PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
ESCOLA DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS CRIMINAIS
DOUTORADO EM CIÊNCIAS CRIMINAIS

RODRIGO OLIVEIRA DE CAMARGO

TRATAMENTO DE DADOS, PERSECUÇÃO PENAL E A GARANTIA DO DIREITO DE DEFESA

Porto Alegre
2022

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
ESCOLA DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS CRIMINAIS
DOUTORADO EM CIÊNCIAS CRIMINAIS

RODRIGO OLIVEIRA DE CAMARGO

TRATAMENTO DE DADOS, PERSECUÇÃO PENAL E A GARANTIA DO DIREITO DE DEFESA

Porto Alegre
2022

Dados Internacionais de
Catalogação na Publicação (CIP)

Ficha Catalográfica

C172t Camargo, Rodrigo Oliveira de

Tratamento de Dados, Persecução Penal e a Garantia do Direito de Defesa / Rodrigo Oliveira de Camargo. – 2022.
210 f.
Tese (Doutorado) – Programa de Pós-Graduação em Ciências Criminais, PUCRS.

Orientador: Prof. Dr. Fabrício Dreyer de Ávila Pozzebon.

1. Tratamento de Dados. 2. Dados Pessoais. 3. Fontes Abertas. 4. Persecução Penal. 5. Paridade de Armas. I. Pozzebon, Fabrício Dreyer de Ávila. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da PUCRS
com os dados fornecidos pelo(a) autor(a).
Bibliotecária responsável: Clarissa Jesinska Selbach CRB-10/2051

RODRIGO OLIVEIRA DE CAMARGO

TRATAMENTO DE DADOS, PERSECUÇÃO PENAL E A GARANTIA DO DIREITO DE DEFESA

Tese para fins de cumprimento de requisito parcial para obtenção do grau de Doutor em Ciências Criminais pelo Programa de Pós-Graduação em Ciências Criminais da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul.

Orientador: Prof. Dr. Fabrício Dreyer de Ávila Pozzebon

Porto Alegre

2022

RODRIGO OLIVEIRA DE CAMARGO

TRATAMENTO DE DADOS, PERSECUÇÃO PENAL E A GARANTIA DO DIREITO DE DEFESA

Tese para fins de cumprimento de requisito parcial para obtenção do grau de Doutor em Ciências Criminais pelo Programa de Pós-graduação em Ciências Criminais da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul.

BANCA EXAMINADORA

_____

Prof. Dr. Fabrício Dreyer de Ávila Pozzebon

_____

Professor Dr. Ricardo Ferreira Breier

_____

Professor Dra. Gustavo Noronha de Ávila

_____

Professor Dr. Alexandre Morais da Rosa

_____

Professora Dra. Keity Saboya

RESUMO

O problema central da investigação é compreender onde se encontra o espaço de garantia da defesa nas atividades de tratamento de dados pessoais e abertos, especialmente no que guarda relação com a com a persecução penal e o respeito à paridade de armas. Problema esse inserido na necessidade, mais do que urgente, de interseccionar as áreas temáticas relacionadas à tecnologia, especificamente o tratamento de dados, com aquelas relativas à investigação criminal, processo penal e o direito de defesa. O tema foi delimitado em torno de métodos de tratamentos de dados à disposição das agências de controle do poder punitivo e, como objetivo geral, nos propusemos a identificar como cada um deles garante o exercício do direito de defesa. A partir daí, passamos a demonstrar como, em relação ao processo penal, tais direitos são, muitas vezes, insuficientes e a propor alternativas a esta realidade para assegurar os princípios constitucionais relacionados ao processo penal em meio às atividades de tratamento de dados, mormente o devido processo legal e suas principais ramificações: contraditório, ampla defesa e paridade de armas. Estruturado em cinco capítulos, o trabalho parte da contextualização do leitor na realidade de uma nova formação social onde a informação advinda do contexto tecnológico passa a ser considerada a chave da economia mundial e que insere a convergência tecnológica como condição de mudança na essência do ser humano e das estruturas de poder, para, então, apresentar o atual estado da arte em relação ao tratamento de dados pessoais e provenientes de fontes abertas para fins de persecução penal e como forma de garantia da defesa. A pesquisa adotou como estratégia metodológica a revisão sistemática, a análise crítica de pesquisa bibliográfica, pesquisa jurisprudencial e análise jurídico-dogmática de marcos nacionais e internacionais. A conclusão nos leva à emergência de discussão sobre a necessidade de novos direitos, prerrogativas e estruturas às defesas para suportar, com segurança, o exercício de suas atribuições, propondo-se alterações nos códigos deontológicos da advocacia e defensoria para assegurar o tratamento de dados como direito inerente às atividades de defesa.

Palavras-chave: Tratamento de Dados. Dados Pessoais. Fontes Abertas. Persecução Penal. Paridade de Armas.

ABSTRACT

The central problem of the investigation is to understand where the space for defense protection is in the activities of processing personal and open data, especially in relation to criminal prosecution and respect for the equality of arms. This problem is inserted in the urgent need to intersect the thematic areas related to technology, specifically data processing, with those related to criminal investigation, criminal procedure and the right of defense. The theme was delimited around data processing methods available to agencies that control punitive power and, as a general objective, we proposed to identify how each one of them protects the exercise of the right to defense. From there, we went on to demonstrate how, in relation to the criminal process, these rights are often insufficient and to propose alternatives to this reality in order to assure the constitutional principles related to the criminal process in the midst of data processing activities, especially the due legal process and its main ramifications: adversarial process, ample defense, and equality of arms. Structured in five chapters, the work begins with the contextualization of the reader in the reality of a new social formation where the information coming from the technological context is now considered the key to the world economy and which inserts the technological convergence as a condition for change in the essence of the human being and the structures of power, in order to then present the current state of the art in relation to the treatment of personal data from open sources for the purposes of criminal prosecution and as a form of defense protection. The research adopted as methodological strategy the systematic review, the critical analysis of bibliographical research, jurisprudential research and legal-dogmatic analysis of national and international frameworks. The conclusion leads us to the emergence of discussion about the need for new rights, prerogatives and structures to the defenses to support, safely, the exercise of their duties, proposing changes in the deontological codes of law and defense to ensure the processing of data as a right inherent to the activities of defense.

Keywords: Data Processing. Personal Data. Open Sources. Criminal Prosecution. Parity of Arms.

SUMÁRIO

INTRODUÇÃO

A temática pesquisada insere-se na linha de pesquisa "Sistemas Jurídico-Penais Contemporâneos" do Programa de Pós-Graduação da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul, fruto das discussões estabelecidas há, aproximadamente, quatro anos no âmbito do curso de Doutorado em Ciências Criminais e que indicam a emergência da inserção do componente tecnologia nos debates afeitos a todos os ramos das Ciências Criminais: Criminologia, Direito Penal, Processo Penal e, até mesmo, Criminalística e Política Criminal.

Nos últimos 20 anos, interessados em transformação digital anunciam que dados são o petróleo do futuro, mas, ao contrário deste, cujas reservas um dia hão de acabar, aqueles são produtos em abundância, cujas ofertas só aumentam. Na última virada do século, entre as maiores 15 empresas do mundo, nenhuma baseava suas atividades no rastreamento e tratamento de dados pessoais, situação totalmente diferente de hoje, já que em torno de metade das companhias que figuram no *ranking* das maiores do globo baseia-se em técnicas de *analytics*. A capacidade de fazer um bom uso desses dados e aproveitar seu potencial oferece uma enorme gama de vantagens. No âmbito da investigação e do processo penal, poderíamos estabelecer como hipótese que isso pode significar algum tipo de vantagem em razão de novas possibilidades, chances, ocasiões ou oportunidades que esta nova realidade cria para superar os níveis de incerteza próprios das atividades inerentes à persecução penal.[1] Por outro lado, não se podem negar os aspectos de garantia da intimidade, privacidade e a proteção de dados pessoais, de forma que também é importante refletir sobre os conjuntos de regras e formas de controle para o uso desses dados.

As mais simples atividades que desenvolvemos atualmente deixam uma enorme cadeia de rastros digitais, os quais, combinados com dispositivos baseados em técnicas de Inteligência Artificial, extraem valor dos dados, fonte de inesgotáveis possibilidades, questão até pouco tempo atrás por nós, das Ciências Criminais, totalmente ignorada. O modelo de *business intelligence*, atividade desenvolvida no cenário corporativo que se debruça sob a captura e formulação de dados e possibilita extrair *insights* e resultados valiosos para o andamento da empresa e previsão dos cenários futuros, agora transcende o mundo dos negócios. A realidade das práticas de tratamento de dados, assim compreendida como toda

[1] GOLDSCHMIDT, James. **Princípios generales del processo: problemas juridicos y políticos del proceso penal.** Vol. II. Buenos Aires: E.J.E.A., [20--]. p. 71-93.

operação realizada com dados de fontes heterogêneas – como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, uso compartilhado, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração –, cada vez mais permeia as atividades inerentes a toda a cadeia de atos do sistema de Justiça, inclusive o criminal. A Era da Informação causou rupturas em todas as estruturas sociais em uma velocidade espantosa, e os paradigmas tradicionais do Direito têm sofrido impactos de todas as ordens, situação que não é diferente nos campos do processo penal e da investigação criminal.

O advento da Lei Geral de Proteção de Dados tratou de regulamentar as atividades de tratamento de dados pessoais em diversos campos, mas ainda não por parte de autoridades públicas para fins de segurança pública e persecução penal – já que seus agentes demandam (e reclamam) certas prerrogativas para o desempenho de suas atividades. Tal quadro reserva espaços para a formulação de legislação específica que, no plano internacional, encontra orientação na Convenção de Budapeste (Diretiva nº 2016/680) e serve de baliza para as propostas hoje existentes no Brasil acerca do tema: o *Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal*, ofertado pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados, e o *Projeto de Lei nº 1.515/2022*, de autoria do deputado Coronel Armando (PL-SC), este atualmente em trâmite na Câmara dos Deputados, instrumentos que nesta tese foram objetos de análise em relação às suas bases principiológicas e a formas de como se garantir os interesses da defesa.

Mas o tratamento de dados para fins de segurança pública e persecução penal não se limita a dados pessoais. O poder computacional e o desenvolvimento de técnicas e ferramentas baseadas em *analytics* passaram a municiar qualquer um que tenha um letramento mínimo para processar quantidades de dados alocados em fontes abertas, entregando valor em termos de inteligência. Isso não é ignorado pelos órgãos responsáveis pela persecução penal, que cada vez mais empregam a técnica para o desempenho de suas atividades nos âmbitos da investigação e do processo. Avanços ocorridos em matéria de investigação judicial com ferramentas de *inteligência de fontes abertas* estão na mira das agências policiais, dos Ministérios Públicos e até mesmo do Tribunal Penal Internacional, que investem em conteúdos, técnicas, ferramentas e abordagens diferenciadas de critérios de busca para que os seus operadores conheçam com profundidade as bases de uma cultura digital, incorporem suas atividades nessas plataformas e orientem-se com respeito ao caráter legal de investigações nas redes.

A tese se concentrou em buscar compreender onde se encontra o espaço da garantia da defesa nas atividades de tratamento de dados pessoais e abertos, especialmente no que guarda relação com a persecução penal e o respeito à paridade de armas, problema inserido na necessidade de interseccionar as áreas temáticas relacionadas à tecnologia, especificamente o tratamento de dados, com aquelas relativas à investigação criminal, ao processo penal e ao direito de defesa. A proposta passou a ser a de compreender os métodos de tratamentos de dados à disposição das agências de controle do poder punitivo, de forma a identificar como cada um deles se relaciona com a garantia do exercício do direito de defesa, tendo por hipótese principal que, em relação ao processo penal e no contexto emergente de investigações sumárias, os direitos existentes e a mera alusão a princípios constitucionais são insuficientes, razão pela qual parece ser necessária a busca de alternativas para dar eficácia ao direito de defesa em meio às atividades de tratamento de dados.

Sobre todos esses aspectos, pouca ou quase nenhuma literatura existe no Brasil, o que nos desafiou a desenvolver as presentes reflexões, que não se limitaram à análise bibliográfica, mas também nos motivou a buscar outras fontes relacionadas às formas como os tradicionais agentes da persecução penal se preparam e se estruturam em uma realidade que exige adaptação aos mecanismos de proteção contra ataques cibernéticos e de antecipação estratégica por meio de dispositivos que prometem performar exponencialmente no âmbito probatório. Isso incluiu a análise, por exemplo, de editais, pelos quais esses órgãos licitam cessões de direitos de uso sobre programas de computador para tratamentos de dados com o objetivo de subsidiar tecnicamente as atividades de inteligência e investigação. A busca não se limitou ao enfrentamento da realidade brasileira, trazendo ao leitor referências produzidas em países da Europa, nos Estados Unidos da América e, também, naqueles mais próximos, a exemplo da Argentina.

A pesquisa adotou como estratégia metodológica a análise crítica de pesquisa bibliográfica, pesquisa jurisprudencial e análise jurídico-dogmática de marcos nacionais e internacionais. O trabalho foi estruturado em cinco capítulos.

No primeiro capítulo, o esforço se concentrou em apontar breves notas daquilo que optamos por chamar de sociedade multidados, uma formação social em que a informação advinda do contexto tecnológico passa a ser considerada a chave da economia mundial e que insere a convergência tecnológica como uma condição de mudança na própria essência do ser humano, na medida em que a Inteligência Artificial será a responsável pela causação de profundas rupturas na forma de organização social e pela próxima revolução na produção econômica, que enxerga o tratamento de dados como o novo ópio da sociedade. Nele, também

foi importante extrair as estratégias utilizadas por grandes corporações para transformar dados e informações através de sua coleta, análise e seu emprego ético e legal sobre a capacidade, a vulnerabilidade e as intenções de concorrentes, com o objetivo de obter maior conhecimento e desencadear decisões assertivas. Não demorou para que os métodos se transformassem em instrumentos de controle para atender interesses de governos, os quais passaram a demandar a ampliação das prerrogativas de acesso a dados de usuários mantidos por empresas e possibilidades de coleta e tratamento de dados pessoais para, em nome dos discursos de defesa nacional e segurança pública, subsidiar processos de investigação e de persecução penal, criando uma série de riscos aos direitos fundamentais associados às atividades. Dentre eles, a tese pinça a paridade de armas.

O segundo capítulo foi destinado a analisar os regramentos específicos relativos à proteção das pessoas no que diz respeito ao tratamento de dados pessoais em âmbito geral e pelas autoridades, organismos ou entidades designados para o exercício da autoridade e dos poderes públicos, para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais. Nesse sentido, foram cotejados instrumentos legais como o Regulamento nº 2.016/679, do Parlamento Europeu e do Conselho (LGPD); a Diretiva nº 95/46/CE (RGPD); a Diretiva nº 2.016/680, do Parlamento Europeu e do Conselho (Convenção de Budapeste); a Lei Orgânica de Proteção de Dados Pessoais e Garantia de Direitos Digitais (LOPDPGDD); o Marco Civil da Internet (Lei nº 12.965/2014); a Lei Geral de Proteção de Dados (Lei nº 13.709/2018); a Lei Orgânica da Espanha nº 13/2015 que altera a Ley de Enjuiciamento Criminal; o Anteprojeto da Comissão de Juristas LGPD Penal e o Projeto nº 1.515/2022, da Câmara dos Deputados, de forma a extrair suas principais categorias e princípios, bem como verificar de que forma oferecem instrumentos para a garantia do direito de defesa. Propôs-se, a partir daí, a análise da decisão que decretou a nulidade por ofensa à paridade de armas em razão do tratamento de dados pessoais, pelo Ministério Público do Estado do Rio Grande do Sul (MPRS), de integrantes da lista de jurados no Caso Kiss, buscando arrolar práticas atentatórias à principiologia estabelecida pela Convenção de Budapeste e delineada no Anteprojeto da Comissão de Juristas para a elaboração da LGPD Penal no Brasil. Esse exercício se deu de modo a, para além de apontar para a efetiva violação da paridade de armas, verificar se tais atividades estão se desenvolvendo dentro de um comportamento lícito, em harmonia com as normas e os projetos que protegem os dados pessoais para as atividades que tenham por escopo prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais

O terceiro capítulo correlaciona o tratamento de dados e produção de inteligência em fontes abertas e sua relação com a persecução penal e o direito de defesa. Busca localizar na doutrina o termo “fonte aberta” como categoria jurídica e compreender sua importância em busca de outros elementos de constatação nas atividades relacionadas à persecução penal, a chamada *inteligência de fontes abertas*.

De um lado, foi importante compreender o desenvolvimento de políticas públicas voltadas aos dados governamentais abertos e à flexibilidade na divulgação das informações públicas para o exercício de uma série de direitos, inclusive nos âmbitos da investigação e do processo e que asseguram eficácia do acesso à informação, fornecendo direitos que podem ser exercidos por intermédio de pedidos de acesso à informação. De outro, a análise denunciou que existe uma persistente confusão entre investigação e inteligência, que agências de aplicação da lei planejam, preparam, coletam e produzem inteligências, baseadas em técnicas e ferramentas para a obtenção de informações por intermédio de dados públicos ou publicados na internet, para a tomada de decisões assertivas e favorecem a definição de linhas de investigação e argumentação.

Como tal atividade não se encontra orientada por princípios claros ou métodos certificados, restou constatado que Polícia e Ministério Público operam com discricionariedade e longe do alcance dos demais sujeitos no campo da *investigação preparatória* por intermédio de práticas subjetivamente orientadas, antecedentes à investigação preliminar e voltadas a conhecer o ambiente criminoso, progressivamente atraídas para a esfera de atribuições do Ministério Público, o quarto capítulo apontou para o empreendimento desviante das atividades usualmente qualificadas como preventivas para fins repressivos.

Outra hipótese que nasceu a partir daí é a de que, assim como o tratamento de dados pessoais, a inteligência de fontes abertas também surge como importante instrumento a favor dos agentes privados, já que permite não apenas fomentar a apresentação de notícias de fatos, instrumentalizar queixas, fazer com que as partes, em qualquer polo de atuação, apresentem evidências obtidas juntamente com as suas alegações, mas também viabilizar a produção de fontes de prova, de forma que, a partir desses elementos, proponha-se a produção de outras. Por sua emergente importância no sistema de Justiça criminal e agências de aplicação da lei, buscou-se fazer uma breve gênese da atividade, de forma a compreender suas origens, seus fundamentos, sua metodologia de trabalho e suas ferramentas, sem a pretensão de esgotar o tema nestes pontos.

Por fim, constatando que a investigação e a acusação gozam de maiores recursos e acesso a melhores tecnologias para obter resultados para propor como meios de prova, a defesa, desprovida de elementos para contrariar, ainda é onerada pela dificuldade de contrapor e colocar em questão a credibilidade da prova, o que impõe a busca por meios normativos e estruturais para superar o abismo entre investigação/acusação e defesa no ambiente tecnológico, o que passa pela mudança do *mind set* defensivo e incorporação da mentalidade do tratamento de dados em suas atividades. Os domínio de ferramentas, acesso a plataformas e emprego de linguagem digitais demandam a mediação entre as narrativas cibernética e jurídica, já que esse aparato tecnológico, antes concentrado exclusivamente nas mãos das autoridades públicas e amplamente utilizadas para o exercício do controle, hoje torna-se disponível para todos os tipos de finalidade e de interesses na obtenção de informações, o que reafirma a emergência no debate sobre a descentralização do poder de investigar. Se informação é coisa pública, investigação significa acesso ao poder de saber, e existe uma modificação significativa na sociedade a partir do advento das experiências tecnológicas e a ampliação de métodos de acesso à informação. Essas circunstâncias fundamentam o direito à participação e a ampliação do direito à informação nos atos que levam a decisões de poder, de forma que se legitima o tratamento de dados pessoais ou abertos pelos responsáveis pela defesa quando isso surgir de uma obrigação legal ou for necessário para o exercício de seus poderes, o que demanda pensar essa perspectiva estruturalmente, normativamente e deontologicamente, em que foram concentrados os esforços para a conclusão desta tese.

1. BIG DATA E TRATAMENTO DE DADOS

1.1. Breves notas sobre a sociedade multidados

Uma grande característica do século XXI é a multiplicidade de informações. Se desde os primórdios das civilizações governos se preocupavam em censurá-las ou apoderar-se delas[2] – o poder do conhecimento e do saber é o maior poder que se instala sobre a Terra[3] –, hoje, nenhum deles pode semear a esperança de centralizá-las: há demasiada informação, e é preciso criar a capacidade de que as pessoas extraiam algum sentido útil dos elementos que recebem, percebam a diferença do que interessa ou não e, sobretudo, desenvolvam a capacidade de combinar fragmentos de dados.

O princípio positivista segundo o qual "quanto maior é o saber, maior é o poder" cristalizou-se de maneira tão formidável em nossa sociedade que parecia uma verdade incontestável de que, com mais conhecimentos científicos, o homem teria mais poder. Hoje, o que já se questiona é como deter o poder que condiciona o saber. Não são poucos os autores que denunciam estruturas de poder e toda a sua maquinaria, que se valem de ideologias de ocultação e criadoras de uma determinada realidade.[4] A história concebeu distintas estruturas de poder com participação mais ou menos equitativa, mas, ao longo do tempo, sempre manteve acesa a relação hegemonia-marginalização.[5]

A informação advinda do contexto tecnológico é considerada a chave da economia mundial, uma substância, talvez a única, que cresce com o uso, ao contrário de bens naturais. Nos dias de hoje, é uma economia em abundância que tende a conceder acesso universal com a melhoria da infraestrutura que ocorrerá, naturalmente ou à força. Isso implica a possibilidade de que seja necessária uma reforma social e política: tal qual fora necessário remover as velhas estruturas do poder monárquico para dar acesso ao povo no processo democrático, o processo de comunicação e controle da informação "poderá ter que ser lançado para fora da nossa existência". Ainda que a transição tenha chegado de forma muito pacífica por conta do uso doméstico das tecnologias, o controle de produção e emissão

---

[2] FOUCAULT, Michel. **A verdade e as formas jurídicas**. 3. ed. Rio de Janeiro: Nau Editora, 2002. p. 7-13.
[3] BACON, Francis. **O progresso do conhecimento.** Tradução, apresentação e notas Raul Fiker. São Paulo: Editora Unesp, 2007. p. 56-93.
[4] WEBER, Max. **Ciência e política: duas vocações**. 18. ed. São Paulo: Cultrix, 2011. p. 62; FOUCAULT, Michel. **Em defesa da sociedade**. São Paulo: Martins Fontes, 1999. p. 30-32; GALBRAITH, J. Kenneth. **Anatomia do Poder**. 2. ed. São Paulo: Pioneira, 1986. p. 1-38.
[5] ZAFFARONI, Raúl Eugenio; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro**: parte geral. 5. ed. São Paulo: Revista dos Tribunais, 2004. p. 62-77.

colocado na mão do usuário traz uma nova dimensão, sobretudo ao que nos interessa especialmente, no que diz respeito à produção e coleta de elementos de informação. O advento da tecnologia de transmissão estimulada pelas redes móveis entrega o poder de difusão na mão dos indivíduos, tornando-os fornecedores de informação em todas as áreas[6] – e a investigação preliminar e o processo penal não estão alheios a essa realidade.

O mundo conectado e interdependente tem dimensões além de fronteiras e nacionalidades, ampliados pela internet, redes sociais e comunicações móveis inteligentes, causando mudanças sociais velozes e drásticas, trazidas pelas possibilidades oferecidas por tecnologias novas e emergentes, afetando cidadãos em suas conexões mais amplas, setor privado, governo e polícia[7]. Conceitos formulados em épocas distintas são totalmente insuficientes para explicar a dinâmica social atual e, sem que detenhamos a vantagem da visão retrospectiva, a certeza moral pode estar fora do nosso alcance. A complexidade global tomou dimensão maior do que aquela a que se acostumaram os nossos cérebros, e a produção das grandes injustiças contemporâneas resultam justamente dessa dificuldade que temos em compreender e nos adaptar a esses vieses estruturais: somos cúmplices desses vieses e simplesmente não temos tempo nem energia para descobrir todos eles. Com a substituição dos processos de tomadas de decisões promovidos pelo advento da Inteligência Artificial, nossos conceitos de humanidade e de vida também deverão sofrer profundas mudanças.[8] Ao passar dos humanos para os algoritmos a autoridade, temos de perceber o universo inteiro como um sistema universal de fluxo de dados e informações.

Hoc Est Corpus. Hocus Pocus: a raça humana estruturou-se em torno de narrativas, não de números gráficos. Mitos, deuses, reis, guerras, conquistas, heróis e vilões permearam o imaginário social e são elementos recorrentes em todas as civilizações na eterna busca para dar sentido à existência. A narrativa sempre foi o núcleo estruturante de uma dada realidade. Para fazer com que parecesse real, o abstrato ganha vida através dos rituais, alternativa encontrada há milhares de anos por sacerdotes e xamãs para que os homens efetivamente acreditassem nessas narrativas.[9] O contraditório de tudo isso é que ritos e rituais também

---

[6] KERCHOVE. **A Pele da Cultura: investigando a nova realidade electrônica**. São Paulo: Annablume, 2009. p. 76.

[7] STANIFORTH, Andrew. Police Use of Open Source Intelligence: The Longer Armo f Law. *In*: AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 21-31.

[8] BECK, Ulrich. **A metamorfose do mundo**: novos conceitos para uma nova realidade. Rio de Janeiro: Zahar, 2018. p. 81-139.

[9] "*The word 'hocus-pocus' is now a common designation (at least in the English language) for 'a cheat or impostor' and refers originally to the conjurer who by legerdemain deceives the people and pretends to work miracles. In German the word is used mainly in the sense of 'sleight-of-hand', designating not the performer, but*

foram – na verdade, ainda são – utilizados justamente para obstaculizar o acesso "à verdade definitiva da vida". Existe um poder ainda pulsante no mundo moderno que é produto do acúmulo de todas essas narrativas e que orienta estruturas sociais e políticas de longa duração, em que o sacrifício, a imposição do sofrimento, dentre todos os rituais, surge como o mais real. Incapazes de corresponder ao ideal, as pessoas voltam-se para o sacrifício como uma solução, prática que igualmente pode vir a ser reproduzida em pleno século XXI.[10]

Para construir a pesquisa que embasou esta tese, partimos da premissa de que investigação e processo são formas de saber-poder. Não é um conteúdo em si, mas uma forma de saber, produto da soma do exercício de um determinado tipo de poder e da utilização de determinado número de técnicas e procedimentos que, por meio da instituição judiciária veio a ser, sobretudo na cultura ocidental, uma forma de autenticação e transmissão de uma verdade.[11] Toda atividade judicial é um "saber-poder", uma combinação de conhecimento (*veritas*) e de decisão (*auctoritas*) na qual, em tal entrelaçamento, quanto maior é o poder tanto menor será o saber, e vice-versa. Como concebido por Montesquieu, o poder é "nulo" em seu modelo ideal da jurisdição, situação inversa da experimentada na realidade atual.[12]

A história do Ocidente concebeu uma forma pela qual os homens deveriam ser julgados, impondo-lhes a maneira de reparar suas condutas e punir algumas outras, práticas regulares modificadas por intermédio da história, definidas a partir de formas racionais que envolvem todas as questões subjetivas do homem e sua relação com o poder e a sociedade. Essa forma de abordagem não se restringe ao direito dado, agasalhando práticas, cultura e estrutura. Não é somente a jurisprudência, mas também os métodos de trabalho dos juristas que levam à ampliação do campo de análise para além das leis e métodos dos Tribunais para completar o estudo das práticas punitivas: sociologia, religião, economia, política, antropologia permitem a análise de outras estratégias de controle da violência, campos que possibilitam enxergar instituições e práticas jurídicas como "gênero de linguagem no qual

---

the deception by which a trick is done, and this seems to be the more original meaning of the term. The word is probably a corruption of the Latin words Hoc est corpus meum, which is the formula spoken by the priest over the sacramental bread and wine, which thereby is claimed to be transformed into the body and blood of Christ. In its modern sense the word can be traced back to the seventeenth century" (BLANTON, Anderson. **Until the Stones Cry Out**: materialities of faith and technologies of the holy ghost in southern appalachia**.** 2011. 294 f. Tese (Doutorado) – Curso de Philosophy, School of Arts and Sciences, Columbia University, Columbia, 2011. Disponível em: https://academiccommons.columbia.edu/doi/10.7916/D87W6QR0/download. Acesso em: 15 jun. 2020).

[10] HARARI, Yuval Noah. **21 Lições para o século 21**. São Paulo: Companhia das Letras, 2018. p. 347-357.

[11] FOUCAULT, Michel. **A verdade e as formas jurídicas**. 3. ed. Rio de Janeiro: Nau Editora, 2002. p. 75-78.

[12] FERRAJOLI, Luigi. **Direito e Razão**: teoria do garantismo penal. 3. ed. São Paulo: Revista dos Tribunais, 2002. p. 38-40.

suas ideias fundamentais são expressas"[13]. O implemento da sociedade tecnológica traz outra velocidade ao problema.

Os fluxos de informação que durante séculos fundaram os poderes dos Estados hoje lhes fogem ao controle, e a saída – a tentativa de controlar a informação pela proibição da difusão da tecnologia da criptografia –, em uma das maiores ironias históricas, deixa Estado e sociedade vulneráveis a ataques vindos da periferia da rede. Uma clara ilustração é o ataque sem precedentes realizado ao sistema informatizado do Tribunal de Justiça do Estado do Rio Grande do Sul (TJRS), que teve seus dados aprisionados por um sistema que emite mensagem de resgate mediante o pagamento em *bitcoins*. Além disso, o surgimento de um estado em rede, formado pela cooperação entre governos do mundo e a extensão dessa rede, criou uma rede eletrônica de governo compartilhado, sendo que Estados formatam essa rede em níveis de distinta abertura[14].

Se a revolução industrial mudou radicalmente o modo de produção da sociedade, a *convergência tecnológica* tem a capacidade de apontar para uma mudança na própria essência do ser humano, modificar a conduta pessoal e afetar seus direitos fundamentais. O desenvolvimento exponencial da Inteligência Artificial, produto da aliança da veloz evolução tecnológica com o resto de tecnologias emergentes, já provocou consequências na configuração de grandes corporações e até mesmo nas próprias pessoas, tendo o direito de proteção de seus dados pessoais sido alçado à condição de direito fundamental em grande parte dos países ocidentais.[15]

Em maior escala e mais acelerada que a Revolução Industrial, estima-se que a Inteligência Artificial será a responsável pela próxima revolução na produção econômica e na forma de organização social, causando amplas rupturas. Tarefas físicas e intelectuais poderão ser realizadas em velocidade e potência superiores à de um ser humano, causando drásticos impactos na produtividade. De tudo. A Inteligência Artificial executará tarefas que podem ser otimizadas usando dados e que não exigem nenhum tipo de interação social. Algoritmos digitais, que podem ser distribuídos sem ou a baixo custo, disseminados, atualizados e melhorados gratuitamente, não oferecem as mesmas limitações daquilo que era produzido durante a Revolução Industrial, produtos físicos que precisavam ser inventados, prototipados,

---

[13] GARAPON, Antonie; PAPAPOULOS, Ioannis. **Julgar nos Estados Unidos e na França**: cultura jurídica francesa e *Common law* em uma perspectiva comparada. Rio de Janeiro: Lumen Juris Editora, 2008. p. 5-18.
[14] CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 132.
[15] PÉREZ ESTRADA, Miren Josune. La inteligencia artificial como prueba científica en el proceso penal español. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 7, n. 2, p. 1385-1410, maio-ago. 2021.

construídos, vendidos e distribuídos. Além da forma de produção, em comparação à Revolução Industrial, dois outros catalisadores que não existiam naquela época prometem alavancar a Inteligência Artificial: a criação da indústria do capital de risco e a posição da China, desta vez lado a lado com o Ocidente no desenvolvimento e na aplicação da tecnologia[16].

Passado o marco zero, o mundo vive outra crise de desorientação, sensação de iminente e permanente catástrofe decorrente da perda das possibilidades narrativas ante a disrupção tecnológica. Se o acelerado processo de urbanização, a falta de solidariedade, as novas formas de organização das relações sociais e a influência da economia na vida dos indivíduos após a revolução industrial anonimizarem o sujeito[17], hoje o sistema político e as demais estruturas organizadas para funcionar em razão de máquinas a vapor e televisores encontram severas dificuldades em se adequar às revoluções em curso por decorrência do implemento tecnológico e da biotecnologia. Nenhum sistema político domina as novas tecnologias e, o que é pior, consegue regular seu potencial – estamos apenas engatinhando e ainda não temos a capacidade, até mesmo técnica – para compreender os impactos que surgirão com a Inteligência Artificial e a revolução de outras tecnologias, como o *blockchain*. Na verdade, o poder disruptivo dessas novas tecnologias, até pouco tempo atrás, sequer parecia estar nas agendas políticas nem mesmo das grandes nações, mas hoje todos os campos e estruturas estão sujeitos às revoluções promovidas pela tecnologia da informação e pela biotecnologia: desde sociedades e sistemas econômicos até mesmo a forma como o corpo ou a racionalidade se expressam. Acreditamos ter adquirido o poder de manipular o mundo à nossa volta e remodelá-lo conforme nossas vontades e intenções, e a experiência tecnológica nos possibilitará o poder de modelar a nossa própria mente e o mundo que está dentro de nós, grande dificuldade enfrentada nos séculos anteriores[18].

Para além das mudanças produzidas pela sociedade do risco global, existe ainda um *otimismo tecnológico determinista*. A ação, guiada pela crença na visão de mundo clássica, é modernamente sustentada no progresso ilimitado, no poder redentor da tecnociência, na disposição de recursos naturais, no crescimento econômico ilimitado e na supremacia política do Estado-nação. Os cenários de incertezas diagnosticados pela teoria da sociedade de risco fizeram todas essas crenças ruir, sobretudo em razão das suas insuficiências teóricas quando

[16] LEE, Kai-Fu. **Inteligência artificial:** como os robôs estão mudando o mundo, a forma como amamos, nos comunicamos e vivemos. Rio de Janeiro: Globo Livros, 2019. p. 181-185.
[17] DURKHEIM; Émile. Da **Divisão do Trabalho Social**. São Paulo: Abril Cultural, 1979; DURKHEIM; Émile. O **suicídio**: estudo de sociologia. São Paulo: Martins Fontes, 2000.
[18] HARARI, Yuval Noah. **21 Lições para o século 21**. São Paulo: Companhia das Letras, 2018. p. 24-28.

sobrepostas diante de cenários catastróficos, possíveis nos dias atuais.[19] Hoje, a humanidade enfrenta um momento de revolução sem precedentes e de incertezas radicais: revolução que produz a desconstrução das narrativas antigas concebidas pelo gênero humano e que se desenvolve em um ambiente repleto de desconfiança sobre o novo. As habilidades exigidas das gerações que hoje se formam, projeta-se, serão distintas das habilidades que desenvolvemos, como humanidade, nos últimos séculos.[20] Mais do que nunca, vivemos em um momento em que reina o princípio da incerteza: as coisas que pareciam fixas e imutáveis, com o advento da tecnologia e a capacitação para projetarmos e construirmos corpos, cérebros e mentes, confirma-se a impossibilidade de produzirmos crenças absolutas, até porque, como se extrai do relativismo de Einstein, "o saber é datado e tem prazo de validade"[21].

Autonomia e liberdade deixam de existir no mundo das redes, não há mais narrativa, mas a construção de predições pelo processamento da máquina. As redes que emergem da resistência de sociedades locais visam a superar o poder de redes globais, reconstruindo o mundo a partir de baixo. Os processos de mudança social conflitiva na Era da Informação giram em torno das lutas para transformar as categorias de nossa existência mediante a formação de redes interativas como formas de organização e mobilização. A internet disponibiliza o substrato que permite o engajamento na produção de uma nova sociedade. De ferramenta organizacional, converte-se em alavanca de transformação social[22]. Em breve, poderá surgir uma nova autoridade. Se em milhares de anos de nossa existência outorgamos a autoridade às leis divinas e apenas com o surgimento do Estado moderno legitimamos, pela narrativa liberal, pessoas para o exercício desses poderes, hoje não é ilusório pensar em uma nova mudança: a autoridade sendo exercida pelo *big data*, pelos algoritmos. A confluência da revolução biotecnológica – que decifra o funcionamento do corpo humano, notadamente cérebro e sentimentos – com a revolução da tecnologia da informação – poder de processamento de dados sem precedentes – produzirá algoritmos de *big data* com capacidade de monitoramento e governo do próprio sentimento humano, lançando para o espaço a crença no mito liberal de que eu exerço pleno controle sobre os processos que formam meus desejos e minhas escolhas: o livre-arbítrio[23]. Orwell, na clássica *1984*, baseia-se na linha de

[19] BECK, Ulrich. **A metamorfose do mundo**: novos conceitos para uma nova realidade. Rio de Janeiro: Zahar, 2018. p. 82-89.
[20] BAVA, Silvio Caccia. **A guerra das ideias**: a disputa das narrativas. Disponível em: https://diplomatique.org.br/a-guerra-das-ideias-a-disputa-das-narrativas/. Acesso em: 21 abr. 2022.
[21] LOPES JÚNIOR. Aury. **Direito Processual Penal**. 16. ed. Saraiva: São Paulo, 2019. p. 423-425.
[22] CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 118.
[23] HARARI, Yuval Noah. **21 Lições para o século 21**. São Paulo: Companhia das Letras, 2018. p. 72-74.

consequências entre um recente passado alemão-italiano e o então presente soviético para personificar o cerne do totalitarismo retratado na vigilância quase que onipresente do *Grande Irmão* e projetar um futuro de possessão absoluta e apoderamento da alma do indivíduo, agora conhecida de dentro para fora.[24]

No contexto tecnológico[25], *Grande Outro* é como passa a ser chamado esse aparato digital penetrante e sem precedentes que renderiza, monitora, computa e modifica o comportamento humano, altamente capaz de gerar aquilo que chama de *poder instrumentário*, método que reduz as experiências humanas a comportamento observável mensurável e, ao mesmo tempo, indiferente ao resultado dessa experiência. Sua finalidade é caçar o produto – dados e informações de comportamento arrancados de sua vida, transformando indivíduos em meras carcaças desalojadas de todo o significado outrora alocado em seus corpos, cérebros e corações – para a entrega de resultados garantidos: "graças às aptidões do *Grande Outro*, o poder instrumentário visa a uma condição de certeza sem terror"[26]. Mas ao mesmo tempo que produz interminável conhecimento agregado para uns, é também interminável fonte de redução de liberdades para outros, pois cria uma falsa consciência em decorrência dos fatos ocultos inerentes aos comandos desse *poder instrumentário*.

Se antes tínhamos o indivíduo no passado, hoje temos perfis. Assim como 1984 critica acidamente os governos totalitários de esquerda e de direita, o terror do stalinismo e a barbárie do nazifascismo, Admirável Mundo Novo também questiona o culto ao avanço da técnica, a linha de montagem, a produção em série e a uniformidade, criando um cenário em que as próprias pessoas são programadas e adestradas para cumprir um papel numa sociedade de castas biologicamente definidas, na qual a racionalidade se torna religião, a ciência em ídolo, tudo em um mundo no qual a experiência do sujeito parece não mais fazer sentido[27].

---

[24] Winston, herói de 1984, último romance de George Orwell, vive aprisionado na engrenagem totalitária de uma sociedade completamente dominada pelo Estado, onde tudo é feito coletivamente, mas cada qual vive sozinho. Ninguém escapa à vigilância do Grande Irmão, a mais famosa personificação literária de um poder cínico e cruel ao infinito, além de vazio de sentido histórico. De fato, a ideologia do Partido dominante em Oceânia não visa a nada de coisa alguma para ninguém, no presente ou no futuro. O'Brien, hierarca do Partido, é quem explica a Winston que "só nos interessa o poder em si. Nem riqueza, nem luxo, nem vida longa, nem felicidade: só o poder pelo poder, poder puro" (ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009).

[25] Não se ignora o *Grande Outro* de Lacan (LACAN, Jacques. Introdução do grande outro. *In*: **O Seminário – Livro 2**: o eu na teoria de Freud e na técnica da psicanálise. Rio de Janeiro: Jorge Zahar, 1985. cap.XIX. p. 296-311), mas, no presente trabalho, é apresentado conforme a construção utilizada por Zuboff (ZUBOFF, Shoshana. **A era do capitalismo da vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020).

[26] ZUBOFF, Shoshana. **A era do capitalismo da vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.

[27] HUXLEY, Aldous. **Admirável Mundo Novo**. 21. São Paulo: Editora Globo, 2001.

Técnicas de *big data* sugerem conhecimento absoluto, uma nova era de conhecimento em que coisas e comportamento humano revelam correlações secretas, até então ocultas. Correlações (*é assim mesmo)* substituem a causalidade (*por quê)*, de forma que a quantificação da realidade movida a dados afasta o espírito do conhecimento; com o *big data*, correlações são desprovidas de concepção, de conhecimento elementar e coincidem com a falta de saber absoluta - a era dos *big data* é uma era sem razão[28].

A rede se apresenta como espaço privilegiado para o exercício da vigilância e regulação da vida cotidiana. Sua capacidade de antecipar ações e planificar eventualidades lhe possibilita determinação de comportamentos e adoção de medidas preventivas, renovando e criando novas técnicas de controle que recaem, de forma desigual e discriminatória, sempre sobre os mesmos corpos. De forma sorrateira, o poder instrumentário do Grande Outro erode a democracia a partir de seu interior. Tecnologias de predição e controle se estruturam pelo contínuo deslocamento da vontade individual, antes encarnada em autodeterminação.

Submissos às supostas leis de ferro da inevitabilidade tecnológica que não toleram qualquer tipo de impedimento, indivíduos são iludidos e desorientados retoricamente para aceitar, declarar e autoautorizar, substituindo a esfera de liberdade individual em nome do conhecimento de terceiros e certeza total, empreendimento inimaginável fora do meio digital. Para além da oferta de conexão social, acesso a informações ou conveniência para poupar tempo, o poder instrumentário serve para alimentar instituições na forma de onisciência, controle e certeza, não tanto para curar instabilidades, mas para explorar vulnerabilidades[29]. Como grandes detentoras de poder social e econômico, empresas de

---

[28] "A *Lógica* hegeliana pode ser lida como a lógica do conhecimento. De acordo com ela, a correlação representa o estágio mais primitivo do conhecimento. Uma forte correlação entre A e B afirma o seguinte: quando A se altera, também ocorre uma alteração em B. Em uma correlação, por mais forte que seja, não se conhece absolutamente o *porquê dessa alteração*. É *simplesmente assim*. Trata-se de uma relação de probabilidade, e não de necessidade. Na correlação, A ocorre *frequentemente* junto com B. É neste ponto que a correlação se diferencia da relação causal. Já a necessidade é distinta por essa relação causal: A *causa* B.
(...)
A causalidade não é o mais alto nível de conhecimento. A reciprocidade é uma relação mais complexa do que a relação causal. Ela afirma: A e B se condicionam mutuamente. Existe uma conexão necessária entre ambos. Mas, mesmo no estágio da reciprocidade, a conexão entre A e B ainda não pode ser *concebida* (*begriffen*).
(...)
Só o «conceito» produz o conhecimento. Ele é C, que *conceitualiza dentro de si* A e B, e através do qual ambos são *conceitualizados*. É a ligação mais elevada, que abrange A e B e a partir da qual a relação entre A e B pode ser fundamentada. Portanto, A e B são «momentos de um terceiro, superior».
(...)
Só a partir do *conceito C* oniabrangente é possível uma *concepção* integral da correlação entre A e B (HAN, Byung-Chul. **Psicopolítica**. O neoliberalismo e as novas técnicas de poder. Trad. Maurício Liesen. Belo Horizonte: Âyiné: 2018. p. 93-98)

[29] "O poder instrumentário reduz a experiência humana a comportamento observável mensurável e, ao mesmo tempo, mantém resoluta indiferença ao resultado dessa experiência. [...] uma forma de observação sem testemunha que produz o anverso de uma religião política violenta íntima e contém uma assinatura de destruição absolutamente diferente: o desprezo remoto e abstrato de sistemas complexos a ponto de serem impenetráveis e os interesses que os criam, carregando indivíduos numa correnteza ruma a alcançar metas alheias. [...]. A

tecnologia são capazes de causar limitações ao exercício dos Direitos Fundamentais dos usuários da rede mundial de computadores, justificando suas práticas pela aceitação dos Termos de Uso das plataformas, instrumentos que definem diversos pontos da relação estabelecida entre empresas e usuários: (i) como o conteúdo gerado será tratado, suspenso ou bloqueado; (ii) se os dados do usuário poderão ser comercializados, monitorados e/ou entregues às autoridades, ou (iii) como disputas judiciais serão resolvidas.

