira de Ciências Criminais**, vol. 65, 2007.

GOMES FILHO, Antonio; BADARÓ, Gustavo. *Prova e sucedâneos de prova no processo penal brasileiro.* **Revista Brasileira de Ciências Criminais**, vol. 65, 2007. GOMES FILHO, Antônio Magalhães. *Provas*. In: MOURA, Maria Thereza Rocha de Assis. **As reformas no processo penal:** as novas leis de 2008 e os projetos de reforma. São Paulo: Editora Revista dos Tribunais, 2008.

GRECO, Luis: **Introdução – o inviolável e o intocável no direito processual penal**. In: Wolter, Jünger: **O inviolável e o intocável no direito processual penal:** reflexões sobre a dignidade humana, proibições de prova, proteção de dados (e separação informacional dos poderes) diante da persecução penal. São Paulo: Marcial Pons, 2018.

INTERNETLAB. **O direito das investigações digitais no Brasil**: fundamentos e marcos normativos, 2022.

JØRGENSEN, Rikke Frank. **Rights Talk:** In the Kingdom of Online Giants. In: JØRGENSEN, Rikke Frank (ed.). **Human Rights in the Age of Platforms**. Cambridge: The MIT Press, 2019, p. 176.

LOPES JR. Aury**. Direito processual penal.** 13ª ed. São Paulo. Saraiva, 2019, p. 671.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data:** a revolution that will transform how we live, work, and think, 2014.

MENDES, Laura. **A autodeterminação informativa:** a história de um conceito. Revista de Ciências Jurídicas Pensar, v.25, n. 4, p.1-18, out/dez 2020.

MITSILEGAS, Valsamis. **The privatisation of mutual trust in Europe's Area of Criminal Justice**: the Case of E-evidence. Maastricht Journal of European and Comparative Law 3, n. 25, 2018, p. 263-265.

POLYVIO, P G. **Illegally obtained evidence and R v Sang**. In: Crime, proof and punishment. Essays in Memory of Sir Rupert Cross,1981, p. 228.

PRADO, Geraldo. **A produção da prova penal e as novas tecnologias:** o caso brasileiro, 2013. Disponível em: https://emporiododireito.com.br/leitura/a-producao-da-prova-penal-e-as-novas-tecnologias-o-caso-brasileiro. Acesso em: set. 2020.

PRADO, Geraldo. **Notas sobre proteção de dados, prova digital e o devido processo penal**, 2020. Disponível em: https://geraldoprado.com.br/artigos/notas-sobre-protecao-de-dados-prova-digital-e-o-devido-processo-penal/. Acesso em: 20 jan. 2021.

PRADO, Geraldo. *Parecer*: investigação criminal digital e processo penal. **Revista Brasileira de Ciências Criminais,** v. 199, ano 31, pp. 315-359. São Paulo: Ed. RT, nov/dez. 2023, p. 316-317.

RAMALHO, David Silva. **Recolha de prova penal em sistemas de computação em nuvem.** Revista de Direito Intelectual, n. 2, 2014, pp. 95-122.

RENAN, Daphne. **The Fourth Amendment as Administrative Governance.** Stanford Law Review, 2016. p. 1052.

SALT, Marcos. **Obtención de pruebas informáticas en extraña jurisdicción:** Los "Conflictos" del principio de territorialidad en un mundo virtual sin Fronteras. In: DUPUY, Daniela. KIEFER, Marianna. CIBERCRIMEN **Aspectos de Derecho penal y procesal penal.** Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet. Buenos Aires: Editora B de F, 2016.

SANT'ANA, Ricardo. **Ciclo de vida dos dados: uma perspectiva a partir da ciência da informação.** Rev. Informação & Informação, Londrina, v. 21, 2016, n.2, p. 116 - 142. Disponível em: https://www.uel.br/revistas/uel/index. php/informacao/article/view/27940. Acesso em: 22 mai 2023.

SANTORO, Antonio Eduardo Ramires**. A imbricação entre maxiprocessos e colaboração premiada**: o deslocamento do centro informativo para a fase investigatória na Operação Lava Jato. Rev. Bras. de Direito Processual Penal, Porto Alegre, v. 6, n. 1, p. 81-116, jan.-abr. 2020, p. 88-90.

SOLOVE, Daniel J. **A taxonomy of privacy. University of Pennsylvania Law Review,** v. 154, jan/ 2006, p. 477 – 560.

STOYKOVA, Radina. **The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations**. Computer Law & Security Review. V. 49, Jul 2023. https://doi.org/10.1016/j.clsr.2023.105801.

TOSZA, Stanislaw. **The e-evidence package is adopted end of a saga or beginning of a new one?** European Data Protection Law Review. v. 9, n. 2, 2023.

UNODC. **Conscientização sobre o local de crime e as evidências materiais em especial para pessoal não-forense,** 2010. Disponível em: <https://www.unodc.org/documents/scientific/Crime_Scene_Awareness_Portuguese_Ebook.pdf

WATT, Eliza. **The right to privacy and the future of mass surveillance**. The International Journal of Human Rights. pp. 773-799, 2021, p. 775.

Submissão: 21/11/2024. Aprovação: 26/11/2024.