Um estudo realizado nas cláusulas dos *Termos de Uso* de companhias como Apple, Facebook, Google, LinkedIn, Microsoft, PayPal, Spotify, Twitter, Vimeo, WhatsApp e YouTube demonstrou que estas não oferecem garantias suficientes aos usuários. Enquanto judicialização dessa relação, deveriam conter cláusulas protetivas dos direitos, mas se trata de mero instrumento de adesão: embora obtido através de um clique em um botão indicativo de sua anuência, essa não se dá de forma suficientemente esclarecida. Redações longas, linguagem técnica e de difícil compreensão, em legítima afronta ao que estabelecem o Marco Civil da Internet, o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados, obstaculizam sua obtenção de maneira esclarecida: esses contratos revelam-se instrumentos jurídicos com propósito de arrefecer, ao invés de reforçar, as responsabilidades dos intermediários de internet em resguardar a privacidade, o acesso à justiça e a liberdade de expressão dos usuários[30].

Outra pesquisa experimental avaliou que indivíduos ignoraram a leitura de políticas privacidade e termos para a obtenção de serviços digitais, revelando que, a partir da velocidade média de leitura de um adulto (250-280 palavras por minuto), a leitura das políticas de privacidade levaria entre 29-32 minutos e dos termos de serviço entre 15-17 minutos. Os resultados apresentados indicaram, entretanto, um tempo médio de leitura das políticas de privacidade de 73 segundos e tempo médio de leitura dos termos de privacidade de 51 segundos, sugerindo que políticas de privacidade são vistas como um incômodo pelo

---

indiferença radical do instrumentarismo é operacionalizada nos métodos desumanizados de avaliação do Grande Outro que produzem equivalência sem igualdade [...] reduzem indivíduos ao mínimo denominador comum de igualdade [...] apesar de todas as formas cruciais que nos diferenciam. Do ponto de vista do Grande Outro, somos estritamente outros: organismos que se comportam. O Grande Outro codifica o ponto de vista do outro como presença global [...] não se importa com o que pensamos, sentimos ou fazemos, contanto com que seus milhões, bilhões, trilhões de olhos e ouvidos sensíveis, atuantes, computacionais possam observar, renderizar, transformar em dados e instrumentalizar os vastos reservatórios de superávit comportamental gerados no tumulto galáctico de conexão e comunicação [...] é o poder instrumentário quem preenche o vazio ao substituir relações sociais por máquinas, o que equivale à substituição da sociedade pela certeza. [...] abre-se mão da liberdade pelo conhecimento de outros [...]" (ZUBOFF. Shoshana. **A era do capitalismo da vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020. p. 427-436).

[30] CARNEIRO, Ramon Mariano. "Li e aceito": violações a direitos fundamentais nos termos de uso das plataformas digitais. **Revista Internet & Sociedade**, São Paulo, Internetlab, n. 1, v. 1, p. 200-229, fevereiro de 2020.

usuário e um obstáculo aos fins da produção digital.[31]

A lógica do "solucionismo" tecnológico, que enxerga a tecnologia como panaceia para problemas que instituições falharam em resolver muitas vezes, é problematizada principalmente em torno da internet e das plataformas tecnológicas baseadas em dados pessoais (Airbnb, Uber, Facebook e WhatsApp…): a depender de como são empregadas, podem servir de ferramenta contrária à democracia. O conto de fadas do "empoderamento do usuário" é denunciado – e desvenda-se um sistema em que informações disponibilizadas gratuitamente são utilizadas de forma a cada vez produzir maiores desigualdades.[32]

As grandes empresas de tecnologia – pregadoras da ideologia libertária e que promoveram a tecnologia para a quebra do anonimato e a drástica redução dos níveis de privacidade – foram as primeiras a usá-lo[33]. Quando a Apple lançou o emblemático "1984", filme que divulgava o Macintosh e que marcou época não apenas na empresa, mas na propaganda mundial, a empresa de Steve Jobs, ao apresentar o computador, anunciou que "1984 não será igual a '1984'", em uma clara alusão de que o mundo dominado pelas políticas totalitárias e de controle seria salvo por um novo computador disruptivo.

Entretanto, a sensação de liberdade produzida pela internet foi de tal monta que ignoramos a expansão de práticas autoritárias de vigilância. O ambiente de trabalho tornou-se território de monitoramento permanente[34]: programas *gatekeeper* exibem todo fluxo produzido na *web* e que está tendo lugar em qualquer organização filiada a ele, revivendo as experiências de penetração automatizada forjadas na Era Industrial, de forma ainda mais pérfida com o advento da internet. Algoritmos registram todas suas atividades: seus históricos de navegação e de consultas no Google indicam suas preferências, suas compras virtuais e movimentações bancárias estratificam você na pirâmide socioeconômica, aplicativos de saúde contam seus passos e batimentos cardíacos, os de transportes registram sua rota e o áudio

---

[31] OBAR, Jonathan A.; OELDORF-HIRSH, Anne. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. **Information, Communication & Society**, p. 1-20, 2018; TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy. **SSRN**. 2016. Disponível em: https://ssrn.com/abstract=2757465 ou em http ://dx.doi.org/10.2139/ssrn.2757465. Acesso em: 27 jun. 2022.

[32] MOROZOV. Evgeny. Big Tech. **A ascensão de dados e a morte da política**. [*S. l.*]: Ub Edition, 2018. p. 43-80.

[33] A grande ironia histórica é que uma das instituições capitais na defesa da liberdade, a livre empresa, é o ingrediente essencial na construção desse sistema de vigilância — apesar da boa vontade geral e da ideologia libertária da maior parte das companhias da internet. Sem a ajuda delas, os governos não teriam o *know-how* e, mais fundamentalmente, a possibilidade de intervir na internet: tudo depende da capacidade de agir sobre provedores de serviços da internet e redes específicas por toda parte.

[34] CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 144.

ambiente da corrida[35], *apps* de reuniões virtuais captam suas expressões e a movimentação de sua retina para reconhecimento facial e para compreender o que lhe chama mais a atenção nos quadrantes da sua tela[36].Tecnologias que permitem tarefas triviais como o *download* de livros, revistas, músicas e filmes armazenados digitalmente possibilitam a editores e companhias de entretenimento registrar e monitorar hábitos de navegação na rede[37].

As máquinas inteligentes do presente exercem funções de aprendizagem que convertem dados em conhecimento; o mundo, a individualidade, o corpo e o comportamento são reduzidos a ativos de informação que podem ser desagregados, reconstituídos, indexados, manipulados, analisados, agrupados, renderizados, comprados e vendidos. A nova razão é a razão de extração e predição: inteligente é apenas um eufemismo utilizado para velar a realidade de que o processo realizado por essas máquinas nada mais é do que a despossessão da experiência humana vivida e sua transformação em matéria-prima[38].

Não demorou para fazer com que governos, tirando proveito da indiferença ignorante dos usuários às burocracias de afastamento do sigilo de dados, desenvolvessem seus próprios programas de vigilância, ajustando métodos tradicionais de controle e exercício de poder com nova sofisticação tecnológica,[39] Governos e grandes corporações disparam na corrida para

---

[35] TILT, Rodrigo Trindade de. **Tá com medo?** App da Uber terá função de gravar toda conversa no carro. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/11/06/uber-introduz-gravacao-de-audio-para-tornar-corridas-mais-seguras.htm?cmpid=copiaecola. Acesso em: 23 abr. 2020.

[36] HARARI, Yuval Noah. **21 Lições para o século 21**. São Paulo: Companhia das Letras, 2018. p. 328-329.

[37] "O maior conglomerado eletrônico de comunicação e publicação do mundo, a AOL-Time Warner, é um caso ilustrativo. O aparelho integrado de multimídia do futuro (ansiosamente buscado pela Microsoft e a AT & T) poderá ter substanciais capacidades de vigilância. Identificadores globalmente únicos (GUID, de *globally unique identifiers*) tornam possível vincular cada documento, mensagem de e-mail ou conversa com a identidade real da pessoa que os enviou. Em novembro de 1999, a Real Jukebox foi contestada por defensores da privacidade quando eles notaram que o aplicativo que executava músicas podia enviar informação à sua companhia matriz, a Real Networks, sobre a música que cada usuário 'baixava', e esta podia ser acoplada a um número ID único que apontava com precisão a identidade do usuário. Temendo publicidade negativa, a Real Networks desativou o GUID. Convém lembrar, contudo, que a identificação digital é a regra e não a exceção na indústria: os produtos de software da Microsoft, como o Word97 e o Powerpoint97, incluem identificadores em cada documento que produzimos com a ajuda desses programas. A partir da identidade desses documentos é possível identificar o computador que os originou" (CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 145).

[38] ZUBOFF. Shoshana. **A era do capitalismo da vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020. p. 269-292.

[39] "Internacionalmente, o programa Echelon, criado pelos Estados Unidos e a Grã-Bretanha durante a Guerra Fria, parece ter sido convertido em espionagem industrial, segundo alegam agências governamentais francesas, mediante a combinação de escuta tradicional e interferência de telecomunicações, com interceptação de mensagens eletrônicas. O programa Carnivore do FBI opera em cooperação (voluntária ou não) com provedores de serviços da internet, registrando tráfego de e-mails, depois peneirando a informação desejada com base em amostragem automática e busca por palavras-chave. Em 2000, o FBI pediu ao Congresso 75 milhões de dólares para financiar programas de vigilância, entre eles o 'Digital Storm', uma nova modalidade de gravação de comunicação telefônica combinada com programas computadorizados para extrair palavras-chave das mensagens" (CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 146).

hackear o indivíduo, saber quem é quem, o que deseja da vida e, com o uso de recursos de *big data* e no aprendizado da máquina para conhecer cada sujeito – talvez até mais do que ele próprio –, exercer dominação e controle. Enquanto as pessoas navegam na internet, assistem YouTube, exploram suas redes sociais e aplicativos de mensagens instantâneas, algoritmos estarão a monitorá-las. Mais além do que a captura do *psicograma individual*, o *big data* viabiliza a extração de um *psicograma coletivo* ou até mesmo o *psicograma do inconsciente*[40]. Essa comodidade custa ao indivíduo o compartilhamento de suas informações, reunidas em uma imensa base de dados estatísticos que opera com precisões absurdas e em tempo real, cada vez mais a serviço da prevenção e repressão.

Acreditando nos perigos gerados ao sigilo e das práticas de espionagem generalizada levada a efeito pelo governo norte-americano, Edward Snowden denunciou as invasões de privacidade e o abuso de poder pelo governo, tornando pública uma série de documentos secretos das agências de espionagem norte-americanas, como um manual de treinamento para agentes que ensinava analistas da NSA (sigla em inglês de *National Security Agency)* sobre novas técnicas de vigilância que se baseavam em inserir (*input)* dados como endereços de *e-mails*, dados de localização do IP, números de telefone para receber (*output*) dados como conteúdos de *e-mail*, "metadados" telefônicos, *logs* de *chat*: um verdadeiro sistema de vigilância estatal generalizado, alheio a qualquer supervisão ou limite, razão pela qual arriscou sua vida e liberdade para promover a conscientização e o debate público orientados à condução de reformas para frear o ímpeto de poder e exigir das instâncias de governo comportamento conforme a Constituição.[41]

Caminhamos para uma nova crise da liberdade. Smartphones trabalham com um modo de *input-output* pobre em complexidade, redutor de negatividade; por intermédio deles, se desaprende a *pensar* em complexidade, eles definham comportamentos que exigem *amplitude* temporal ou *visibilidade ampla*, demandam o curto prazo e ocultam *o longo e o lento*[42].

Essa era da *psicopolítica digital* avança da vigilância passiva ao controle ativo, transforma a negatividade da decisão livre na positividade de um estado de coisas: a pessoa se "positiviza" em coisa, quantificável, mensurável e controlável, produto da ação do *big data* como instrumento que entrega conhecimento sobre as dinâmicas da comunicação social.

---

[40] HAN, Byung-Chul. **Psicopolítica**. O neoliberalismo e as novas técnicas de poder. Tradução Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 36.
[41] GLENN GREENWALD. **Sem lugar para se esconder**: Edward Snowden, a NSA e a espionagem do governo americano. Tradução Fernanda Abreu. Rio de Janeiro: Sextante, 2014.
[42] HAN, Byung-Chul. **No enxame**: perspectivas do digital. Trad. Lucas Machado. Petrópolis: Vozes, 2018. p. 45.

Objeto de devoção do digital, o *smartphone* é comparado ao rosário na concepção de objeto em que o manuseio envolve autocontrole e autoexame – quanto mais entrego a vigilância ao indivíduo, mais eficiente é a dominação. Neste cenário cristianizado, curtir é o amém, manifestação de subordinação ao contexto de dominação, e as redes sociais, em especial Facebook, a igreja ou a sinagoga do digital.[43]

Empresas de tecnologia da informação colaboram decisivamente na reconstrução dos modelos do controle e da repressão não apenas porque precisam quebrar a privacidade de seus clientes para auferir lucro com a venda de seus dados, mas também porque precisam do suporte governamental para preservar direitos de propriedade na economia baseada na conectividade.[44] Dados de usuários são compilados sem o conhecimento ou consentimento informado de seus titulares mediante trocas em relações desiguais de poder: são entregues em troca de produtos ou serviços digitais, o que faz com que o uso de tecnologias biométricas se expanda exponencialmente[45] e atraia *players* sempre ligados ao exercício do poder: capital, inteligência humana, pesquisa, proteção de governos e ecossistemas de institucionalização.

Viabilizando o surgimento de novas técnicas e ferramentas desenvolvidas para facilitar o acesso a conteúdos não catalogados ou facilmente encontrados, proliferam-se rastreadores e ferramentas de busca para esses ambientes. O fenômeno *big data* surgido nos últimos 30 anos, decorrente do avanço dos computadores e do aumento de capacidade de armazenamento e processamento de dados, viabilizou o vasculhamento desses dados e o surgimento de novas e poderosas formas de posicionar-se em relação às coisas do mundo: podem ser descobertos padrões e tendências dentro desses imensos conjuntos, mas de difícil detecção sem o uso das ferramentas analíticas corretas para destacar os pontos de interesse sobre determinado alvo.

1.2. O novo ópio

A expansão de técnicas de coleta de informações visa à aquisição de elementos para preparar e executar programas de intervenção social por parte das instituições públicas e desenvolvimento de estratégias empresariais privadas, assim como para exercitar o controle de adequação do comportamento dos cidadãos. A organização da sociedade avança baseada na lógica da acumulação e circulação da informação, alçada à condição de recurso-base e em torno da qual se estabelecem novas situações de poder. Surge, pois, o problema da

[43] HAN, Byung-Chul. **Psicopolítica**. **O neoliberalismo e as novas técnicas de poder**. Tradução Maurício Liesen. Belo Horizonte: Âyiné, 2018. p. 23-24.
[44] CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 150.
[45] PITCH, Tamar. **La sociedad de la prevención**. Buenos Aires: Ad Hoc, 2009. p. 151-154.

legitimação do poder fundado na informação, processo que expõe a incapacidade, sobretudo do Estado, de manter a hegemonia sobre uma infraestrutura informativa, cada vez mais ampla e sofisticada, além da promessa de garantia efetiva e respeito aos direitos individuais[46].

Interconexões e atividades no ciberespaço podem vir de diversas origens, como servidores localizados em diferentes países, imagens de satélite, fóruns de mercado específicos, dados obtidos através da Internet das Coisas (IoT), produzindo quantidade de dados sem precedentes na história. Conectar-se está cada vez mais acessível, quase sem custo; o número de dispositivos usados em interação está aumentado: *laptops*, *tablets*, telefones celulares e outros, produzindo informações em volume incalculável e em todos os continentes, o que também torna difícil filtrar, peneirar, selecionar e sintetizar essas informações. O ciberespaço ocupa todas as áreas da sociedade: setores público e privado cada vez mais fazem uso dele, devido às vantagens que oferece e por não ser necessário nenhum treinamento para nele poder interagir[47].

Sob a perspectiva de guerra, a política informacional naturalmente conduziu à possibilidade de guerras informacionais e novas doutrinas de controle e segurança apropriadas à Era da Internet. O sistema é vulnerável – não em seu centro, mas em sua periferia –, e a capacidade de obter informação crítica, poluir bancos de dados ou devastar sistemas-chave de comunicação torna-se uma arma de escolha no novo ambiente tecnológico. O problema crítico de segurança não está necessariamente nos computadores do Ministério da Defesa, mas em toda a rede de que depende a vida cotidiana. Nesse palco, desenvolvem-se questões que decorrem da formação de um ambiente de informação global, que inclui o ciberespaço e todos os outros sistemas de informação, o que nos leva às considerações sobre a *noopolitik*. *Noopolitik* se contrapõe à *realpolitik*, a abordagem tradicional em termos de promoção do Estado mediante negociação, força ou uso potencial de força que não desaparece na Era da Informação, mas permanece centrada no Estado, em uma era organizada em torno de redes, inclusive redes de Estados.

A guerra também está sendo transformada por redes de computadores: a nova fronteira do exercício do poder no cenário mundial – a razão de ser dos Estados continua sendo sua aptidão de exercer violências em defesa dos seus interesses – torna-se justamente se adequar a esse conjunto de ideias globais de forma tão propícia quanto possível a um

[46] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 28-36.
[47] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**, Bogotá, v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.

dado conjunto de interesses. Veja-se o exemplo tecnológico das comunicações eletrônicas, sistemas de vigilância, aviões não tripulados e munições guiadas por satélite, armas decisivas na confrontação militar.[48] O desenvolvimento de novas tecnologias de informação e comunicação acabou por produzir reformas significativas na infraestrutura de vigilância global, a ponto de o recente conflito entre Rússia e Ucrânia receber a estampa de guerra híbrida[49].

Além da abundância de informações e ferramentas, as habilidades exigidas para um futuro próximo também passam a ser o centro das observações. Ainda que não saibamos ao certo quais as especificidades dessas mudanças para os próximos anos, ela é a única certeza em si mesma. Estima-se que, além da capacidade de lidar com mudanças, aprender coisas novas e manter o equilíbrio mental em condições pouco familiares, o pensamento crítico, a comunicação, a colaboração e a criatividade possam ser as quatro aptidões fundamentais para os próximos 50 anos – período de tempo em que até mesmo as estruturas físicas e cognitivas das instituições e convenções poderão se desmanchar no ar.

O homem deparar-se-á com uma situação totalmente sem precedentes: estará inundado por enorme quantidade de informações e, ao mesmo tempo, poderá não dominar ou até mesmo deter os recursos e meios necessários para absorvê-las e analisá-las – um mundo de profundas incertezas em que o *bug* de informações nada mais é do que uma característica que lhe é inerente[50]. Não existe serventia ao indivíduo receber 500 jornais por dia se não possui a capacidade de lê-los: antes mesmo do *boom* tecnológico, em "Janela da Alma" Saramago observou que estamos na era do audiovisual, bombardeados com estímulos que afetam os nossos sentidos a todo instante: acessamos centenas de canais de TV, outras centenas de revistas e jornais, dentre outros veículos de informação que contribuem para que vejamos o

---

[48] CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 133.

[49] "O conceito passa pela implementação de uma estratégia de confronto que não passa necessariamente por um conflito militar. O uso de 'fake news', ataques informáticos ou espionagem é frequente, sendo que o principal objetivo é desestabilizar um Governo internamente. Após uma primeira fase de influência e desestabilização, normalmente, observa-se a substituição de Governos. O mecanismo de uma guerra híbrida é complexo, e geralmente, recorre a pesquisas que podem ceder informações sobre a população do país atacado. Por norma, estas pesquisas observam questões de cariz psicológico, sociológico e antropológico, podendo assim delinear um quadro caracterizador da sociedade em questão. Com base nestes dados, os agentes que impulsionam este tipo de guerra tornam-se capazes de prever situações. É, por exemplo, através de ataques informáticos que os países atacantes podem tentar ter acesso a informação relevante.
As novas tecnologias são um fator que facilita as guerras híbridas. Por outro lado, este confronto caracteriza-se por ser mais assimétrico pois costuma ter outros atores envolvidos. Além disso, a questão torna-se mais complexa porque durante o decorrer do conflito não é fácil perceber quem ataca primeiro" (RÚSSIA-Ucrânia: O que é uma guerra híbrida? **JN**. 15 fevereiro 2022. Disponível em: https://www.jn.pt/mundo/russia-ucrania-o-que-e-uma-guerra-hibrida-14592565.html. Acesso em: 20 abr. 2022).

[50] HARARI, Yuval Noah. **21 Lições para o século 21**. São Paulo: Companhia das Letras, 2018. p. 322-327.

mundo como os prisioneiros no mito da caverna Platão. A profusão de informações é tanta que esses "prisioneiros da caverna" nem têm tempo para processá-las[51]. Trabalhar com dados confiáveis favorece as conclusões da análise e proporciona um ambiente seguro para a tomada de decisões. Se os dados vêm de um ambiente controlado e a quantidade é razoável, a confiabilidade pode ser validada usando diferentes técnicas de inteligência; se o volume de dados é alto, isso pode produzir sobrecarga de insumos, dificultando seu processamento na velocidade em que são adquiridos, e isso pode causar o colapso de processos subsequentes[52].

No mundo de interdependência e moldado pela velocidade da informação e da comunicação, a capacidade de atuar sobre fluxos tornar-se-á ferramenta essencial para a promoção de um programa político: uma diplomacia destinada não apenas a governos, mas a sociedades, e que vira estratégia de segurança para evitar confrontação, aumentar oportunidades e promover a hegemonia cultural e política. Essa capacidade demanda do Estado infraestrutura tecnológica e uma ordem liberal da informação que garanta a circulação de elementos e, sobretudo, flexibilidade para mudar ideias e opiniões para se conectar ao ambiente global em sua complexidade[53]. Contudo, como a estratégia política é um meio para a fabricação de poder, opõe-se, de um lado, a inauguração de uma informação global e de um espaço de comunicação tão abertos quanto possível a seus diversos participantes e, do outro, a estratégia de informação como um campo necessário à promoção de seus próprios interesses e valores dentro das regras do jogo.

Essa eclosão da Inteligência Artificial no âmbito jurídico por intermédio do uso indiscriminado de dados e a crença cega de que a máquina que os converte por meio dos algorítimos oferece a resposta mais rápida para todos os problemas são encarados como o novo ópio da sociedade, ignorando os riscos de que se tornem, também, instrumentos de discriminação, segregação, repressão e controle. Assim como os graves erros cometidos no passado, os quais, hoje, conhecedores da história tiveram a oportunidade de constatar, o futuro digital seguramente nos reserva espaço para a perpetuação de muitos desses prejuízos

---

[51] JANELA da Alma. Direção/Roteiro: JARDIM, João; CARVALHO, Walter. Rio de Janeiro: Copacabana Filmes e Produções, 2001. *Online* (73 min). Disponível em: https://www.youtube.com/watch?v=_I9l7upG0DI. Acesso em: 28 jun. 2022.

[52] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**, Bogotá, v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.

[53] CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 133.

acumulados.[54]

1.3. Competição analítica

A competitividade imposta pela globalização dos segmentos da cadeia produtiva passou a relacionar conhecimento a progresso, fazendo surgir a atividade de *business intelligence*, instrumento de produção, de salvaguarda do conhecimento e importante elemento no exercício do processo decisório[55], levado a efeito através de um conjunto de tecnologias e processos que utilizam dados e relatórios para compreender o desempenho e que aborda uma série de questões sobre as atividades empresariais, a *analytics*[56]. A incessante motivação pelo lucro exigiu modificações e que empresas desenvolvessem estratégias para transformar dados e informações sobre concorrentes em vantagem competitiva, de forma que a coleta, a análise e o emprego ético e legal desses dados relativos à capacidade, à vulnerabilidade e às intenções de concorrentes, com o objetivo de obter maior conhecimento e desencadear decisões esclarecidas, tornaram-se uma necessidade constante dentro de corporações[57]; questões que a *analytics* pode responder passaram a representar valor elevado e a determinar a proatividade do sistema[58], fazendo nascer a competição analítica.

Processos de decisão baseados em fatos são críticos para um elevado desempenho, e organizações passaram a adotar distintas abordagens para obter uma vantagem competitiva com dados. O equacionamento da *analytics* com a tecnologia de informação analítica aliado aos aspectos humanos e organizacionais da concorrência analítica é apontado como o grande diferenciador; a capacidade de executar o negócio com eficiência, eficácia e estar pronto e informado para tomar as decisões mais inteligentes, as quais têm reunido sistematicamente dados e análises por detrás, são tratados hoje como uma corrida ao armamento, exigindo o desenvolvimento contínuo de novas medidas, novos algoritmos e novas abordagens de tomada de decisões. *Concorrentes analíticos* são organizações que selecionam capacidades distintivas nas quais baseiam suas estratégias e depois aplicam dados extensivos, análise estatística e quantitativa e tomada de decisão ancorada em fatos para apoiar as capacidades.

---

[54] DIZ, Fernando Martín. Justicia Predictiva: inteligencia artificial y algoritmos aplicados al proceso judicial en materia probatoria. *In*: DE MATA, Frederico Bueno. **El Impacto de las Nuevas Tecnologías Disruptivas en el Derecho Procesal**. [*S. l.*]: Thomson Reuters Aranzadi, 2022. p. 132-133.

[55] MAYER-SCHONBERG, Viktor; RAMGE, Thomas. **Reinventing Capitalism in the Age of Big Data**. New York: Basic Books, 2018. p. 66-81.

[56] DEVENPORT, Thomas H; HARRIS, Jeanne G. **Competing on Analytics**: the new science of winning. [*S. l.*]: Harvard Business School Publishing Corporation, 2006. *E-book.* p. 13-57.

[57] MAYER-SCHONBERG, Viktor; RAMGE, Thomas. **Reinventing Capitalism in the Age of Big Data**. New York: Basic Books, 2018. p. 66-81.

[58] DEVENPORT, Thomas H; HARRIS, Jeanne G. **Competing on Analytics**: the new science of winning. [*S. l.*]: Harvard Business School Publishing Corporation, 2006. *E-book*. p. 13-57.

Espremem até à última gota de valor de processos e decisões-chave, já que, independentemente das capacidades enfatizadas numa estratégia, a *analytics* pode impulsioná-las a um nível superior. A nova geração de tomadores de decisão a crescer com computadores está para entrar nas organizações e instituições e à procura de novas formas de geri-los com a ajuda da tecnologia, trazer sentido aos dados através de computadores e *softwares*, capacidade esta que atingiu a maioridade. Os fabricantes de *software* analítico expandiram a funcionalidade dos seus produtos nos últimos anos; *hardwares* estão capacitados para uma análise incrivelmente rápida e gestão de grandes bases de dados.

Quem optar pela concorrência analítica elimina o trabalho de adivinhação dos seus processos e modelos de negócio. *Softwares* analíticos e de orientação estatística, cada vez mais sofisticados, com mais e mais variadas capacidades analíticas aos seus conjuntos de ferramentas, terão disponibilidade ampliada e serão acessíveis por todos os tipos de organizações, ainda que as variáveis-chave continuem sendo humanas[59].

No campo empresarial, aponta-se para a existência de provas consideráveis de que as decisões baseadas na *analytics* têm mais probabilidades de serem corretas em relação àquelas baseadas na intuição, e que saber dentro dos limites dos dados e da análise é melhor do que acreditar, pensar ou sentir. Não se ignoram, entretanto, as circunstâncias em que as decisões não podem ou não devem ser baseadas em *analytics* diante da capacidade que seres humanos desenvolveram em tomar decisões sobre a personalidade e as intenções, e é raro que a análise formal também o faça, mas a intuição é apenas um guia quando apoiada em anos de perícia: decisores têm de usar a intuição quando não têm dados e devem tomar uma decisão muito rápida.

A partir da coleta e tratamento de dados pessoais é possível segmentar usuários por grupos de interesse específicos e direcionar anúncios de forma mais eficiente, na medida em que, quanto mais se sabe sobre o usuário, quanto mais de seus dados são coletados, maior é a

---

[59] "Em *Good to Great*, por exemplo, Jim Collins observa que os resultados revolucionários são obtidos por uma série de boas decisões, diligentemente executadas e acumuladas em cima de outras ... [empresas boas a grandes] tomaram muito mais boas decisões do que más, e tomaram muito mais boas decisões do que empresas de comparação. Infundiram todo o processo com os factos brutais da realidade. Não se pode absolutamente tomar uma série de boas decisões sem primeiro confrontar os factos brutais.
As organizações podem adoptar várias abordagens para obterem uma vantagem competitiva com os dados. Algumas podem recolher dados únicos ao longo do tempo sobre os seus clientes e perspectivas que os concorrentes não conseguem igualar. Outras podem organizar, normalizar, e manipular dados que estão disponíveis para outros de uma forma única. Outros ainda podem desenvolver um algoritmo proprietário que leva a análises melhores e mais perspicazes sobre as quais podem tomar decisões. E alguns diferenciam-se ao incorporarem a análise num processo comercial distinto. Independentemente da abordagem, para que as empresas sustentem uma vantagem competitiva, a análise deve ser aplicada judiciosamente, bem executada, e continuamente renovada" (DEVENPORT, Thomas H; HARRIS, Jeanne G. **Competing on Analytics: the new science of winning**. [*S. l.*]: Harvard Business School Publishing Corporation, 2006. *E-book*. p. 13-57).

precisão sobre o alvo. A coleta de dados pessoais tornou-se praxe em companhias, sobretudo no setor de internet, e, silenciosamente, sem perceber, o usuário teve seus hábitos e preferências de navegação monitorados por meio da utilização de diversos mecanismos tecnológicos diferentes de coleta de dados, como os *cookies*, pequenos arquivos enviados durante a comunicação estabelecida entre o dispositivo do usuário e o servidor do *site* visitado e que funcionam como identificadores que possibilitam reconhecer o dispositivo em visitas futuras e armazenar informações sobre suas preferências. Graças a eles, itens podem ser adicionados e mantidos em "carrinhos" virtuais ou quais preferências de exibição podem ser configuradas para visitas futuras; algumas dessas tecnologias têm sido desenvolvidas para atuar de forma persistente, inclusive ignorando preferências expressas do usuário em não se submeter a essas práticas intrusivas.

O amplo acesso a esses tipos de dados sobre usuários permitiu às corporações estabelecerem gigantescos bancos de dados, repletos de informações que, tratadas, podem revelar – a partir das consultas em palavras-chave, visitas a sítios eletrônicos, compras realizadas, leituras realizadas, amigos com quem mantém contato e lugares por onde se passou – aspectos importantes da personalidade do usuário e permitir sua segmentação com base nesses dados e inferências, processo que preocupa em razão: (i) da dificuldade de cientificar usuários sobre a utilização desses mecanismos de coleta e dos atores envolvidos nesse processo; (ii) da insuficiência da noção de "consentimento informado" e a impossibilidade de o usuário não consentir, sob pena de não ter acesso ao serviço; (iii) da possibilidade de cruzamento de informações entre bancos de dados, criando superperfis; (iv) da possibilidade de adoção de práticas discriminatórias com base em inferências; (v) da possibilidade de manipulação do usuário com base nas informações coletadas, questões enfrentadas e reguladas de maneiras diferentes, especialmente no que tange aos limites definidos para a coleta e tratamento de dados pessoais, até mesmo em razão das diferenças olímpicas entre os modelos adotados nos Estados Unidos, na Europa e no Brasil[60].

1.4. Transformando dados em inteligência

Sistemas de Inteligência Artificial oferecem a capacidade de reunir e analisar elementos de algum ambiente e praticar ações em busca de cumprir os objetivos programados na máquina por um operador humano; outros ainda têm a capacidade de aprender e se adaptar

[60] ANTONIALLI, Dennys; CRUZ, Francisco Brito. **Privacidade e internet**: desafios para a democracia brasileira. Rio de Janeiro: Centro Edelstein de Pesquisas Sociais; São Paulo: Fundação Fernando Henrique Cardoso, 2017. p. 14-18.

ao longo do tempo a partir da correlação entre os dados alimentados e os que o próprio sistema recolhe. Apesar dos *inputs* humanos, apresentam relativa autonomia para escolher, dentre as possibilidades de ação, a que lhe parece a mais adequada para a resolução da equação enfrentada. O manejo de técnicas baseadas em Inteligência Artificial com a ciência digital forense pode oferecer vantagens indiscutíveis durante as etapas de uma investigação: a análise e a correlação de dados auxiliam a diminuir a quantidade de dados a analisar pelo *expert*; ajudam a estabelecer ligações entre dados que poderiam passar despercebidas pelo observador humano; podem reduzir a ocorrência de equívocos nos processos de aquisição, preservação, análise e interpretação dos dados e direcionam o emprego de métodos mais seguros para a preservação dos elementos durante a investigação[61]. No que guarda relação com a tramitação e busca de dados, há de se considerar em primeira ordem a superioridade de desempenho da Inteligência Artificial em relação ao processamento humano, já que possui a capacidade de classificar, revisar e compilar documentos e informações com muito mais eficácia do que a mente humana[62].

A quantidade de *big data* produzida de forma gratuita e diariamente, aliada ao aumento da disponibilidade de capacidade computacional a custo inexpressivo, representaram o contexto ideal ao surgimento de condições para aumentar o aproveitamento dos algoritmos em busca de resultados mais eficientes nos processos de tomadas de decisões, agora confiados a uma relação codificada em razão da perda de confiança na falta de objetividade humana.

A *justiça preditiva* – que nos Estados Unidos é denominada "ciência da previsão jurídica quantitativa" – anuncia a previsibilidade como principal ferramenta orientada a auxiliar nos processos de tomadas de decisão, sua capacidade de, a partir do tratamento de dados mediante algoritmos, fazer prognoses quanto às possibilidades e assegurar previsões confiáveis aos sujeitos do processo (juízes e partes)[63]. Atua sobre a lógica empresarial da

---

[61] FIDALGO, Sónia. A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo. *In*: RODRIGUES. Anabela Miranda (coord.). **A Inteligência Artificial no Direito Penal**. Coimbra: Edições Almedina, 2020. p. 135-136.

[62] FENOLL, Jordi Nieva. **Inteligencia Artificial y Proceso Judicial**. Madrid: Marcial Pons, 2018. p. 31.

[63] Produto do manejo de aplicações digitais jurídicas (*legal techs*), Justiça Preditiva é encarada como a utilização de sistemas de computação para a entrega de previsões de resultados, campo ainda subexplorado e com a capacidade de produção de "novos saberes", por enquanto com expressiva incidência apenas nos sistemas de *common law*. O emprego de inovações tecnológicas e Inteligência Artificial no processo de tomada de decisões oferecem vantagens, riscos e demandam o estabelecimento de limites, envolvendo questões jurídicas, epistemológicas e éticas. Ainda paira desconfiança em torno da aplicação de instrumentos tecnológicos e da possibilidade de concessão de processos de tomadas de decisões ao algoritmo, cuja definição assumida no Estudo do Conselho da Europa, de 2017, refere-se aos "processos codificados para transformar dados entrados em resultados, baseados em cálculos específicos". Estabelece correlação entre um conjunto inicial de dados ou elementos lançados (*input*) e uma consequência precisa (*output*) (RODRIGUES. Anabela Miranda. Inteligência artificial e Direito Penal – a justiça preditiva entre a Americanização e a Europeização. *In*: RODRIGUES.

concorrência analítica, que teve, no âmbito governamental, seus primeiros usos envolvendo a defesa nacional, mas no atual ambiente é amplamente utilizada não apenas para a inteligência militar, incluindo análise automatizada das comunicações de texto e de voz, mas também em muitos níveis de governo, com especial ênfase na análise de estatísticas criminais, como com o uso do CompStat[64]. No sistema legal chinês, a empresa iFlyTek atua oferecendo aplicação de Inteligência Artificial aos Tribunais usando um sistema de referência cruzada de provas de casos anteriores para comparar os elementos apresentados e procurar padrões factuais contraditórios, tudo de forma a orientar magistrados – inclusive com elementos gráficos – na análise de provas e formulação de decisões, para que o façam de maneira informada[65].

Do cenário de desenvolvimento tecnológico também aparecem instrumentos de controle para atender interesses comerciais e de Governo; *tecnologias de identificação*, t*ecnologias de vigilância* e t*ecnologias de investigação* emergem como processos de restrição da liberdade, comumente ancoradas em dois pressupostos fundamentais: (i) conhecimento assimétrico dos códigos na rede e (ii) capacidade de definir um ambiente específico de comunicação suscetível de controle. São tecnologias que operam seus controles sob duas condições básicas: (i) amparados em um *software* confidencial e patenteado de forma que controladores conhecem os códigos da rede e o controlado não, tornando-o presa fácil de uma estrutura desconhecida, e; (ii) os controles são exercidos com base num espaço definido na rede, pois, ainda que seja a internet uma rede global, seus pontos de acesso não o são.

Tecnologias de identificação incluem o uso de senhas, *cookies* e procedimentos de autenticação que usam assinaturas digitais para permitir que outros computadores verifiquem a origem e as características do correspondente que interage com eles. *Tecnologias de vigilância* têm a capacidade de promover a verificação de um dado servidor na origem de uma mensagem, já que se baseiam em tecnologias de identificação para localizar o usuário individual. São responsáveis por interceptações de mensagens, rastreamento de fluxos de comunicação a partir de uma localização específica e monitoramento contínuo, viabilizando a identificação, no provedor de serviços da internet, do responsável pelo uso de tecnologias. Finalmente, *tecnologias de investigação* referem-se à construção de bancos de dados a partir dos resultados da vigilância e do armazenamento

---

Anabela Miranda (coord.). **A Inteligência Artificial no Direito Penal**. Coimbra: Edições Almedina, 2020. p. 22-24.

[64] DEVENPORT, Thomas H; HARRIS, Jeanne G. **Competing on Analytics**: the new science of winning. [*S. l.*]: Harvard Business School Publishing Corporation, 2006. *E-book*. p. 51-52.

[65] LEE, Kai-Fu. **Inteligência artificial**: como os robôs estão mudando o mundo, a forma como amamos, nos comunicamos e vivemos. Rio de Janeiro: Globo Livros, 2019. p. 141-143.

de informação, dados que podem ser agregados, desagregados, combinados e identificados de acordo com o objetivo e o poder legal: no ambiente tecnológico atual, informação eletronicamente transmitida é gravada, podendo vir a ser processada, identificada e combinada em unidades de análise coletiva ou individual.[66]

Reconhecida como uma possibilidade real e com muitas aplicações no âmbito do Direito Processual, a utilização de dados e seu tratamento por intermédio de algoritmos viabiliza o exercício de predições que auxiliam seus operadores de diferentes formas no desenvolvimento das atividades frente ao processo. Essa área tem experimentado um crescimento significativo e, com a profusão exponencial da Inteligência Artificial, é possível que isso venha a ocorrer ainda mais. O impacto da Inteligência Artificial nas nossas vidas já produziu o rompimento de muitas estruturas e setores da sociedade como foram conhecidos durante anos. Ainda que diante da pluralidade de definições possíveis em razão das características que pode representar em um setor de aplicação específico, a Comissão Europeia, no memorando Inteligência Artificial para Europa, a define como "sistemas que manifestam um comportamento inteligente, pois são capazes de analisar seu entorno e passar à ação – com certo grau de autonomia – com o fim de alcançar objetivos específicos".

O desenvolvimento da Inteligência Artificial tem a ver com o uso ou disponibilidade dessas quantidades massivas de dados coletados (*big data* ou macrodados), analisados e acumulados de maneira constante por algoritmos, com a finalidade de gerar correlações, tendências e padrões, e que proporciona ferramentas incríveis que, já se estuda a possibilidade, possam ter emprego na fase probatória do processo penal. É na qualidade desses dados em que se baseia o algoritmo para apontar um resultado que é necessário dispensarem maior atenção[67]. A condução de uma ou de um conjunto de operações envolvendo dados é considerada como *tratamento de dados*: práticas comuns, como manter arquivos de clientes, coletar detalhes e dados de pessoas por meio de um questionário,

---

[66] CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 142-144.

[67] *Algoritmos* são uma série de equações criadas a partir de um processo estatístico, matemático, complexo e humano, que inclui a coleta, preparação e análise de dados em diversas etapas que se entrelaçam para atender a uma instrução concreta, com vista a solucionar um problema previamente estabelecido, o que faz através da utilização de uma imensa base de dados ordenados. Sua finalidade não é certificar a verdade de uma hipótese, mas buscar correlações deterministas entre dados. Algoritmos mais avançados, inteligentes e eficientes em antecipar comportamentos são conhecidos por usar aprendizagem automática da máquina, a *machine learning*, mas carregam consigo o problema de que seu funcionamento (*código fonte*) é incompreensível, circunstância que causa obstáculos à legitimidade de suas decisões (PÉREZ ESTRADA, Miren Josune. La inteligencia artificial como prueba científica en el proceso penal español. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 7, n. 2, p. 1385-1410, maio-ago. 2021).

atualização de arquivos de fornecedores, realizar contratos entre empresas[68]. Em nível global, por tratamento de dados entende-se toda operação realizada com dados, 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. Surgem novos desafios em matéria de proteção de dados, na medida em que a coleta e compartilhamento registraram um aumento significativo, produto da profusão tecnológica que permite o tratamento de dados numa escala sem precedentes para o exercício de diversas funções, inclusive a prevenção, a investigação, a detecção e a repressão de infrações penais e a execução de sanções penais. É justamente sobre o impacto do tratamento de dados para fins de persecução penal e seus reflexos no direito de defesa que se debruçará esta tese.

O domínio do ciberespaço agrega elementos à inteligência clássica, resultando em novos formatos de inteligência baseados em ferramentas que outras fontes de dados não possuem, demandando conhecimento de analistas para que sejam utilizados e explorados, já que, com o uso adequado dessas ferramentas, tudo obtido pode ser analisado e convertido em dados úteis, trazendo oportunidades à inteligência criminal.[69]

A confecção de repositórios com infindável quantidade de registros de navegação, preferências, fotos ou atividade na rede por parte do setor privado atrai o interesse dos Estados, que, cientes da existência de ricos bancos de informações, passaram a demandar (i) a ampliação das prerrogativas de acesso a dados de usuários mantidos por empresas e (ii) possibilidades de coleta e tratamento de dados pessoais pelo próprio Estado para, em nome da segurança nacional, subsidiar processos de investigação e de persecução penal. Ao mesmo tempo em que administra (em seus órgãos e subdivisões) outros bancos de dados potencialmente sensíveis, já que inerente à atividade administrativa, justifica a necessidade de coleta e tratamento de dados pessoais para a promoção de eficiência das políticas públicas em escala.

O clima entre as autoridades e empresas provedoras de aplicações de internet tem se acirrado. A retórica e o requerimento de medidas extremas indicam a busca dos bancos de dados mantidos por intermediários, o que ocorre a partir de medidas como bloqueios, que se inserem em uma complexa trama de impasses políticos e jurídicos e suscitam resistências, de

[68] CNIL – Comission Nationale de l'informatique e des Libertés. **Dados Pessoais:** definição. Disponível em: https://www.cnil.fr/en/personal-data-definition. Acesso em: 11 abr. 2022.
[69] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**, Bogotá, v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.

ordem técnica (criptografia) ou jurisdicional (dado armazenados por pessoa jurídica fora do território nacional), das empresas, circunstância que tem evidenciado antagonismo entre os setores, catalisado pela avidez de autoridade ao acesso facilitado às informações produzidas no uso de aplicações de internet. Como exemplos, o acordo celebrado entre o Tribunal de Justiça Eleitoral e a Serasa Experian que autorizava o compartilhamento de dados cadastrais dos cidadãos à Justiça Eleitoral com a empresa, que, de posse dos dados, poderia enriquecer seus bancos de dados para posterior comercialização – fato este que, em 2013, deu causa a uma repercussão tamanha que obrigou o Tribunal a rever e cancelar o acordo; o caso da utilização e do acesso aos dados gerados a partir do uso de cartões que facilitam o pagamento adiantado de viagens no sistema de transporte público de metrópoles brasileiras, como o "Bilhete Único", que coletam e permitem o tratamento de informações sobre viagens dos usuários e podem revelar detalhes de seu dia a dia no sistema de transporte público; o caso da "Farmácia Popular", programa federal para aquisição de medicamentos a baixo custo e que permitia que empresas privadas de "gestão de programas de benefícios em medicamentos" coletassem e armazenassem informações sensíveis de cidadãos, sem a sua organização ou supervisão de uma autoridade[70].

A profusão da capacidade de memória, de processadores cada vez mais eficientes, a diminuição do custo operacional e a aplicação da ciência matemática através da estatística, unidas ao desenvolvimento da Inteligência Artificial, fornecem condições para a criação de potentes mecanismos de análise automatizada de dados, metodologias essas que acabam fornecendo elementos úteis a qualquer processo de tomada de decisões[71], incluindo investigações criminais ou a prova do processo penal. Novas ferramentas tecnológicas permitem analisar expressivas quantidades de dados, provenientes de fontes fechadas ou abertas, de forma muito rápida e intuitiva, tudo com o objetivo de criar valor. Sua principal característica é que, ao viabilizar a análise e o tratamento massivo de dados, permite a apreensão de sentido que seria impossível a partir da análise de poucos dados. Da coleta de

[70] "A recente onda de ataques e atentados terroristas ao redor do mundo tem suscitado inúmeras discussões sobre as necessidades de aumento das capacidades de vigilância dos Estados. Na França, o Estado decretou estado de emergência, o que aumentou consideravelmente as prerrogativas de investigação por parte das autoridades. Na Alemanha, discutem-se reformas legislativas para tornar mais céleres os processos de investigação. No Reino Unido, foi aprovada, em 16 de novembro de 2016, uma das legislações mais agressivas em termos de vigilância do mundo. Nos Estados Unidos, desde os ataques de 11 de setembro, foi encampada uma intensa reforma legislativa para fortalecer o aparato de vigilância nacional, o que se consubstanciou, principalmente, na aprovação do 'USA Patriot Act'" (ANTONIALLI, Dennys; CRUZ, Francisco Brito. **Privacidade e internet**: desafios para a democracia brasileira. Rio de Janeiro: Centro Edelstein de Pesquisas Sociais; São Paulo: Fundação Fernando Henrique Cardoso, 2017. p. 31-42).

[71] BOEING, Daniel Henrique Arruda; ROSA, Alexandre Morais da. **Ensinando um Robô a Julgar: pragmáticas, discricionariedades, heurísticas e vieses no uso de aprendizado de máquina no judiciário**. 1ª Ed. Florianópolis: Emais Academia. 2020. P. 25-31.

dados de múltiplas fontes (primeira fase), a ferramenta passa a correlacionar os dados obtidos por categorias – processo conhecido como mineração – para aplicar-lhes os algorítmos e, assim, estabelecer correlações e padrões de comportamento que fazem surgir conhecimento antes oculto na complexidade dos dados (segunda fase), os quais agora podem ser interpretados para a formulação de hipóteses (processo de inferência) ou confirmação de conclusões (processo de valoração). Em razão da heterogeneidade de fontes de informação que podem oferecer dados úteis à investigação de fatos criminosos e à prova ao processo (dados em dispositivos eletrônicos, fontes abertas ou dados à disposição dos provedores de serviço), aplicam-se numerosas técnicas de exploração de dados que, reunidos e classificados, permitem a eleição da melhor decisão ao caso em análise.[72]

No âmbito da investigação e da prova, os usos atuais da Inteligência Artificial demonstram o desenvolvimento de ferramentas que auxiliam na reconstrução de fatos baseados em vestígios digitais. Programas que constroem histórias coerentes baseadas em dados existentes, que elaboram hipóteses e estratégias acusatórias e defensivas ou que, ante a ocorrência de determinado delito, fazem prognósticos sobre as justificações do acusado estão entre essas aplicações. Essas ferramentas ampliam, de forma sem precedentes, o campo da investigação. Mais além, possibilitam a localização de indícios a partir desses rastros digitais com o uso de técnicas de mineração (*data mining*): se antes essa localização dependia exclusivamente da intuição, imaginação e experiência da autoridade policial, hoje minerar dados permite, com até 68% de assertividade, a recuperação elementos dos possíveis cenários de fatos ocorridos e a indicação de onde podem ser encontrados ditos indícios. Na esfera da argumentação jurídica, para atividade que demanda trabalho de persuasão e que não depende exclusivamente de variáveis previsíveis, a Inteligência Artificial municia as partes com suporte documental impressionante, coisa que qualquer humano levaria anos ou décadas para reunir e avaliar.[73]

Mineradores serão os novos agentes da investigação preliminar e do processo penal. A partir de técnicas de mineração de dados, orientadas a explorar, analisar e classificar massivas quantidades de dados – que implicam uma verdadeira devassa na intimidade das pessoas – já é possível estabelecerem-se padrões, regras e uma infinidade de relações que interessam a todos os tipos de tomadores de decisão, criando possibilidades de acesso a novas oportunidades de coleta. Minerar dados tem a capacidade de revelar circunstâncias

---

[72] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 213-216.
[73] FENOLL, Jordi Nieva. **Inteligencia Artificial y Proceso Judicial**. Madrid: Marcial Pons, 2018. p. 26-28.

imperceptíveis pela consciência humana[74]. Em que pese bastante a avançada mineração ou a análise detalhada de dados, a mineração de texto está em fase inicial e é provável que se expanda consideravelmente ao longo dos próximos anos: a quantidade de informação textual na internet irá alimentar um rápido aumento da mineração de texto.[75]

Se utilizadas em determinados casos e a partir de parâmetros seguros, transparentes e controlados pelos cidadãos, tecnologias biométricas oferecem benefícios na facilitação de processos, na integridade de protocolos e na garantia da identidade dos indivíduos envolvidos em uma relação. Em seu atual estado de desenvolvimento, contudo, não se pode ignorar que a utilização irrestrita apresenta consequências negativas que levam à exclusão social ou à erosão da confiança social, com reflexos na liberdade individual e seu desenvolvimento no contexto democrático[76].

Por isso, a grande preocupação do momento está em estabelecer regras específicas relativas à proteção das pessoas no que diz respeito ao tratamento de dados pelas autoridades, organismos ou entidades designados para o exercício da autoridade, e pelos poderes públicos, para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais.

---

[74] MORAIS, Flaviane de Magalhães Barros Bolzan de; MARQUES, Leonardo Augusto Marinho; SARKIS, Jamilla Monteiro. Dados Pessoais no Processo Penal: Tutela da Personalidade e da Inocência Diante da Tecnologia. **Revista Brasileira de Ciências Criminais**, São Paulo, ano 30, v. 190, p. 117-156, maio/jun. 2022. DOI: https://doi.org/10.54415/rbccrim.v190i190.120.

[75] DEVENPORT, Thomas H; HARRIS, Jeanne G. **Competing on Analytics**: the new science of winning. [*S. l.*]: Harvard Business School Publishing Corporation, 2006. *E-book*. p. 156-165.

[76] PITCH, Tamar. **La sociedad de la prevención.** Buenos Aires: Ad Hoc, 2009. p. 151-154.

2. TRATAMENTO DE DADOS PESSOAIS E PERSECUÇAO PENAL

2.1. Tratamento de dados pessoais, Marco Civil da Internet e Lei Geral de Proteção de Dados

Para a *Commission Nationale de l'Informatique et des Libertés,* dados pessoais são quaisquer dados anônimos que podem ser verificados duas vezes para identificar um indivíduo específico. Para determinar se uma pessoa é identificável, considera *todos os meios que foram colocados à disposição do controlador* para a definição de dados pessoais. São descritos como informação relativa a uma pessoa singular identificada ou identificável de forma direta (sobrenome, primeiro nome etc.) e/ou de forma identificação indireta (ID, número etc.).[77]

No âmbito da União Europeia, a proteção de dados de caráter pessoal é objeto tanto da *Carta dos Direitos Fundamentais* como do seu *Tratado de Funcionamento,* sem prejuízo de normas específicas para o regime de proteção de dados pessoais, como é o caso do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho[78], que tutela a proteção de dados de pessoas físicas no que guarda relação com o tratamento e a livre circulação de seus dados pessoais e do qual se projeta a Diretiva 95/46/CE, também conhecida como Regulamento Geral de Proteção de Dados (RGPD)[79], instrumento europeu aplicável a qualquer estrutura, independentemente do setor ou dimensão, e que rege a coleta e o processamento de dados pessoais de forma igualitária em todo o território da União Europeia. Trata-se de uma continuação da Lei Francesa de Proteção de Dados, de 1978, que estabelece regras sobre a coleta e uso de dados em território francês, concebida sob os objetivos de fortalecer os direitos das pessoas, capacitar os atores que processam dados e dar credibilidade ao regulamento graças a uma cooperação reforçada entre as autoridades de proteção de dados[80]. Ou ainda o caso da Diretiva 2016/680, do Parlamento Europeu e do Conselho, referente à proteção de pessoas físicas no que guarda relação com o tratamento de seus dados

---

[77] CNIL – Comission Nationale de l'informatique e des Libertés. **Dados Pessoais:** definição. Disponível em: https://www.cnil.fr/en/personal-data-definition. Acesso em: 11 abr. 2022.

[78] EUR-Lex – Acess to European Union Law. **Document 32016R0679**. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE). 04/05/2016**.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 21 jun. 2019.

[79] DELGADO MARTÍN, Joaquín. **Investigación tecnológica y prueba digital en todas las jurisdicciones**. Madrid: España, 2018. p. 131-132.

[80] MINISTÈRE DE LA ÉCONOMIE DE FINANCES E DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE. **Le règlement général sur la protection des données (RGPD), mode d'emploi**. 16/07/2019. Disponível em: https://www.economie.gouv.fr/entreprises/reglement-general-sur-protection-des-donnees-rgpd. Acesso em: 11 abr. 2022.

pessoais pelas autoridades competentes, para fins de prevenção, investigação, detenção e persecução penal ou execução de sanções penais, além de sua livre circulação a partir do que estabelece a Decisão Marco 2008/977/JAI do Conselho[81].

Dentre os dados pessoais existem, ainda, os dados de categoria especial, aqueles que revelam origem étnica ou racial, opiniões políticas, convicções religiosas ou filosóficas, afiliação sindical e que realizam tratamento de dados genéticos, coletam dados biométricos que ajudem a identificar de maneira unívoca uma pessoa física, dados relativos à saúde ou aqueles relativos à vida e à orientação sexual; dados de condenações a aplicação de penas, medidas de segurança ou sanções administrativas; quando puder causar significativos prejuízos econômicos ou morais aos afetados ou quando o tratamento puder privar os afetados de seus direitos e liberdades individuais, ou impedir-lhes o exercício de controle sobre os seus próprios dados pessoais. Esses dados sensíveis merecem proteção especial, dado que o contexto do tratamento pode implicar riscos para direitos e liberdades fundamentais, razão pela qual não deverão ser objeto de tratamento[82].

A eles, impõe-se a adoção de medidas técnicas e administrativas especiais e proporcionais aos riscos que oferecem. Por regra geral, há *proibição de tratamento* pelo encarregado, admitindo a lei exceções que autorizam o tratamento desses tipos de dados especiais[83]. Vinculam-se à ideia de fontes fechadas as que possuem como expressão inerente a restrição de acesso, sigilo necessário, acesso dependente do rompimento de violação de garantia fundamental, a qual pode ser lícita ou ilícita. O tratamento desses dados só é autorizado: (i) se estritamente necessário; (ii) se sujeito a garantias adequadas dos direitos e liberdades do titular dos dados; (iii) se for autorizado: (a) pelo direito da União ou de um Estado-membro, (b) se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular ou (c) se relacionado com dados manifestamente tornados públicos pelo titular.

Ou seja, de regra, regulamentos de proteção de dados definem as hipóteses em que tais dados podem ser legitimamente utilizados por terceiros e estabelecem mecanismos para proteger os titulares dos dados contra usos inadequados. A licitude do tratamento desse tipo de dado estará vinculada ao consentimento do interessado ou à outra base jurídica que o

---

[81] DELGADO MARTÍN, Joaquín. **Investigación tecnológica y prueba digital en todas las jurisdicciones.** Madrid: España, 2018. p. 131-132.

[82] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 462-464.

[83] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 405-406.

legitime, princípio estabelecido no Considerando 40 do RGPD, dentre os quais encontra-se o exercício de poderes públicos (Considerando 45 do RGPD), arrolado dentre as condições gerais para a licitude do tratamento (art. 6º RGPD).

Ainda no âmbito europeu, há a observância da Lei Orgânica de Proteção de Dados Pessoais e Garantia de Direitos Digitais (LOPDPGDD), base da adaptação do ordenamento jurídico espanhol ao RGPD, a qual regula as obrigações do usuário no processo de transferência e tratamento informações que, em modo de imagem, áudio ou texto, permitem a identificação de uma pessoa e, assim, ter o controle da utilização dos dados que as pessoas disponibilizam. A lei garante novos direitos digitais não contemplados no RGPD e introduz questões como transparência e deveres de informação, a conservação de dados, o consentimento, os sistemas internos de reclamação anônima, os sistemas de informação de crédito, o bloqueio de dados, a *Data Protection Oficial* (DPD) e o regime sancionatório aplicável[84].

Instrumentos e práticas de proteção e tratamento de dados são relativamente recentes no Brasil. O Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu princípios, garantias, direitos e deveres para o uso da internet, e, posteriormente, o advento da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), passou, pela primeira vez, a dispor de forma ampla sobre o tratamento de dados pessoais em meios analógicos e digitais, por pessoa natural e pessoas jurídicas de direito público e privado, com o objetivo de proteger direitos fundamentais como a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural. Logo em seguida, a emergência do impacto tecnológico demandou ao legislador brasileiro emendar a Constituição Federal (Emenda Constitucional nº 115/2022) para, com respaldo nos direitos fundamentais previstos no art. 5º, inciso X, e art. 5º, inciso LXXII, inserir, também ao artigo 5º, inciso que incluiu a proteção de dados pessoais no rol de direitos e garantias fundamentais do cidadão (art. 5º, inciso LXXIX), atribuindo-lhe a condição de cláusula pétrea, direito fundamental autônomo e implicitamente positivado, antes reconhecido pelo Supremo Tribunal Federal (STF) em decisão proferida pelo Plenário na ADI 6.387 MC-Ref/DF, julgada em 2020[85].

---

[84] ESPANHA. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. **Agência Estatal Boletín Oficial del Estado**: Espanha, seção I – Disposiciones generales, n. 294, p. 119788-119857, 6 de dezembro de 2018. Disponível em: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673. Acesso em: 11 abr. 2022.

[85] BRASIL. Supremo Tribunal Federal. **ADI 6.387 MC-Ref/DF**. Relator: Min. Rosa Weber, 17 de novembro de 2020. Disponível em: https://bit.ly/2X3Gg3B. Acesso em: 31 agosto de 2022. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15345022689 &ext=.pdf. Acesso em: 20 abr. 2022.

No que tange ao Marco Civil da Internet (Lei nº 12.965/2014), uma lei ainda tímida ante a complexidade e profundidade do fenômeno digital, pode-se destacar, em relação ao tratamento de dados de usuários da internet, que a norma busca assegurar: (i) que sejam realizados para finalidades (a) que justifiquem sua coleta, (b) não vedadas em lei, e (c) especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; e (ii) que haja consentimento expresso sobre o tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas (art. 7º, incisos VIII e IX). Ademais, estabelece que, em qualquer operação de tratamento de dados pessoais, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (art. 11).

Já a Lei Geral de Proteção de Dados (Lei nº 13.709/2019 – LGPD) é destinada à regulamentação de operações de tratamento realizada por pessoa natural ou jurídica, de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que, em relação ao que interessa ao objeto do nosso estudo, (i) o tratamento tenha por objetivo o fornecimento de serviços ou o tratamento de dados de indivíduos localizados no território nacional e (ii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional. O emprego da LGPD é afastado expressamente quando o tratamento de dados pessoais for (i) realizado por pessoa natural para fins exclusivamente particulares e não econômicos ou (ii) realizado para fins exclusivamente: (a) de segurança pública; (b) defesa nacional; (c) segurança do Estado ou (d) atividades de investigação e repressão de infrações penais, quatro hipóteses para a qual a lei prevê legislação específica que preveja medidas proporcionais e necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular. O tratamento de dados pessoais realizados para fins de segurança pública e atividades de investigação e repressão de infrações penais serão abordados em tópico apartado, em razão da existência de Projeto e Anteprojeto de Lei que buscam regular a matéria no Brasil.

Além de definir termos como dado pessoal, dado pessoal sensível, tratamento, controlador ou operador – apenas para citar as categorias mais recorrentes na pesquisa (art. 5º) –, a LGPD aponta os princípios relacionados à atividade de tratamento de dados (boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas – art. 6º) e elenca hipoteses em que é possível a realização de tratamento de dados por órgãos alheios às autoridades públicas (consentimento pelo titular; cumprimento de obrigação legal ou

regulatória pelo controlador; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral; para a proteção da vida ou da incolumidade física do titular ou de terceiro; para a tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou para a proteção do crédito – art. 7º). Importante frisar que a LGPD também regula o tratamento de dados pessoais cujo acesso é público; não proíbe a atividade, mas aponta o dever em considerar-se a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização (art. 7º, parágrafo 3º).

O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam, ao apoio de atividades do controlador (art. 10). Nesse caso, somente os dados pessoais necessários para o fim almejado poderão ser tratados, além de impor-se ao controlador o dever de adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse, já que a autoridade nacional de proteção de dados poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais quando o tratamento tiver como fundamento legítimo interesse.

Quando o tratamento de dados pessoais for condição para o fornecimento de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer seus direitos na condição de titular, previstos no art. 18. Sem o consentimento do titular, o tratamento de dados pessoais sensíveis poderá ocorrer quando indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador ou no exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (art. 11, II, alíneas “a” e “d”). Em se tratando de tratamento de dados pessoais de crianças e de adolescentes, este deve ser realizado observando *o princípio de melhor interesse do menor*, nos termos do que prevê o artigo 14 da LGPD, o qual faz referência implícita ao Estatuto da Criança e do Adolescente – ECA (*legislação pertinente*), além de impor que, nesse caso, há de ocorrer o consentimento específico e destaque dado por pelo menos um dos pais ou o responsável legal.

A *duração do tratamento* é limitada pelo seu término, não havendo previsão expressa para o seu início. As hipóteses previstas em lei dão conta de que o término ocorrerá (i) quando se verificar (a) que a finalidade foi alcançada ou (b) que os dados deixaram de ser necessários

ou pertinentes ao alcance da finalidade específica almejada; (ii) no fim do período de tratamento, quando dado por autorização; (iii) em caso de revogação do consentimento dado pelo titular, resguardando as hipóteses de interesse público; (iv) em razão de determinação da autoridade nacional, em casos de violação ao disposto na LGPD.

Aos agentes de tratamento de dados pessoais – controlador e operador –, a LGPD aponta o dever de que mantenham registro das operações de tratamento de dados pessoais realizadas, sobretudo quando justificado em legítimo interesse (art. 37), já que a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente às operações realizadas (art. 38). Esse relatório deverá indicar, ao menos: (i) a descrição dos tipos de dados coletados; (ii) a metodologia utilizada para a coleta e para a garantia da segurança das informações; (iii) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (art. 38, parágrafo único).

Ao *operador* cumpre a função de realizar o tratamento obedecendo as orientações do controlador, que, por sua vez, verificará a observância das *próprias instruções* e das *normas sobre a matéria* (art. 39), sendo conferido à autoridade nacional, em nome da necessidade e da transparência, o poder de disposição sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros (art. 40). Ao controlador, indicar o encarregado pelo tratamento de dados pessoais, a quem cumpre, por sua vez: (i) em relação aos titulares, receber reclamações e comunicações, prestar esclarecimentos e adotar providências; (ii) em relação à autoridade nacional, receber comunicações e adotar providências; (iii) em relação aos funcionários e contratados, orientar a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; em relação ao controlador e as normas complementares, cabe a ele executar as demais atribuições determinadas.

Ambos, controlador e operador, estão sujeitos à *reparação dos danos* causados em função de violação à legislação de proteção de dados pessoais, sendo obrigados a repará-los (art. 42), a não ser que comprovem: (i) não ter realizado o tratamento de dados pessoais que lhes é atribuído; (ii) que, ainda que realizado o tratamento de dados pessoais, não houve violação à norma de proteção de dados ou (iii) quando for o dano decorrente de culpa exclusiva do titular dos dados ou de terceiro (art. 43).

A LGPD aponta como causa de *irregularidade do tratamento de dados* quando este ocorrer com inobservância à lei ou quando não puder fornecer a segurança que o titular dele pode esperar, considerados, dentre outros: (i) o modo pelo qual é realizado; (ii) o resultado e

os riscos que razoavelmente dele se esperam; (iii) as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (art. 44). Até mesmo em função disso, indica aos controladores e operadores a adoção de boas práticas e governança dos dados, os quais, individualmente ou por meio de associações, poderão formular regras que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas para os envolvidos, ações educativas, mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (art. 50).

Para estabelecer regras de boas práticas, controlador e operador devem ter em conta, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular. Ao controlador é possibilitado, ainda, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados: (i) implementar programa de governança em privacidade que (a) demonstre o seu comprometimento em adotar processos e políticas internas para garantir o cumprimento de normas e práticas relativas à proteção de dados pessoais; (b) seja aplicável aos dados pessoais sob seu controle, independentemente da forma que coletados; (c) seja adaptado à estrutura, à escala e ao volume das operações e à sensibilidade dos dados tratados; (d) estabeleça políticas e salvaguardas com base em processo de avaliação de impactos e riscos à privacidade; (e) almeje estabelecer relação de confiança com o titular, com atuação transparente e mecanismos de participação; (f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; (g) conte com planos de resposta a incidentes e remediação; (h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas. O controlador deve, ainda, preocupar-se em demonstrar a efetividade de seu programa quando apropriado ou a pedido da autoridade nacional – a quem ainda cumpre estimular a adoção de padrões técnicos que facilitem o controle, pelos titulares, de seus dados pessoais (art. 51) – ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta (art. 50, parágrafo 2º).

Por opção expressa do legislador ao não contemplar o tratamento de dados para segurança pública e persecução penal no âmbito de aplicação da Lei Geral de Proteção de Dados, encaminhamo-nos para a produção de referências legislativas que trataram de inaugurar o tema e que prometem produzir alto impacto no pensar as Ciências Criminais e, no âmbito do processo penal, investigação criminal e prova.

2.2. Tratamento de dados pessoais para fins de prevenção, investigação, detecção e repressão de infrações penais ou para execução penal

Por dados obtidos e incorporados por *agentes públicos*, há de se considerar, em primeiro lugar, que policiais, membros do Ministério Público e juízes podem obter legitimamente dados pessoais sempre que o façam no cumprimento de missão realizada em interesse público ou de poderes públicos.[86] Dessa forma, justifica-se a incorporação de dados de caráter pessoal aos processos judiciais, os quais podem ser ricas fontes para a investigação de delitos ou para formação da prova em qualquer jurisdição. Entretanto, deve essa atividade estar submetida a um regime jurídico singular, de forma a harmonizar o direito fundamental à proteção de dados a outros direitos fundamentais, como a tutela judicial efetiva, o direito de defesa, a liberdade de informação e a publicidade de atos processuais, tudo de forma a satisfazer, dentre outros fins, a proteção da independência judicial e dos procedimentos judiciais (art. 23, 1.f do RGPD)[87].

O tratamento de dados pessoais por parte de autoridades públicas com finalidade preventiva, sobretudo diante da necessidade de proteção a ameaças modernas à segurança pública, tem se demonstrado uma questão ainda complexa. Nesse sentido, à parte das normas de nível constitucional e de processo penal, deve existir um arcabouço legislativo que regule o tratamento pessoal de dados para fins de prevenção de ilícito, fazendo com que o conteúdo de dados obtidos em investigação criminal por violação de dispositivos eletrônicos ou transmitidos por uma rede de informações só possam ser inseridos ao processo penal se obtidos por um concreto meio de prova admitido pela lei processual e desde que observado regularmente o procedimento previsto para sua coleta e tratamento.

Em alguns países europeus, à parte das normas constitucionais e de processo penal, a regulamentação para a obtenção e o aporte de elementos eletrônicos ao processo penal se dão por intermédio de uma série de leis orgânicas que estabelecem regimes jurídicos específicos para medidas de investigação tecnológicas restritivas de direitos fundamentais e de incorporação de dados contidos em suportes eletrônicos ao processo penal. Na Espanha, por exemplo, uma reforma promovida na *Ley de Enjuiciamento Criminal* pela Lei Orgânica nº 13/2015 estabeleceu que a incorporação de dados pessoais se submete a um regime jurídico

---

[86] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 416-419.

[87] DELGADO MARTÍN, Joaquín. **Investigación tecnológica y prueba digital en todas las jurisdicciones.** Madrid: España, 2018. p. 134-135.

singular, na medida em que o direito à proteção de dados convive com direitos fundamentais e princípios constitucionais de toda ordem.

Lá, admite-se a utilização de meios tecnológicos contra a delinquência desde que acompanhados de medidas que mitiguem seus efeitos negativos, sobretudo através do controle jurisdicional, sujeito ainda à observância dos princípios da especialidade, idoneidade, proporcionalidade, além dos princípios da excepcionalidade e necessidade.[88] Seguindo essa premissa, o artigo 23 da LGPD brasileira ressalva que o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, justificando-se, assim, quando empregado na persecução do interesse coletivo, inclusive no âmbito penal, eis que premente a necessidade de coleta de dados da pessoa imputada para fins de persecução.

As regulamentações relacionadas ao manuseio da *internet*, de novas tecnologias e até mesmo de simples obtenção de elementos de investigação ou de provas obtidos por intermédio de computadores são ilustres desconhecidos do diploma processual penal e de leis processuais penais extravagantes brasileiras. No que diz respeito ao emprego de dados pessoais em atividades relacionadas à segurança pública e à persecução penal, a proteção de dados em matéria penal carece de regulamentação, o que ensejou a reunião de uma Comissão de Juristas com o escopo de propor o projeto de "Lei de Proteção de Dados para Segurança Pública e Persecução Penal", apresentado em junho de 2020 à Câmara dos Deputados[89], e a proposição de outro Projeto, o Projeto de Lei nº 1515/2022, de matriz securitária e orientado pela lógica da defesa nacional e da segurança pública, baseado em três pilares: proteção dos direitos fundamentais de segurança, liberdade e de privacidade; eficiência da atuação dos órgãos responsáveis e intercâmbio de dados pessoais entre autoridades competentes[90].

2.3. A Convenção de Budapeste

Preocupados com a utilização de redes informáticas e informações eletrônicas para o cometimento de infrações criminais e de que as provas sejam armazenadas e transmitidas através das redes, Estados-membros do Conselho da Europa e outros países ratificaram a

[88] DELGADO MARTÍN, Joaquín. **Investigación tecnológica y prueba digital en todas las jurisdicciones.** Madrid: España, 2018. p. 361-382.
[89] MORAIS, Flaviane de Magalhães Barros Bolzan de; MARQUES, Leonardo Augusto Marinho; SARKIS, Jamilla Monteiro. Dados Pessoais no Processo Penal: Tutela da Personalidade e da Inocência Diante da Tecnologia. **Revista Brasileira de Ciências Criminais**, São Paulo, ano 30, v. 190, p. 117-156, maio/jun. 2022. DOI: https://doi.org/10.54415/rbccrim.v190i190.120.
[90] AGÊNCIA CÂMARA DE NOTÍCIAS. **Projeto altera Lei de Proteção de Dados para resguardar segurança pública e defesa nacional**. Disponível em: https://www.camara.leg.br/noticias/893704-projeto-altera-lei-de-protecao-de-dados-para-resguardar-seguranca-publica-e-defesa-nacional/. Acesso em: 27 ago. 2022.

Convenção sobre Cyber Delinquência do Conselho da Europa, também conhecida como Convenção de Budapeste, referência que pauta a política global no que guarda relação com a criminalização de condutas e desenvolvimento de ferramentas jurídicas no âmbito da investigação criminal. Trata-se de um instrumento jurídico firmado por 46 dos 47 países do Conselho da Europa (exceção feita à Rússia), que estabelece as bases da política penal comum em face da delinquência relacionada à informática, promovendo uma abordagem sob aspectos concretos para atuação no ciberespaço.

Levando em consideração os novos desafios em matéria de proteção de dados pessoais ante a evolução tecnológica e a globalização, o aumento da coleta e do compartilhamento de dados pessoais, a necessidade de facilitação para transferência de dados para países terceiros e organizações internacionais e a profusão tecnológica que passou a permitir o tratamento de dados pessoais em escalas sem precedentes, a Convenção de Budapeste reconhece a necessidade: (i) de cooperação eficaz entre Estados e iniciativa privada no combate à cibercriminalidade; (ii) de proteger os interesses ligados ao uso e desenvolvimento das tecnologias da informação; (iii) de conceder poderes para combater infrações, facilitando a detecção, investigação e o procedimento criminal e garantir equilíbrio entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais, em especial a liberdade de procurar; (v) de receber e transmitir informações e ideias de qualquer natureza, sem considerações de fronteiras.

No contexto da orientação internacional, o tratamento de dados pessoais pelas autoridades consiste em qualquer operação ou conjunto de operações efetuadas sobre dados pessoais ou conjuntos de dados pessoais para efeitos criminais, com ou sem o emprego de meios automatizados, tais como coleta, registro, organização, estruturação, conservação, adaptação ou alteração, recuperação, consulta, utilização, comparação ou interconexão, limitação do tratamento, apagamento ou destruição. Excepcionalmente, dados pessoais poderão ser tratados quando o tratamento for *estritamente necessário*, mediante a *adoção de medidas técnicas e organizativas* em razão dos maiores *riscos* que pendem sobre esses tipos de dados e somente nos casos previstos – *autorizados por lei*, *se for necessário para a proteção dos interesses vitais do titular dos dados ou de um terceiro*, se *relacionados a dados manifestamente tornados públicos por seu titular*[91].

[91] "(37) Os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, merecem uma proteção especial, dado que o contexto do tratamento desses dados pode implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo 'origem racial' na presente diretiva que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. Tais dados pessoais não

Esse é o produto da normativa de proteção ao tratamento de dados relacionados a infrações e condenações penais, em que também estão previstas disposições que regulam procedimentos, medidas cautelares e de segurança conexas ao tratamento de dados pessoais. Aqui, prevê-se a possibilidade do tratamento de dados pessoais para fins de prevenção, investigação, detenção ou ajuizamento de processos pela prática de infração penal ou de execução de pena, atividades submetidas ao regime da Diretiva 2016/680 do Parlamento Europeu, que produz uma série de efeitos na utilização de dados pessoais em aplicação judicial e cria uma série de obrigações com órgãos de Estado em razão de sua aplicação direta ou interpretação conforme o direito interno em relação ao seu conteúdo[92]. Estabelece um regime de proteção de dados pessoais apoiado na aplicação de regras orientadas a propor um nível elevado e coerente de proteção dos dados pessoais de pessoas singulares e facilitar o intercâmbio de dados entre as autoridades competentes dos Estados-membros, de maneira a assegurar a eficácia da cooperação judiciária em matéria penal e de cooperação policial.

Por outro lado, também assegura a sistematização de direitos dos titulares dos dados oponíveis aos agentes públicos, assim definidos: (i) direito ao acesso (art. 14 da Diretiva 2016/689), que se traduz no direito conferido ao titular dos dados para obter do responsável pelo tratamento de dados a confirmação da ocorrência dessa atividade, ter acesso a esses dados e às informações coletadas a partir deles; (ii) direito à retificação ou à supressão de dados pessoais e limitação do seu tratamento (art. 16 da Diretiva 2016/689), assegurando a norma uma série de obrigações de informações sobre o responsável pelo tratamento. O exercício desses direitos depende de procedimentos em conformidade com o direito interno e, quando se referem a dados que interessem ao processo penal, às normas próprias dessa jurisdição.[93]

---

deverão ser objeto de tratamento, a menos que este esteja sujeito a garantias adequadas dos direitos e liberdades do titular dos dados e seja permitido em casos autorizados por lei ou, se ainda não tiver sido autorizado por lei, se for necessário para a proteção dos interesses vitais do titular dos dados ou de um terceiro, ou ainda se estiver relacionado com dados que tenham sido manifestamente tornados públicos pelo titular dos dados. As garantias adequadas dos direitos e liberdades do titular dos dados podem, por exemplo, incluir a possibilidade de recolher esses dados apenas em ligação com outros dados sobre a pessoa singular em causa, a fim de garantir devidamente a segurança dos dados recolhidos, o estabelecimento de regras mais rigorosas sobre o acesso do pessoal da autoridade competente aos dados ou a proibição da transmissão desses dados. O tratamento desses dados deverá também ser autorizado por lei quando o titular dos dados tiver dado o seu acordo expresso, nos casos em que o tratamento de dados é particularmente intrusivo para o titular. Todavia, o consentimento do titular dos dados não deverá constituir em si mesmo fundamento jurídico do tratamento de dados pessoais pelas autoridades competentes" (Considerando n.º 37 da Convenção de Budapeste – Diretiva 2016/680 do Parlamento Europeu).

[92] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 451-452.

[93] DELGADO MARTÍN, Joaquín. **Investigación tecnológica y prueba digital en todas las jurisdicciones.** Madrid: España, 2018. p.142-143.

Enquanto atribuição da polícia ou de outras autoridades de aplicação da lei voltadas a prevenção, investigação, detecção e repressão de infrações penais, incluindo as atividades policiais sem conhecimento prévio de que um incidente constitui ou não uma infração penal, a Convenção de Budapeste regulamenta o exercício de medidas coercivas ou para a manutenção da ordem pública quando necessárias para (i) a salvaguarda e prevenção de ameaças à segurança pública e aos interesses fundamentais da sociedade protegidos por lei e (ii) a prática de infrações penais.

Além de trazer definição legal às estruturas tecnológicas, orienta países a prever normas de Direito Penal material – com a criminalização de condutas no ambiente digital, normas de Direito Processual – voltadas à investigação, produção de provas eletrônicas e estabelecer meios de cooperação internacional –, além da participação em uma rede com o objetivo de assegurar a prestação de assistência às investigações ou aos procedimentos relativos a infrações penais ou para recolher provas eletrônicas de uma infração penal de maneira mais ágil.[94]

O instrumento não impede que os Estados-membros especifiquem as operações e os procedimentos de tratamento na legislação processual penal nacional no que se refere ao tratamento de dados pessoais por Tribunais ou outras autoridades judiciais, em particular no que respeita aos dados pessoais que constem de uma decisão judicial ou de um registro relacionado com uma ação penal, mas proporciona garantias contra o risco de abusos e de arbitrariedade ao impor aos Estados-membros o dever de, ao menos, especificar os objetivos, os dados pessoais a tratar, as finalidades do tratamento e os procedimentos destinados a preservar a integridade e a confidencialidade dos dados pessoais, bem como os procedimentos para sua destruição.

Em geral, a regulamentação da obtenção, a cessão e o tratamento dos dados pessoais nesse campo tem sido deficitária; atividades inerentes aos processos penais nacionais não foram consideradas nas primeiras levas das Leis Gerais de Proteção de Dados, mas encontram um regime próprio a partir do Considerando nº 35, o qual refere que, para efeitos da Diretiva 2016/680 do Parlamento Europeu, o consentimento do titular dos dados não deverá constituir fundamento jurídico oponível ao tratamento de dados pessoais pelas autoridades competentes, as quais podem incluir não apenas as autoridades públicas propriamente ditas, como

[94] LA FUENTE; Elvira Tejada de. Introducción: Ciberseguridad y Ciberdelincuencia: respuestas desde el Estado de Derecho. La Armonización Legislativa Transnacional, en particular: las medidas de investigación criminal en la Convención de Budapest. *In*: ZARAGOZA TEJADA, Javier Ignácio. **Investigación Tecnológica y Derechos Fundamentales**: comentarios a las modificaciones introducidas por la Ley 13/2015. Navarra: Editorial Aranzadi, 2017. p. 25-72.

autoridades judiciárias, a polícia ou outras autoridades de aplicação da lei, mas também organismos ou entidades designados para o exercício da autoridade e dos poderes públicos para efeitos da Diretiva[95].

Uma das bases jurídicas que exclui a exigência do consentimento do interessado e legitima a obtenção e o tratamento de dados pessoais por forças e corpos de segurança estatal – sobretudo nas atividades de investigação e coleta de elementos de autoria e materialidade da prática de uma infração penal – está ancorada no cumprimento de missão realizada em interesse público ou de poderes públicos, aqueles levados a efeito por autoridade competente investida com poderes pelo Estado para prevenção, investigação, detecção, persecução ou execução penal, além daqueles necessários à proteção e à prevenção de ameaças à segurança pública. Para ser lícito, o tratamento de dados pessoais deverá ser necessário para a execução de uma missão de interesse público por uma autoridade competente para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Ao responsável pelo tratamento compete estabelecer, se aplicável e na medida do possível, uma distinção entre diferentes categorias de titulares de dados, tais como: (a) pessoas às quais existem motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal; (b) pessoas condenadas por uma infração penal; (c) vítimas de uma infração penal ou pessoas relativamente às quais certos fatos encaminhem à compreensão de que possam vir a ser vítimas de uma infração penal; (d) terceiros envolvidos numa infração penal, tais como pessoas que possam ser chamadas a testemunhar em investigações penais

[95] "Para ser lícito, o tratamento de dados pessoais nos termos da presente diretiva deverá ser necessário para a execução de uma missão de interesse público por uma autoridade competente com base no direito da União ou dos Estados-Membros para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Estas funções deverão abranger a proteção dos interesses vitais do titular dos dados. O exercício das funções de prevenção, investigação, detecção ou repressão de infrações penais conferidas institucionalmente por lei às autoridades competentes permite-lhes exigir que as pessoas singulares cumpram o que lhes é solicitado. Neste caso, o consentimento do titular dos dados, na aceitação do Regulamento (UE) 2016/679, não deverá constituir a fundamento jurídico do tratamento de dados pessoais pelas autoridades competentes. Caso seja obrigado a cumprir uma obrigação legal, o titular dos dados não tem verdadeira liberdade de escolha, pelo que a sua reação não poderá ser considerada uma livre manifestação da sua vontade. Tal não deverá obstar a que os Estados-Membros prevejam por lei a possibilidade de o titular dos dados consentir que os seus dados pessoais sejam tratados para as finalidades previstas na presente diretiva, nomeadamente que sejam efetuados testes de ADN no âmbito de investigações penais ou controlada a sua localização por meio de etiquetas eletrónicas tendo em vista a execução de sanções penais" (UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**: p. L 119/89-L 119/131, 4.5.2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 11 abr. 2022).

relacionadas com infrações penais ou em processos penais subsequentes, pessoas que possam fornecer informações sobre infrações penais, ou contatos, ou associados aos suspeitos, ou condenados pela prática de uma infração penal.

A obtenção do dado há de ser necessária para a investigação de um fato específico, jamais podendo admitir-se a procura especulativa, sem "causa provável", alvo definido, finalidade tangível ou com desvio de finalidade, para além dos limites autorizados, de elementos capazes de atribuir responsabilidade penal, o que configura a prática de *fishing expedition*[96], investigação especulativa indiscriminada, sem objetivo certo ou declarado, já descartada pelos Tribunais brasileiros.[97] Assim, a coleta e o tratamento de dados pessoais deve ser excepcional e subsidiária – somente se a finalidade do tratamento não puder ser obtida por outros meios – e, em ocorrendo, há de ser feita somente em dados adequados e necessários, sem excessos, para uma investigação concreta com fins explícitos e legítimos, os quais serão determinados no momento da coleta dos dados e que não excedam o tempo necessário em busca de ditos fins.[98]

Atividades de obtenção e tratamento de dados partem de princípios gerais previstos no Regulamento 2016/679 do Parlamento Europeu e do Conselho da União Europeia, que são os da *legalidade*; da *necessidade* e da *proporcionalidade da medida* e no respeito aos *interesses legítimos do indivíduo* afetado. Mas a partir de seu Considerando 26[99], a Diretiva 2016/680 estabelece um rol específico de princípios aplicáveis ao tratamento de dados para efeitos de

[96] ROSA, Alexandre Morais; SILVA, Viviani Ghizoni; MELO E SILVA, Philipe Benoni. ***Fishing Expedition* e Encontro Fortuito na Busca e Apreensão**. Florianópolis: EMais, 2019.

[97] AgRg no RMS nº 62.562.

[98] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 411.

[99] O tratamento de dados pessoais tem de ser feito de forma lícita, leal e transparente para com as pessoas singulares em causa, e exclusivamente para os efeitos específicos previstos na lei. Tal não obsta, em si mesmo, a que as autoridades de aplicação da lei exerçam atividades tais como investigações encobertas ou videovigilância. Tais atividades podem ser executadas para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, desde que estejam previstas na lei e constituam uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os interesses legítimos da pessoa singular em causa. A lealdade de tratamento, que constitui um dos princípios da proteção de dados, é uma noção distinta do direito a um tribunal imparcial, tal como definido no artigo 47º da Carta e no artigo 6º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH). As pessoas singulares deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos seus dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente ao tratamento desses dados. Em especial, os efeitos específicos do tratamento deverão ser explícitos e legítimos e deverão estar determinados no momento da recolha dos dados pessoais. Os dados pessoais deverão ser adequados e relevantes para os efeitos para os quais são tratados. É especialmente necessário garantir que os dados pessoais recolhidos não sejam excessivos nem conservados durante mais tempo do que o necessário para os efeitos para os quais são tratados – e só deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados são conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar prazos para o seu apagamento ou revisão periódica. Os Estados-membros deverão prever garantias adequadas aplicáveis aos dados pessoais conservados durante períodos mais longos, a fim de fazerem parte de arquivos de interesse público ou de serem utilizados para fins científicos, estatísticos ou históricos.

prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais. São eles: *licitude e lealdade, limitação da finalidade, minimização, exatidão, limitação do prazo de conservação, integridade e confidencialidade, responsabilidade, proteção de dados por defeito e "desde o desenho"*.

Por *licitude e lealdade* (art. 8 da Diretiva 2016/680) atribui-se a necessidade de que dados pessoais sejam tratados por uma autoridade competente se e à medida que for necessário para o exercício de sua atribuição, cabendo ao ordenamento jurídico interno ao menos especificar os objetivos do tratamento, os dados pessoais a tratar e as finalidades do tratamento. *Lealdade, ou transparência*, pressupõe um sistema de acesso sobre o tratamento que esteja sendo realizado com os dados, de forma a assegurar ao afetado pelo tratamento condições de tomar conhecimento da realização do tratamento e obter da autoridade informações precisas sobre as circunstâncias da obtenção, as finalidades, qual será o tipo de tratamento a que estará sujeito, o que será feito com o resultado do tratamento, se os resultados retroalimentarão novas pesquisas para produzir novos dados e se serão cedidos ou comunicados a terceiros. A fim de assegurar a lealdade do tratamento em relação ao titular dos dados, este deverá ser informado sobre o fundamento jurídico do tratamento e a duração da conservação dos dados, à medida que tais informações adicionais sejam necessárias, tendo em conta as circunstâncias específicas em que os dados são tratados.

A *limitação de finalidade* orienta que a coleta de dados ocorrerá com finalidade determinada, explícita e legítima, assegurando-se, ainda, que não serão tratados posteriormente com finalidades alheias à original para fins incompatíveis com os da prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais. Se os dados pessoais forem tratados para uma finalidade distinta daquela para a qual foram recolhidos, esse tratamento deverá ser permitido apenas se em conformidade com as disposições legais aplicáveis e for necessário e proporcional para a prossecução dessa outra finalidade.

Para garantir que os dados não sejam excessivos nem conservados durante mais tempo do que o necessário para os efeitos para os quais são tratados, o princípio da *minimização* (art. 4º, 1.c, da Diretiva 2016/680) assegura que o tratamento ocorrerá apenas em dados adequados, pertinentes e não excessivos em relação aos fins pretendidos. *Minimização de dados* significa que o tratamento se limita ao adequado e necessário para atingir os fins a que se destina[100] e, na mesma medida que o princípio da *limitação do prazo de conservação* (art.

[100] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 403-404.

4º, 1.e, c/c art. 5º da Diretiva 2016/680), determina que os dados devem ser conservados apenas pelo período necessário para os fins aos quais se destina, havendo, inclusive, orientação para que Estados fixem prazos para a supressão dos dados ou para uma revisão periódica, de forma a averiguar a necessidade de conservação dos dados.

As autoridades competentes deverão assegurar que não sejam transmitidos nem disponibilizados dados pessoais incorretos, incompletos ou desatualizados, valor consagrado pelo princípio da *exatidão* (art. 4º, 1.d, da Diretiva 2016/680), orientado a garantir a exaustividade e fiabilidade dos dados pessoais transmitidos ou disponibilizados. Este princípio aplica-se tendo em conta a natureza e a finalidade do tratamento em causa, ganhando especial importância quando diante de processo judicial, já que muitas declarações que contêm dados pessoais são baseadas em percepções subjetivas e nem sempre verificáveis.

Já o *princípio da integridade e confidencialidade* (art. 4º, 1.f, da Diretiva 2016/680) impõe o emprego de segurança adequada ao tratamento de dados – vedação de tratamento não autorizado ou ilícito –, assim como de medidas técnicas apropriadas, orientadas a evitar a perda, a destruição, a inutilização ou os danos acidentais aos dados pessoais[101]. Aponta para o emprego de técnicas e gestão adequadas para evitar a *violação de dados pessoais* (art. 3.11 da Diretiva 2016/680), o acesso ou a utilização desses dados e do equipamento utilizado por parte de pessoas não autorizadas, levando em conta as técnicas e tecnologias avançadas, os custos da sua aplicação em função dos riscos e a natureza dos dados pessoais a proteger. A propósito, decorre do princípio da *responsabilidade* (art. 19 da Diretiva 2016/680) o dever do responsável pelo tratamento de dados em aplicar medidas técnicas e organizacionais adequadas, além de estar em condições de demonstrar que o tratamento realizado se encontra em conformidade com a Diretiva 2016/680.

Dos princípios da *integridade* e da *responsabilidade* decorre a obrigação de que sejam conservados registros cronológicos de operações em sistemas de tratamento automatizado, como a recolha, alteração, consulta, divulgação – incluindo transferências –, interconexão ou apagamento, assim como o registro e a identificação da pessoa que consultou ou divulgou dados pessoais, os quais deverão ser utilizados exclusivamente para efeitos de verificação da licitude do tratamento, autocontrole, garantia da integridade e segurança dos dados e das ações penais.

Finalmente, o princípio da *proteção de dados por defeito e "desde o desenho"* (art. 4º, 1.h, da Diretiva 2016/680) indica que, levando em consideração o custo de aplicação, a

[101] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 403-404.

natureza, o âmbito, o contexto e os fins, o responsável pelo tratamento deve aplicar – seja no momento de determinação dos meios, seja no momento de execução do tratamento – procedimentos e técnicas voltadas a reduzir ao máximo o tratamento de dados pessoais, pseudonimizar assim que possível os dados pessoais, dar transparência de forma a permitir que os interessados supervisionem o tratamento de dados, melhorar o sistema de segurança, enfim, medidas concebidas para aplicar os demais princípios de proteção de dados. Ademais, que os desenvolvedores de produtos, serviços e aplicações baseados em dados também tenham em conta, além do estado atual da técnica, o direito fundamental à proteção de dados pessoais.

Compreendido como uma medida voltada a preservar a segurança e evitar o tratamento em violação à proteção dos dados pessoais, deverá ser realizada uma avaliação dos riscos que o tratamento implica, cabendo ao responsável pelo tratamento aplicar medidas que os atenuem e promovam um nível de segurança adequado, de maneira a observar o respeito à confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função do risco e da natureza dos dados pessoais a proteger.

2.4. O Anteprojeto da Comissão de Juristas – LGPD Penal

De forma a demonstrar a necessidade, a estrutura e os principais conceitos para regular o tratamento de dados pessoais no âmbito da segurança pública e de atividades de persecução e repressão de infrações penais no Brasil, a Comissão de Juristas, instituída por Ato do Presidente da Câmara dos Deputados, apresentou Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal[102]. A lacuna legislativa existente no ordenamento jurídico brasileiro é produto da opção expressa do legislador ao não contemplar o tratamento de dados para segurança pública e investigação criminal no âmbito de aplicação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018). A constatação de que a matéria está sujeita a ponderações específicas e de que existe reivindicação da sociedade e das autoridades competentes para regulação do tema, surgida no processo de debate da própria LGPD, indicaram a emergência do debate.

Apontando para a necessidade prática de que órgãos responsáveis por atividades de segurança pública e de investigação/repressão criminais detenham segurança jurídica para exercer suas funções com maior eficiência e eficácia de forma, compatível com as garantias

[102] BRASIL. Câmara dos Deputados. **Anteprojeto de lei da Comissão de Juristas sobre o Tratamento de Dados Pessoais para fins de Segurança Pública e persecução penal**. Brasília: Câmara dos Deputados, 2020.

processuais e os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade dos titulares de dados envolvidos, o projeto indica balizas e parâmetros aplicáveis a qualquer operação de tratamento de dados pessoais realizada por autoridades competentes em atividades de segurança pública e de persecução penal (art. 3º) – excluído expressamente o tratamento realizado para fins exclusivos de defesa nacional e segurança do Estado (art. 4º), equilibrando a proteção do titular contra mau uso e abusos, como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações.

Inspirado na Lei Geral de Proteção de Dados brasileira e na Diretiva 680/2016 da União Europeia, o projeto da LGPD Penal estrutura-se em 12 capítulos, com 68 artigos que abordam oito eixos de análise: (i) âmbito de aplicação da Lei; (ii) condições de aplicação; (iii) base principiológica; (iv) direitos e obrigações; (v) segurança da informação; (vi) tecnologias de monitoramento; (vii) transferência internacional de dados; (viii) a autoridade de supervisão – para disciplinar princípios, diretrizes e linhas mestras da proteção de dados e harmonizar os deveres do Estado na prevenção e na repressão de ilícitos criminais às observâncias das garantias processuais e prerrogativas fundamentais dos cidadãos brasileiros no que tange ao tratamento de dados pessoais e com a pretensão de complementar o microssistema legislativo de tratamento de dados para fins de segurança pública e de investigação criminal, hoje existente em leis esparsas e voltadas à regulamentação de quebras de sigilo no contexto processual penal.

A disciplina da LGPD Penal aponta como fundamentos (art. 2º) a dignidade, os direitos humanos, o livre desenvolvimento da personalidade e o exercício da cidadania pelas pessoas naturais; a autodeterminação informativa; o respeito à vida privada e à intimidade; a liberdade de manifestação do pensamento, de expressão, de informação, de comunicação e de opinião; a presunção de inocência; a confidencialidade e a integridade dos sistemas informáticos pessoais e garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal. Estes devem ser observados em relação a *categorias de titulares dos dados* (art. 7º), divididas em: (i) as pessoas em relação às quais existem indícios suficientes de que cometeram uma infração penal; (ii) as pessoas em relação às quais existem indícios suficientes de que estão prestes a cometer uma infração penal; (iii) as pessoas processadas pela prática de infração penal; (iv) as pessoas condenadas definitivamente pela prática de infração penal; (v) as vítimas de uma infração penal ou pessoas em relação às quais certos fatos indicam que podem ser vítimas de uma infração penal; (vi) outras pessoas, tais como testemunhas, pessoas que possam fornecer informações, ou contatos, ou associados das pessoas referidas nos incisos

I a V, dentre as quais o responsável pelo tratamento deve estabelecer uma clara distinção, assim como deve distinguir, na medida do possível, dados pessoais baseados em fatos de dados pessoais baseados em avaliações pessoais (art. 8º).

Um dos requisitos para o tratamento de dados exige que este deva ser realizado quando necessário para o cumprimento de atribuição legal de autoridade competente, na persecução do interesse público, na forma de lei ou regulamento. Deve o tratamento de dados ocorrer, portanto, por intermédio de uma autoridade competente no papel de controlador (artigo 9º, inciso I), condição de licitude e legitimidade que exigem um comando legal para que o tratamento de dados ocorra, e cuja atribuição para o tratamento de dados seja conferida por lei em sentido estrito (leis ou regulamentos). A legalidade estrita é exigida somente nas hipóteses cuja repercussão e cujo dano são mais sensíveis: (i) no tratamento de dado sensível; (ii) no tratamento de dados para os quais a Constituição ou leis infraconstitucionais resguardam o direito ao sigilo, ancorado em maiores expectativas de privacidade do titular; (iii) na utilização de tecnologia de monitoramento e/ou tratamento de dados de elevado risco, nas quais a potencialidade de dano a direitos, garantias e liberdades de titulares é alta. Ainda como requisitos para o tratamento de dados a LGPD Penal aponta para a possibilidade com vistas à execução de políticas públicas previstas em lei, na forma de regulamento (artigo 9º, inciso II) e para a proteção da vida ou da incolumidade física do titular ou de terceiro contra perigo concreto e iminente (artigo 9º, inciso III).

Há expressa vedação ao tratamento de dados pessoais para atividades de segurança pública e de persecução penal por pessoa de direito privado (art. 10). O anteprojeto estabelece, entretanto, uma ressalva aos procedimentos sob a tutela de pessoa jurídica de direito público, determinando que estes serão objeto de informe específico ao Conselho Nacional de Justiça, sem prejuízo de outras exigências legais. Além disso, a LGPD Penal prevê direitos dos titulares e as obrigações dos agentes de tratamento: aos titulares, o texto assegura: (i) direitos de acesso aos dados; (ii) de retificação; (iii) à proteção contra a discriminação; (iv) o direito à explicação de processos automatizados; aos agentes de tratamento, impõe como obrigações (i) a necessidade de elaboração de relatórios de impacto à proteção de dados pessoais em casos de tratamento de dados pessoais sensíveis, sigilosos, ou operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados e (ii) a manutenção de registros detalhados das atividades de tratamento.

Se a noção de acesso à informação e transparência é anunciada como um de seus pilares, o anteprojeto alia o dever de conferir transparência a modalidades de tratamento de dados realizadas pela autoridade competente e operações que pretendam gerar confiança em

suas legitimidade e integridade a mecanismos de supervisão e controle institucional, tudo de forma a assegurar garantia de publicidade aos tipos, escopo e finalidades de usos de dados.

Importante orientação apresentada pelo Anteprojeto da LGPD Penal guarda relação com a conceituação de tecnologia de monitoramento (art. 42). Nos termos propostos – sempre condicionada à previsão legal específica, análise de impacto regulatório e a relatório de impacto à proteção de dados –, *tecnologia de monitoramento* é compreendida como equipamento, programa de computador ou sistema informático que possa vir a ser usado ou implementado para tratamento de dados pessoais captados ou analisados em vídeo, imagem, texto ou áudio. Com inspiração em legislações de Nova Iorque e do Estado de Washington, expressos no parágrafo 1º do referido art. 42 estão demarcados os critérios para identificação de utilizações desse tipo de tecnologia que representem alto risco: natureza dos dados envolvidos, as finalidades específicas do tratamento ou mesmo a possibilidade de tratamento discriminatório como critérios mínimos para tal avaliação.

O compartilhamento de dados entre autoridades públicas competentes para os fins da lei, entre estas e autoridades públicas cuja atribuição legal não versa sobre investigações e segurança pública, e autoridades competentes e pessoas jurídicas de direito privado também recebeu atenção do anteprojeto, fixando requisitos para o tratamento desses diferentes fluxos: devem estar regrados por autorização legal ou judicial, resguardada a possibilidade de atuações conjuntas e colaborações, quando estas também forem lícitas.

O artigo 6º consolida uma base de princípios inspirados na LGPD que devem guiar as etapas e as cadeias do tratamento de dados pessoais no âmbito da investigação. O tratamento de dados deve: (i) estar embasado em hipótese legal (*licitude*); (ii) ocorrer para fins legítimos, específicos, explícitos e informados ao titular, vedado tratamento posterior de forma incompatível (*finalidade*); (iii) ser realizado com pertinência às suas finalidades e com o mínimo suficiente para consecução dos objetivos do tratamento (*adequação*). Deve haver, ainda, (v) compatibilidade do tratamento com seus objetivos e serem assegurados (*proporcionalidade*) (vi) livre acesso às garantias de facilidade e gratuidade ao acesso às informações (*livre acesso*) de (vii) formas claras, precisas e acessíveis (*qualidade dos dados*) (viii) sobre o tratamento que está sendo realizado nos dados dos titulares e sobre o seu responsável (*transparência*). Os dados devem (ix) ser atualizados com exatidão, clareza, relevância (*segurança*); (x) empregadas medidas técnicas e administrativas para a sua não violação (*prevenção*) e (xi) evitar a realização do tratamento para fins discriminatórios ilícitos ou abusivos (*não discriminação*), cabendo (xii) a responsabilização e prestação de contas em caso de violação (*responsabilização*).

Em comparação à Diretiva 2016/680 do Parlamento, ainda que subdivididos os princípios em categorias distintas, o Anteprojeto da LGPD Penal tutela as mesmas circunstâncias previstas nos princípios exortados pela Convenção de Budapeste, inovando apenas no que guarda relação com a orientação para evitar a realização do tratamento para fins discriminatórios ilícitos ou abusivos, o princípio da *não discriminação*, não contemplado expressamente na norma internacional.

2.5. O Projeto de Lei nº 1515/2022 da Câmara dos Deputados

Com forte influência na mentalidade orientada ao resguardo da segurança pública e defesa nacional, também existe o Projeto de Lei nº 1515/2022 (PL nº 1515/2022)[103], de autoria do deputado Coronel Armando (PL-SC), atualmente em trâmite na Câmara dos Deputados e que se anuncia como instrumento para regular: (i) a proteção dos direitos fundamentais de segurança, liberdade e de privacidade; (ii) a eficiência da atuação dos órgãos responsáveis; (iii) o intercâmbio de dados pessoais entre autoridades competentes e que tem o objetivo de orientar a aplicação da LGPD para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública e de investigação e repressão de infrações penais.

Está estruturado em nove capítulos, com 59 artigos, e chama a atenção: (i) pela segmentação da disciplina das atividades de tratamento de dados pessoais entre as atividades de defesa do Estado e Defesa Nacional (art. 7 a art. 8) – não regulada pelo Antprojeto da Comissão de Juristas –, o tratamento de dados em atividades de Segurança Pública (art. 9 a art. 13) e o tratamento de dados para fins de investigação e repressão de infrações penais (art. 14 a art. 19); (ii) pelo fato de abrir mão dos princípios da não discriminação (abordado pelo Anteprojeto da Comissão de Juristas) e da *responsabilização* e prestação de contas (disposto tanto na Convenção de Budapeste como no Anteprojeto da Comissão de Juristas); (iii) por buscar promover alterações na Lei das Organizações Criminosas (Lei nº 12.850/2013), na Lei de Lavagem de Dinheiro (Lei nº 9.613/1998), no Marco Civil da Internet (Lei nº 12.965/2014) e na Lei que dispõe sobre a identificação criminal do civilmente identificado (Lei 12.037/2009), sempre ampliando poderes de acesso, tratamento e compartilhamento de dados por agentes públicos, propostas estas que, de uma forma geral, deixa clara sua opção por uma

[103] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1515/2020**, de 7 de junho de 2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274. Acesso em: 20 jun. 2022.

matriz securitária[104], em que a defesa social surge como principal objetivo[105] e o fundamento do direito de punir do Estado se estrutura no interesse coletivo/social e na proteção dos bens indispensáveis à vida em sociedade, pois o poder punitivo não pode ser obstaculizado por garantias que, na prática, servem apenas para protelar a realização da justiça[106].

Concretamente, sobretudo no que guarda relação ao Tratamento de Dados Pessoais pra fins de Investigação Criminal e Processo Penal, destina Seção Especial que (i) assegura às autoridades públicas, com observância às regras de Direito Processual Penal, o tratamento e o compartilhamento de dados pessoais e de dados pessoais sensíveis (art. 14), garantindo (ii) o acesso e o compartilhamento, entre autoridades competentes, a dados pessoais e a bancos de dados controlados por órgãos e entidades da administração pública (art. 15), (iii) o tratamento e compartilhamento de dados pessoais e dados pessoais sensíveis para finalidades de inteligência de segurança pública (Decreto nº 3.695/2000), investigação e repressão de infrações penais (art. 16), (iv) o acesso de autoridades competentes, a dados pessoais e a bancos de dados controlados por órgãos e entidades da Administração Pública, inclusive dos órgãos integrantes do Subsistema e Inteligência de Segurança Pública (Sisp) para fins de inteligência de segurança pública, investigação e repressão de infrações penais, o qual se dará: (iv.a) mediante previsão legal; (iv.b) por cooperação voluntária por parte do particular, quando em conformidade com a LGPD; (iv.c) por contrato, acordo de cooperação ou instrumento congênere (art. 17 c/c art. 12); (v) o acesso, o tratamento e o compartilhamento a dados pessoais e a bancos de dados controlados por pessoas jurídicas de direito privado, por meio de (v.a) requisição do delegado de polícia ou do membro do Ministério Público, com a indicação do fundamento legal, (v.b) cooperação voluntária do titular dos dados, (v.c) contrato, acordo de cooperação ou instrumento, ou por intermédio de (v.d) canal técnico de inteligência de Estado (art. 17 c/c art. 12) e, finalmente, (vi) o acesso a dados pessoais controlados por pessoas jurídicas de direito privado que estejam sujeitos a sigilo legal ou constitucional, o que deve dar-se mediante regulação pela legislação processual penal, autorização judicial ou, ainda, na forma de seu art. 12 (requisição do Ministério Público, cooperação voluntária do titular, contrato, acordo de cooperação ou instrumento).

Sua lógica pautada no dever estatal de eficiência nas atividades de segurança e de defesa nacional e na garantia do direito à segurança pública não deixa muitos espaços para

---

[104] SILVEIRA, Felipe Lazzari; CAMARGO, Rodrigo Oliveira de. O Legado Tecnicista do Pacote Anticrime. **Revista Brasileira de Ciências Criminais**, São Paulo, ano 28, n. 168, p. 19-36, junho 2020.

[105] ROCCO, Arturo. **Sul concetto del diritto subietivo di punire**. Opere Giuridiche. Scrtitti giuridici vari. Roma: Società Editrice Del Foro Italiano, 1933. v. III. p. 148.

[106] MANZINI, Vincenzo. **Trattato de Procedura Penle e di Ordenamento Giudiziario.** Torini: Fratelli Bocca Editori, 1920. v. I. p. 95.

que as propostas se desenvolvam de forma compatível com muitas garantias processuais e direitos fundamentais, o que também serve para deixar clara a importância da luta pelo espaço da defesa nas atividades de tratamento de dados.

2.6. Caso Kiss e o tratamento de dados pessoais de pretendentes a jurados para a formação do Conselho de Sentença[107]

Por ocasião da apreciação dos recursos de apelação ofertados pelas defesas no caso do incêndio da boate Kiss, uma das maiores tragédias – factual e jurídica – recentes da história do Brasil, a 1ª Câmara Criminal do Tribunal de Justiça do Estado do Rio Grande do Sul (TJRS), por maioria, anulou o julgamento realizado pelo Tribunal do Júri, reconhecendo, dentre tantas outras, uma nulidade por ofensa à paridade de armas em razão do tratamento de dados pessoais, pelo Ministério Público do Estado do Rio Grande do Sul (MPRS), de integrantes da lista de jurados. Por ocasião do sorteio para a formação do Conselho de Sentença na data do júri, os representantes do órgão responsável pela acusação impugnaram 108 pessoas, motivando suas recusas com base em dados pessoais obtidos – e tratados – a partir do Sistema de Consultas Integradas, ferramenta a que tem acesso livre em razão de convênio firmado com o Poder Executivo do Estado do Rio Grande do Sul, através da Secretaria de Segurança Pública, visando ao acesso ao seu banco de dados, e que oferece enorme panorama de informações sigilosas sobre as pessoas.

O Provimento nº 17/2022 da Procuradoria-Geral de Justiça do Estado do Rio Grande do Sul, o qual disciplina a aplicação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) no âmbito do MPRS, prevê que dados pessoais à disposição da instituição poderão ser tratados quando o tratamento tiver por escopo o cumprimento de atribuições legais, observados os princípios da finalidade, adequação e necessidade, e houver (i) respaldo em interesse público, social, difuso, coletivo, individual indisponível, funcional ou administrativo, ou (ii) amparo em previsão legal específica[108]. Nesses casos, o MPRS é o

---

[107] O desenvolvimento do presente capítulo acabou sendo utilizado para a produção de um artigo publicado no Boletim do IBCCRIM (CAMARGO, Rodrigo Oliveira de. Ilicitude da Devassa: Tratamento de Dados Pessoais de Jurados em Face dos Princípios da Convenção de Budapeste e do Anteprojeto da LGPS-Penal no Brasil. **Boletim do IBCCRIM**, São Paulo, ano 30, n. 159, p. 10-12, out/2022).

[108] Caminhos semelhantes estão sendo trilhados pelo Ministério Público de Minas Gerais, voltados ao desenvolvimento de tecnologias de Inteligência, informação e investigação (Dini). Objeto de reformulações no período entre 2017 e 2020, o Gabinete de Segurança e Inteligência (GSI) da instituição passou a ser diretamente vinculado à Procuradoria-Geral de Justiça e deu visibilidade às atividades de inteligência e contrainteligência ministerial. A Resolução PGJ nº 12, de 8 de setembro de 2017, estabeleceu critérios de governança das atividades de Segurança e de Inteligência pela instituição do Sistema de Segurança Institucional do Ministério Público do Estado de Minas Gerais (Seginst) e do Sistema de Inteligência do Ministério Público do Estado de Minas Gerais (Simp), além de criar o Comitê de Políticas e Gestão Estratégica de Segurança Institucional

controlador dos dados pessoais a sua disposição, e a ele compete decidir sobre o tratamento desses dados, cabendo aos seus membros, servidores e estagiários a condição de operadores de dados pessoais, sendo que os sistemas internos da instituição devem manter registro das operações de tratamento de dados pessoais que realizarem os agentes de tratamento. O provimento prevê, ainda, a estruturação de tratamento de dados pela Instituição em torno do Núcleo de Inteligência – Nimp, um Laboratório de Dados e Inovação – MPRS.Labs e a Divisão de Tecnologia da Informação e Comunicação, órgãos autorizados a realizar tratamento estruturado de dados pessoais, em nome do controlador (neste caso, do MPRS).[109]

O Provimento 20/2010 do mesmo MPRS já trabalhava com a reestruturação, a redefinição das atribuições e o funcionamento do Núcleo de Inteligência e a criação, as atribuições e o funcionamento do Laboratório de Tecnologia. O Núcleo de Inteligência surge com a função de produzir conhecimento de imediata ou potencial influência sobre o processo decisório e as ações ministeriais, utilizando-se, para tanto, do exercício metodológico das atividades de inteligência, desempenhados por *unidades de operações* e *unidades de análise de dados e informações*. Nessa estrutura, às *unidades de operação* compete coletar dados, informações e conhecimento necessários às atividades dos membros do MPRS, além de buscar dados, informações e conhecimentos com o objetivo de atender às necessidades da *unidade de análise de dados e informações*; a estas, compete a produção de conhecimentos mediante a aplicação de metodologia própria, utilizando-se da análise dos dados e informações obtidas pela *unidade de operações* ou qualquer outra fonte, tornando-os utilizáveis para a tomada de decisões, o planejamento de operações e para o conhecimento de fatos úteis no desenvolvimento das atividades dos órgãos do MPRS, além de produzir relatórios das análises realizadas, dando ciência ao Nimp sobre os assuntos demandados e o conhecimento produzido. Destaca-se, ainda, neste contexto, a *unidade de inteligência de sinais* – com atribuições de análise técnica acerca de matéria correlata à área de Inteligência de Sinais; a *unidade de inteligência de imagens* – cujo escopo está voltado para produzir conhecimentos na área da inteligência de imagens e processar dados e informações referentes ao geoprocessamento e ao tratamento de imagens –, assim como a *unidade de tecnologia da*

(CSEG) e do Comitê de Controle de Atividade de Inteligência (Cint) (MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS. **Segurança e Inteligência**. Disponível em: https://gestaoestrategica.mpmg.mp.br/areas_tematicas/seguranca_inteligencia.html. Acesso em: 15 ago. 2022).

[109] RIO GRANDE DO SUL. Ministério Público do Estado do Rio Grande do Sul. **Provimento nº 68/2020 – PGJ – Revogado pelo Provimento nº 17/2022 – PGJ**. Disponível em: https://www.mprs.mp.br/legislacao/provimentos/14204/. Acesso em: 15 ago. 2022.

informação, responsável por tratar os dados e informações, viabilizando a sua análise pelas *unidades de análise de dados e informações*.[110]

Mesmo assim, pode-se dizer que o MPRS incorreu em prática atentatória à principiologia estabelecida pela Convenção de Budapeste e delineada no Anteprojeto da Comissão de Juristas para a elaboração da LGPD Penal no Brasil, justificando-se sob diversos aspectos, portanto, o reconhecimento da nulidade no ponto pelo Tribunal de Justiça do Estado do Rio Grande do Sul. Para além da ofensa ao princípio da paridade de armas, assim como reconhecido, por maioria, pelo TJRS, a licitude da própria atividade de tratamento de dados pessoais de jurados fica comprometida pela ocorrência de uma série de ilicitudes que encaminha à nulidades.

A primeira delas decorre da circunstânvcia de que o tratamento sobre a base de dados dos jurados não foi feito sobre nenhum fato específico. A atividade traduziu-se em flagrante pescaria probatória, de forma que importavam quaisquer dados que pudessem justificar alguma recusa. Eventual fato relevante obtido passaria a importar após a aquisição do dado, não antes, como exige o princípio.

Por outra perspectiva, também podemos apontar que o tratamento de dados pessoais dos jurados realizado pela acusação reside no terreno da ilicitude em decorrência do fato de que, em que pese anunciada, no caso concreto, uma série de reuniões prévias com os pretendentes a compor o Conselho de Sentença, em momento algum lhes foram asseguradas condições de tomar conhecimento de sua realização e obter da autoridade informações precisas sobre as circunstâncias da obtenção, as finalidades, qual seria o tipo de tratamento a que foram sujeitados, o que foi feito com o resultado do tratamento, se os resultados retroalimentariam novas pesquisas ou e se seriam cedidos ou comunicados a terceiros. E, tampouco, se o tratamento se limitou ao adequado e necessário para atingir os fins a que se destinava ou ao estritamente adequado e necessário para atingir os fins a que se destinava.

Sob essa perspectiva de análise, não é desarrazoado afirmar que o MPRS incorreu em prática atentatória à principiologia estabelecida pela Convenção de Budapeste e delineada no Anteprojeto da Comissão de Juristas para a elaboração da LGPD Penal no Brasil, justificando-se sob diversos aspectos, portanto, o reconhecimento da nulidade no ponto pelo TJRS. Para além da ofensa ao princípio da paridade de armas, assim como reconhecido pelo

[110] RIO GRANDE DO SUL. Ministério Público do Estado do Rio Grande do Sul. **Provimento nº 20/2010**. Dispõe sobre a reestruturação, a redefinição das atribuições e o funcionamento do Núcleo de Inteligência e a criação, as atribuições e o funcionamento do Laboratório de Tecnologia Contra a Lavagem de Dinheiro do Ministério Público do Estado do Rio Grande do Sul. Porto Alegre: Procuradoria-Geral de Justiça, 21 de maio de 2010. Disponível em: https://www.mprs.mp.br/legislacao/provimentos/5172/. Acesso em: 15 ago. 2022.

TJRS, a licitude da própria atividade de tratamento de dados pessoais de jurados fica comprometida: além de jurados não figurarem na categoria de titulares de dados que podem ter seu direito fundamental afastado para fins de segurança pública e persecução penal, ela ocorreu em violação a diversos dos princípios que sustentam as exceções à regra de proibição do tratamento de dados pessoais.

2.7. Direito ao Acesso

A proteção eficaz dos dados pessoais não apenas exige que sejam reforçados os direitos dos titulares dos dados e as obrigações de quem trata dados pessoais, mas que haja reforço dos poderes para controlar e assegurar a conformidade com as regras de proteção dos dados pessoais, razão pela qual a LGPD, a Convenção de Budapeste e o Anteprojeto da LGPD Penal no Brasil reforçam os direitos pessoais de acesso aos dados recolhidos que lhes digam respeito e de exercer esse direito com facilidade – as informações dirigidas aos titulares dos dados deverão ser de fácil acesso e compreensão e formuladas em termos claros e simples, adaptadas às necessidades das pessoas vulneráveis – e a intervalos razoáveis, a fim de tomar conhecimento do tratamento e verificar a sua licitude.

O uso cada vez mais frequente de computadores para o tratamento de informações pessoais inviabiliza considerar o cidadão como mero fornecedor de dados, sem que a ele caiba algum poder de controle. Atividades de coleta de informações não apenas tornam organizações públicas e privadas capazes de planejar e executar suas ações, como também viabiliza o surgimento de novas formas de concentração de poder ou de consolidação de outras já existentes. Surge, aí, a legítima reivindicação para que cidadãos possam exercer maior controle sobre aqueles que detêm a informação, o que lhes assegura um crescente *plus-poder*.

Ao prometer o acesso à informação, a internet surge como instrumento da democracia, dependendo apenas da boa vontade do governo para facilitar aos cidadãos o conhecimento de todos os registros públicos e informações não sigilosas: interagir é exercitar o direito de solicitar informações e respostas da máquina governamental. A discussão em torno do direito ao acesso ganhou o palco central a partir das problemáticas que envolvem a proteção de dados e a circulação de informações. O valor do embate pode ser extraído de duas afirmações do princípio que estão na origem de desdobramentos que interessam: (i) a *queda da impenetrabilidade das coletâneas de informações*, antes concentradas em mãos públicas e privadas, e (ii) a adoção de critérios de *controles exercidos diretamente pelos interessados*, e

não mais aqueles que decorrem do reconhecimento de uma posição formal de direito, cuja tutela era confiada a órgãos diferentes. O uso do instrumento direito ao acesso, porém, ainda é feito de forma muito modesta por seus interessados; uma crítica mais ácida ainda sustenta que se limitaria ao "direito de saber ter sido fichado", o que, em substância, significa defender que não confere nenhum real poder do indivíduo ao controle sobre informações coletadas.[111]

Pois, nesse viés, a atenção deve direcionar-se para a compreensão dos meios de reação individual a esses instrumentos de controle social e, nesse movimento, compreender que alguns desses meios de controle outrora disponíveis para o indivíduo possam ser perdidos, mas que igualmente podem ser (re)compensados pela criação de um novo aparato global de controle, mais vigilante e incisivo. A nova perspectiva do problema do controle não pode ficar limitada às fronteiras tradicionais: ela se dilata em dimensões coletivas, por intermédio do uso de instrumentos que ampliam a esfera individual e se destinam à compreensão de novas formas de autodisciplina corporativa, burocrática ou estatal. Significa a necessidade de avaliar a posição e o significado dessa nova infraestrutura para identificar a correta dimensão em que o problema do controle está inserido, até porque estamos diante questões que interessam a uma multiplicidade de sujeitos e empregam diversos meios que encaminham à compreensão de que todas as soluções devem ser tomadas em sentido coletivo[112]. Existe um enorme campo ainda inexplorado pelo advento das novas tecnologias, que está ligado a uma gama de riscos que podem surgir com o avanço que as programações políticas e institucionais ainda não foram capazes de acompanhar. A ineficiência dos aparatos da administração pública suplanta obstáculos que dificultam as conexões e integração de sistemas informativos que já se tornam possíveis com a tecnologia.

Há toda uma potencialidade implícita no exercício do direito ao acesso a ser desenvolvida, podendo o seu escasso uso ser atribuído a alguns obstáculos que ainda devem ser superados, como o seu completo desconhecimento, o elevado custo de acesso, o desnível de poder entre os indivíduos e detentores da informação (grandes burocracias públicas e privadas) e o excesso de proibições de acesso a determinados níveis de profundidade das informações. No processo penal brasileiro, some-se o estilo inquisitório[113] que orienta as

---

[111] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 66-67.
[112] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 36-38.
[113] CORDERO, Franco. **Procedimiento Penal**. Santa Fé de Bogotá: Editorial Themis, 2013. t. I. p. 19-90; PRADO, Geraldo. **Sistema Acusatório: a conformidade constitucional das Leis Processuais Penais**. 3 ed. Rio de Janeiro: Lumen Juris, 2005; COUTINHO, Jacinto Nelson de Miranda. Sistema acusatório: cada

políticas nesse campo. O reforço da posição dos indivíduos surge como pilar central a suportar as intervenções possíveis para condicionar o futuro do direito ao acesso, seja como forma de tornar mais eficiente o direito ao acesso, seja para ultrapassar o hiato de poder existente entre os sujeitos e os detentores do poder-saber.

Desequilíbrios entre a igualdade de partes e o direito de defesa não podem ser ignorados: é concreta a possibilidade de que uma das partes se valha desse recurso enquanto a outra, sem condições financeiras e materiais, não tenha o mesmo tipo de acesso. Aquele que emprega ferramentas baseadas em Inteligência Artificial será favorecido pela possibilidade de, com mais dados, produzir um maior número de cruzamentos, obtendo vantagens argumentativas em relação ao seu oponente. Pode ocorrer, ainda, que o direito de defesa acabe relativizado pelo não fornecimento de informações sobre os elementos constitutivos de determinado programa de Inteligência Artificial e seus algoritmos, causando prejuízo em razão do desconhecimento de como foi obtido determinado resultado ou predição. Para que sejam utilizadas como elemento de assistência à prova ou como meio de prova no processo, é impositivo que o uso de aplicações tecnológicas possa, em relação ao seu conteúdo, dados inseridos, automatização e configuração algorítmica ser explicado, conhecível e entendível pelos sujeitos do processo. Só assim estar-se-á respeitando o direito de defesa e o devido processo legal[114].

A compreensão de direito ao acesso prevalece sobre o âmbito do direito às informações pessoais, e suas disciplinas tendem a conjugar-se; o direito de acesso a determinadas categorias de informações concentradas em mãos públicas e privadas é mais elaborado e abrangente do que o simples direito a ser informado, uma versão menos ativa e dinâmica. Isso permite o desenvolvimento de relações institucionais e inovações tecnológicas que podem facilitar a generalização do direito ao acesso com a eliminação de obstáculos físicos que, em um passado não muito distante, inviabilizavam ou dificultavam o acesso à informação. O exercício efetivo do direito ao acesso às informações pessoais acaba por viabilizar o alcance a outra série de informações – acesso a documentos administrativos, de entidades públicas e privadas –, desdobramento que produz conflitos e incompatibilidades entre a tutela da privacidade – que restringe a circulação de determinados tipos de

---

parte no lugar constitucionalmente demarcado. *In* **Revista de Informação Legislativa**. Brasília. a. 46 n. 183 julho./set. 2009, p. 103-115.

[114] DIZ, Fernando Martín. Justicia Predictiva: inteligencia artificial y algoritmos aplicados al proceso judicial en materia probatoria. *In*: DE MATA, Frederico Bueno. **El Impacto de las Nuevas Tecnologías Disruptivas en el Derecho Procesal**. Thomson Reuters Aranzadi, 2022. p. 152-153.

informações – e o direito ao acesso à informação, já que apresentam, em um primeiro momento, finalidades entre si inconciliáveis. Em campos diversos se desenvolvem técnicas que buscam compor todos os interesses relacionados às tutelas da privacidade e do acesso à informação. Buscam-se estabelecer critérios capazes de equilibrar os interesses em conflito, havendo de ser relacionados em um conjunto de regras gerais resultantes da conjugação de diversos princípios entre si.[115]

Pessoas têm o direito de acessar – e de exercer esse direito com facilidade – os dados que lhes digam respeito para tomar conhecimento do tratamento, verificar a sua licitude, ser informadas das finalidades a que se destina, a duração e quem são os destinatários, inclusive no caso de outros países. Também, o direito a que os dados inexatos sejam *retificados* – o direito de retificação não deverá afetar o conteúdo do depoimento de uma testemunha –, em especial no que diz respeito a fatos que sejam apagados em caso de tratamento em desconformidade. É direito da pessoa que o tratamento seja limitado sempre que conteste a exatidão dos dados pessoais e não possa ser apurado se os dados são exatos ou não ou, ainda, quando os dados pessoais tiverem de ser conservados para efeitos de prova.

A Convenção de Budapeste indica a previsão de regras para facilitar o exercício, pelo titular dos dados, dos direitos que lhe são conferidos, incluindo procedimentos para solicitar, a título gratuito, o acesso aos seus dados pessoais, a retificação e o apagamento dos dados pessoais e a limitação do tratamento. Trata-se de pedidos formulados pelo titular dos dados, sobre os quais o responsável pelo tratamento deverá ser obrigado a responder sem demora injustificada, salvo em casos de limitações aos direitos de acesso.

A partir disso, seria possível desenhar um Sistema de Proteção de Dados Pessoais no Processo Penal – baseado em reconhecimento de direitos aos titulares; procedimentos para exercícios de ditos direitos; a existência de uma autoridade de controle e supervisão de arquivos judiciais e do Ministério Público – e de Princípios de Tratamento de Dados Aplicáveis ao Processo Penal, licitude e lealdade, limitação da finalidade, minimização, exatidão, limitação do prazo de conservação, integridade e confidencialidade, responsabilidade, proteção de dados por defeito e desde o desenho –, categorizando Dados Especialmente Sensíveis e dispondo sobre o Tratamento de Dados relacionados a

[115] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 67-71.

condenações e infrações penais, atribuindo relevância à figura do Delegado de Proteção de Dados e distinguindo os Interessados na Tutela dos Dados em processo penal.[116]

Quanto aos dados contidos em arquivos judiciais no processo penal regulados pela Diretiva 2016/680, esta reconhece – ainda que possa ser limitado pelo Estado por medidas legais que os restrinjam total ou parcialmente – o direito a obter confirmação sobre a ocorrência de tratamentos de seus dados e, em caso positivo, ao acesso aos dados e determinadas informações; o direito à retificação ou supressão de dados pessoais e a limitação de seu tratamento, criando obrigações de informação ao responsável pelo tratamento e estabelece direitos relacionados às decisões individuais não unicamente automatizadas.[117] Para a Diretiva, é obrigação dos Estados-membros regular tais procedimentos em seus ordenamentos internos, a teor do que estipula o Considerando 49 – ao estabelecer que o exercício de tais direitos em uma investigação criminal ou processo penal dar-se-á em conformidade com o Direito Processual nacional[118] – e o Considerando 107 – que atribui a regulação do exercício de direitos dos interessados em matéria de informação, acesso, retificação, supervisão e limitação de tratamento relacionados aos dados pessoais, assim como das restrições a tais direitos no marco do processo penal de cada Estado[119-120].

Cabe ao responsável pelo tratamento – observando a natureza, o âmbito, o contexto e as finalidades do tratamento de dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares – executar medidas adequadas, eficazes e estar em

---

[116] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 454-466.

[117] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 454-455.

[118] "Caso os dados pessoais sejam tratados no âmbito de uma investigação criminal ou de um processo judicial em matéria penal, os Estados-Membros deverão poder dispor que o exercício do direito à informação, ao acesso aos dados pessoais e à sua retificação ou apagamento, bem como à limitação do tratamento, seja feito nos termos das regras nacionais aplicáveis aos processos judiciais" (UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**: p. L 119/89-L 119/131, 4.5.2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri= CELEX:32016L0680. Acesso em: 11 abr. 2022).

[119] "A presente diretiva não obsta a que os Estados-Membros possam aplicar disposições respeitantes ao exercício dos direitos dos titulares de dados em matéria de informação, de acesso e de retificação ou apagamento dos dados pessoais e de limitação do tratamento no âmbito de uma ação penal, bem como eventuais restrições desses direitos, na legislação processual penal nacional" (UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**: p. L 119/89-L 119/131, 4.5.2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri= CELEX:32016L0680. Acesso em: 11 abr. 2022).

[120] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 456.

condições de demonstrar que o tratamento de dados se encontra em conformidade, o que inclui a elaboração e a execução de garantias específicas para o tratamento de dados pessoais de pessoas singulares vulneráveis, como crianças. Para isso, é imprescindível, desde a coleta, a alteração, a consulta, a divulgação até a ocorrência de transferências, como interconexão ou apagamento, a manutenção dos registros cronológicos de todas as categorias de atividades de tratamento realizadas sob sua responsabilidade. Para que se possa determinar a justificação e verificar a licitude do tratamento de dados pessoais, também devem ser mantidos registros sobre quem consultou ou divulgou dados pessoais, de forma a promover autocontrole, garantir a integridade e a segurança dos dados e ações penais.

Ao assegurar a titularidade de dados pessoais e garantir direitos fundamentais da liberdade, intimidade e privacidade aos titulares dos dados, o Anteprojeto para a LGPD Penal brasileira também garante o direito de obter junto ao controlador em relação aos dados por ele tratados, mediante requerimento expresso ou de representante legalmente constituído: (i) a confirmação da existência de tratamento; (ii) o acesso aos dados; (iii) a correção de dados incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei; (v) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, assim como também garante ao titular o direito de peticionar em relação aos seus dados contra o controlador perante o Conselho Nacional de Justiça ou em juízo, quando cabível *habeas data*. Em caso de impossibilidade de adoção imediata da providência, o controlador enviará ao titular resposta em que ou poderá comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente, ou indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

Nos casos em que a prestação de informações puder causar prejuízo para investigações, inquéritos ou processos judiciais, para a prevenção, detecção, investigação ou repressão de infrações penais ou para a execução de sanções penais, à proteção da segurança do Estado ou à defesa nacional, ou a proteção de direitos e garantias de terceiros, a lei prevê que a prestação de informações e a concessão e o acesso a dados pode ser adiada, limitada ou recusada se e enquanto tal for necessário e proporcional, cabendo ao responsável pelo tratamento informar ao titular dos dados, por escrito e sem demora, os motivos que levaram à recusa ou da limitação do acesso, indicando quando cessarão os motivos apontados na justificativa. Essa comunicação pode ser omitida apenas quando sua prestação puder prejudicar qualquer uma das finalidades, informado-se o titular dos dados a possibilidade de

levar o pedido ao Conselho Nacional de Justiça ou de intentar ação judicial, oportunidade em que o controlador deverá disponibilizar ao CNJ informação sobre a omissão de informação ao titular dos dados e os motivos de fato e de direito que fundamentaram a recusa ou a limitação do direito de acesso.

Já a confirmação de existência ou o acesso a dados pessoais serão providenciados em formato simplificado ou declaração clara e completa, fornecida, salvo exceções previstas, no prazo de até 15 (quinze) dias, contado da data do requerimento do titular, indicando a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comerciais e industriais. Esses dados deverão ser armazenados em formato que favoreça o exercício do direito de acesso, podendo ser fornecidos por meio de documento eletrônico, desde que inteligível, seguro e idôneo.

A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

O direito de acesso à informação e à transparência impõem às autoridades competentes o dever de informar as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre: (i) a base legal; (ii) a finalidade; (iii) os objetivos específicos; (iv) os procedimentos; (v) as práticas utilizadas para a execução dessas atividades. Esse acesso deve se dar em veículos de fácil acesso, preferencialmente em sítios eletrônicos, de forma clara, adequada e ostensiva, incluindo informações para o atendimento do princípio do livre acesso sobre: (i) a finalidade específica do tratamento; (ii) a forma, escopo e duração do tratamento; (iii) as políticas de retenção, descarte e acesso; (iv) a identificação do controlador; (v) informações de contato do controlador; (vi) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; (v) responsabilidades dos agentes que realizarão o tratamento; (vi) direitos do titular, com menção explícita aos direitos contidos em Lei.

Assim, pode-se dizer que o direito ao acesso se efetiva no momento em que o titular dos dados esteja na posse de um resumo completo por via de uma cópia dos dados pessoais sujeitos a tratamento num formulário, que lhe permita tomar conhecimento desses e verificar sua exatidão e o seu tratamento em conformidade com diretiva, de modo que possa exercer os direitos que esta lhe confere. Entretanto, ainda que importantes obrigações sejam oponíveis ao responsável pelo tratamento dos dados pessoais (art. 13 da Diretiva 2016/680)[121], podem ter

[121] "Art. 13. Informações a facultar ou a fornecer ao titular dos dados 1. Os Estados-Membros preveem que o responsável pelo tratamento faculte ao titular dos dados pelo menos as seguintes informações: a) A identidade e

sua aplicação suspensa para evitar a obstaculização de questionamentos, investigações e procedimentos oficiais ou a propositura de medidas para reprimir infrações penais ou a execução de sanções, proteger a segurança pública, a segurança nacional e os direitos e liberdade de outras pessoas.[122]

Os Estados-membros deverão poder adotar medidas legislativas que visem a atrasar, limitar ou recusar a informação prestada a titulares de dados ou a restringir, total ou parcialmente, o acesso aos dados pessoais que lhes digam respeito, desde que tal constitua uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos da pessoa singular em causa para não prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou legais, procurar não prejudicar a prevenção, a investigação, a detecção e a repressão de infrações penais ou a execução de sanções penais, salvaguardar a segurança pública ou a segurança nacional ou, ainda, proteger os direitos e as liberdades de terceiros. O responsável pelo tratamento deverá avaliar, através de uma análise concreta de cada caso individualmente, se o direito de acesso deverá ser total ou parcialmente restringido. As recusas ou restrições do acesso deverão, em princípio, ser comunicadas por escrito ao titular dos dados com os motivos de fato ou de direito que fundamentam a decisão.

---

os contactos do responsável pelo tratamento; b) Os contactos do encarregado da proteção de dados, se for caso disso; c) As finalidades do tratamento a que os dados pessoais se destinam; d) O direito de apresentar reclamação à autoridade de controlo e de obter os contactos dessa autoridade; e) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que dizem respeito ao titular, bem como a sua retificação ou o seu apagamento e a limitação do tratamento. 2. Para além das informações a que se refere o n.o 1, os Estados-Membros preveem por lei que o responsável pelo tratamento forneça ao titular dos dados, em determinados casos, as seguintes informações adicionais, a fim de lhe permitir exercer os seus direitos: a) O fundamento jurídico do tratamento; b) O prazo de conservação dos dados pessoais ou, se tal não for possível, os critérios usados para definir esse período; c) Se aplicável, as categorias de destinatários dos dados pessoais, inclusive nos países terceiros ou nas organizações internacionais; d) Se for caso disso, informações adicionais, especialmente se os dados pessoais forem recolhidos sem conhecimento do seu titular. 3. Os Estados-Membros podem adotar medidas legislativas que prevejam o adiamento, a limitação ou a não prestação aos titulares dos dados das informações a que se refere o n.o 2 se e enquanto tais medidas constituírem medidas necessárias e proporcionadas numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de: a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais; b) Evitar prejudicar a prevenção, detecção, investigação ou repressão de infrações penais ou a execução de sanções penais; c) Proteger a segurança pública; d) Proteger a segurança nacional; e) Proteger os direitos e as liberdades de terceiros. 4. Os Estados-Membros podem adotar medidas legislativas a fim de determinar as categorias de tratamento suscetíveis de ser abrangidas, total ou parcialmente, por uma das alíneas do nº 3" (UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**: p. L 119/89-L 119/131, 4.5.2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri= CELEX:32016L0680. Acesso em: 11 abr. 2022).

[122] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 458-459.

Registre-se que, de forma a assegurar o dever de *accountability*, a autoridade máxima de cada autoridade competente para o tratamento de dados pessoais publicará anualmente em seu sítio relatórios estatísticos de requisição de dados pessoais sigilosos para atividades de persecução penal, fazendo constar: (i) o número de pedidos realizados; (ii) a natureza dos dados solicitados; (iii) as categorias de pessoas jurídicas de direito privado aos quais os dados foram requeridos; (iv) quando o dado for protegido por reserva de jurisdição, o número de pedidos deferidos e o número de pedidos indeferidos judicialmente à luz dos pedidos totais realizados; (v) o número de titulares afetados por tais solicitações.

2.8. A autoridade de controle

Parte importante desse sistema é a *autoridade de controle*, a quem, com a missão de assegurar o respeito aos direitos e liberdades relacionados ao direito fundamental à proteção de dados pessoais e facilitar a livre circulação de dados, é atribuída a responsabilidade de supervisionar a aplicação da Diretiva 2016/680. Os responsáveis pelo tratamento dos dados são obrigados a cooperar com a autoridade de controle e a facultar-lhe os registros, a pedido, para fiscalização de operações de tratamento. Trata-se de órgão de supervisão independente, voltado a assegurar o cumprimento das normas relacionadas a dados pessoais por órgãos jurisdicionais e autoridades independentes, a exemplo do Ministério Público.[123]

A propósito, os considerandos 20 e 97 da Diretiva estabelecem a condição de autoridade judicial independente ao Ministério Público, em razão da natureza e das funções constitucionais a ele atribuídas, o que lhe assegura o tratamento de dados pessoais.[124] Na

[123] "Embora a presente diretiva se aplique também às atividades dos tribunais nacionais e outras autoridades judiciais, a competência das autoridades de controlo não deverá abranger o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência dos juízes no desempenho das suas funções jurisdicionais. Esta exceção deverá ser estritamente limitada às atividades judiciais relativas a processos judiciais, não se aplicando a outras atividades a que os juízes possam estar associados por força do direito do Estado-Membro. Os Estados-Membros podem também prever a possibilidade de a competência das autoridades de controlo não abranger o tratamento de dados pessoais efetuado por outras autoridades judiciais independentes no exercício da sua função jurisdicional, nomeadamente o Ministério Público. Em todo o caso, o cumprimento das regras da presente diretiva pelos tribunais e outras autoridades judiciais independentes deverá ficar sempre sujeito a uma fiscalização independente nos termos do artigo 8º, nº 3, da Carta (UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**: p. L 119/89-L 119/131, 4.5.2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 11 abr. 2022).

[124] "(20) A presente diretiva não obsta a que os Estados-Membros especifiquem as operações e os procedimentos de tratamento na legislação processual penal nacional no que se refere ao tratamento de dados pessoais pelos

Espanha, por exemplo, a Instrução nº 2/2019 regulamenta o tratamento de dados pelo Ministério Público no exercício de sua função jurisdicional no âmbito penal, distinguindo em três categorias os tipos de atuação: com fins de servir à investigação, prisão ou acusação; com fins de promoção de diligências de investigação ou na tramitação de representação por atos infracionais.

Mas e quem exerce a autoridade de controle no Ministério Público? A Instrução nº 2/2019 contempla a possibilidade de criação de um organismo específico dentro da própria instituição para que assuma essa função. A Diretiva 2016/680 propõe que a competência das autoridades de controle não deverá abranger o tratamento de dados pessoais efetuado pelos Tribunais no exercício da sua função jurisdicional e que Estados-membros podem prever a possibilidade de a competência das autoridades de controle não abranger o tratamento de dados pessoais efetuado por outras autoridades judiciais independentes no exercício da sua função jurisdicional, nomeadamente o Ministério Público. Ao fim e ao cabo, é o ordenamento jurídico interno que deverá dispor quais operações de tratamento ficarão submetidas às autoridades de controle ou, ainda, adotar outra solução. Na Espanha, a Instrução nº 2/2019 também cria o Delegado de Proteção de Dados (DPD) do Ministério Público, sujeito que exercerá suas funções com suporte em uma rede de delegados adjuntos, hierarquicamente postos.[125]

Traduz-se no direito de o titular dos dados não se confortar com uma decisão que avalie aspectos que lhe digam respeito baseada em tratamento automatizado e cujos efeitos lhe sejam adversos ou o afetem de forma significativa, de forma que a atividade deve revestir-se de garantias adequadas através de: (i) informação específica; (ii) direito de obter a intervenção humana; (iii) manifestar o seu ponto de vista; (iv) obter uma explicação sobre a decisão tomada na sequência dessa avaliação ou (v) contestar a decisão.

---

tribunais e as outras autoridades judiciais, em particular no que respeita aos dados pessoais que constem de uma decisão judicial ou de um registo relacionado com uma ação penal.
[...]
(97) A presente diretiva não prejudica as disposições relativas à luta contra o abuso sexual, a exploração sexual de crianças e a pornografia infantil, previstas na Diretiva 2011/93/UE do Parlamento Europeu e do Conselho" (UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**: p. L 119/89-L 119/131, 4.5.2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 11 abr. 2022).

[125] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 445.

Em se tratando de pedidos manifestamente infundados ou excessivos, como solicitar informações de forma injustificada e repetida ou abusar do direito a receber informações, o responsável pelo tratamento poderá cobrar uma taxa ou recusar dar seguimento ao pedido. Ainda, informações como (i) a identidade do responsável pelo tratamento, (ii) a existência da operação de tratamento, (iii) as finalidades do tratamento, (iv) o direito de apresentar reclamação e (v) o direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais e sua retificação ou apagamento ou a limitação do tratamento deverão ser facultadas ao titular dos dados, as quais poderão ser disponibilizadas pelo sítio *web* da autoridade competente.

Em caso de recusa ao titular dos dados do direito à informação, ao acesso aos dados pessoais ou à retificação, ao apagamento ou à limitação do tratamento, a ele é reconhecido o direito de solicitar que a autoridade nacional de controle verifique sua licitude. Assim, agindo em nome do titular dos dados, deverá prestar informações sobre a realização das verificações ou revisões necessárias, assim como informar ao titular dos dados o direito de intentar ação judicial. Em caso de tratamento de dados pessoais em investigação criminal ou processo judicial em matéria penal, orienta-se que o exercício do direito à informação, ao acesso aos dados pessoais e à sua retificação ou ao seu apagamento, bem como à limitação do tratamento, seja realizado nos termos das regras nacionais aplicáveis aos processos judiciais.

O responsável pelo tratamento de dados pode designar, ainda, um *encarregado de proteção de dados* – sujeito previsto na Secção 3 da Diretiva 2016/680 e cujas atribuições incluem informar e aconselhar os empregados e o responsável pelo tratamento dos dados que efetuem o tratamento quanto às obrigações que lhes incumbem; fiscalizar a conformidade com a diretiva e outras normas sobre proteção de dados e com as políticas do responsável pelo tratamento de dados em matéria de proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e a formação do pessoal implicado nas operações de tratamento de dados e as auditorias correspondentes; cooperar com a autoridade de controle, funcionar como ponto de contato com a autoridade de controle em assuntos relacionados com o tratamento[126]. Em geral, não se trata de pessoa alheia à organização em que opera o

[126] UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**: p. L 119/89-L 119/131, 4.5.2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 11 abr. 2022.

responsável pelo tratamento, mas sim alguém que pertença à própria, com dedicação exclusiva ou parcial[127].

[127] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 464-465.

3. TRATAMENTO DE DADOS ABERTOS E PERSECUÇÃO PENAL

3.1. Tratamento de dados abertos

Tecnologias de informação e comunicação geram cada vez mais dados, mais precisos e em maior quantidade: pagamentos de cartão de crédito, conexões em redes *wi-fi*, compartilhamento de localizações ou marcação de amigos em fotos – as quais geram metadados com outras inúmeras informações –, *likes* em suas atividades de interesse, câmeras privadas filmando espaços públicos e outras infinitas possibilidades. Todos esses dados representam valor comercial e estão sendo cada vez mais buscados; "rastros" deixados pelo uso das tecnologias da informação são cada vez mais explorados.[128]

O que antes era terreno de um número reduzido de indivíduos com tempo ocioso e hábitos obsessivos de internet, agora está informando a pesquisa e o jornalismo em uma ampla gama de campos e instituições, inclusive para práticos do Direito. De acordo com um artigo publicado pela revista *The Economist*, pesquisas de código aberto "atingiram a maioridade"[129], sendo crescente a possibilidade de que a disponibilização de informações permita o exercício dos poderes de controle por indivíduos e grupos, o que também concorre para um maior equilíbrio sociopolítico. Essa tendência realista considera as novas formas de coleta e tratamento de informações permitidas pelo acesso crescente aos dispositivos eletrônicos de armazenamento – cada vez mais intuitivos, menores em tamanho e maiores em capacidade – e o aumento da gestão de dados por parte de instituições públicas e privadas, causando transformações irreversíveis na distribuição e no uso do poder. Identificar onde estão concentrados a disponibilidade e o domínio da informação para que sejam utilizados como instrumento de poder permite a projeção de formas de contrapoder e de controle, tendo nas possibilidades oferecidas pela tecnologia uma importante aliada na produção de novas formas de gestão do poder, que ofereçam novas capacidades e possibilidades de expansão. Mesmo diante de um cenário de afronta os direitos e as garantias fundamentais pelo advento do uso abusivo das tecnologias em processos decisórios, nada impede que sejam estabelecidas novas estratégias que recorram ao uso da tecnologia da informação para um controle social maior sobre os participantes do processo e que, ainda assim, lhes assegurem maior

[128] CNIL – Comission Nationale de l'informatique e des Libertés. **Dados Pessoais:** definição. Disponível em: https://www.cnil.fr/en/personal-data-definition. Acesso em: 11 abr. 2022.
[129] THE people's panopticon: Open-source intelligence comes of age. **The Economist – edição semanal**, [*S. l.*], agosto 2021. Disponível em: https://www.economist.com/weeklyedition/2021-08-07. Acesso em: 11 abr. 2022.

participação[130].

Há de se diferenciar quais os tipos de atividades desenvolvidas pelos usuários da internet para poder aplicar, de forma adequada, garantias constitucionais. Como princípio geral, quaisquer tipos de dados difundidos pelos usuários na internet têm caráter público, sendo presumido seu consentimento tácito a partir de publicações de conteúdo por intermédio da rede mundial de computadores, o que exclui a possibilidade de incidência do direito à intimidade. A inserção de conteúdo na internet por meio de canais abertos proporciona que os dados sejam acessados por qualquer usuário, inclusive permitindo, sem restrições, a busca de provas eletrônicas pela investigação, sem que afete direitos fundamentais. Atividades como *ciberpatrulha* (destinadas à prevenção de delitos a partir de atividades de vigilância do fluxo de usuários na rede) ou análise de fontes abertas (dirigidas à busca de informações inseridas na *web* e que contribuam à elucidação de ilícitos já cometidos) são muito comuns e estão a serviço dos órgãos de investigação de forma irrestrita, sem que haja violação das garantias fundamentais[131].

Os dados manifestamente tornados públicos pelo titular ganham especial relevo. Informações pessoais, expressões online de sentimento pessoal, fotografias de lugares e acontecimentos locais inundam as redes, pessoais e profissionais, de formas nunca antes imaginadas. O poder computacional e o desenvolvimento de técnicas e ferramentas baseadas na Ciência dos Dados passaram a municiar qualquer um que tenha um letramento computacional mínimo para processar quantidades maciças desses dados e, por isso, encontram valor em termos de inteligência.[132]

A categoria *fontes abertas* está, pois, relacionada aos dados que podem ser encontrados livremente, à disposição do público (acesso público) e sem limites geográficos. Nelas, podem ser encontradas informações de interesse à investigação (públicas e privadas) de qualquer tipo de ilícito – delito ou não –, as quais poderão ser objeto de processamento e análise para localizar novos dados em busca de outros elementos de constatação, a chamada *inteligência de fontes abertas*. No contexto tecnológico, trata-se de métodos baseados em técnicas de investigações na *web* e em redes sociais, o qual permite colecionar um volume de dados sobre as pessoas, que cada vez mais realizam todos os tipos de atos jurídicos por

---

[130] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 24-25.
[131] DELGADO MARTÍN, Joaquín. **Investigación tecnológica y prueba digital en todas las jurisdicciones.** Madrid: España, 2018. p. 105-107.
[132] WILLIANS. Heather J; BLUM, Ilana. **Defining second generation Open Source Intelligence (OSINT) for the Defense Enterprise**. National Defense Research Institute. Santa Mônica: RAND Corporation, 2018. p. 1.

intermédio de comunicações e relacionamentos que impactam em todas as esferas de sua vida – pessoal, familiar, econômica, financeira ou social.

O Convênio contra a Ciberdeliquência, instrumento voltado à aplicação de uma política penal comum com o objetivo de proteção da sociedade ante a ciberdeliquencia, dispõe sobre *fonte aberta* em seu art. 32.a, dispositivo que estabelece o acesso a dados com consentimento ou quando estejam acessíveis ao público e, nesse sentido, que uma parte poderá, sem a autorização da outra, ter acesso a dados informáticos armazenados acessíveis ao público, independente de sua localização geográfica[133].

A *Carta Ética Europea para el uso de inteligencia judicial en sistemas judiciales*[134] estabelece a noção de dados abertos esclarecendo, em primeiro lugar, sobre a confusão entre o acesso à informação e o acesso à informação sob a forma de base de dados. Para o Conselho Europeu, *dados* são *letras e números sem sentido* e *informações* são *dados incluídos num contexto* que os confere sentido, o que leva à conclusão de que dados abertos são *informação.* Também não devem ser confundidos com os seus meios de processamento ou métodos de tratamento, definidos como Ciência dos Dados, ou com a utilização de Inteligência Artificial, motores de busca avançada e robôs legais, que apenas são *aplicações algorítmicas alimentadas com dados*, em nada se relacionando com a política de dados abertos.

Ativista dos dados abertos, especialista e palestrante de políticas públicas na *Harvard Kennedy School of Government*, o professor David Eaves propôs a criação das denominadas três "leis" dos dados abertos, um conjunto de testes para avaliar se um dado pode ser considerado aberto: (i) se o dado não pode ser encontrado e indexado na *web*, ele não existe; (ii) se não estiver aberto e disponível em formato compreensível por máquina, não pode ser reaproveitado; (iii) se algum dispositivo legal não permitir sua replicação, ele não é útil. Inicialmente projetado para dados abertos governamentais, esse conjunto de orientações hoje também se aplica aos dados abertos de forma geral, mesmo fora de ambientes governamentais, como em empresas privadas, organizações da sociedade civil e organismos internacionais[135].

---

[133] COUNCIL OF EUROPE. Convenio sobre la ciberdelincuencia. **Serie de Tratados Europeos**, Budapeste, n. 185, 23.XI.2001. Disponível em: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf. Acesso em: 5 abr. 2022.

[134] COMISSÃO EUROPEIA PARA A EFICÁCIA DA JUSTIÇA (Cepej). Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente - adoptada pela CEPEJ na sua 31.ª reunião plenária: Estrasburgo, 3 e 4 de dezembro de 2018. Disponível em: https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0. Acesso em: 5 abr. 2022.

[135] BRASIL. Portal Brasileiro de Dados Abertos. **O que são dados abertos?** Disponível em: https://dados.gov.br/pagina/dados-abertos. Acesso em: 8 abr. 2022.

3.2. Dados governamentais abertos

Dados governamentais em formato aberto são aqueles que, segundo a definição da *Open Knowledge Internacional*[136], qualquer pessoa pode livremente acessá-los, utilizá-los, modificá-los e compartilhá-los para qualquer finalidade, estando sujeitos a, no máximo, exigências que visem a preservar sua proveniência e sua abertura, sendo, desde o final dos anos 2000, disponibilizados por meio de portais de dados abertos, o que contribuiu significativamente para transparência, participação, inovação e geração de valor econômico. Especialistas têm investido na criação de uma nova forma de colaboração, em que participantes de diversos setores trocam seus dados com escopo na criação de valor público de forma a fornecer melhores: (i) consciência situacional e resposta; (ii) projeto e entrega de serviço público; (iii) criação e transferência de conhecimento; (iv) predição e previsões; (v) avaliação e avaliação de impacto[137] – e a disponibilização de bases de dados estruturadas para *download* público apresenta-se como ferramenta essencial.

Estudo publicado[138] sobre estratégias adotadas por Estados Unidos, Reino Unido, Espanha, Dinamarca e Austrália para abertura de dados abertos destacou três propósitos centrais na adoção dessa política: (i) aumentar controle social e fomentar participação política: ideia associada à publicação de dados do governo para capacitar cidadãos a exercerem seus direitos; (ii) promover o serviço e a inovação de produtos: novas oportunidades de inovação geradas por dados governamentais abertos; (iii) fortalecer a aplicação da lei: envolvimento dos cidadãos e fortalecer a aplicação da lei e a segurança[139].

Esse é propósito declarado do Open Government Partnership (OGP), organização não governamental que reúne cerca de 70 Estados-membros (incluindo do Conselho da Europa) com representantes da sociedade civil e gigantes digitais, imbuída no sentido de melhorar a

---

[136] OPEN KNOWLEDGE FOUNDATION. Disponível em: https://okfn.org/. Acesso em: 8 abr. 2022.
[137] GOVLAB. Disponível em: https://datacollaboratives.org/introduction.html#section7/7d. Acesso em: 8 abr. 2022.
[138] HUIJBOOM, Noor; VAN DEN BROECK. Tijs. **Open data**: An international comparison of strategies. 2011. Disponível em: https://www.researchgate.net/publication/285735704_Open_data_An_international_comparison_of_strategies. Acesso em: 20 abr. 2022.
[139] "A estratégia britânica propõe fortalecer o papel da sociedade civil, a inovação governamental, mas também promover negócios e empreendedorismo com os dados governamentais, linha também adotada pela Dinamarca; ainda no mesmo sentido, a Espanha, apenas com diferença de propor como elementos centrais o fortalecimento da democracia e da 'sociedade do conhecimento'; a estratégia americana, lançada como primeiro ato do governo Obama através do 'Open Government Memorandum and Plan', propõe, além da transparência e abertura governamental, promoção da eficiência e efetividade no governo" (CRAVEIRO, Gisele da Silva; MACHADO, Jorge A. S.; SOLETTO; Juliana Strumiello. Um balanço da demanda de dados abertos no Brasil. **Revista Internet & Sociedade**, v. 1, n. 2, p. 273-296, dez. 2020. Disponível em: https://revista.internetlab.org.br/um-balanco-da-demanda-de-dados-abertos-no-brasil/. Acesso em: 3 jan. 2022).

transparência das atividades públicas, incentivar os cidadãos na elaboração e avaliação das políticas públicas e garantir a integridade do serviço público e de quem o executa através do tratamento de quantidades consideráveis de informação, organizadas em *big data*[140]. O Brasil foi um dos fundadores e o primeiro co-presidente da OGP como postulante à liderança da parceria, mas que ainda não tinha em vigor uma legislação de acesso à informação pública.

Políticas públicas voltadas ao governo aberto não se limitam à transparência passiva, mas também ativa: avanços tecnológicos, massificação do acesso e movimentos da sociedade demandam por flexibilidade na divulgação das informações públicas, viabilizando melhor *accountability*, mas ainda existe pouca literatura acadêmica sobre a demanda por dados governamentais abertos no Brasil, sendo relevante qualquer contribuição no debate sobre a interação dos movimentos dos dados governamentais abertos e Direito à Informação no país: em razão de suas conhecidas desigualdades, *déficits* no serviço público, índices elevados de corrupção, baixa participação social, além de um ambiente político-institucional instável, ainda se demanda uma política de dados abertos fortificadora da democracia e da cidadania.

Produto da coalizão de entidades da sociedade civil, organizações de mídia e pesquisadores, o Fórum de Direito de Acesso a Informações Públicas, que atua desde 2003 por iniciativa da Associação Brasileira de Jornalismo Investigativo (Abraji), é uma organização sem conotação político-partidária nem fins lucrativos e que teve participação decisiva no exercício do controle social para a implementação de acesso à informação. Criado com o objetivo de agregar organizações da sociedade civil e pressionar governo e sociedade pela regulamentação do direito de acesso à informação pública previsto em 1988, o Fórum também se dedica a que governos mantenham sistemas de gerenciamento e preservação de documentos públicos de forma a facilitar o seu acesso futuro, na medida em que documentos e informações produzidas por agentes públicos, governantes ou políticos não pertencem a ele nem ao Estado, mas ao cidadão. Seus objetivos e princípios estão orientados para: a (i) promoção e incentivo do debate sobre o direito de acesso a informações públicas no Brasil e temas correlatos, como a LGPD, legislações sobre dados abertos e sobre gestão e manutenção de registros públicos; (ii) defender a Lei de Acesso a Informações Públicas e sua preservação como instrumento legal que garanta e facilite o acesso do público no Brasil a documentos públicos produzidos pelos Três Poderes da República, bem como aos documentos de governos estaduais e municipais; (iii) orientar os órgãos públicos para que tenham a

[140] OPEN GOVERNMENT PARTNERSHIP. **Europe Regional Meeting** – october, 11-12, 2022. Disponível em: https://www.opengovpartnership.org/. Acesso em: 11 abr. 2022.

preocupação de arquivar documentos públicos de forma a facilitar acesso futuro, bem como de manter sistemas permanentes para seus gerenciamento e preservação; (iv) desenvolver atividades voltadas para a divulgação a respeito do direito de acesso a informações públicas e da Lei de Acesso a Informações Públicas[141].

A Open Knowledge Brasil (OKBR), Rede pelo Conhecimento Livre, é o capítulo da Open Knowledge International, uma organização da sociedade civil sem fins lucrativos e apartidária, baseada na utilização e no desenvolvimento de ferramentas cívicas, elaboração de projetos, análises de políticas públicas, jornalismo de dados e promoção do conhecimento livre, *online* e *offline*, nos diversos campos da sociedade e aptos a gerar benefícios sociais. A partir do momento em que reconhece a pluralidade de fontes de dados sendo acessadas por diferentes atores e com diferentes usos e implicações, defende o uso responsável e ético dos dados, atuando para levantar discussões e questionamentos sobre os limites no uso de dados e como a privacidade e a vigilância são consideradas em diferentes contextos.[142]

Na Califórnia, um grupo de trabalho de 30 pessoas reuniu-se em 2007 para definir os Princípios dos Dados Abertos Governamentais, além de afirmar que a conformidade com os princípios precisa ser verificável e uma pessoa deve ser designada como contato responsável pelos dados de forma a assegurar que sejam: (i) *completos*: dados públicos são disponibilizados, não sujeitos a limitações válidas de privacidade, segurança, controle de acesso ou reguladas por estatutos; (ii) *primários*: dados deverão ser publicados conforme coletados na fonte, com fina granularidade, e não de forma agregada ou transformada; (iii) *atuais*: devem ser disponibilizados na velocidade necessária para preservar o seu valor; (iv) *acessíveis*: disponibilizados ao mais amplo público possível e para os mais variados propósitos; (v) *processáveis por máquina*: dados são razoavelmente estruturados para possibilitar o seu processamento automatizado; (vi) *acesso não discriminatório*: disponíveis a todos, sem exigência de identificação ou registro; (vii) *formatos não proprietários:* disponibilizados em formato sobre o qual nenhum ente tenha controle exclusivo; (viii) *licenças livres:* não sujeitos a restrições por regulações de direitos autorais, marcas, patentes ou segredo industrial, ainda que se permitam restrições razoáveis de privacidade, segurança e controle de acesso desde que regulada por estatutos.[143]

---

[141] PROPOSTA de corte de 58% no orçamento do DataSUS compromete direito à saúde, à informação e à proteção de dados, alerta Fórum. Fórum de Direito de Acesso a Informações Públicas. Disponível em: https://informacaopublica.org.br/. Acesso em: 21 dez. 2021.

[142] OPEN KNOWLEDGE BRASIL. Disponível em: https://ok.org.br/sobre/. Acesso em: 21 dez. 2021.

[143] BRASIL. Portal Brasileiro de Dados Abertos. **O que são dados abertos?** Disponível em: https://dados.gov.br/pagina/dados-abertos. Acesso em: 8 abr. 2022.

Dez anos depois da primeira reunião realizada na Califórnia, com base no progresso desenvolvido por 30 dos países que assinaram o documento, publicaram o Open Data Barometer, um medidor global de como os governos publicam e usam dados abertos para responsabilidade, inovação e impacto social, que mede a prontidão, a implementação e o impacto das políticas de dados abertos dos países e descreve medidas necessárias para o avanço das políticas de dados abertos. O relatório conclui que governos ainda têm um longo caminho para superar a simples promessa ao progresso na implementação e no impacto de dados abertos, precisam mudar radicalmente sua abordagem aos dados abertos e concentrar seus esforços na governança de dados, assim compreendida como "políticas, estruturas e processos de tomada de decisão, recursos e ferramentas usadas para melhorar como os governos criam e usam dados abertos em todos os departamentos"[144].

Dados públicos abertos podem, então, ser considerados como subconjunto de dados de fonte aberta, disponibilizados por conta de um esforço feito em torno de políticas de transparência para publicar dados em formatos que possam ser lidos por máquinas, para ganhar transparência nas organizações. Decorrem de políticas de transparência, as quais orientam que governos publiquem dados detalhados de suas folhas de pagamento ou dos gastos realizados com pequenas empresas e empresários individuais que têm contratos de serviços com o governo local, para que sejam seguidos por pessoas específicas.

3.3. Pedido de acesso à informação

Como produto de acordos estabelecidos internacionalmente com a Organização para Cooperação e Desenvolvimento Econômico (OCDE), a Organização dos Estados Americanos (OEA) e a Organização das Nações Unidas (ONU) e que demandaram a disponibilização de instrumentos legais que encaminhassem à verdadeira intenção dos países signatários no combate de práticas corruptas através da reunião de uma série de legislações que, de uma forma ou de outra, tinham por objetivo a prevenção, o combate ou a erradicação dessas práticas[145], em 2011 o Brasil reuniu esforços na aprovação da Lei nº 12.527/11, Lei de Acesso à Informação (LAI), e, de forma a aderir ao regime jurídico e global de acesso à informação, lançou o Portal Brasileiro de Dados Abertos, governança de política pública instituída com a

[144] WORLD WIDE WEB FOUNDATION. Contents. Disponível em: https://opendatabarometer.org/leadersedition/report/#executive-summary. Acesso em: 20 abr. 2022.

[145] CAMARGO. Rodrigo Oliveira de; WEBBER, Lair. A dogmática e a política criminal do combate à corrupção e à criminalidade econômica nos últimos 80 anos: retrospectiva e perspectiva. *In*: REALE JR., Miguel Reale; MOURA, Maria Thereza de Assis. **Coleção 80 anos do Código Penal**. [*S. l.*]: Thompsons Reuters – Revista dos Tribunais, 2021. v. III. p. 289-324.

criação da Infraestrutura Nacional de Dados Abertos (Inda) por meio da Instrução Normativa SLTI nº 4, de 12 de abril de 2012[146].

No âmbito da garantia da defesa, pode-se dizer que a LAI surge como instrumento de resistência ao poder de requisição de documentos pelos agentes públicos: sua finalidade de assegurar ao indivíduo, em face do poder público e seus agentes, transparência, publicidade, controle social e dever de *accountability*, essenciais à eficácia do acesso à informação, fornecendo direitos que podem ser exercidos por intermédio de pedidos de acesso à informação, expedientes de natureza administrativa e com efeitos no Poder Judiciário por meio de Mandado de Segurança em caso de inobservância do Direito.[147] Garante-se, assim, intrumento adequado para desocultar práticas oportunistas levadas a efeito por agentes públicos[148], ganhando especial contorno em razão de sua aplicação na defesa de direitos fundamentais, já que o art. 21 da LAI veda a negativa de acesso à informação quando esta for necessária à tutela judicial ou administrativa de direitos fundamentais e, por isso, de todo aplicável à investigação criminal e processo penal em razão da garantia da ampla defesa, do contraditório, do direito à prova e da garantia das liberdades contra as ingerências ilegais e/ou com abuso de poder.

Requerer informação sobre (i) a existência de investigações arquivadas ou em andamento; (ii) alguns tipos de registros de agentes públicos, como histórico funcional, escalas de serviços; (iii) a geolocalização de viaturas, imagens de câmeras ou dados de outros dispositivos funcbionais utilizados na consecução de atos administrativos (iv) procedimentos, regras e métodos aplicados à Cadeia de Custódia; (v) dados gerais sobre *denúncias anônimas* que suportaram diligências; (vi) a existência de alguma testemunha, prova ou diligência não materializada nos autos; (vii) a participação de Unidades de Inteligência[149] – o que também viabilizará o exercício do direito ao acesso e demais direitos previstos nas LGPD e LGPD Penal – são apenas alguns exemplos da ampla gama de possibilidades e benefícios que o exercício dos pedidos de acesso à informação podem oferecer à defesa. Esses pedidos podem ser formulados durante a investigação, o processo ou para fins de instruir ações constitucionais, e a negativa ao acesso, se não inicidir sobre nenhuma hipótese que afaste a

[146] BRASIL. Portal Brasileiro de Dados Abertos. Disponível em: https://dados.gov.br/. Acesso em: 11 abr. 2022.
[147] BRASIL. Supremo Tribunal Federal. **Inq. 4.831-DF**. Relator: Min. Celso de Mello, 05 de dezembro de 2020. Acesso em: 31 agosto de 2022. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15345201506&ext=.pdf. Acesso em: 20 abr. 2022.
[148] ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico: de acordo com a teoria dos jogos e MCDA-A**. Florianópolis: Emais, 2021. p. 437-443.
[149] ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico: de acordo com a teoria dos jogos e MCDA-A**. Florianópolis: Emais, 2021.p. 437-443.

aplicação da LAI por conflito com a LGPD ou não for ocorrer nenhuma causa de restrição ao acesso previsto na própria LAI, pode ser combatida através de Mandado de Segurança.

Por outro lado, tem-se discutido que, em razão do *status* constitucional atribuído àquelas, as garantias previstas na LAI não devem se sobrepor aos direitos assegurados pela LGPD, gerando um importante debate sobre a convergência da LGPD e a LAI. Em razão da tutela constitucional, dados pessoais demandam maior atenção por parte do Estado, e, quando postos em conflito com outros interesses, devem prevalecer: como exceção à transparência intrínseca às democracias, a LAI atribui aos órgãos e às entidades do poder público assegurar a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso (inciso III do artigo 6º da Lei nº 12.527/2011). Tanto a LAI como o Decreto nº 7.724/2012 que a regulamenta preveem hipóteses de restrições de acesso de naturezas substancial ou procedimental: a primeira restrição está relacionada ao conteúdo da solicitação de informação, que pode ser objeto de classificação por requisitos de segurança, sigilo originário ou sigilo legal; já, a segunda, vincula-se à forma do pedido: genéricos, desproporcionais ou que exijam trabalho adicional. O parágrafo 3º do artigo 7º da LAI estabelece sigilo aos documentos preparatórios, que servem como fundamento às decisões e aos atos administrativos, ao menos até que o ato respectivo se concretize, entendimento reforçado pela Súmula Vinculante nº 14, do Supremo Tribunal Federal (STF), ao vedar o acesso a diligências em andamento. Da mesma forma, o artigo 23 permite atribuir sigilo à investigação promovida através de inquérito policial, de forma que o nível de transparência adotado poderá ser observado em razão de como funcionam estruturas legais e institucionais (*o que*, o *quanto*, *como* e *por quem* ou *por quantos* pode ser visto) ou de como operam as estruturas políticas que o estabelecem, já que o controle de informações, como já exposto, é recurso de poder fundamental no seio do Estado[150].

A política de dados abertos deve, também, ser analisada à luz das possibilidades de tratamento posterior que oferece, independentemente da sua natureza, sendo importante a criação de mecanismos de filtragem para a redução dos riscos decorrentes de utilização abusiva. Grande quantidade de informação pública, que exige uma ampla publicidade, já é divulgada através das tecnologias da informação e contém uma série de outros dados que podem ser reutilizados. Já são percebidas preocupações e até mesmo críticas com o modelo

[150] POSSAMAI, Ana Júlia; SOUZA, Vitoria Gonzatti de. Transparência e Dados Abertos Governamentais: Possibilidades e Desafios a partir da Lei de Acesso à Informação. **Administração Pública e Gestão Social**, v. 12, n. 2, 2020. Disponível em: https://periodicos.ufv.br/apgs/article/view/5872/5460. Acesso em: 27 ago. 2022.

econômico em que os dados da jurisprudência pública – a *priori*, em conformidade com os requisitos legais de proteção de dados pessoais – seriam coletados, tratados e reutilizados pelo setor privado.

Uma das 13 categorias de classificação formulada pela Associação Brasileira de Lawtechs e Legaltechs das empresas voltadas a produtos e serviços de inovação para a área jurídica é a Extração e Monitoramento de Dados Públicos[151], cuja atuação está sedimentada na coleta e na compilação de atos oficiais administrativos e judiciais e que promove a disponibilização de dados sensíveis ao indivíduo e com potencial de violação a direitos fundamentais. Fundamentam-se essas atividades na importância da publicidade processual, na relevância da transparência das atividades públicas e na democratização do acesso à informação, ainda que pesquisas demonstrem que, de suas atividades, também ocorram a superexposição dos dados pessoais.[152]

Preocupado no ponto, o ciclo de avaliação 2016-2018 do Conselho da Europa Comissão Europeia para a Eficiência da Justiça centrou-se na questão de decisões judiciais fornecerem dados abertos para os quais é utilizado algum processamento de IA e sobre a aplicação da anonimização ou pseudoanonimização de dados no âmbito do quadro europeu, previstos nos regulamentos gerais de proteção de dados, promovendo questão específica destinada a identificar medidas aplicadas pelos Estados-membros. Vinte e três países declararam que estão a pseudoanonimizar alguns tipos de litígios, apagando dados que tornam as partes ou testemunhas identificáveis, mas declaram dificuldade em medir o impacto dos dados abertos na eficiência e na qualidade da justiça e até mesmo incredulidade que estes dados possuam condições de fornecer informações significativas – uma vez que permitirão descarregar um conjunto de dados em bruto, mas seu significado permanece obscuro –, atribuindo à iniciativa privada a reutilização desses dados para recolher as informações fornecidas por seus clientes para o exercício de suas funções.[153]

Por outro lado, o requisito fundamental para que dados sejam considerados abertos é que sejam transparentes, informativos e que terceiros possam utilizá-los para análise e

---

[151] AB2L – ASSOCIAÇÃO BRASILEIRA DE LAWTECHS & LEGALTECHS. **Radar maio** 2022. Disponível em: https://ab2l.org.br/wp-content/uploads/2022/06/RADAR-MAIO-2022.pptx-7.png. Acesso em: 3 jul. 2022.

[152] MORAIS, Flaviane de Magalhães Barros Bolzan de; MARQUES, Leonardo Augusto Marinho; SARKIS, Jamilla Monteiro. Dados Pessoais no Processo Penal: Tutela da Personalidade e da Inocência Diante da Tecnologia. **Revista Brasileira de Ciências Criminais**, São Paulo, ano 30, v. 190, p. 117-156, maio/jun. 2022. DOI: https://doi.org/10.54415/rbccrim.v190i190.120.

[153] COMISSÃO EUROPEIA PARA A EFICÁCIA DA JUSTIÇA (CEPEJ). **Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente adoptada pela CEPEJ na sua 31.ª reunião plenária**. Estrasburgo, 3 e 4 de dezembro de 2018. Disponível em: https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0. Acesso em: 27 ago. 2022.

desenvolvimento. Quando utilizado, o exercício do direito causa desconforto e reação refratárias de muitas organizações, evidenciando o impacto do uso do direito ao acesso pelos cidadãos; também, seria legítimo considerar que o reconhecimento formal do direito ao acesso tenha induzido aos coletores de informações a se adequarem às prescrições legislativas.

3.4. Inteligência Policial no Brasil

Inteligência é produto de um movimento analítico e sigiloso de transformação da massa bruta de dados em informações explicativas e preditivas de fatos ou ameaças, através de processo definido e voltado ao suporte para a tomada de decisões mais assertivas. Opera atendendo a métodos e técnicas de avaliação de dados, processo que se adapta aos contextos, tendências, informações depuradas e análises de risco e de oportunidades. Trata-se de um ramo voltado à produção de conhecimento por sua importância ou natureza estratégica, o qual abrange a coleta de dados disponíveis em bancos e cuja aplicação de metodologias específicas por setores estruturados, dedicados e especializados os transforma em conhecimento de interesse para avaliação e decisão.[154]

Ainda que o consenso entre acadêmicos e agências de aplicação da lei pareça ver a *inteligência* como o produto de avaliação e análise da matéria bruta de informação, existem divergências em como a inteligência pode ser definida. Para uns, resume-se a mera aquisição, organização, recuperação, análise, interpretação e proteção sistemática e proposital de informações; outros, em vez de um processo definido, categorizam inteligência como "informação produzida para direcionar ação policial" e "um modo de informação que foi interpretado e analisado para informação ações futuras de controle social contra um alvo identificado"; outra descrição mais prática de inteligência no meio policial é de "informação que agregou mais valor depois de coletada e avaliada"[155].

São exemplos de procedimentos e técnicas de inteligência o reconhecimento, a vigilância, a infiltração, a desinformação, a provocação, a entrevista, a obtenção de dados em locais de acesso restrito, a interceptação de sinais, a identificação de pessoas, as comunicações sigilosas, a leitura da fala, a análise de veracidade, o emprego de meios

[154] MANDARINI. Marcos. **Segurança Corporativa Estratégica**: fundamentos. Barueri: Manole, 2005.
[155] STANIFORTH, Andrew. Police Use of Open Source Intelligence: the longer arm of law. *In*: AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation: from strategy to implementation**. Genebra: Springer, 2016. p. 21-31.

eletrônicos e a fotointerpretação.[156] Diversos tipos de inteligência – militar, política, econômica, social, ambiental, da saúde e cultural – oferecem informações importantes para a tomada de decisões, mas, equivocadamente, presumida para ser reunida exclusivamente por meios secretos ou disfarçados. Enquanto, de fato, algumas inteligências são conhecidas apenas em altos níveis de governo, outras consistem em informações amplamente disponíveis em escala, acessibilidade e alta taxa de retorno em comparação aos recursos mínimos investidos.

É ferramenta que viabiliza a simulação de hipóteses e cenários por meio da interpretação de dados e situações, e que empregada na definição de objetivos, políticas e planos pode ser chamada de inteligência estratégica, cada vez mais utilizada nas sociedades globalizadas, que se baseiam no desenvolvimento de sistemas de inteligência para enfrentar os desafios causados pela incerteza e que, com isso, trazem consigo novas políticas para responder ao fenômeno das novas ameaças à segurança baseados em segurança inteligente.[157]

Usado pelo FBI e pela Escola do Reino Unido de Policiamento, existem razões e estratégias próprias na aquisição de inteligência estratégica, em muitas organizações orientadas por um processo de governança conhecido como "ciclo de inteligência", que se move da identificação da inteligência requisitada pelas fases de coleta e análise de dados à fase de retorno, em que a inteligência coletada é medida ante requisitos iniciais que permitem a identificação de novos requisitos. Está ancorada em quatro princípios básicos com o objetivo de estabelecer, consolidar e profissionalizar o processo: (i) *legalidade*: o trabalho de inteligência deve ser legal, para um propósito legítimo, necessário e proporcional; (ii) *treinamento*: oficiais e colaboradores devem ser instruídos, treinados e equipados para seus postos com o processo de gerenciamento de inteligência; (iii) *segurança e sigilo*: essenciais ao estabelecer um ambiente de inteligência efetivo e profissional; (iv) *contextualização*: atividade organizacional e em parceria deve ser baseada em conhecimento dos problemas e seus contextos; (v) *efetividade*: inteligência serve para nada, se não utilizada; (vi) *objetividade*: uso de inteligência como ferramenta requer objetividade e mente aberta, tanto da parte do analista como do subsequente usuário; (vii) imparcialidade: a avaliação deve ser

[156] MELO, Felipe Pereira de Melo. **A utilização dos serviços de inteligência no Inquérito Policial**. Curitiba: Íthala, 2017. p. 47-60.
[157] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**, Bogotá, v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.

correta e imparcial, baseada no conhecimento das circunstâncias predominantes existentes naquele tempo.[158]

No Brasil, o Decreto nº 8.793/2016, que fixa a Política Nacional de Inteligência, descreve atividade de inteligência como "exercício permanente de ações especializadas, voltadas para a produção e difusão de conhecimentos, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado". Divida nos ramos de inteligência[159] e contrainteligência[160], está voltada às atividade de assessoramento oportuno - fornecimento de informações oportunas, abrangentes e confiáveis, necessárias ao exercício do processo decisório[161] - e de atividade especializada - alicerçada em um conjunto de valores profissionais e em uma doutrina comum[162] -, de forma que não se confundem com a investigação criminal.

A Agência Brasileira de Inteligência (Abin) é seu órgão central e tem por finalidade fornecer ao presidente da República informações e análises estratégicas, oportunas e confiáveis, necessárias ao exercício das respectivas funções[163]. Na qualidade de órgão da

---

[158]STANIFORTH, Andrew. Police Use of Open Source Intelligence: the longer arm of law. *In*: AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation: from strategy to implementation**. Genebra: Springer, 2016. p. 21-31.

[159] Atividade que objetiva produzir e difundir conhecimentos às autoridades competentes, relativos a fatos e situações que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e do Estado

[160] Atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado"

[161] À Inteligência compete contribuir com as autoridades constituídas, fornecendo-lhes informações oportunas, abrangentes e confiáveis, necessárias ao exercício do processo decisório. Cumpre à Inteligência acompanhar e avaliar as conjunturas interna e externa, buscando identificar fatos ou situações que possam resultar em ameaças ou riscos aos interesses da sociedade e do Estado. O trabalho da Inteligência deve permitir que o Estado, de forma antecipada, mobilize os esforços necessários para fazer frente às adversidades futuras e para identificar oportunidades à ação governamental.

[162] A Inteligência é uma atividade especializada e tem o seu exercício alicerçado em um conjunto sólido de valores profissionais e em uma doutrina comum. A atividade de Inteligência exige o emprego de meios sigilosos, como forma de preservar sua ação, seus métodos e processos, seus profissionais e suas fontes. Desenvolve ações de caráter sigiloso destinadas à obtenção de dados indispensáveis ao processo decisório, indisponíveis para coleta ordinária em razão do acesso negado por seus detentores. Nesses casos, a atividade de Inteligência executa operações de Inteligência – realizadas sob estrito amparo legal –, que buscam, por meio do emprego de técnicas especializadas, a obtenção do dado negado.

[163] "Abin não consiste em órgão responsável pela condução de investigações criminais. Na literalidade do artigo 4º da precitada lei, compete-lhe: (1) planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o presidente da República; (2) planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade; (3) avaliar as ameaças, internas e externas, à ordem constitucional; e (4) promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento dessa atividade intelectiva" (VIEIRA, Luis Guilherme; ROSA, Alexandre Morais da. Veto a uso das agências de inteligência e nulidade das investigações (parte 2). **Revista Consultor Jurídico**. 7 de dezembro de 2022. Disponível em https://www.conjur.com.br/2022-dez-08/vieirae-rosa-veto-uso-agencias-inteligencia-parte, acesso em 15.12.2022.)

administração pública, o compartilhamento de dados com a polícia judiciária somente poderá ocorrer se autorizada pelo chefe do Gabinete Institucional da Presidência da República; e, ainda assim, desde que haja compromisso da guarda do sigilo legalmente imposto, sob pena de responsabilidade administrativa, civil e criminal, à luz do que determina Lei nº 9.893/1999, artigo 9º, caput, e §§ 1º e 2º.

Sua competência institucional está limitada (i) ao conhecimento e execução de ações destinadas à colheita e à análise de informes necessários ou úteis ao assessoramento do chefe do Executivo; (ii) ao planejamento, execução e proteção de conhecimentos sensíveis, relativos à segurança do Estado e da sociedade; (iii) à avaliação de ameaças à ordem constitucional; e (iv) à formação e desenvolvimento de recursos humanos, na elaboração de uma doutrina de inteligência e na realização de estudos em ordem a aprimorá-la[164].

Trata-se, pois, de um procedimento sistemático e padronizado para produzir elementos de informação aptos a construir um cenário de redução de incertezas para suportar tomadas de decisões, com o tempo aperfeiçoado por sua categorização a partir da fonte dos dados, se originados de pessoas (HumInt), imagens (ImInt), sinais (SigInt) ou fontes abertas (OsInt). Este conceito de origem ou fonte da informação é alçado a uma condição de elemento fundamental no campo da inteligência, pois será o responsável por condicionar a metodologia e os procedimentos para a exploração e obtenção de resultados úteis, assim como na análise das informações coletadas.[165]

Quando órgãos de inteligência trabalham buscando produzir conhecimentos para assessorar o processo decisório tendo como destinatário final o chefe do Poder Executivo, estão orientados ao estabelecimento de políticas criminais de gestão pública que objetivam fornecer subsídios para o mapeamento da criminalidade e para a produção de estatísticas e informações que servem para planejar a atuação pública voltada ao controle e à prevenção à criminalidade. Não se destina, portanto, às atividades de persecução penal, mas ao planejamento preventivo para a elaboração de políticas públicas e para a preparação frente a ameaças vindouras.

Sua atividade é sigilosa e informal, características essenciais à sua regularidade, já que se refere à movimentação prévia à apuração ou à ocorrência do crime; um exercício

---

[164] VIEIRA, Luis Guilherme; ROSA, Alexandre Morais da. Veto a uso das agências de inteligência e nulidade das investigações (parte 3). **Revista Consultor Jurídico**. 7 de dezembro de 2022. Disponível em https://www.conjur.com.br/2022-dez-09/vieirae-rosa-veto-uso-agencias-inteligencia-parte, acesso em 15.12.2022.

[165] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**, Bogotá, v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.

permanente e sistêmico para identificar e acompanhar ameaças reais ou potenciais à segurança pública do Estado[166]. A concepção política de inteligência tradicionalmente apresenta o sigilo como inerente aos assuntos do Estado: diplomaticamente chamado de "discrição" e de *arcana imperii* (os mistérios do governo), sigilo e embuste – ou falsidade deliberada e mentira descarada – são usados como meios legítimos para alcançar fins políticos desde os primórdios da história documentada. Com o Estado formado de esteio em uma já considerável burocracia, o Brasil herdou a valorização da organização de serviços de inteligência edificados na não transparência, de forma que serviços de inteligência tradicionalmente funcionam na clandestinidade e realizam seu trabalho buscando, no próprio país, as ameaças à estabilidade política.[167]

Desde sua criação no Brasil, em 1933, com a Delegacia Especial de Segurança Política e Social (DESPS) transformada em Divisão de Polícia Política e Social (DPS) no ano de 1944 e, no início regime militar, em Serviço Nacional de Informações (SNI), a *inteligência policial* ou atuou na perseguição aos dissidentes do governo, ou na vigilância e repressão de adversários do regime.[168] Com a democratização, instituições policiais sofreram reformas na área de inteligência, e a inteligência policial teve seu escopo voltado para o combate ao crime organizado, o contraterrorismo, a lavagem de dinheiro, o narcotráfico, a sonegação fiscal, mas com imprecisão dos limites de atuação entre órgãos de polícia e analistas de inteligência.

Em 1999, a Lei nº 9.883 instituiu o Sistema Brasileiro de Inteligência e definiu como inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental. Regulamentada pelo Decreto nº 3.695 com a finalidade de coordenar e integrar as atividades de inteligência de segurança pública do País e de suprir governos federal e estaduais com informações para subsidiar a tomada de decisões no âmbito da segurança pública, em 2000 criou o Subsistema de Inteligência de Segurança Pública; este, por sua vez, regulamentado pela Resolução nº 1º, instrumento que

---

[166] VIEIRA, Luis Guilherme; ROSA, Alexandre Morais da. Veto a uso das agências de inteligência e nulidade das investigações (parte 1). **Revista Consultor Jurídico**. 7 de dezembro de 2022. Disponível em https://www.conjur.com.br/2022-dez-07/vieirae-rosa-veto-uso-agencias-inteligencia-parte, acesso em 15.12.2022.

[167] MATHIAS, Suzeley Kalil; ANDRADE, Fabiana de Oliveira. O Serviço de Informações e a cultura do segredo. **Dossiê: Relações Civis Militares e Segurança Nacional**, Varia História: Belo Horizonte, v. 28, n. 547, p. 537-554, jul/dez 2012, Disponível em: https://repositorio.unesp.br/bitstream/handle/11449/8818/S0104-87752012000200004.pdf?sequence=1&isAllowed=y. Acesso em: 27 ago. 2022.

[168] ANDRADE, Fabiana de Oliveira. **A Escola nacional de Informações**: a formação dos agentes para a inteligência durante o regime militar. 2014. 138 f. Dissertação (Mestrado) – Universidade Estadual Paulista Júlio de Mesquita Filho, Faculdade de Ciências Humanas e Sociais, 2014. Disponível em: http://hdl.handle.net/11449/121960. Acesso em: 8 abr. 2022.

definiu inteligência policial como "conjunto de ações que empregam técnicas especiais de investigação, visando a confirmar evidências, indícios e a obter conhecimentos sobre a atuação criminosa dissimulada e complexa, bem como a identificação de redes e organizações que atuem no crime, de forma a proporcionar um perfeito entendimento sobre a maneira de agir e operar, ramificações, tendências e alcance de condutas criminosas".

Em 2001, com a intenção de dirigir, planejar, coordenar, controlar, avaliar e orientar as atividades de Inteligência na Polícia Federal, além de planejar e executar operações de contrainteligência e antiterrorismo, foi criada a Diretoria de Inteligência Policial, estrutura que garante troca de dados, informações e conhecimentos por meio do fluxo de comunicações que transita pela instituição através de Unidades de Inteligência Policial. Além disso, com o intuito de zelar pela implementação, consolidação e atualização da doutrina de Inteligência da Polícia Federal, foi criada, ainda, a Divisão de Doutrina de Inteligência e Treinamento (Dint), que materializa todo o resultado da atividade de Inteligência da Polícia Federal, uma vez concluídos os procedimentos pertinentes ao ciclo de produção de conhecimento, através de um documento denominado Relatório de Inteligência, cuja natureza pode ser classificada como *informe*, *informação*, *estimativa* ou *apreciação* e que, devido a sua classificação legal, não pode ser juntado a inquéritos policiais.

Com a entrada em vigor da LAI, sobreveio no âmbito da Polícia Federal a Portaria nº 2975/2012 – DG/DPF, de forma a dotar as unidades de Inteligência da Polícia Federal de condições para que seus responsáveis, por poderes delegados, efetuassem a classificação das informações em grau de reserva, já que se atribui ao sigilo fator determinante na obtenção do resultado, o que também pode ocorrer nas situações em que o próprio Poder Judiciário atribui Segredo de Justiça à investigação ou quando legislação regula a matéria e estabelece o sigilo concernente, a exemplo da interceptação de comunicações telefônicas[169].

Estendida a atividade de inteligência a outros órgãos da administração pública federal a partir da criação do SISBIN, as policias passaram a implantar núcleos, seções ou departamentos exclusivos para essa atividade, criando um cenário extremamente confuso entre as atividades de inteligência e as atividades de investigação realizadas pelos órgãos de justiça criminal brasileiros. Relegado a um segundo plano, o aspecto de produção de conhecimento voltado ao processo decisório perdeu espaço para um aspecto investigativo, destinado à produção de provas, de maneira que a atividade de inteligência assume uma

[169] VERONESE, Jorvel Eduardo Albring. Lei de Acesso à Informação e os Reflexos sobre a Produção de Inteligência na Polícia Federal. **Revista Brasileira de Inteligência**, v. 8, p. 49-59, 1.09.2013. Disponível em: https://rbi.enap.gov.br/index.php/RBI/article/view/105. Acesso em: 8 abr. 2022.

configuração particularmente desvinculada da inteligência praticada pela Abin, remodelando-se para uma forma de inteligência de segurança pública, realizada pelas polícias, como se fossem diferentes atividades e não uma única com objetos distintos. Esta concepção equivocada pode ter origem em aspectos como (i) a inexistência de manuais de trabalho, (ii) uma cultura de valorização da prática em detrimento da discussão acadêmica, (iii) as técnicas operacionais semelhantes entre investigação e operações de inteligência e (iv) o fato de a palavra "operações" ter conceitos diferentes podem, todos, ser os fatores que levaram ao processo de confusão que coloca a inteligência como uma espécie de investigação mais apurada[170].

Antes algo complementar à investigação preliminar, parece que a atividade de inteligência, hoje, com ela confunde-se, de forma que é legítimo definir os seus limites ante as atividades de persecução penal.

3.5 Limites à Inteligência Policial

O texto do art. 144 da Constituição Federal Brasileira não suporta categorias como inteligência de segurança pública ou a inteligência policial, assim como o Código de Processo Penal e leis esparsas que complementam as diretrizes constitucionais relacionadas à investigação e ao processamento de crimes sem qualquer tipo de consideração no ponto. Com o pretexto de disciplinar a organização e o funcionamento da segurança pública nos termos do parágrafo 7º do art. 144 da Constituição Federal de 1988, a Lei 13.675/2018 – que criou o Plano Nacional de Segurança Pública e Defesa Social e instituiu o Sistema Único de Segurança Pública – introduziu atividades de inteligência ao rol das atribuições da segurança pública, forma encontrada para naturalizar a incorporação das atividades de inteligência no rol das atividades de segurança pública, fragmentando suas fronteiras.

Com fundamento na usurpação de atribuições das forças de defesa e da introdução de atribuições de guerra em face de cidadãos no interior do território nacional, em pleno estado de paz, questiona-se, inclusive, a constitucionalidade material de atribuições de inteligência para órgãos de segurança pública[171], assim como a própria licitude do resultado da

---

[170] KRAMER, Rodrigo. Incompreensão do conceito de inteligência na segurança pública. *In*: **Revista Brasileira de Inteligência**. Brasília: Abin, n. 10, dezembro 2015, pg. 73-82. Disponível em: https://rbi.enap.gov.br/index.php/RBI/article/view/128/103, acesso em 26. dez. 2022.

[171] "Dentre as instituições elencadas e as atribuições assinaladas à segurança pública não se encontra nada a respeito de atividades de inteligência. As referências expressas ao patrulhamento ostensivo (art. 144, §§ 2º, 3º, 5º, da CRFB), à preservação da ordem pública (art. 144, § 5º, da CRFB) e à prevenção do tráfico ilícito de

inteligência como prova, já que sua produção se dá de forma alheia às disposições da investigação preliminar. Informações produzidas em atividades de inteligência acostadas nos em relatórios não se prestam à produção probatória, restando restritas a representação de "*notitia criminis* para que a polícia investigue fatos criminosos"[172].

A usurpação das atribuições da polícia judiciária pelos órgãos de inteligência na condução da investigação criminal frente o manejo preventivo de fontes de dados é realidade que deve ser corretamente dimensionada; trata-se de investigação levada a efeito sem controle de legalidade, cada vez mais institucionalizadas em razão da legitimação material e formal-procedimentalmente promovidas pelo Judiciário, a partir de uma orientação deturpada da Constituição Federal e do Código de Processo Penal, quando consentem com a investigação criminal levada a efeito por quem deveria atuar no âmbito de segurança de ações governamentais e conferem licitude/legitimidade à prova produzida. Esta atuação permite a produção de elementos muitas vezes irrepetíveis por aqueles cuja atividade exige o emprego, de maneira a resguardar suas ações, métodos, profissionais e fontes, de meios sigilosos[173].

Além disso, trata-se de uma questão de flagrante lógica jurídica: se a investigação não culmina na produção de provas[174], inteligência, que nem investigação é, sequer poderá produzi-las: o produto da operação de inteligência não passa de um relatório sobre o conhecimento adquirido. A ausência absoluta de controle sobre quais informações ou por

---

entorpecentes, do contrabando e do descaminho (art. 144, § 1º, II, da CRFB) são insuficientes para que se fale em atividades inteligência. A disposição mais vaga trata da prevenção ao tráfico, ao contrabando e ao descaminho pela Polícia Federal.

Todavia, não menciona expressamente os modos de execução das atividades de prevenção, o que implica em dizer que, tratando-se de atividade estatal, não se pode interpretar omissões como restrições a direitos fundamentais por meio de práticas não expressamente reconhecidas. Isso porque as atividades estatais, dentre as quais a persecução penal, precisam ser realizadas nos estritos limites da legalidade (art. 5º, II, da CRFB).

[...]

A usurpação de atribuições entre instituições de segurança pública já é parte do cotidiano. Nada obstante tal usurpação, os Tribunais Superiores vêm consolidando a jurisprudência contrária a tal movimento. Por exemplo, a usurpação de atribuições de policiamento ostensivo e repressivo pelas Guardas Municipais é frequentemente declarada ilícita (STJ, *HC* 561.329 e 667.461; STF, RE 1.281.774). Outro exemplo, quiçá o mais famoso, é o da Operação Satiagraha, na qual oficiais e agentes de inteligência da ABIN auxiliaram a Polícia Federal na utilização de grampos telefônicos, o que resultou na declaração de ilicitude das informações produzidas pelas arapongas (STJ, *HC* 149.250). Ressalta-se: ainda que fosse admissível o aproveitamento de resultados cognitivos oriundos da coleta e depuração de dados úteis à tomada de decisões, as informações produzidas seriam inúteis se não fossem estruturadas em relatório técnico (STF, *HC* 512.290)" (CANI, Luiz Eduardo; NUNES, João Alcantara**.** Diante de Argos: Notas sobre a ilicitude das informações produzidas em atividade de inteligência. **Boletim do IBCCRIM.** São Paulo: IBCCRIM, ano 30, n. 157, p. 11-12, ago/2022).

[172] MARTINS JÚNIOR, Ayrton Figueiredo. **Atividade de Inteligência: uma proposta de controle judicial**. 2015. 152 f. Dissertação (Mestrado) – Curso de Programa de Pós-Graduação em Ciências Criminais, Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2015.

[173] VIEIRA, Luis Guilherme; ROSA, Alexandre Morais da. Veto a uso das agências de inteligência e nulidade das investigações (parte 1). **Revista Consultor Jurídico**. 7 de dezembro de 2022. Disponível em https://www.conjur.com.br/2022-dez-07/vieirae-rosa-veto-uso-agencias-inteligencia-parte, acesso em 15.12.2022.

[174] LOPES JÚNIOR. Aury. **Direito Processual Penal**. 16. ed. Saraiva: São Paulo, 2019. p. 160-161.

quais meios foram obtidas muitas vezes é um convite para o abuso, e facilmente pode arrastar as informações produzidas em atividades de inteligência ao terreno da ilegalidade.

Apesar de ausência de atribuição constitucional, a práxis encara inteligência policial como gênero das atividades de inteligência de segurança pública, apontando inegáveis pontos de contato com a investigação preliminar, como as finalidades de realização de diagnósticos e prognósticos sobre o desenvolvimento de situações de interesse da segurança pública, de forma a subsidiar seus usuários no processo decisório e o assessoramento de operações de prevenção e repressão: inteligência e investigação criminal são manifestações que operam sob o discurso da garantia da segurança pública, ambas obtêm como produto a informação, mas aplicam-lhe destinações e finalidades diferentes. Por outro lado, em cada caso existe um critério temporal que distingue uma da outra: o momento da ocorrência de uma infração penal. A inteligência é desencadeada antes da ocorrência de infração penal visando a interromper sua execução; a investigação é posterior à infração penal[175].

Aplicada à polícia judiciária e à segurança pública, a ideia é de que inteligência deva produzir conhecimento de interesse de atividade policial que identifique a forma de agir criminosa para estabelecer, por exemplo, níveis de comando, mapeamento de itinerários, focos de criminalidade, tendências e estatísticas, além, evidentemente, de ser meio de assessoramento das atividades de prevenção e investigação do crime, imediata ou potencial, com o intuito de prevenir e maximizar o combate ao crime e possibilitar a tomada de decisões assertivas.[176] Emprega um conceito que carrega consigo um componente pré-crime, do levantamento de elementos preparatórios pela exploração de cenários para detectar e agir antes que ameaças se manifestem.[177]

Inteligência policial, portanto, não se confunde com investigação criminal: há uma persistente confusão entre investigação e inteligência, quando, na verdade, trata-se de ferramentas distintas, com métodos e finalidades próprias[178]. Enquanto a investigação criminal procura elucidar crimes e contravenções, a inteligência policial visa a conhecer

[175] NUNES, João Alcântara. **Diagnóstico de Inteligência de Fontes Abertas para fins de persecução penal no contexto da sociedade do controle**. 2021. (Monografia –Trabalho de Conclusão de Curso) – PUCRS: Porto Alegre. 2021.
[176] LEITE, Sara Souza. O Emprego das Fontes abertas no Âmbito da Atividade de Inteligência Policial. **Revista Brasileira de Ciências Policiais**. Brasília, v. 5, n. 1, p. 11-45, jan/jun 2014.
[177] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**. Bogotá, v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.
[178] LEITE, Sara Souza. O Emprego das Fontes abertas no Âmbito da Atividade de Inteligência Policial. **Revista Brasileira de Ciências Policiais**. Brasília, v. 5, n. 1, p. 11-45, jan/jun 2014.

atores e fenômenos mais abrangentes, dados indispensáveis ao processo decisório nas atividades de polícia[179].

Neste sentido, no julgamento do HC nº 149.250/SP, o Superior Tribunal de Justiça, reconheceu a violação aos arts. 144, § 1º, IV, da Constituição Federal e 4º, do Código de Processo Penal e aos. 1º, III, e 5º, X, XII, LVI, ambos da Constituição Federal e 157, do Código de Processo Penal, ocorrida durante a denominada Operação Satiagraha, em razão de (i) ter sido realizada uma investigação criminal à margem de inquérito policial, substituído pela atuação da Agência Brasileira de Inteligência - ABIN e de investigador particular, meses antes da instauração formal do inquérito policial e (ii) ter ocorrido intromissão estatal abusiva e ilegal na esfera da vida privada, da intimidade, da honra e da imagem, proscrita submissão do sujeito à condição de 'objeto' das investigações, violando o Princípio da Dignidade Humana, bem como a obtenção de prova ilícita, em virtude de ter sido obtida em contrariedade à previsão legal[180]. Para a Corte, a Lei nº 9.883/1999 determina as funções e o *modus operandi* da Abin de forma taxativa, não sendo aceitável uma interpretação elástica e em desconformidade com o espírito do legislador[181]: não é de sua atribuição ainvestigação de crimes.

Atos de investigação são levados a efeito uma vez ocorrido o ilícito criminal, uma resposta reativa à violação dos direitos e liberdades públicas.[182] Inteligência policial é uma atividade de assessoramento à tomada de decisões das Polícias Judiciária e ostensiva (ou Polícia Militar), voltada a obtenção, análise, produção e difusão de conhecimento sobre ocorrências que interessem à Segurança Pública, com especial ênfase no âmbito do controle e combate à criminalidade.[183] Não está voltada à produção de provas, mas de conhecimento

---

[179] VIEIRA, Luis Guilherme; ROSA, Alexandre Morais da. Veto a uso das agências de inteligência e nulidade das investigações (parte 2). **Revista Consultor Jurídico**. 7 de dezembro de 2022. Disponível em https://www.conjur.com.br/2022-dez-08/vieirae-rosa-veto-uso-agencias-inteligencia-parte, acesso em 15.12.2022.

[180] BRASIL. Superior Tribunal de Justiça. **HC nº 149.250-SP**. Relator: . Ministro Adilson Vieira Macabu (Desembargador Convocado do TJ/RJ), 07 de junho de 2011. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200901925658&dt_publicacao=05/09/2011. Acesso em: 22 dez. 2022.

[181] VIEIRA, Luis Guilherme; ROSA, Alexandre Morais da. Veto a uso das agências de inteligência e nulidade das investigações (parte 3). **Revista Consultor Jurídico**. 7 de dezembro de 2022. Disponível em https://www.conjur.com.br/2022-dez-09/vieirae-rosa-veto-uso-agencias-inteligencia-parte, acesso em 15.12.2022.

[182] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**, Bogotá, v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.

[183] O Manual de Inteligência Policial da DIP (Polícia Federal) conceitua Inteligência policial como "atividade de produção e proteção de conhecimentos, exercida por órgão policial, por meio do uso de metodologia própria e de técnicas acessórias, com a finalidade de apoiar o processo decisório deste órgão, quando atuando no nível de assessoramento, ou ainda, de subsidiar a produção de provas penais, quando for necessário o emprego de suas

qualificado voltado à tomada de decisões estratégicas por órgãos responsáveis pela segurança pública, especialmente diante de ocorrência de crimes, razão pela qual não se pode falar, *a priori*, em ilegalidade no compartilhamento de conhecimento.[184]

A sinergia entre as disciplinas pode encontrar pontes de comunicação através dos resultados das investigações (perpetradores, modus operandi, datas, vítimas etc.), pois constituem fonte de elementos para a elaboração da inteligência criminal.

3.6. Inteligência de Fonte Aberta

A inteligência criminal recorre a várias fontes de informação que afetam ou podem afetar a segurança pública, um amálgama de dados que auxilia diferentes agências de aplicação da lei a tomar decisões na luta contra o crime e que se mostrou flexível para acomodar diferentes disciplinas e fontes de inteligência criminal para obter dados sempre precisos na luta contra novas formas de criminalidade, sobretudo fontes mais difusas baseadas no ciberespaço (CybInt) e que não faziam parte dos ciclos clássicos de inteligência.[185]

A prospecção baseada em Tecnologia da Informação e Comunicação que fomenta a pesquisa e análise de dados gerados na *web* para produção de informações nada mais é do que atividade de inteligência digital, processo voltado exclusivamente a obter dados para a auxiliar na produção de conhecimento, facilitando sua concepção e seu aprimoramento, que se utiliza da imensa gama de meios tecnológicos, digitais, telemáticos e de interpretação de sinais, ganhando cada vez mais espaço no meio das atividades de segurança pública, investigação e processo.[186] Credita-se a lentidão das comunidades de inteligência em apreciar o valor das fontes obtidas por meio da internet por duas razões: (i) primeiro, porque confiar em informações abertas e suas restrições de privacidade são contrários à ideia tradicional de que agências de inteligência buscam informações através de tratamento dissimulado e

---

técnicas e metodologias próprias, atuando, neste caso, no nível operacional" (BRASIL. Departamento de Polícia Federal. **Manual de Doutrina de Inteligência Policial – Volume I**. Brasília, 2011).

[184] LEITE, Sara Souza. O Emprego das Fontes abertas no Âmbito da Atividade de Inteligência Policial. **Revista Brasileira de Ciências Policiais**. Brasília, v. 5, n. 1, p. 11-45, jan/jun 2014.

[185] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**. Bogotá, v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.

[186] BARRETO, Alexandre Gonçalves; WENDT; Emerson. **Inteligência e Investigação Criminal em Fontes Abertas**. Rio de Janeiro: Brasport, 2020. p. 1-4.

secreto[187] e (ii) porque fontes devem ser de valor, atribuindo-se mais credibilidades àquelas de acesso difícil, arriscado e caro, confundindo o método com o produto ou o segredo com o conhecimento[188].

Ainda que subutilizadas, há muito agências de aplicação da lei planejam, preparam, coletam e produzem inteligências a partir de informações publicamente disponíveis e em fontes abertas para adquirir conhecimento.[189] Considerada um mosaico de inteligências, fontes abertas são um combinado de "segredos roubados, relatórios diplomáticos e coleção técnica"[190]. Com o passar do tempo, a coleta de informações passou de encontros fortuitos com pessoas de carne e osso para a coleta abrangente e indiscriminada de dados na internet, cuja disponibilidade é cada vez mais crescente em decorrência da combinação dos avanços tecnológicos e comerciais.

O conceito de inteligência de fonte aberta segue a definição atribuída pelo FBI e incorporada pelos Estados Unidos na Secção 931 da Lei Pública 161309[191]: inteligência produzida de informação publicamente disponível, coletada, explorada e disseminada de forma oportuna para uma audiência apropriada com o objetivo de alcançar inteligência específica e informação. Trata-se de inteligência baseada nas informações que estão disponíveis livremente a partir de fontes públicas, como jornais, revistas, críticas, rádio, telejornais, e, o que é mais comum nos dias atuais, em redes sociais e internet[192]. Pode ser informação obtida através de transmissões estrangeiras, documentos oficiais publicamente disponíveis ou na *web*[193].

Contudo, ainda que informações de fontes abertas possam ser publicamente disponíveis, a recíproca não é verdadeira: nem toda informação publicamente disponível é de fonte aberta. Informações publicamente disponíveis são dados, fatos, instruções ou outros materiais publicados, ou transmitidos para o consumo do público geral; disponível mediante

---

[187] WILLIANS. Heather J; BLUM, Ilana. **Defining second generation Open Source Intelligence (OSINT) for the Defense Enterprise**. National Defense Research Institute. Santa Mônica: RAND Corporation, 2018. p. 21.
[188] SCHAUER, Florian; STöRGER, Jan. The Evolution of Open Source Intelligence (OSINT). **Journal of U.S. Intelligence Studies**, v. 19, n. 3, 2013. p 53-54.
[189] STANIFORTH, Andrew. Police Use of Open Source Intelligence: the longer arm of law. *In*: AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 21-31.
[190] SMITH, Russel Jack. **The Unknow CIA: My Three Decades With the Agency.** Pergamon-Brassey's, 1989.
[191] WILLIANS. Heather J; BLUM, Ilana. **Defining second generation Open Source Intelligence (OSINT) for the Defense Enterprise**. National Defense Research Institute. Santa Mônica: RAND Corporation. 2018. p. 21.
[192] AKHGAR, Babak. OSINT as an integral part of the National Security Apparatus. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 5.
[193] BAZZEL, Michael. **Open Source Intelligence Techniques**: resources for searching and analyzing online information. 6th ed. [*S. l.*: *s. n.*], 2016.

requerimento para um membro do público geral; legalmente visto ou ouvido por qualquer observador casual, ou disponibilizado em reunião aberta para o público geral.

O Manual de Osint, da Organização do Tratado do Atlântico Norte (Otan), divide informações e inteligência de fonte aberta em quatro categorias: dados de fonte aberta, informações de fonte aberta, inteligência de fonte aberta e inteligência de fonte aberta validada. Para sua utilização no exercício do controle punitivo, defende a utilização da categoria inteligência de fonte aberta, assim entendida como uma informação deliberadamente revelada pelo seu titular, discriminada, destilada e disseminada para um público seleto, de forma a responder a uma questão específica e sob a qual poder-se-ia "atribuir um elevado grau de certeza"[194]. Advém de pessoa ou grupo que fornece informações sem expectativas de privacidade – a informação, a relação, ou ambos, não são protegidos do conhecimento público – e pode ser proveniente de inteligência humana, sinais, comunicações, imagens, medida e sinais, telemetria e eletrônica[195], as conhecidas "disciplinas de coleção de inteligência", que nada mais são do que as formas da reunião de inteligência. Como as disciplinas de inteligência são definidas é uma importante questão, porque as definições, além de ditarem como a informação é tratada, também faz os profissionais da inteligência tenderem a pensá-las como únicas e distintas, ao passo que uma estrutura mais eficaz tende a vê-las como sobrepostas: disciplinas de coletas de informações raramente são independentes, e as definições são por vezes conduzidas mais pelas autoridades reguladoras das agências do que por diferenças distintas entre os métodos de coleta ou do próprio material[196].

Caracterizam-se por serem acessíveis, onipresentes e valiosas e, atualmente, são a fonte de inteligência utilizada como recurso em todas as fases no ciclo de produção de inteligência, talvez a arma mais útil para um investigador, acima de todas as outras fontes e todas as outras inteligências. Com a vida *online,* estima-se que entre 80% a 95% de toda a

[194] GIBSON, Helen. Acquisition and Preparation of data for OSINT Investigations. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 69-93.
[195] STANIFORTH, Andrew. Police Use of Open Source Intelligence: The Longer Armo f Law. *In*: AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 21-31
[196] WILLIANS. Heather J; BLUM, Ilana. **Defining second generation Open Source Intelligence (OSINT) for the Defense Enterprise**. National Defense Research Institute. Santa Mônica: RAND Corporation, 2018. p. 21-22.

informação usada pela comunidade de inteligência venha de fontes abertas, inclusive na luta contra o crime e o terrorismo[197].

Um *player* relevante nesse mercado é a Cellebrite, fornecedora líder em soluções de inteligência digital e que se anuncia como provedora de "inteligência digital para um mundo mais seguro" e a "única empresa capaz de fornecer às equipes investigativas uma solução abrangente de inteligência digital para a coleta, colaboração e análise de dados digitais de uma linha completa de fontes". Líder global no setor com mais de 60 mil licenças implementadas em 150 países, oferece às forças da lei, da área militar, de inteligência e de empreendedores soluções para perícias forenses, triagens e análises digitais, ajudando a que se concentrem menos na coleta de informações e mais em análises aprofundadas e descoberta de elementos úteis a uma investigação**.**

Reconhecendo o crescente papel da tecnologia da informação em investigações, produz soluções tecnológicas com o objetivo de tornar dados acessíveis, colaborativos e acionáveis. Uma delas, lançada em 2017, permite coleta, preservação e análise em tempo real de dados de domínio público, incluindo informações de localização, perfis, imagens, arquivos e comunicações dos aplicativos de redes sociais mais populares. O Ufed Cloud Analyzer oferece ao usuário acesso imediato e análise de "provas digitais irrefutáveis" de fontes em nuvens de domínio público, com pesquisa e coleta integradas que economizam tempo à equipes de investigação e demais profissionais envolvidos, além de eliminar o processo manual de pesquisa e captura de evidências em diversos locais**.**

Segundo a Cellebrite, inserir técnicas informatizadas de pesquisa em dados de domínio público permite à investigação acessar e compartilhar "provas" com a geração de relatórios dinâmicos e de simples manuseio, além de viabilizar acesso a recursos de exame de textos e imagens, reduzindo custos e riscos enquanto se aperfeiçoa o fluxo de trabalho e se reduz o tempo para "produzir as provas"**.** Para a empresa, o volume de evidências potenciais armazenadas em fontes abertas é produto do crescimento exponencial da popularidade e adesão às redes sociais, aplicativos de mensagens e outros aplicativos móveis públicos. Extrair e visualizar dados disponíveis publicamente permitem rastrear comportamentos, revelar conexões comuns e correlacionar "provas críticas"[198]**.**

---

[197] GIBSON, Helen. Acquisition and Preparation of data for OSINT Investigations. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 69-93.

[198] UFED Cloud Analyzer. **Cellebrite**. Disponível em: https://cellebrite.com/pt/a-cellebrite-lanca-uma-ferramenta-para-extracao-de-dados-de-midias-sociais-de-dominio-publico-com-solidez-forense/. Acesso em: 12 ago. 2022.

O domínio sobre técnicas de Osint não apenas estão a serviço e podem ser utilizados pelos órgãos a serviço da persecução penal: são ferramentas que podem auxiliar todas as partes da investigação ou processo na tomada de decisões estratégicas em busca da confirmação de suas hipóteses. Como está baseado em técnicas e ferramentas para a obtenção lícita de informações por intermédio de dados públicos ou publicados na internet – a *priori*, inteligência em fontes abertas não envolve *hacking* ou invasão ilícita em contas de redes sociais, *e-mails*, computadores ou celulares, práticas que encontram limites constitucionais e infraconstitucionais[199] –, esse tipo de inteligência está sendo cada vez mais útil na tomada de decisões estratégicas em várias esferas, públicas e privada.

É um recurso de interesse de ambos os setores; não apenas autoridades oficiais lucram com os resultados da inteligência de fontes abertas: é um agente que gera dados acessíveis a todos, pois contribuem para alimentar a internet com informações valiosas e importantes. O *site* Global Market Insights: Insights to Innovation publicou pesquisa apontando que o tamanho do mercado da indústria de inteligência de fontes abertas, que cresceu exponencialmente em razão da pandemia de Covid-19, ultrapassou a cifra de US$ 5 bilhões em 2020, e projetam-se lucros de mais de 25% entre 2021 e 2027, em razão do crescente aumento da procura por coleta de dados de fontes publicamente disponíveis para obter *insights* e permitir que organizações compreendam melhor as estratégias adotadas por rivais e tomem contramedidas.[200]

Nesse contexto, as inteligências de fontes abertas são apresentadas como grande instrumento a favor dos agentes privados, dado que, livremente dispostas ao público na internet, a obtenção desses dados não apresenta obstáculos geográficos e não afeta direitos fundamentais. Esse tipo de atuação pode não apenas fomentar a apresentação de notícias de fatos, instrumentalizar queixas, fazer com que as partes, em qualquer polo de atuação, apresentem essas evidências digitais juntamente com as suas alegações, mas também viabilizar a produção de fontes de prova de forma com que, a partir desses elementos, proponha-se, em juízo, a produção de outras, como prova testemunhal, documental ou pericial.[201]

A categoria está legitimada no pressuposto de que o próprio titular consente com a

---

[199] NICOLITT, André. Prova ilícita, hackeamento, incompetência e suspeição: as subversões de Ferrajoli. **Revista Brasileira de Ciências Criminais**, São Paulo, ano 29, v. 184, p. 141-159, outubro de 2021.
[200] INDUSTRY Trends. **GMI – Global Market Insights**. Disponível em: https://www.gminsights.com/industry-analysis/open-source-intelligence-osint-market? ref=hackernoon.com. Acesso em: 25 abr. 2022.
[201] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 221-224.

inserção de seus dados na internet ou nas redes sociais, de forma que independe de autorização judicial para que se acesse aquilo que já é público (SSTS 236/2008; 292/2008 e 776/2008): informações de postagens estão sujeitas aos termos de uso e privacidade impostos pelos provedores de serviços das plataformas que os usuários se valem para registrar e publicar sua informação. Quando alguém lança na rede mundial dos computadores elementos que qualquer usuário pode ter acesso, esse consentimento tácito não representa afetação à intimidade, à proteção de dados pessoais ou ao segredo das comunicações, mormente quando os dados objetos de análise tenham sido obtidos de forma legítima e integrados a arquivos que tenham obedecido todas as normas de proteção a dados pessoais[202].

3.7. Inteligência em fontes abertas: uma breve gênese

A gênese do Open Source Intelligence (Osint) como categoria remonta ao surgimento da inteligência como instrumento de apoio às decisões e ações de um governo. O embrião da técnica teria surgido no final da década de 1930, mas foram os trabalhos desenvolvidos na Universidade de Princeton para monitorar, gravar, traduzir, transcrever e analisar programas de rádio de propaganda em ondas curtas que estavam sendo transmitidos nos Estados Unidos pelas potências do Eixo, em que se começou a empregar o rádio como uma fonte primária de inteligência, ganhando impulso e importância definitivos após o ataque japonês a Pearl Harbor[203], quando o sistema passa a se chamar Foreign Broadcast Intelligence Service (FBIS)[204], pioneiro na institucionalização e profissionalização de capacidade autônoma de monitoramento da mídia estrangeira.

Logo, a palavra impressa entrou no rol de atenção de agências de inteligência, a exemplo da criação, nos Estados Unidos, do Comitê Interdepartamental para Aquisição de Periódicos Estrangeiros, com objetivo de formar uma rede global de coleta e reunião de publicações que trouxessem ao governo informações estrangeiras ou, na Inglaterra, do *Digest of Foreign Broadcasts*, posteriormente nomeado como *Summary of World Broadcasts* e, agora, conhecido como *BBC Monitoring*, serviço civil, e mais tarde comercial, de escrutínio

---

[202] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p.157-158; p. 174-175.

[203] SCHAURER, Florian; STöRGER, Jan. The Evolution of Open Source Intelligence (OSINT). **Journal of U.S. Intelligence Studies**, v. 19 n. 3, p. 53-56, 2013. p 53. Disponível em: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-48-no-3/sailing-the-sea-of-osint-in-the-information-age/. Acesso em: 20 abr. 2022.

[204] WILLIANS. Heather J; BLUM, Ilana. **Defining second generation Open Source Intelligence (OSINT) for the Defense Enterprise**. National Defense Research Institute. Santa Mônica: RAND Corporation, 2018. p. 4.

do jornalismo impresso estrangeiro e da radiodifusão solicitado pelo governo britânico à BBC e estabelecido com o declarado objetivo de "erguer uma Torre de Babel moderna, onde, com concentração exemplar, eles ouvem as vozes de amigos e inimigos"[205]. Esses agentes tiveram desempenho em qualidade e quantidade tão boas quanto a dos agentes tradicionais, a ponto de seu trabalho ser reconhecido pelo Escritório de Serviços Estratégicos como indispensáveis e a mais extensa fonte de informação disponível, muitas vezes colaborando com a obtenção de informações mais precisas[206].

Após a Segunda Guerra, quando todas as potências acabaram explorando e desenvolvendo recursos de Osint, a prospecção de dados em fontes abertas seguiu contribuindo com analistas e oficiais, logo encontrando emprego na Guerra Fria[207] e funcionando como parte importante de toda inteligência: mas da mesma forma que auxiliaram a CIA a discernir sinais da cisão Pequim-Moscou a partir da leitura de propagandas do início da década de 1950, analistas do Serviço de Informação de Transmissão Estrangeira (FBIS)[208] e da Divisão de Documentos Estrangeiros (FDD) também se equivocaram ao descartar como desinformação muitas evidências abertas. Independentemente disso, após a Guerra Fria, o valor da inteligência em fontes abertas já estava mais do que evidenciado[209].

O termo Osint teria sido cunhado pela primeira vez no final dos anos 1980 por militares americanos, sustentando a necessidade de uma reforma da inteligência para lidar com a natureza dinâmica das exigências informacionais, sobrevindo, em 1992, a Intelligence Reorganization Act, em que se definiram os objetivos da coleta de informações com base em todas as fontes disponíveis à Comunidade de Inteligência pública e não pública dos EUA: fornecimento de inteligência (i) objetiva; (ii) oportuna: e (iii) livre de preconceitos. A partir de 1994, o serviço de inteligência norte-americano estabeleceu o Community Open Source Program Office (Cospo) e, em 1996, a Comissão Aspin-Brown – instrumento encarregado de revisar "a eficácia e adequação" das atividades de inteligência dos EUA no "ambiente global

---

[205] SCHAURER, Florian; STöRGER, Jan. The Evolution of Open Source Intelligence (OSINT). **Journal of U.S. Intelligence Studies**, v. 19 n. 3, p. 53-56, 2013. p. 53. Disponível em: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-48-no-3/sailing-the-sea-of-osint-in-the-information-age/. Acesso em: 20 abr. 2022.

[206] MERCADO, Stephen C. **Sailing the Sea of OSINT in the Information Age**. p. 1-2. Disponivel em: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-48-no-3/sailing-the-sea-of-osint-in-the-information-age/. Acesso em: 20 abr. 2022.

[207] SCHAURER, Florian; STöRGER, Jan. The Evolution of Open Source Intelligence (OSINT). **Journal of U.S. Intelligence Studies**, v. 19 n. 3, p. 53-56, 2013. p. 53. Disponível em: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-48-no-3/sailing-the-sea-of-osint-in-the-information-age/. Acesso em: 20 abr. 2022.

[208] WILLIANS. Heather J; BLUM, Ilana. **Defining second generation Open Source Intelligence (OSINT) for the Defense Enterprise**. National Defense Research Institute. Santa Mônica: RAND Corporation, 2018. p. 6.

[209] MERCADO, Stephen C. **Sailing the Sea of OSINT in the Information Age**. p. 3-4. Disponivel em: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-48-no-3/sailing-the-sea-of-osint-in-the-information-age/. Acesso em: 20 abr. 2022.

pós-guerra fria" e de apresentar um relatório de suas descobertas e recomendações –[210], ambos esforços voltados para aproveitar o universo de informação agora disponíveis em fontes abertas[211].

No Primeiro Simpósio Internacional sobre Código Aberto, realizado em 1992, líderes das comunidades de inteligência reconheceram que os desafios e dinâmicas do século XXI aumentariam a demanda por Osint, decorrência das mudanças resultantes do aumento da computação pessoal, da grande capacidade de armazenamento digital, dos motores de busca e das redes de comunicação de banda larga, fatores que levariam a um crescimento exponencial na comercialização da informática, caracterizando uma mudança revolucionária na abordagem da comunidade de inteligência à gestão, coleta, processamento e disseminação de código aberto. Vislumbrava-se a transformação das fontes abertas em "discípulo de inteligência de difícil gestão 'altamente estruturadas'", mas, até 2004, ainda era uma disciplina ainda não fortemente integrada, diversificada e descentralizada, espalhada por toda a extensão e profundidade da comunidade. A comunidade de inteligência ainda desconfiava de suas próprias explorações e capacidades não classificadas, seus recursos eram sub-representados e subfinanciados, além de reconhecer deficiências na política externa de fonte aberta, formação, gestão, elementos que levaram à criação do Defense Open Source Council[212], principal mecanismo governamental para o uso de Osint[213].

O 11 de setembro provou ser um divisor de águas para Osint, com a criação da Comissão 09/11 (*National Commission on Terrorist Attacks Upon the United States*)[214], que, em 2004, recomendou a criação de uma Agência de Código Aberto, conceito retomado em

---

[210] "Preparing for the 21st Century: An Appraisal of U.S. Intelligence: The Intelligence Authorization Act for Fiscal Year 1995 (P.L. 103-359) created the Commission on the Roles and Capabilities of the United States Intelligence Community. This bipartisan panel was charged with reviewing "the efficacy and appropriateness" of U.S. intelligence activities in the 'post-cold war global environment' and with submitting a report of its findings and recommendations to the President and the Congress. The Commission's report, 'Preparing for the 21st Century: An Appraisal of U.S. Intelligence', was released on March 1, 1996. It addresses such issues as the size and secrecy of the intelligence budget; the organization of U.S. Intelligence Community; management of the CIA; covert action; economic intelligence; intelligence support to policy makers and military operations; space reconnaissance; 'right-sizing' intelligence agencies; and oversight of intelligence" (ESTADOS UNIDOS DA AMÉRICA. United States Government Publishing Office (GPO) – GovInfo. **Content Details –** Preparing for the 21st Century: An Appraisal of U.S. Intelligence. Disponível em: https://www.govinfo.gov/app/details/GPO-INTELLIGENCE/. Acesso em: 17 abr. 2022).

[211]SCHAURER, Florian; STöRGER, Jan. The Evolution of Open Source Intelligence (OSINT). **Journal of U.S. Intelligence Studies**, v. 19 n. 3, p. 53-56, 2013. p. 54. Disponível em: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-48-no-3/sailing-the-sea-of-osint-in-the-information-age/. Acesso em: 20 abr. 2022.

[212] ESTADOS UNIDOS DA AMÉRICA. Departament of Defense. **Instruction Number 3115.12**. Disponível em: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/311512p.pdf?ver= 2019-03-06-093811-687. Acesso em: 22 abr. 2022.

[213] WILLIANS. Heather J; BLUM, Ilana. **Defining second generation Open Source Intelligence (OSINT) for the Defense Enterprise**. National Defense Research Institute. Santa Mônica: RAND Corporation. 2018. p. 7.

[214] Disponível em: https://www.9-11commission.gov/. Acesso em: 20 abr. 2022.

2005 com as recomendações da *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Comissão *World News Collection*)[215], provendo as necessidades do governo americano em inteligência de código aberto sobre questões políticas, militares, econômicas e técnicas estrangeiras, além da mídia habitual de um universo em expansão[216]. O atentado demonstrou que os Estados Unidos colhiam dados de tudo que contivesse palavras como bomba, terrorismo, martírio, atentado e outras, produzindo uma vasta imensidão de dados que dificultava o trabalho dos analistas, que não conseguiam processar tudo em tempo hábil e oportuno[217].

A internet mudou muito no mesmo período. Conteúdos *online* mudam para páginas *web* dinâmicas, expressão da introspecção, na rede, de conteúdo gerado pelo próprio utilizador e da profusão das plataformas de comunicação social como Facebook.com (2004), YouTube.com (2005) e Twitter (2006), transição descrita como a *emergência da Web* 2.0[218], termo popularizado na Conferência *Web* 2.0. A virada para a chamada *segunda geração da Osint* ocorre em 2005, com a criação do *Open Source Center*, cumprindo requisito estabelecido pelo *Intelligence Reform and Terrorism Prevention Act,* de 2004, que exigiu a criação de um centro de inteligência destinado – para além da coleta, análise, produção e disseminação de inteligência de código aberto – à formação em exploração e análise, desenvolvimento de ferramentas e testagem de novas tecnologias relacionadas às *fontes abertas*, órgão que passou a se chamar *Open Source Enterprise* em 2015[219].

Em 2018, o Chefe da Equipe de Inteligência e Análise de Código Aberto do Exército para Inteligência, que atua sob a supervisão do *National Open Source Committee* e o *Defense Open Source Council*, reconheceu a evolução e a expansão do papel da inteligência a partir da inclusão da melhoria de condições de trabalho em torno das fontes abertas, anunciando um novo ponto de inflexão para a próxima evolução em *Open Source Intelligence* em razão da

---

[215] THE WMD COMMISSION REPORT. **Final Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction**. Disponível em: https://irp.fas.org/offdocs/wmdcomm.html. Acesso em: 25 abr. 2022.

[216] SCHAURER, Florian; STöRGER, Jan. The Evolution of Open Source Intelligence (OSINT). **Journal of U.S. Intelligence Studies**, v. 19 n. 3, p. 53-56, 2013. p 54. Disponível em: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-48-no-3/sailing-the-sea-of-osint-in-the-information-age/. Acesso em: 20 abr. 2022.

[217] LEITE, Sara Souza. O Emprego das Fontes abertas no Âmbito da Atividade de Inteligência Policial. **Revista Brasileira de Ciências Policiais**, Brasília, v. 5, n. 1, p. 11-45, jan/jun 2014. p 23-24.

[218] A Web 2.0 é um termo criado pela empresa americana O'Reilly Media em 2004 para designar o conceito da web enquanto plataforma, manifestação da segunda fase da evolução da internet que trouxe (i) a interação entre pessoas para o ambiente *online*, mudando a forma como os usuários o utilizavam e (ii) *softwares* colaborativos para criação de conteúdo, redes sociais, *blogs* e a tecnologia de informação, alterando a condição dos usuários: eles deixam de ser apenas espectadores e passam a interagir, produzir conteúdo e se comunicar com pessoas.

[219] WILLIANS. Heather J; BLUM, Ilana. **Defining second generation Open Source Intelligence (OSINT) for the Defense Enterprise**. National Defense Research Institute. Santa Mônica: RAND Corporation, 2018. p. 1-6.

própria evolução ambiental em torno do *big data*, de *Data Science* e da Inteligência Artificial: o futuro será impactado pela IA e seus derivados, aumentando capacidades de análises preditivas, e as fontes abertas surgem como fonte de informações incompreensivelmente grande, com comprovado valor de inteligência. A integração das comunidades de ciência e tecnologia relacionadas à Inteligência Artificial irão apenas aumentar e melhorar, alcançando às populações e aos Estados-nação meios cada vez mais poderosos para compartilhar, manipular e gerar informações publicamente disponíveis.[220]

A prevalência do uso da Osint no sistema de Justiça criminal e agências de aplicação da lei se desenvolvem no atual cenário de grandes problemas ao redor do globo (Nova Iorque, Paris, Bruxelas, Nice, Munique), incluindo não apenas terrorismo, crime organizado e ataques cibernéticos, mas também desastres naturais e acidentes em grandes escalas, os quais podem causar inexplicáveis abalos aos cidadãos, comunidades, serviços públicos, negócios e economia. O ponto comum entre muitos desses ataques são a utilização de plataformas e aplicações baseadas na internet por grupos terroristas ou indivíduos. Redes sociais tornaram-se a plataforma predileta de entidades criminosas para a promoção, disseminação, doutrinação metodológica, recrutamento, formação de cartéis ou transferência ilícita de informações e valores para o financiamento de operações ilícitas por organizações em detrimento de sujeitos ou organizações vulneráveis[221].

Osint já vem sendo utilizada como uma das fontes-chave de inteligência para segurança nacional, mas sua abrangência está transcendendo os limites da prevenção, já que a amplitude de seus usos atuais e potenciais é enorme, ainda que não possa e nem deva ser a única fonte de inteligência com a qual se deva contar: ela torna-se ainda mais poderosa quando capaz de fornecer informações adicionais e novas direções se associada à inteligência obtida em fontes fechadas. Existe uma abordagem que combina a colaboração de soluções eficientes e inovadoras de Osint e se baseia em na reunião entre governo e setor privado,

---

[220] "*We are at the tipping point for the next evolution in Open Source Intelligence described by environmental terms such as Big Data, Data Science, and Artificial Intelligence (AI). Our future will be impacted by AI—that derivative of AI—machine learning—enables us to perform predictive analysis. This environment is an unfathomably large, yet proven, source of information containing immense intelligence value. We are making efforts to better integrate with the science and technology communities that relate to AI. Rapid improvements in technology enable populations and nation states with an increasingly more powerful means to share, manipulate, and generate publicly available information. The National Open Source Committee and Defense Open Source Council offer the intelligence and defense communities an enterprise solution by providing tools, training and promoting information sharing*" (ROBLES. Victor M. (*executive insight – chief*). Open Source Intelligence & Analytics Team, rmy G-2 for Intelligence. **Digital Government Institute**. Disponível em: https://digitalgovernment.com/tags/defense-open-source-council/. Acesso em: 22 abr. 2022).

[221] AKHGAR, Babak. OSINT as an integral part of the National Security Apparatus. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 3-4.

incluindo as agências de controle, indústria e academia.

Somados a níveis de incerteza econômica e instabilidade política, defende-se que governos devem estar preparados para responder a ataques de forma rápida e eficaz, fazendo com que, desde 11 de setembro de 2001, haja uma mudança na utilização e na importância da inteligência de fontes abertas na proteção da segurança nacional.[222] Sua utilização vem sendo apresentada como elemento hábil para a tomada de decisões necessárias em crises, humanitárias ou emergenciais e em áreas relacionadas à atuação do crime organizado e terrorismo.[223] Sob a perspectiva de segurança nacional, justifica-se que soluções baseadas em inteligência de fontes abertas podem melhorar a capacidade de atuação das agências do sistema de Justiça e dos serviços de segurança, ofertando acesso a outros tipos de inteligência que podem fornecer suporte às atividades de coordenação e tomada de decisões estratégicas, cujo eixo central deve estar ancorado na coleta e exploração de dados existentes no ambiente de internet, o que inclui o desenvolvimento de aplicações (recursos e serviços) aprimoradas para reunir, analisar, visualizar e combinar dados relevantes para cada hipótese.[224]

A metodologia de análise de todas as fontes em torno de um determinado alvo ou evento para estabelecer seu contexto, cronologia e/ou participantes foi popularizada pelo grupo *Bellingcat*, criado em julho de 2014 por Eliot Higgins, que se esmerou na análise de dados relativos à destruição do voo MH17 da Malaysian Airlines, abatido em 17 de julho do mesmo ano, e que apontou para o envolvimento de sistemas russos na destruição do dispositivo. Mais tarde, o grupo civil identificou o envolvimento de agentes do serviço de inteligência militar russo no envenenamento do ex-agente Sergei Skripal e de sua filha Elena em 2018, assim como foi fonte determinante de informações no conflito entre Rússia e Ucrânia no ano de 2022[225], mapeando incidentes de danos civis na Ucrânia[226], documentando os tipos de munições utilizadas no conflito[227], rastreando o uso de munições em áreas civis[228]

---

[222] STAINFORTH, Andrew. Open Source Intelligence and the Protection of National Security. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation: from strategy to implementation**. Genebra: Springer, 2016. p. 11-20.

[223] MARZELL, Laurence. OSINT as a part of the Strategic National Security Landscape. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 33-34.

[224] AKHGAR, Babak. OSINT as an integral part of the National Security Apparatus. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 7.

[225] BELL¿NGCAT. Disponível em: https://www.bellingcat.com/. Acesso em: 14 abr. 2022.

[226] HOSPITALS Bombed and Apartments Destroyed: Mapping Incidents of Civilian Harm in Ukraine. **Bell¿ngcat**. Disponível em: https://www.bellingcat.com/news/2022/03/17/hospitals-bombed-and-apartments-destroyed-mapping-incidents-of-civilian-harm-in-ukraine/. Acesso em: 14 abr. 2022.

[227] HIGGINS, Eliot. These are the Cluster Munitions Documented by Ukrainian Civilians. **Bell¿ngcat**. Disponível em: https://www.bellingcat.com/news/rest-of-world/2022/03/11/these-are-the-cluster-munitions-documented-by-ukrainian-civilians/. Acesso em: 14 abr. 2022.

ou acompanhando o deslocamento e os conflitos entre tropas russas e ucranianas[229].

A atividade está a se tornar cada vez mais complexa, tanto em termos de fontes como de métodos.[230] Em torno dos indícios, cria-se uma difusa rede de vigilância voltada à tomada de decisões estratégicas com mapeamento dos riscos, produto da interdependência de agências públicas e *players* pertencentes ao mercado privado, refundando uma política criminal atuarial focada em prevenção, a partir da análise de individualizados formados com base em dados recolhidos em diversos bancos.[231] Insiste-se em um determinismo comportamental em torno de indícios e rastros, em que o corpo é visto como fonte de dados, dividido em partes, para que possam ser analisados, ordenados e classificados, para que possam ser estruturados perfis de risco ou técnicas preditivas mais com base nos rastros deixados no passado do que em fatos presentes, ignorando motivações pessoais ou causas sociais.[232]

3.8. Metodologia de trabalho e ferramentas

A metodologia de trabalho da inteligência de fontes abertas divide-se entre a fase de coleta, a fase de análise e o processo de extração de conhecimento. Na primeira etapa, chamada de coleção, fixado o alvo ou objetivo, dados publicamente disponíveis são extraídos de fontes abertas relevantes para a geração de inteligência, em que a internet, em razão do volume de material disponibilizado e do fácil acesso, funciona como recurso de excelência. Na segunda, uma vez coletada a matéria-prima, ela é tratada para gerar informações; dados, por si só, não são úteis, motivo pelos quais incide, neste momento,

---

[228] INVASION of Ukraine: Tracking use of Cluster Munitions in Civilian Areas. **Bell¿ngcat**. Disponível em: https://www.bellingcat.com/news/2022/02/27/ukraine-conflict-tracking-use-of-cluster-munitions-in-civilian-areas/. Acesso em: 14 abr. 2022.

[229] "*The Russia-Ukraine Monitor Map is a crowdsourced effort by the Center for Information Resilience (CIR) and the wider open source community to map, document and verify significant incidents during the conflict in Ukraine. Its aim is to provide reliable information for policymakers, journalists as well as justice and accountability bodies about the evolving situations both on-the-ground and online. Bellingcat and the Conflict Intelligence Team have also begun to contribute to the map in recent days. All content reviewed for this project has been collected and submitted to Mnemonic for preservation*" (TRICK, Benjamin. Follow the Russia-Ukraine Monitor Map. **Bell¿ngcat**. Disponível em: https://www.bellingcat.com/news/2022/02/27/follow-the-russia-ukraine-monitor-map/. Acesso em: 14 abr. 2022).

[230] WILLIANS. Heather J; BLUM, Ilana. Defining second generation Open Source Intelligence (OSINT) for the Defense Enterprise. **National Defense Research Institute**. Santa Mônica: RAND Corporation. 2018. p. 1-6.

[231] DIETER, Maurício Stegemann. **Política Criminal Atuarial: a criminologia do fim da História.** 2012. (Doutorado – Direito do Estado) – Programa de Pós-Graduação da Faculdade de Direito da Universidade Federal do Paraná, Curitiba: UFPR. 2012. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/28416/R%20-%20T%20-%20MAURICIO%20STEGEMANN%20DIETER.pdf?sequence=1. Acesso em: 30 dez. 2021.

[232] PITCH, Tamar. **La sociedad de la prevención.** Buenos Aires: Ad Hoc, 2009. 151-154.

interpretação humana. Daí advém a extração do conhecimento, na terceira etapa, em que a informação é tomada como entrada para sofisticados algoritmos de inferência projetados em razão dos avanços computacionais, possibilitando a detecção de padrões, perfis de comportamento, a previsão de valores ou correlacionar eventos.[233]

Antes das etapas de análise e extração de inteligência, o investigador precisa expandir o conjunto de dados sobre o alvo, considerando técnicas de *mecanismos de pesquisa, redes sociais, endereço de e-mail, nome de usuário, nome real, localização, endereço IP* e *nome de domínio*, cada qual com inúmeras ferramentas disponíveis na rede mundial para a coleta de dados a partir de um único dado atômico sobre esse alvo. A partir do resultado da consulta inicial, podem surgir novos dados que demandam diferentes técnicas para obter mais dados. Essas transações, que fomentam a propagação da investigação e representam a etapa de coleção, são conhecidas como *transferência de dados*, em que a saída (*output*) da técnica de origem torna-se a entrada (*input*) para alimentar a técnica de destino.[234]

Proliferam-se nas redes ferramentas de exploração da informação em fontes abertas através de processos de indexação voltado a exibir, com resposta rápida ao usuário, um índice do conteúdo verificado sobre a informação buscada. Os mais comuns, conhecidos e mundialmente utilizados são os *motores de busca*, forma mais rudimentar de aplicação de inteligência de fontes abertas. Outros motores são concebidos para territórios específicos[235] ou, ainda, projetados para navegação na *dark web*, onde têm lugar investigações contra o tráfico de drogas, pornografia infantil, venda de armas ou terrorismo.

O Google, por exemplo, reúne informações de muitas fontes diferentes, incluindo páginas da *web*; conteúdo enviado pelo usuário, como envios ao Google Meu Negócio e ao Google Maps, livros digitalizados, bancos de dados públicos na internet e “muitas outras

---

[233] PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access**, v. 8, p. 10282-10304, 9 jan. 2020. DOI: 10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/8954668. Acesso em: 24 fev. 2022.

[234] PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access**, v. 8, p. 10282-10304, 9 jan. 2020. DOI: 10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/8954668. Acesso em: 24 fev. 2022.

[235] *Yandex* (Rússia e na Europa Oriental) implementa operadores de pesquisa para restringir a pesquisa por URL, tipo de arquivo, idioma, data e assim por diante. *O Baidu* (Ásia) inclui não apenas a barra de pesquisa de palavras-chave típica, mas recursos adicionais, como uma rede social, uma seção de perguntas e respostas, uma biblioteca virtual ou uma enciclopédia. *Yamli* ou *Eiktub* (comunidade árabe), mas bem empregados, interessante somente em investigações sobre pessoas, grupos e empresas pertencentes a comunidades específicas (PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access**, v. 8, p. 10282-10304, 9 jan. 2020. DOI: 10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/ 8954668. Acesso em: 24 fev. 2022).

fontes", seguindo três etapas para gerar resultados das páginas da *web*: (i) rastreamento: quanto melhor a máquina entender o *site*, mais conseguirá levar seu conteúdo até as pessoas que estão à procura dele[236]; (ii) indexação: identificar o conteúdo da informação registrada no índice do Google, um grande banco de dados armazenado em uma quantidade enorme de computadores[237]; (iii) exibição e classificação: encontrar a resposta mais relevante no próprio índice com base em fatores como localização, idioma e dispositivo (computador ou *smartphone*)[238].

Promovem busca de informações na rede mundial dos computadores a partir de uma consulta textual que corresponda à entrada, retornando informações ao usuário. Devido à quantidade de número de resultados possíveis, pode até ser contraproducente para o usuário se não souber especificar as solicitações dentro do mecanismo de busca conforme o resultado desejado[239]. O Google ou Bing suportam filtros para refinar pesquisas e recuperar exatamente o tipo de informação buscada; já o Yahoo não permite filtros específicos, mas permite restringir a data, idioma ou país dos resultados. O mecanismo de pesquisa DuckDuckGo viabiliza uma abordagem de preservação da privacidade, pois não rastreia o usuário nem direciona o endereço IP ou o histórico de pesquisa, mas torna as descobertas homogêneas para os usuários, independentemente de hábitos, preferências, localização ou histórico de pesquisa.

Além dos buscadores conhecidos do grande público, existem os metabuscadores, ferramentas altamente avançadas, personalizadas ou segmentadas por especialidades

---

[236] Procedimento baseado em pesquisa constante de novas páginas e adição à própria lista de páginas conhecidas; além disso, algumas são detectadas quando o proprietário de um *site* envia um *sitemap* (lista de páginas) para o Google rastrear. Com um host da web gerenciado, é possível solicitar ao Google que rastreie todas as suas páginas novas ou atualizadas. Depois que o buscador descobre o URL de uma página, ele visita ou *rastreia* a página para descobrir o que há nela, renderiza a página e analisa o conteúdo textual e não textual, e o layout para decidir a posição que aparecerá nos resultados da pesquisa (COMO funciona a Pesquisa Google (para iniciantes). **Google**. Disponível em: https://developers.google.com/search/docs/beginner/how-search-works#:~:text=they're%20 wrong.-,Indexing,tries%20to%20understand%20the%20page. Acesso em: 26 out. 2021).

[237] Depois que descoberta a página, o Google tenta identificar seu conteúdo, que se dá pela análise do conteúdo da página, catalogação de arquivos de imagens e vídeos incorporados e tentativa de identificar sobre o que ela trata. Essa informação fica registrada no índice do Google, um grande banco de dados armazenado em uma quantidade enorme de computadores (COMO funciona a Pesquisa Google (para iniciantes). **Google**. Disponível em: https://developers.google.com/search/docs/beginner/how-search-works#:~:text=they're%20wrong.-,Indexing, tries%20to%20understand%20the%20page. Acesso em: 26 out. 2021).

[238] Quando o usuário faz uma consulta, o Google tenta encontrar a resposta mais relevante no próprio índice com base em vários fatores: tenta determinar as respostas mais adequadas e de qualidade mais alta, bem como avaliar outras considerações que fornecerão a melhor experiência do usuário. Para isso, leva em conta aspectos como localização, idioma e dispositivo (computador ou smartphone). O Google não aceita pagamento para atribuir aos *sites* uma classificação mais alta. A classificação é feita de maneira programática (COMO funciona a Pesquisa Google (para iniciantes). **Google**. Disponível em: https://developers.google.com/search/docs/beginner/how-search-works#:~:text=they're% 20wrong.-,Indexing,tries%20to%20understand%20the%20page. Acesso em: 26 out. 2021).

[239] Para técnicas de refinamento da pesquisa, *vide* BARRETO, Alexandre Gonçalves; WENDT; Emerson. **Inteligência e Investigação Criminal em Fontes Abertas**. Rio de Janeiro: Brasport, 2020. p. 51-59.

(localizar pessoas através de redes sociais; localizar pessoas pela atividade profissional; localizar pessoas desaparecidas; consultar estabelecimentos; monitorar redes sociais e páginas da *web*; localização de videos; acompanhamento de informações sobre transportes; pesquisa de mapas, endereços e rotas; veículos, multas; dados de telefonia fixa e móvel; tribunais e órgãos de justiça; informações policiais; pesquisa de domínios, senhas de *e-mails*…). Metabuscador é um instrumento buscador de buscadores, um portal que se vale de informações de outros portais para selecionar a melhor informação de cada um deles, combinando os melhores dados para responder (*output*) ao impulso lançado pela palavra-chave ou tema (*input*). Sua utilização não é exclusiva no desenvolvimento de uma investigação levada a efeito por inteligência em fontes abertas, mas é apenas mais um recurso disponível a quem emprega esse método para a busca de evidências.[240]

Ainda que nada substitua o circuito humano para analisar e dar sentido ao que seja relevante ou não, dados de fontes abertas podem ser obtidos com pesquisas automatizadas em apoio às pesquisas manuais para auxiliar na rápida reunião de informação; rastreadores digitais, por vezes chamado de *spider*, automatizam processos de busca seguindo *links*, indiscriminadamente ou de acordo com regras predeterminadas. Rastreadores fornecem um bom ponto de partida para investigação por inteligência de fontes abertas, sobretudo quando sobre seu objeto houver significativa quantidade de informações de interesse na rede, mas tempo insuficiente para seguir *links* ou ler páginas para atribuir relevância à informação.

Metadados digitais são etiquetas dentro do HTML – abreviação para a expressão inglesa *HyperText Markup Language*, que significa “Linguagem de Marcação de Hipertexto” – que descrevem o conteúdo da página em um formato específico e permite extrair um título, descrição, autor e mais para o objeto de busca. O Twitter e o Facebook, por exemplo, criaram sus próprias versões de metadados, que podem ser incluídas em páginas conhecidas como *Card Markup*[241] e *Open Graph*[242]. Essas marcações são frequentemente usadas por publicitários tentando promover suas páginas mais eficientemente, mas também possuem importância significativa para investigadores de fontes abertas.

Formas incomuns de recuperar dados, as Interfaces de Programação de Aplicativos fornecem acesso automatizado a seus resultados a partir de uma questão específica. Têm

---

[240] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p.157-158; p. 175-176.

[241] UM dia isto tudo poderá ser seu. **Twitter**. Disponível em: https://dev.twitter.com/cards/markup. Acesso em: 20 abr. 2022.

[242] Disponível em: https://developers.facebook.com/docs/reference/opengraph/. Acesso em: 20 abr. 2022.

barreiras baixas para entrada e possibilitam acesso a dados para um usuário em um formato familiar, que ainda pode ser importado para outras ferramentas, o que as tornam em ferramentas úteis no âmbito da inteligência de fontes abertas. Geralmente demandam registro em uma chave para aquele serviço particular, as quais terão acessos limitados, restringindo o conteúdo de dados em um período específico de tempo.

Uma interface de programação de aplicativos é composta por um conjunto de primitivas que integram a definição e a manipulação de objetos em uma representação compatível com uma linguagem de programação orientada a objetos. Explora recursos básicos de modelos de dados orientados a objetos e baseia-se nas extensões de um metamodelo ancorado em quatro abstrações: classificação, generalização, agregação e composição. Sua implementação sobre um gerenciador relacional emula um gerenciador de dados orientado a objetos.[243]

Na prática, oportunizam a obtenção de dados sobre amigos ou seguidores de determinados usuários, seus *tweets*, o que "favoritaram" ou listas que criaram. O Twitter disponibiliza essa ferramenta, pela qual usuários podem baixar uma proporção significativa de todos *tweets* que mencionam uma palavra-chave ou *hashtag*, podendo ser ainda reduzidos por especificações de geolocalização, sentimento, períodos de tempo e mais[244], havendo, ainda, outras ferramentas, como Exiftool[245], TheHarvester[246], Checker User Name[247].

---

[243] SOUSA, Elaine Parros Machado de. **Emulação de um Gerenciador de Dados Orientado a Objetos através de uma Interface de Programação de Aplicativos sobre um Gerenciador Relacional**. 2020. Dissertação (Mestrado em Ciências de Computação e Matemática Computacional) – Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo – ICMS-USP São Carlos, 2020. Disponível em: https://www.teses.usp.br/teses/disponiveis/55/55134/tde-01072003-163859/publico/Sousa_Mestrado.pdf. Acesso em: 27 ago. 2022.

[244] UM dia isto tudo poderá ser seu. **Twitter**. Disponível em: https://dev.twitter.com/rest/public/search. Acesso em: 22 ago. 2022.

[245] Exiftool é um programa *open source* de leitura e escrita de metadados em arquivos de imagem, vídeo, texto e áudio, com suporte a centenas de extensões. São inúmeras as possibilidades de análise e produção de informações. No que diz respeito aos arquivos em PDF, exemplifica-se com os casos de extração de autos em vários sistemas de processo eletrônico do Poder Judiciário brasileiro: no arquivo baixado, um dos metadados que pode ser visualizado é o registro do nome e número do CPF do usuário responsável pelo *download*. Em relação às fotos, entre informações como modelo de câmera ou smartphone utilizado para obtenção da imagem e variados dados técnicos, destacam-se os dados de geolocalização consistentes em coordenadas de GPS hábeis a identificar de forma precisa o local em que foi registrada a imagem naquele determinado momento.

[246] Ferramenta *open source* (seu código fonte está disponível no repositório GitHub), desenvolvida em Python, que se propõe à coleta e sistematização de dados disponíveis em diferentes fontes públicas como as indexadas pelas ferramentas de busca Google, Bing e DuckDuckGo, além de bases de dados como Shodan, redes sociais como LinkedIn e Twitter, entre outras. Seu escopo atende principalmente profissionais de cibersegurança ofensiva na realização de testes de penetração (*pentesting*), uma vez que, ao reunir diversos dados disponíveis na rede acerca de um domínio, possibilita a produção de informações sobre potenciais cenários de vulnerabilidade e exposição de um alvo. A maior parte dos seus recursos opera de forma passiva, ou seja, não há interação direta com o domínio-alvo. Para fins de investigação, através dela é possível coletar nomes e endereços de *e-mail* de

Twitter Arquivador é um adicional ao Google Sheets que permite buscas e retorná-las em planilhas em forma de tabela com o texto do *tweet*, usuário e nome, data e horário, a identidade do *tweet* e informações básicas do usuário. Similarmente, NodeXL[248] é uma rede que fornece funcionalidade para importar dados diretamente da *Interfaces de Programação de Aplicativos* do Twitter.

Mídias sociais representam, hoje, o tesouro da informação sobre determinados eventos, pessoas e suas relações, ainda que a coleta efetiva e eficiente desses dados não seja uma tarefa simples. Possuem seu próprio acrônimo na família da inteligência, concebido como *Inteligência de Mídias Sociais*, e ganharam expressividade a partir dos tumultos ocorridos em Londres no ano de 2011, que expuseram a ineficácia de determinadas agências em lidar com informações postadas em mídias sociais. Após o evento, o diagnóstico foi de que faltou poder humano, procedimentos e processos para extrair dados de mídias sociais e torná-los em inteligência capaz de auxiliar na compreensão da dinâmica dos tumultos e, por consequência, na proatividade e rapidez das respostas.

Dados pagos: o termo "aberto" em inteligência de fonte aberta não deve ser confundido com gratuidade. Companhias privadas oferecem acesso pago a dados sobre as pessoas, o que, no âmbito da inteligência, fornece vantagens aos investigadores, porque elas já não os controlam ou mesmo têm ciência sobre a sua existência. Isso inclui dados como os Thomson Reuters' World Check[249], que agrega dados de indivíduos considerados de alto risco, como suspeitos de terrorismo ou integrantes do crime organizado. Subconjunto de

---

funcionários da empresa vinculada ao domínio pesquisado, reunir informações sobre sua estrutura organizacional, subdomínios, entre outros.

[247] Considerando a imensurável gama de fontes disponíveis, *softwares* e aplicações que realizam a automação de tarefas otimizam e – por diversas vezes – possibilitam a realização de coletas qualificadas de dados. Para mapeamento de plataformas em que um alvo possa ser titular de um perfil ou conta cadastrada, como Facebook, Reddit, Flickr etc., seria necessário pesquisar manualmente através de nomes de usuário (*usernames*) em centenas de *sites*. Considerando que, comumente, utiliza-se o mesmo nome em diversos cadastros, é possível valer-se de serviços de checagem da disponibilidade de usernames para identificar em quais *sites* o alvo potencialmente possui cadastro. Existem dezenas de ferramentas com funções análogas, de forma que a opção pela exemplificação que segue se deu em face da base de dados da Knowem.com possuir maior variedade de fontes em comparação com as demais. A empresa KnowEm LLC oferece, enquanto serviço, o auxílio a empresas na identificação da disponibilidade de seus nomes na web, com intuito de proteger a marca comercial, além de ajudar em eventuais restituições a *sites* em que houver cadastros indevidos. Dito isso, é importante ter em mente que a ferramenta disponibilizada no *site* da KnowEm não é *open source*, apesar de ser gratuita. Através dela é possível realizar consultas de forma unificada em mais de 500 fontes, em busca de locais da *web* em que o alvo possui perfis.

[248] Disponível em: https://nodexl.codeplex.com/. Acesso em: 13 abr. 2022.

[249] THOMSON Reuters World-Check Uncover Risk. Take Action. **Thomson Reuters** – the answer companhy. Disponível em: https://www.sifma.org/wp-content/uploads/2019/01/Refinitiv-WC_brochure.pdf. Acesso em: 13 abr. 2022.

dados pagos, *dados consentidos*, como os fornecidos por LexisNexis[250], GBG[251], 192.com e Experian[252], exigem pagamento para o acesso de documentos específicos ou uma assinatura que permite um certo número de pesquisas por mês. Contêm informações de empresas, pessoas, números de telefone, endereços, *e-mails* e outras informações pessoais que indivíduos consentem em disponibilizar, razão pela qual podem ser usadas para validar ou estender o conhecimento que se possa ter sobre um alvo de seu interesse.

A *deep web* é o *locus* de conteúdo que não pode ser catalogado pelo Google ou outras ferramentas de busca, incluindo informações provenientes de fóruns, *sites* não acessíveis sem nome de usuário e senha ou páginas com conteúdo gerado dinamicamente; sua parte específica, a *dark web*, apenas pode ser acessada através de navegadores específicos como o Tor[253] ou sistemas operacionais, como o Tails. Estima-se que de 80% a 90% do conteúdo da internet não esteja disponível em ferramentas de busca tradicionais. A prática comum de pesquisa é um modelo que não funciona bem para casos de uso de governos e agências de controle, pois perdem informações na *deep web* e ignoram o conteúdo compartilhado entre as páginas. Vale-se de uma abordagem centralizada que pesquisa na internet com o mesmo conjunto de ferramentas para todas as consultas, além de ser um processo manual que requer a entrada exata do critério de pesquisa, com uma entrada por vez, e que não organiza ou agrega resultados além de uma lista de *links*.

Analisados os dados obtidos pelo manejo das diferentes técnicas de inteligência de fontes abertas, devem eles ser compreendidos para gerar informações valiosas, empregando-se métodos como análise léxica[254], análise semântica[255], análise geoespacial[256] e análise de

---

[250] LexisNexis é uma empresa que fornece pesquisa jurídica assistida por computador, bem como serviços de pesquisa de negócios e gerenciamento de riscos. Disponível em: https://www.tracesmart.co.uk/datasets. Acesso em: 13 abr. 2022.

[251] Global Benefits Group é uma empresa de seguros. Disponível em: https://www.gbgplc.com/uk/products. Acesso em: 13 abr. 2022.

[252] WHO we are. **Experian**. Disponível em: https://www.experianplc.com/. Acesso em: 13 abr. 2022.

[253] TOR Project. Disponível em: www.torproject.org. Acesso em: 13 abr. 2022.

[254] Dados brutos devem ser examinados para extrair entidades e relações do texto. É essencial aplicar processos de tradução ao idioma usado na investigação Osint e filtrar ruídos que não agregam valor de frases que não agregam valor (PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access**, v. 8, p. 10282-10304, 9 jan. 2020. DOI: 10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/8954668. Acesso em: 24 fev. 2022).

[255] Ter um saco de palavras não é útil se o significado não for extraído. Com esse propósito de entender os dados, algoritmos de processamento de linguagem natural estão sendo utilizados atualmente. Além disso, as técnicas de análise de sentimentos permitem a contextualização de postagens ou opiniões subjetivas para classificar o estado emocional do autor (por exemplo, positivo, negativo ou neutro). Finalmente, os procedimentos de descoberta da verdade abordam a desafiadora tarefa de resolver conflitos em dados de várias fontes que se opõem a posições sobre o mesmo assunto (PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access**, v. 8, p. 10282-10304, 9 jan. 2020. DOI:

mídias sociais[257]. O produto dessas técnicas é conhecido como *informações de saída*, normalmente categorizadas em três, mas podendo ser expandidas conforme os diferentes tipos de informações de saída que se complementam: informações pessoais[258], informação organizacional[259] e informações de rede[260].

Decorridas as duas primeiras etapas que atribuem valor às informações coletadas e que levarão a um melhor reconhecimento do alvo, existe a necessidade de tratamento dos resultados de análise (*output info*), o que se faz por intermédio de técnicas de mineração de dados e Inteligência Artificial, que permitem inferir questões abstratas e complexas sobre o alvo, não explicitamente publicadas na rede. São elas: *correlação* de relacionamentos entre pessoas, eventos ou dados em geral para revelar associações não explícitas no conjunto de dados; *classificação* de acordo com categorias predefinidas voltada à organização e à extração de conhecimento de quantidades grandes de informação; *detecção de outlier* ou detecção de anomalias, utilizadas para a observação de comportamento ou ações que diferem dos padrões; *clustering* ou fragmentação de dados em *clusters*, viabilizando considerar diferentes

---

10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/8954668. Acesso em: 24 fev. 2022).

[256] Os dados coletados de redes sociais, eventos, sensores ou endereços IP valem a pena ser analisados a partir de uma perspectiva baseada em localização. Nesse sentido, o uso de mapas ou gráficos facilita a representação e compreensão dos dados, além de extrair conexões significativas entre incidentes ou pessoas (PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access**, v. 8, p. 10282-10304, 9 jan. 2020. DOI: 10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/8954668. Acesso em: 24 fev. 2022).

[257] Os recursos trazidos pelas mídias sociais modernas permitem que os pesquisadores realizem análises aprofundadas dos usuários. Nesse cenário, a análise de dados sociais permite a criação de uma rede de contatos, interações, lugares, comportamentos e gostos em torno do assunto. (PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access**, v. 8, p. 10282-10304, 9 jan. 2020. DOI: 10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/8954668. Acesso em: 24 fev. 2022).

[258] Fundem os detalhes de identidade da pessoa que são obtidos principalmente a partir do nome real, endereço de e-mail, nome de usuário, redes sociais e técnicas de mecanismos de pesquisa. (PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access**, v. 8, p. 10282-10304, 9 jan. 2020. DOI: 10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/8954668. Acesso em: 24 fev. 2022).

[259] É formada por aspectos de uma equipe ou empresa composta por indivíduos. É essencialmente recolhido por meio de redes sociais, motores de busca, técnicas de localização, nome de domínio e endereço IP. PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access,** v. 8, p. 10282-10304, 9 jan. 2020. DOI: 10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/8954668. Acesso em: 24 fev. 2022).

[260] As informações de rede abrangem dados técnicos de sistemas e topologias de comunicação que geralmente são obtidas por meio de técnicas de localização, nome de domínio e endereço IP (PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access**, v. 8, p. 10282-10304, 9 jan. 2020. DOI: 10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/8954668. Acesso em: 24 fev. 2022).

condições ou heurísticas e que auxilia a revelar formas de se comportar na rede, tipos de perfis *online* ou categorizar formas de atacar indivíduos, organizações ou infraestruturas; *regressão* linear, baseada na ideia de redes neurais, que retorna valores numéricos ou fatos que atende a uma função linear e padrões de rastreamento para detectar regularidades nos dados.[261]

Tomada de decisões assertivas evitam o desperdício de oportunidades e favorecem a definição de linhas de investigação. A formulação de hipóteses, técnica reconhecida no meio de investigadores criminais, funciona como ponto de partida, um meio de estabelecer a explicação, a teoria ou a inferência mais lógica ou provável do porquê e como um delito foi praticado, atividade que, entretanto, necessita de material suficiente e confiável nos quais basear-se. O uso de inteligência de fontes abertas garante um novo, rico e detalhado espectro de dados para informar as hipóteses dos investigadores[262], ainda que a inteligência que pode ser desenvolvida no ciberespaço não se limite ao emprego de fontes abertas, já exitindo quem advogue pela criação de uma disciplina de ciberinteligência, mais ampla que a concebida na época da inteligência de código aberto, e que não deveria se limitar à inteligência gerada a partir do ciberespaço[263].

Ao produzir riscos de segurança mesmo enquanto mitigam ou eliminam outros, investigações de código aberto apresentam vários desafios. Embora o acesso ao ciberespaço seja público, suas circunstâncias favorecem o anonimato dos usuários que nele podem interagir, o que pode ter impacto importante.[264] O uso de Osint por agências de inteligência e investigação depende, hoje, do senso ético de quem o opera. Agentes de gerenciamento de governança de inteligência devem zelar pelo uso apropriado e profissional do conjunto e da análise de informações, assim como cumprir com deveres legais e estatutários para

---

[261] PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access**, v. 8, p. 10282-10304, 9 jan. 2020. DOI: 10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/8954668. Acesso em: 24 fev. 2022.

[262] STANIFORTH, Andrew. Police Use of Open Source Intelligence: The Longer Armo f Law. *In*: AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 21-31.

[263] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**, Bogotá, v. 19, n. 36, pp. 1121-1136, outubro-dezembro 2021.

[264] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**, Bogotá, v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.

disponibilizar e compartilhar informações, sobretudo se a intenção da coleta é para que seja utilizada como evidência em procedimentos criminais.[265]

Vale lembrar o que já apontamos: a LGPD regula o tratamento de dados pessoais cujo acesso é público; não proíbe a atividade, mas aponta o dever em se considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização, razão pela qual parece ser necessário que governos tomem uma atitude para garantir maior transparência e responsabilização sobre o uso dessas tecnologias, tanto pelo setor público quanto pelo privado, de forma a garantir o pleno funcionamento das democracias.[266]

[265] STANIFORTH, Andrew. Police Use of Open Source Intelligence: The Longer Armo f Law. *In*: AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 21-31.

[266] HUREL, Louise Marie; FRANCISCO, Pedro Augusto P; TELES, Daisy. **Pegasus, a ponta do iceberg da fragilidade no controle de inteligência**. Disponível em: https://www.fundacaoastrojildo.org.br/pegasus-a-ponta-do-iceberg-da-fragilidade-no-controle-de-inteligencia/. Acesso em: 29 dez. 2021.

4. INTELIGÊNCIA DE FONTES ABERTAS E SEGURANÇA NACIONAL?

4.1. Osint e segurança nacional

Do ponto de vista da *cibersegurança* e da *ciberdefesa*, inteligência de fontes abertas melhoram mecanismos de proteção contra ataques cibernéticos e permitem antecipação estratégica, incluindo o uso de *plugins* para coleta de informações e *machine learning* para análise de sentimentos. Considerando inteligência de fontes abertas como ferramenta fundamental nos modernos Centros de Operações de Segurança, os sistemas de gerenciamento de informações e eventos de segurança (*Security Information and Event Management*) atuais ainda têm limitações nos métodos e meios que usam para coletar eventos, armazenar dados e relatar informações. Esses sistemas formam a espinha dorsal da sociedade digital: desenvolvem papel relevante em infraestruturas de TIC onipresentes e são usados para o seu monitoramento através de sensores e ferramentas para correlacionar eventos obtidos e descobrir ameaças às organizações.

O projeto europeu DiSIEM tem como objetivo a exploração e a integração de fontes de dados das diversas inteligências *Open-source* disponíveis na rede para melhorar a segurança e reagir a vulnerabilidades descobertas na infraestrutura ou prever ameaças emergentes, informações que serão destinadas aos usuários dos referidos sistemas. Visa ao aprimoramento dos sistemas de gerenciamento de informações e eventos de segurança existentes com tecnologia relacionada à diversidade, usando um conjunto de sensores e detectores de anomalias; agregando suporte para coleta de informações de infraestrutura de dados de inteligência de código aberto em fontes da internet; criando vias de visualização das informações coletadas e fornecendo métricas e modelos de segurança para aprimorar tomadas de decisões relacionadas à segurança; viabilizando o uso de nuvens para armazenamento seguro em longo prazo dos eventos.

O Centro de Excelência para Terrorismo, Resiliência, Inteligência e Pesquisa do Crime Organizado (Centric), unidade de pesquisa multidisciplinar com foco em segurança, localizado na Sheffield Hallam University, promete fornecer soluções para desafios contemporâneos de segurança mais urgentes da Europa através de pesquisa inovadora, capacidades tecnológicas avançadas, experiência profissional e treinamento. Desde 2012, atua com o objetivo estratégico em desenvolver e facilitar a colaboração entre cidadãos, órgãos de aplicação da lei, indústria e academia, quatro partes interessadas no domínio da segurança.

Mantém vínculos estreitos com várias agências de controle nacionais e internacionais, grupos de especialistas em segurança e fornecedores de tecnologia líderes em colaboração, assegurando que ofereça "soluções inovadoras informadas pela realidade operacional da aplicação da lei moderna".

Reunindo especialistas em disciplinas como contraterrorismo e radicalização, consciência situacional, gestão de crises e resposta a desastres, inteligência de código aberto, cibercrime e ciberterrorismo, tráfico humano e escravidão moderna, policiamento comunitário, segurança e vigilância fronteiriça, busca oferecer avanços em pesquisa e tecnologia para o domínio da segurança, mantendo habilidades especializadas em áreas como plataformas de consciência situacional, gestão do conhecimento, desenvolvimento de aplicativos móveis, mineração de dados, análise e visualização, *Serious Game Training*, realidade virtual e aumentada.[267]

Também em 2012, envolvendo seis departamentos e agências federais no compromisso com o avanço da ciência da análise de dados, o governo Obama incentivou avanços na análise de dados com o lançamento da "Iniciativa de Pesquisa e Desenvolvimento de *Big Data*", cabendo à *Defense Advanced Research Projects Agency* o desenvolvimento do programa XData, que criaria ferramentas para assimilar e processar montanhas de dados obtidas em diferentes tipos e tamanhos e, em seguida, fornecer formas de visualização para que usuários pudessem estimar tendências e obter valor desses dados.[268]

A *Defense Advanced Research Projects Agency* anuncia como missão "fazer investimentos cruciais em tecnologias inovadoras para a segurança nacional" para colocar os Estados Unidos na condição de iniciador, e não a vítima de surpresas tecnológicas estratégicas, dado o episódio do lançamento do Sputnik em 1957. Seus resultados incluem capacidades militares, armas de precisão, tecnologia furtiva, além de ícones da sociedade moderna, como internet, reconhecimento automatizado de voz e tradução de idiomas e

[267] CIVILnEXT. Disponível em: https://civilnext.eu/. Acesso em: 26 out. 2021.

[268] Conforme Todd Park, assistente do presidente e diretor de tecnologia dos EUA, o governo e militares estão criando montanhas de dados que contém insights poderosos sobre como podemos melhorar nossas operações [...]. Os dados só são úteis, porém, se forem aplicados, e nosso objetivo aqui hoje é construir as ferramentas que podem transformar dados governamentais e militares em um recurso nacional para encontrar eficiências no governo e formas de fortalecer nossa segurança nacional. O Programa XDATA da DARPA e a comunidade de pesquisadores e artistas que eles reuniram serão fundamentais para o avanço do estado da arte em análise de Big Data". Arati Prabhakar, diretor da *Defense Advanced Research Projects Agency*, complementa: "Existem benefícios óbvios de segurança nacional em poder extrair informações significativas dos conjuntos de dados que coletamos [...] O desafio é processar e interagir com esses dados porque há muitos deles. Se pudermos desenvolver as ferramentas computacionais, algoritmos escaláveis e interfaces de usuário intuitivas, as implicações vão muito além do DoD também." (**Extracting Relevance from Mountains of Data**. Disponível em: https://www.darpa.mil/news-events/2013-02-13. Acesso em: 22 fev. 2022).

receptores do Sistema de Posicionamento Global pequenos o suficiente para serem incorporados em inúmeros dispositivos de consumo. Trabalha dentro de um ecossistema de inovação com parceiros acadêmicos, corporativos e governamentais, "com foco constante nos Serviços militares da Nação" para criar oportunidades estratégicas e opções táticas. Compreende aproximadamente 220 funcionários do governo em seis escritórios técnicos, incluindo cerca de 100 gerentes de programa, que juntos supervisionam cerca de 250 programas de pesquisa e desenvolvimento.[269]

Em 2014, anunciou o programa Memex "para avançar no estado da arte em indexação de conteúdo e pesquisa na *web* na Internet" com escopo na produção e desenvolvimento de uma nova geração de tecnologias de busca para "revolucionar a descoberta, organização e apresentação de resultados de busca", objetivando permitir que seus usuários possam "estender o alcance dos recursos de pesquisa atuais e organizar de forma rápida e completa subconjuntos de informações com base em interesses individuais" e que os resultados de suas pesquisas possam ser "imediatamente úteis para domínios e tarefas específicos, e melhorar a capacidade de encontrar e organizar informações de missão crítica publicamente disponíveis na Internet". O programa promove a busca de informações públicas de domínio específico definido pelo usuário e acabou sendo utilizada com sucesso para combater o tráfico de seres humanos.[270]

No início de 2016, o Centric fundou o Osint Hub, espaço físico-virtual para a operacionalização, disseminação e desenvolvimento das suas capacidades adquiridas. Um conjunto de conhecimentos foi introduzido no Hub em razão da colaboração direta entre agências de controle e equipes de investigadores. Nasce da participação centrada em projetos da União Europeia, em colaboração com a aplicação da lei, como um grande parceiro técnico responsável pela entrega do painel de conscientização situacional dos projetos, saliente na *web*, extração de entidades, organização de conteúdo, mídias sociais e funcionalidades de

[269] ABOUT DARPA. **DARPA**. Disponível em: https://www.darpa.mil/about-us/about-darpa. Acesso em: 22 fev. 2022.

[270] O programa Memex recebe seu nome e inspiração de um dispositivo hipotético descrito em "As We May Think", um artigo de 1945 para o The Atlantic Monthly escrito por Vannevar Bush, diretor do Escritório de Pesquisa e Desenvolvimento Científico dos EUA (OSRD) durante a Segunda Guerra Mundial. Concebido como um computador analógico para complementar a memória humana, o memex (uma combinação de "memória" e "índice") armazenaria e faria uma referência cruzada automática de todos os livros, registros e outras informações do usuário. Essa referência cruzada, que Bush chamou de indexação associativa, permitiria aos usuários pesquisar de forma rápida e flexível grandes quantidades de informações e obter *insights* com mais eficiência. O memex pressagiava e encorajava cientistas e engenheiros a criar hipertexto, internet, computadores pessoais, enciclopédias *online* e outros grandes avanços de TI das últimas sete décadas (**MEMEX Aims to Create a New Paradigm for Domain-Specific Search**. Disponível em: https://www.darpa.mil/news-events/2014-02-09. Acesso em: 22 fev. 2022).

agregação de dados – todos construídos sobre ferramentas de última geração oferecidas por provedores líderes, comunidades de código aberto e pesquisas acadêmicas. A ideia de um Hub que não se limita às informações destinadas à seara pública, é a de padronizar a busca de informações e reunir todas as ferramentas necessárias para investigações Osint em um só lugar[271]. Para combater o uso da tecnologia por organizações criminosas e terroristas, autoridades igualmente buscam aproveitar o poder tecnológico.

Em pesquisa realizada com o propósito de demonstrar a utilização de inteligência de fontes abertas em operações de assuntos internos dos Estados tendo como base as organizações espanholas, verificou-se que existem evidências "sutis" que confirmam as que Agências de Aplicação da Lei (LEAs) espanholas valem-se das técnicas. Em 2007, o diretor da Agência Nacional de Inteligência espanhola referiu que fontes abertas seriam "fundamentais para a elaboração e o trabalho da Inteligência"; em 2010, ao anunciar a criação de um código de ética para agentes especiais, insistiu que a inteligência moderna não se baseava apenas em presença física: "pode-se obter mais informações sentado em um computador, explorando mensagens dos bandidos". A Agência Espanhola de Inteligência Militar produziu e manteve carregados no *site* do Estado-Maior da Defesa Espanhol *slides* sobre inteligência de fontes abertas, datados de 2008; o Ministério da Defesa espanhol abriu em 2017 licitação para o "Desenvolvimento da ferramenta Osint baseada na plataforma IDOL HAVEN".

A pesquisa identificou projetos do Exército espanhol em curso, criando um modelo chamado Brigada 2035, que incorpora avanços tecnológicos para melhorar operações, sendo uma das funções específicas do projeto a Inteligência, estabelecendo a inteligência de fontes abertas como uma responsabilidade fundamental: o plano anual de recrutamento do Ministério do Interior da Espanha, para o ano de 2019, apontou investimentos em "sistemas de obtenção de Osint no ciberespaço".

No âmbito das atividades ligadas à segurança nacional, é preciso reforçar as ações de controle interno e externo[272], o que deve ocorrer sem prejuízo da elaboração de princípios norteadores das atividades de inteligência e de regulação específica para procedimentos voltados ao emprego de tecnologias de monitoramento, a exemplo do Regulamento de

[271] OSINT hub. Disponível em: https://osinthub.org/#about. Acesso em: 26 out. 2021.

[272] O primeiro é exercido pelo Poder Executivo Federal, uma vez que é o responsável direto pelas atividades de inteligência. Este deve garantir que o GSI e a ABIN operem dentro dos princípios democráticos da Constituição. O Poder Legislativo, por sua vez, tem que assumir sua prerrogativa no exercício do controle externo às instituições de inteligência. No caso, o espaço no qual essas questões precisam ser levantadas e debatidas é a Comissão Mista de Controle das Atividades de Inteligência (CCAI). Integrada por membros do Senado e da Câmara dos Deputados, ela é responsável pela fiscalização e controle dessas atividades.

Tecnologias de Uso Dual da União Europeia (2009), atualizado em 18 de julho de 2021, que, para além de reconhecer os riscos para repressão de grupos e violações de direitos humanos que essas tecnologias apresentam, inclui controles de exportação e aquisição para tecnologias de vigilância cibernética (*cyber surveillance*)[273].

Em 10 de maio de 2021, o Conselho da União Europeia aprovou o texto do novo Regulamento sobre controle de exportação, intermediação, assistência técnica, trânsito e transferência de bens de uso duplo (ou *dual use*). Originalmente, com a publicação do Regulamento (CE) nº 3381/94 do Conselho, instituiu-se um regime comunitário de controle da exportação de bens de "dupla utilização", definindo-os como *bens susceptíveis de ter uma utilização civil e militar.* Em 2000, por intermédio do Regulamento (CE) nº 1334/2000 do Conselho, ocorreu a criação de um regime comunitário de controle das exportações de produtos e tecnologias de dupla utilização, diversas vezes alterado até defini-los como *produtos, incluindo suportes lógicos e tecnologia, que possam ser utilizados tanto para fins civis como para fins militares, incluindo todos os bens que possam ser utilizados tanto para fins não explosivos como para de qualquer modo auxiliar no fabrico de armas nucleares ou outros engenhos explosivos nucleares*. Na assinatura do Tratado de Lisboa da União Europeia, o Regulamento (CE) nº 428/2009 do Conselho[274] consolida o regime comunitário europeu de controle das exportações, transferências, corretagem e trânsito de produtos de dupla utilização e estabelece que os produtos de "dupla utilização" devem ser sujeitos a um controle eficaz quando são exportados da União, quando nela transitam ou quando são entregues num país terceiro através de um serviço de corretagem prestado por um corretor residente ou estabelecido na União. Entre outros aspectos e critérios, mantém a definição de produtos de duplo uso e indica um catálogo que permite dar aplicação prática aos controles internacionalmente acordados, em relação a equipamentos conjuntos, equipamentos de ensaio, inspeção e produção, materiais, suportes lógicos e tecnologia dos bens em apreço, dentre as quais destacam-se as categorias: eletrônica, computadores, telecomunicações e segurança da

[273] HUREL, Louise Marie; FRANCISCO, Pedro Augusto P; TELES, Daisy. **Pegasus, a ponta do iceberg da fragilidade no controle de inteligência**. Disponível em: https://www.fundacaoastrojildo.org.br/pegasus-a-ponta-do-iceberg-da-fragilidade-no-controle-de-inteligencia/. Acesso em: 29 dez. 2021.

[274] UNIÃO EUROPEIA. Consejo de la Unión Europea. REGLAMENTO (CE) nº 428/2009 DEL CONSEJO de 5 de mayo de 2009, por el que se establece un régimen comunitario de control de las exportaciones, la transferencia, el corretaje y el tránsito de productos de doble uso. **Diario Oficial de la Unión Europeia**, p. 134-268, 29.5.2009. Disponível em: https://www.boe.es/doue/2009/134/L00001-00269.pdf. Acesso em: 20 ago. 2022.

informação, navegação e aviação, engenharia naval ou aeroespaço e propulsão[275].

A importância para a utilização do método baseado em inteligência em fontes abertas durante conflitos militares ficou evidenciada durante a invasão promovida pela Rússia à Ucrânia, em 2022, quando grupos de especialistas em fontes abertas direcionaram os seus esforços para dar olhos com precisão às forças ucranianas que, recorrendo às imagens produzidas por câmeras de vigilância particulares e públicas, em fotos e imagens de radar tiradas por satélites civis, apontavam, no Google Maps, o avanço das tropas russas, indicando onde estavam os recursos militares ou eram feitos os ataques efetuados, viabilizando o abate de fileiras russas por forças ucranianas, em minoria expressiva.

Em apoio à Ucrânia, proliferaram-se na *deep web* fóruns onde informação é trocada de forma segura: o *Anonymus* espalhou a sua tradicional mensagem de combate[276], reunindo os esforços e recursos necessários para atacar a Rússia[277]. A plataforma Twitter suspendeu diversos perfis de pesquisadores em fontes abertas que compartilhavam imagens e vídeos das regiões de Donbas e Luhansk, os quais passaram a sustentar que a suspensão da conta poderia ter sido parte de uma campanha de denúncia em massa destinada a desabilitar contas Osint durante uma invasão russa, causando preocupação que a remoção das contas do Twitter que compartilham Osint pudesse beneficiar os objetivos militares russos na região. Em nota, a empresa afirmou que disse que uma ação foi tomada contra essas contas por engano e que as suspensões decorreram de erro da própria companhia, afastando a hipótese aventada pelos pró-ucraninos de que teria se tratado de campanha coordenada por robôs russos para denunciar os perfis por violação aos termos de uso da rede[278].

No Brasil, durante a realização dos Jogos Olímpicos e Paralímpicos Rio 2016, a Secretaria Extraordinária para Grandes Eventos criou, dentro de sua estrutura organizacional, o Núcleo de Fontes Abertas, setor vinculado à Coordenação-Geral de Inteligência da Diretoria de Inteligência, cujos integrantes deveriam utilizar informações disponíveis na internet para produzir conhecimento relevante para aplicação na segurança dos jogos e cujos resultados

---

[275] COELHO, Adelino de Matos. O "Duplo Uso" – Uma Questão De Terminologia. **Revista Militar**, n. 2629/2630, p. 131-146, fevereiro/março de 2021. Disponível em: https://www.revistamilitar.pt/artigo/1537. Acesso em: 27 ago. 2022.

[276] Disponível em: https://www.instagram.com/tv/CbKZN9wIX7H/?utm_source=ig_web_copy_link. Acesso em: 19 mar. 2022.

[277] MATEUS COLEHO. Nuno. **A Nova Ordem Digital. A trama adensa-se e descobrem-se as verdades...** Disponível em: https://cnnportugal.iol.pt/guerra/ucrania/nuno-mateus-coelho-a-nova-ordem-digital-a-trama-adensa-se-e-descobrem-se-as-verdades/20260426/621a26960cf21a10a421b8b3. Acesso em: 19 mar. 2022.

[278] **Twitter accounts sharing video from ukraine are being suspended when they're needed most**. Disponível em: https://www.theverge.com/2022/2/23/22947769/twitter-osint-russia-ukraine-invasion-suspended-error. Acesso em: 19.mar. 2022.

eram rapidamente transmitidos. A capacitação dos agentes, a testagem dos métodos e a utilização de ferramentas tecnológicas adequadas foram apontadas como fatores determinantes para o aperfeiçoamento das técnicas empregadas na utilização de informações relevantes para o cumprimento de sua missão institucional.[279]

4.2. Dos discursos de prevenção às práticas de repressão penal

O discurso da segurança centraliza a justificação da guerra preventiva e da guerra contra a criminalidade, ignorando a diferença existente entre inimigo interno, inimigo externo e o estrangeiro. Uma das formas de militarizar o sistema político é transpor doutrinas formuladas pelos militares para outros ambientes por meio de políticas governamentais, o que historicamente ocorre na área de segurança pública.[280] Elementos como a crise econômica, a descrença na política, o medo dos "inimigos" (posição ocupada por estereótipos do criminoso comum, do "colarinho branco", do terrorista, do imigrante pobre) existentes no contexto atual justificam e reforçam o surgimento de discursos para que Estados e grupos rotulem criminosos, equiparados a inimigos, sobre características transformadas em potencial risco ao cometimento de delitos.[281] A retórica de guerra preventiva, que justifica a deflagração da guerra em meio a uma democracia e é reforçada pela onda de atentados terroristas iniciados em 11 de setembro de 2001, tem entre suas tarefas estabelecer novos limites entre nós e eles, o interior e o exterior; como é impossível distinguir interior e exterior, esses limites apresentam-se frágeis e os inimigos[282] confundem-se conosco[283], produzindo-se uma política criminal que aceita diferenciar, a partir da reputação, os criminosos dos demais cidadãos, estendendo à população a aplicação de medidas concebidas inicialmente para o criminoso ou terrorista em potencial[284].

Da transição da sociedade panóptica à sociedade sinóptica e internético-

---

[279] BARRETO, Alexandre Gonçalves; WENDT; Emerson. **Inteligência e Investigação Criminal em Fontes Abertas**. Rio de Janeiro: Brasport, 2020. p. 65-71.
[280] PENIDO, Ana; STÉDILE, Miguel Enrique. **Ninguém regula a América: guerras híbridas e intervenções estadunidenses na América Latina**. São Paulo: Fundação Rosa Luxemburgo: Expressão Popular, 2021. p. 134-135.
[281] THOMPSON, Augusto. **Quem são os criminosos? O crime e o criminoso**: Entes políticos. 2. ed. Rio de Janeiro: Lumen Juris, 2007.
[282] JAKOBS, Günther; MELIÁ, Manuel Cancio. **Direito penal do inimigo**: noções e críticas. Tradução André Luís Callegari e Nereu José Giacomolli. Porto Alegre: Livraria do Advogado, 2005.
[283] PITCH, Tamar. **La sociedad de la prevención**. Buenos Aires: Ad Hoc, 2009. p. 165-166.
[284] AGAMBEN, Giorgio. A propósito de Tiqqun. *In*: TIQQUN. **Contribuição para a guerra em curso**. São Paulo: n-1 edições, 2019. p. 265.

personocêntrica desenvolvem-se novos sistemas de valoração do ser humano[285], emergem novas *classes perigosas*, um refugo formado por seres classificados como inadequados à reintegração e ao convívio, incapazes de exercer funções úteis após sua reabilitação: pessoas em estado de exclusão reiteradamente produzido pela modernidade líquida[286], fazendo com que ferramentas e técnicas de campanha global contra o terrorismo estejam sendo utilizadas em prol do combate à criminalidade local[287].

O caráter preventivo associado à segurança pública vincula-se à ideia de evitar a prática de crimes em determinados lugares e em precisas circunstâncias.[288] Hoje, o simples acessar *sites* de redes sociais revelam informações pessoais, imagens e ligações entre amigos e associados que aceleram e informam e respostas das agências de aplicação da lei.[289] A ascensão e disponibilidade da inteligência de fontes promete a entrega de desempenho[290], e agências de aplicação da lei vêm reconhecendo a necessidade de aplicar técnicas similares com o escopo de melhorar sua capacidade investigativa e potencializar habilidades para detectar e responder à criminalidade[291]. Ainda que a tecnologia e o acesso a orçamentos sejam distintos dos militares, diante do barateamento do acesso não apenas a registros de imagens, tempo e posicionamento de oriundos de fontes abertas, como também dados de voz e comunicação, vemos um movimento das agências de aplicação da lei se apoiando nas capacidade operacional e *expertise* militar, valendo-se de sua ampla inteligência mista e de ciclo, em que fontes de dados, processamento de informações e análises são heterogêneas e compartilhadas[292], técnicas que avançam sua expansão não apenas sob a investigação criminal, mas que também se colocam a serviço de estratégias em cautelares processuais penais, estabelecendo um modelo de prevenção do cometimento de delitos. Nesse viés,

---

[285] VALENTE. Manuel Monteiro Guedes. O reforço dos Princípios Constitucionais na obtenção da prova no mundo digital. **RDJP**, Brasília, ano 2, n. 3, p. 11-25, jan/jun 2018.
[286] BAUMAN, Zygmunt. **Modernidade Liquida**. Rio de Janeiro: Editora Zahar, 2001.
[287] O´NEIL; Cathy. **Algoritmos de Destruição em Massa**: como o big data aumenta a desigualdade e ameaça a democracia. Santo André: Editora Rua do Sabão, 2020. p. 144-163.
[288] PRADO, Geraldo. Proteção de dados, prova digital e devido processo legal. **VI Seminário Internacional "Proteção de dados pessoais na segurança pública e investigação criminal"**. Câmara dos Deputados do Congresso Nacional Brasileiro: Brasília, jul-2020. Disponível em: https://www.youtube.com/watch?v=J4m5yiQnLbI&feature=youtu.be. Acesso em: 20 abr. 2022.
[289] *Agência de aplicação da lei* é o termo utilizado, para fins do presente trabalho, para representar a tradução da expressão americana *Law Enforcement Agencies*.
[290] STANIFORTH, Andrew. Police Use of Open Source Intelligence: the longer arm of law. *In*: AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 21-31.
[291] AKHGAR, Babak. OSINT as an integral part of the National Security Apparatus. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 4-5.
[292] MARZELL, Laurence. OSINT as a parto f the Strategic National Security Landscape. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 33-34.

técnicas são confundidas com objetivos, conduzindo o processo penal à encruzilhada entre método de hipervigilância e técnica de garantia da liberdade[293].

Por outro lado, como a inteligência em fontes abertas cresceu exponencialmente nos últimos anos, sobretudo com o desenvolvimento de ferramentas que auxiliam na análise de dados, hoje ela também é formada por outros setores da sociedade civil que trabalham em rede na verificação de informações: qualquer sujeito com letramento de dados pode usar dados abertos; a própria internet oferta cursos voltados a ensinar as habilidades direcionados ao uso e desenvolvimento de inteligência de dados abertos[294], cujos maiores consumidores

[293] PRADO, Geraldo. Proteção de dados, prova digital e devido processo legal. **VI Seminário Internacional "Proteção de dados pessoais na segurança pública e investigação criminal"**. Câmara dos Deputados do Congresso Nacional Brasileiro: Brasília, jul-2020. Disponível em: https://www.youtube.com/watch?v=J4m5yiQnLbI&feature=youtu.be. Acesso em: 20 abr. 2022.

[294] *"The Certified in Open Source Intelligence (C|OSINT) program is the first and only globally recognized and accredited board certification on open source intelligence. You will learn real-world applicable skills that are utilized by law enforcement, military intelligence, private investigators, loss prevention, cyber defenders and attackers all use to help aid in their investigations. Our goal is to create an industry-leading body of knowledge and skill sets that meet the McAfee Institute's high standards that can be taught, tested and validated so you can be successful in your career regardless if you are in law enforcement, intelligence, loss prevention, private investigations, information security, or cybersecurity. This program is completely online and self-study once the modules are released and are delivered over a 6 weeks period of time. One module is released each week to study, learn, and test your competency. Every week students will participate in a number of hands-on labs using the methodologies taught during that week. More than 30 labs in this certification program use the web and dark web to help teach you the real-world skills you need to be successful*" (CERTIFIED in Open Source Intelligence (C|OSINT). **Niccs** – National Initiative for Cybersecurity Careers and Studies. Disponível em: https://niccs.cisa.gov/training/search/mcafee-institute/certified-open-source-intelligence-cosint. Acesso em: 20 abr. 2022).

"POR QUE FAZER O CURSO: Você consome muito conteúdo sobre Inteligência Cibernética e ainda não entende como coletar resultados e colocá-los em prática? Não sabe como usar informações que podem ser coletadas para aumentar a atividade de inteligência? A Inteligência de Fontes Abertas (OSINT) virou uma necessidade para todos os tipos de organizações, tanto governamentais como empresariais, pois pôde-se compreender o seu potencial para acelerar o crescimento. Com isso, organizações de inteligência estão aumentando seus investimentos e a formação em OSINT. Neste curso você irá aprender um passo-a-passo de como utilizar a técnica OSINT de forma prática e assim construir uma estrutura básica de coleta de inteligência em fontes abertas (OSINT). Além disso, terá a oportunidade de um amplo diálogo e troca de experiências com instrutores com mais de 20 anos de experiência em inteligência cibernética, atuando com análise e prevenção de ameaças e fraudes cibernéticas e disseminação de conteúdo educativo sobre o assunto para profissionais e empresas.

OBJETIVOS: Capacitar você a construir o passo-a-passo de uma coleta de informações, contendo a estrutura de: Armazenamento de informações, Coleta e Análise" (INTELIGÊNCIA Cibernética em Fontes Abertas (Curso). **Daryus**. Disponivel em: https://www.daryus.com.br/curso/inteligencia-cibernetica-em-fontes-abertas-osint. Acesso em: 23 abr. 2022).

"*Curso de Técnicas y Herramientas Avanzadas en Ciberinvestigación OSINT: Aprende a investigar de forma rápida, profesional y segura en Internet, las redes sociales, la Deep Web y la Dark Web. Comprende e interioriza la metodología para ejercer de forma segura, anónima, legal y profesional cualquier ciberinvestigación en un entorno policial, militar o empresarial. Conoce cómo securizar tus dispositivos para asegurar la confidencialidad de tu identidad, de la investigación y de tu organización, y domina las técnicas y herramientas avanzadas de ciberinvestigación para poder obtener información de personas y organizaciones*" (SEISDEDOS, Carlos. Curso de Técnicas y Herramientas Avanzadas en Ciberinvestigación OSINT. **Lisa News**. Disponível em: https://www.lisanews.org/formacion/curso-tecnicas-herramientas-avanzadas-ciberinvestigacion-osint/. Acesso em: 23 abr. 2022).

são desde entusiastas, acadêmicos, jornalistas, cientistas de dados em empresas privadas, até organizações da sociedade civil e instâncias de governo[295]: a comunidade é composta por todos os tipos de pessoas, muitas das vezes completamente anônimas, e Inteligência de Fontes Abertas (Osint) virou uma necessidade para todos os tipos de organizações.

A Inteligência Artificial já não mais se atém à prevenção. Seus dispositivos prometem performar exponencialmente no âmbito probatório pela produção de *evidências digitais* baseadas, na fase preliminar, naquilo que vem sendo chamado de *prova algorítmica,* um rico acervo dos dados que são objetos do nosso cotidiano ligado à internet, gerados sem qualquer intervenção humana e que produzem conhecimento determinante para a investigação criminal.[296]

Como parte de um misto de inteligência amplo e essencial para o completo Ciclo de Inteligência, a utilização de Osint na tomada de decisão pelas agências de aplicação da lei é festejada como elementos de participação em um sistema de cooperação integrado para a governança de informações, capaz de agregar fontes de inteligência aberta às fechadas que, juntas, operam como uma melhor forma para embasar a tomada de decisões estratégicas. Como outros dados, o uso da inteligência deve ser compreendido, integrado e usado de forma unificada e como parte de outros elementos disponíveis para tomadores de decisão, tudo como forma de produzir inteligência confiável para embasar suas tarefas[297].

"*SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis.The amount of data being pushed to the Internet each minute is staggering. Hundreds of hours of video, hundreds of thousands of images, and more text than can be indexed with a search engine. Couple that massive amount of data with websites that restrict access, those on unindexed servers, and data in the dark web, and you will quickly understand that gaining a strong foundation in how to search, collect, and analyze data from Internet-facing platforms no matter where they are located is important. This is what SEC487 does. It starts with how to collect and analyze data and quickly moves into teaching techniques to gain access to and then to harvest content from websites. It touches on a broad array of Open-Source Intelligence (OSINT) topics from setting up an OSINT analysis platform to accessing the dark web. It is an entry-level course that is far from basic and will empower students to seek, find, and use data from sources around the world. If you are relying on search engine indexes to find and gather data, it's a guarantee that you're missing information. SEC487 is a foundational course in open-source intelligence (OSINT) gathering that teaches students how to find, collect, and analyze data from the Internet. Far from being a beginner class, this course teaches students the OSINT groundwork to be successful in finding and using online information, reinforced with over 25 hands-on exercises"* (SANS487: Open-Source Intelligence (OSINT) Gattering and Analisys. **SANS**. Disponível em: https://www.sans.org/cyber-security-courses/open-source-intelligence-gathering/. Acesso em: 24 abr. 2022).

[295] BRASIL. Portal Brasileiro de Dados Abertos. **O que são dados abertos?** Disponível em: https://dados.gov.br/pagina/dados-abertos. Acesso em: 24 abr. 2022.

[296] RODRIGUES. Anabela Miranda. Inteligência artificial e Direito Penal – a justiça preditiva entre a Americanização e a Europeização. *In*: RODRIGUES. Anabela Miranda (coord). **A Inteligência Artificial no Direito Penal**. Coimbra: Edições Almedina, 2020. p. 14-17.

[297] MARZELL, Laurence. OSINT as a parto f the Strategic National Security Landscape. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 33-34.

Há equívoco em considerar que o Ministério Público inicie uma investigação somente depois de conhecida a existência de um crime, de que o seu poder depende apenas da abstrata configuração de tarefas, funções, faculdade de intervenção que a lei processual distribui entre os sujeitos processuais e de que é investido da verificação exclusiva da notícia-crime. A prática judiciária revela um número crescente de procedimentos instaurados com a falta dessas condições, alargando-se a área dos comportamentos subsumíveis: uma conduta isoladamente considerada lícita pode conotar-se como se ilícita fosse analisada sob um viés de contexto criminoso. Assim, deve o acusador, antes de iniciar a investigação preliminar, delimitar o campo da atividade futura, selecionando os fatos a investigar. Coloca-se um problema de delimitação do campo investigativo: nessa fase ou até mesmo em momentos anteriores ao início da investigação propriamente dita, concentra-se um notável potencial de atividade investigativa, cujo bom uso depende da capacidade de autocontrole, já que Polícia e Ministério Público operam com discricionariedade e longe do alcance dos demais sujeitos. A conjugação do agir discricionário fora do procedimento penal e da ausência de sujeição a regras terminou por relegar a questão àquelas processualmente insignificantes – a problemática concernente à busca e formação da notícia-crime ocupam lugar marginal na literatura processual penal.[298]

Surge a chamada *investigação preparatória*, moderna versão da *inquisitio generalis* e que se traduz em prática investigativa subjetivamente orientada, antecedente à investigação preliminar e voltada a conhecer o ambiente criminoso. Usualmente atividade ocasional de polícia, a investigação preparatória é progressivamente atraída para a esfera de atribuições do Ministério Público, empreendendo a atividade preventiva em função repressiva, em alinhamento aos contemporâneos investimentos em procedimentos de prevenção; especialmente na luta contra o crime organizado, atividades qualificadas como preventivas serão desviadas para fins repressivos, partindo-se do pressuposto de que uma conduta penal ou foi praticada, ou está em curso. Ao mesmo tempo que passamos a considerar compatíveis com a atividade processual repressiva a persecução de finalidades preventivas, atividades preventivas admissíveis sob o pressuposto de hipotética ocorrência criminosa revelarão vocação repressiva.

[298] ORLANDI, Renzo. Investigações preparatórias nos procedimentos de criminalidade organizada: uma reedição da inquisitio generalis? Tradução Ricardo Jacobsen Gloeckner e Luiz Eduardo Cani. *In*: TERRA, Luiza Borges (org.). **Lições Contemporâneas do Direito Penal e do Processo Penal**. São Paulo: Tirant lo Blanch, 2021. p. 371-391.

Na instauração da investigação preparatória, o sujeito ativo usufrui de uma amplíssima discricionariedade. Destinados ao conhecimento de determinados ambientes criminosos, "procedimentos de prevenção" representam a ocasião para conduzir *investigações preparatórias*, em que informações obtidas para prevenir podem desencadear uma atividade repressiva. Denota-se flagrante assimetria entre os sujeitos da investigação; o Ministério Público desfruta de conhecimentos acumulados e ordenados em sua complexa trama histórica.

A ênfase na relação causal entre crimes antecedentes e crimes-fim foi o que possibilitou a relativização da distinção entre as atividades preventiva e repressiva. Em razão da abertura concedida por tipos penais associativos, delimitar a fronteira do fato penalmente relevante torna-se atividade de difícil execução, recaindo a tarefa nas mãos de quem realiza a investigação preparatória, cuja tendência para proceder se desenvolve a partir de "teoremas" – premissa da investigação que fornece critérios para reconhecer condutas relevantes[299].

O início se resume à constatação da existência de indícios – clássico pressuposto-limite ao órgão investigativo –, usualmente atestados por uma notícia-crime, esta não mais pressuposto, mas agora objetivo da investigação preparatória: as incursões buscam "inspirações", ainda que suspeitas, independentemente se obtidas em documento anônimo, cruzamento de dados, estatísticas ou de qualquer outra forma, até mesmo de um devaneio investigativo. Por ser atividade externa aos procedimentos penais, é conduzida em sigilo absoluto, sem conhecimento dos alvos envolvidos, razão pela qual sob eles não recaem quaisquer garantias constitucionais e não podem reclamar direitos processuais.

Se o início da atividade repressiva precede o início da investigação preliminar em procedimentos contra a criminalidade organizada, deve essa "investigação preparatória" ser objeto de observação, sobretudo em razão de deficiência em sua regulamentação, relativizada em razão do discurso de prevenção. Se ela representa o *start* de toda a marcha, é preciso

[299] "Aqui o investigador se encontra em uma posição não muito diferente daquela que ocupava o juiz na velha inquisitio generalis. Tanto agora como à época, a individualização dos fatos penalmente relevantes é operada, em concreto, da mesma forma, com vagas indicações normativas. Tanto hoje como à época, a acusação é construída também com base em pressupostos extra normativos. De fato, certos comportamentos aparentemente 'neutros' podem assumir uma coloração criminosa, se vistos à luz de determinados conhecimentos sociológicos ou criminológicos. Daqui a tendência dos investigadores (e até dos magistrados julgadores) para proceder a partir de 'teoremas': no que se percebe, muitas vezes e polemicamente, um excesso de subjetivismo por parte da investigação e, portanto, um lado discutível da atividade judiciária. Mas o 'teorema' representa frequentemente uma premissa necessária da investigação, como fornece um critério para reconhecer as condutas penalmente relevantes dentro de uma quantidade indiferenciada de condutas potencialmente lícitas. Também o 'teorema', em suma, contribui à descoberta da veritas criminis, qualificando-se, assim, como ato da moderna inquisitio generalis" (ORLANDI, Renzo. Investigações preparatórias nos procedimentos de criminalidade organizada: uma reedição da inquisitio generalis? Tradução Ricardo Jacobsen Gloeckner e Luiz Eduardo Cani. *In*: TERRA, Luiza Borges (org.). **Lições Contemporâneas do Direito Penal e do Processo Penal**. São Paulo: Tirant lo Blanch, 2021. p. 371-391).

intervir com dispositivos legais destinados a limitar o uso de dados e informações para fins de reconstrução de uma *notitia criminis*, sem que isso induza à antecipação das garantias defensivas.[300]

A importância apenas aumenta ante a possibilidade oferecida pelos meios informáticos para armazenar, selecionar, trocar com velocidade e em quantidades de dados pessoais. Países ainda não consideraram adequadamente abusos de informações obtidas em domínio público, ganhando especial destaque, neste ponto, a discussão desenvolvida em torno do direito à "autodeterminação informativa" como direito fundamental da pessoa[301], argumento idôneo a justificar a limitação ao uso de dados pessoais para finalidades investigativas, seja ela de caráter preventivo ou repressivo[302].

4.3. Inteligência de fontes abertas e instituições policiais

Para o policiamento, a abordagem conduzida por inteligência justifica-se pelo auxílio na reunião de elementos. Como a criminalidade raramente é aleatória, a tecnologia e a reunião

[300] Como seria levado a pensar quem interpretasse em sentido (talvez excessivamente) amplo o termo "procedimento" no art. 24, parágrafo 2, da Constituição italiana (ORLANDI, Renzo. Investigações preparatórias nos procedimentos de criminalidade organizada: uma reedição da inquisitio generalis? Tradução Ricardo Jacobsen Gloeckner e Luiz Eduardo Cani. *In*: TERRA, Luiza Borges (org.). **Lições Contemporâneas do Direito Penal e do Processo Penal**. São Paulo: Tirant lo Blanch, 2021. p. 371-391).

[301] Desde 1983, o Tribunal Constitucional alemão propôs a elaboração do conceito de autodeterminação informativa (*Informationelle Selsbstebestimmungsercht*), entendimento este que também foi adotado pelo art. 18.4 da Constituição Espanhola, que, embasado no art. 8 da Carta dos Direitos Fundamentais da União Europeia, confere ao próprio indivíduo o domínio sobre seus dados pessoais, o que lhe assegura o poder de controle e o direito de decidir sobre a destinação sobre registros de natureza pessoal. Por essa construção, qualquer utilização indevida de dados pessoais que um sujeito produz quando se relaciona no ambiente virtual afeta o direito fundamental à proteção de dados, os quais jamais podem ser utilizados sem que haja o consentimento por parte dos interessados, detentores dos direitos de acesso, cancelamento e retificação de qualquer tipo de informação relativa à sua individualidade. Impõe-se, assim, uma série de deveres jurídicos que visam à proteção de dados individuais, atribuindo-se ao seu titular uma série de faculdades e poderes jurídicos de livre disposição, os quais só se tornarão efetivos se observados por terceiros (DELGADO MARTÍN, Joaquín. **Investigación tecnológica y prueba digital en todas las jurisdicciones.** Madrid: España, 2018. p. 129-132).

[302] De um lado, há quem – tratando tais dados da mesma maneira que fotografias ou impressões digitais atribuíveis ao imputado (§ 81b do StPO) – considera o seu uso sujeito às cláusulas gerais que atribuem à polícia o poder de buscar as notícias-crime (§ 163 do StPO): para remediar o eventual arbítrio policial o interessado pode recorrer ao juiz administrativo, a quem pertence, portanto, a última palavra acerca da conservação dos dados pessoais para fins preventivos e repressivos. Assim, por exemplo: VERWALTUNGSGERICHTSHOF Mannheim: Kriminalpolizeiliche personenbezogene Akten nur zu präventiv-polizeilichem Zweck. **Neue Juristische Wochenschrift**, v. 47, 18 de maio de 1987. p. 3022. Quem, em vez disso, considera que tais dados recaem na esfera de influência do assim chamado direito à autodeterminação informativa considera indispensável uma específica regulamentação legal do poder de polícia neste campo: a lei deve estabelecer antecipadamente tanto os pressupostos quanto os limites temporais da conservação de dados pessoais para fins preventivos e repressivos. Assim: VERWALTUNGSGERICHT Frankfur: Ermächtigungsgrundlage zur Aufbewahrung erkennungsdienstlicher Unterlagen. **Neue Juristische Wochenschrift**, v. 36, 18 de fevereiro de 1987. p. 2248. N.T. StPO é a abreviação de *Strafprozessordnung*, a ordenança processual penal alemã (ORLANDI, Renzo. Investigações preparatórias nos procedimentos de criminalidade organizada: uma reedição da inquisitio generalis? Tradução Ricardo Jacobsen Gloeckner e Luiz Eduardo Cani. *In*: TERRA, Luiza Borges (org.). **Lições Contemporâneas do Direito Penal e do Processo Penal**. São Paulo: Tirant lo Blanch, 2021).

de elementos de fontes abertas justificam-se pela possibilidade de estruturação do "padrão de movimento criminoso": estilos de vida, comunicações, capacidades e intenções podem ser inferidos e, então, definidas opções de intervenção. Inteligência policial não é tanto um modo de trabalho, mas de pensamento.

No âmbito das agências de aplicação da lei, o uso e a integração de informação publicamente disponível e de fontes abertas garantem que agentes tenham acesso a informações publicamente disponíveis para tomar decisões informativas. Pode ser realizada por monitoramento, mineração de dados e pesquisa, abrangendo ampla gama de informação e recursos disponíveis, tais como: mídia, documentos profissionais e acadêmicos, dados públicos, comunidades *online* de internet – e o conteúdo gerado por usuários, como *sites* de comunicação social, *sites* de compartilhamento de foto e vídeo, *wikis* e *blogs* – e/ou informação geoespacial, agregando valor às operações policiais na habilidade de obter inteligência relacionada à investigação ou incidente de forma célere, confiável e acionável. Possui disponibilidade, profundidade e alcance que permitem que agências de aplicação da lei satisfaçam requerimentos de inteligência e informação sem uso de suporte humano especializado e meios técnicos de baixo custo, auxiliando em atividades de vigilância e reconhecimento, além de oferecer informação que aponta a outros meios técnicos de coleta[303].

Trabalhos e projetos exploram a aplicação da inteligência de fontes abertas para investigações criminais no combate ao cibercrime e ao crime organizado, na detecção de ações ilegais ou prevenção de crimes futuros, como ataques terroristas, assassinatos ou estupros, aplicando a técnica para trazer desempenho em precisão de processos e prisões de culpados ou a dados forenses digitais de uma variedade de dispositivos para aprimorar a análise de inteligência criminal. Os projetos europeus ePoolice[304] e Caper[305] desenvolvem

[303] STANIFORTH, Andrew. Police Use of Open Source Intelligence: the longer arm of law. *In*: AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016. p. 21-31.

[304] "O projeto ePoolice Project (Early Pursuit Against Organized Crime Using EnvirOnmental Scanning, the Law and IntelligenCE Systems) é financiado pela Comissão Europeia no âmbito do Sétimo Programa-Quadro para Pesquisa e Desenvolvimento Tecnológico (FP7). A lista de parceiros que trabalham no projeto ao lado do UNICRI inclui agentes da lei e especialistas acadêmicos especializados em questões de crime organizado e redes criminosas. O objetivo geral do projeto é criar um sistema internacional de varredura ambiental dedicado ao combate às redes criminosas. Os sistemas de varredura ambiental funcionarão com base em um repositório de todas as informações e conhecimentos relevantes, incluindo informações digitalizadas e conhecimentos derivados, aprendidos ou hipotéticos, bem como os metadados necessários para avaliação de credibilidade e confiança, rastreabilidade e gerenciamento de proteção de privacidade. Especificamente, o sistema suportará: Fontes de informação díspares e diversas formas de mídia (texto livre, vídeo, áudio); Suporte bilíngue (inglês e alemão); Divulgação e intercâmbio de informações e conhecimentos de potencial interesse para as agências de aplicação da lei; Visualização de ameaças de OC potencialmente emergentes/avaliação de ameaças de OC; Alerta precoce em caso de detecção de novas ameaças de OC potencialmente emergentes; Hipóteses e notas do usuário – que podem ser armazenadas e usadas por outros; *eedback* do usuário sobre as descobertas para refinamento do conhecimento de domínio do sistema; análise e tomada de decisão no tratamento de ameaças de OC emergentes, considerando a validade e a gravidade das ameaças detectadas. O sistema de varredura ambiental ePoolice fornecerá uma visão geral sistemática do ambiente ao redor para melhor apreciar, avaliar e

modelos para escanear dados abertos automaticamente, sob a promessa de "analisar a sociedade e detectar o crime organizado emergente".

Entendendo que o alerta estratégico precoce surge como um importante meio para a aplicação da lei no combate ao crime e com o objetivo de (i) detectar a existência de atividades ilícitas conduzidas pelo crime organizado e organizações criminosas subjacentes o mais cedo possível para evitar a formação de sistemas criminais mais fortes e (ii) prever a evolução do crime organizado por intermédio de um sistema de varredura ambiental que avalia e desenvolve cenários de futuras ameaças, o projeto ePoolice desenvolve, desde janeiro de 2013, um protótipo de sistema de varredura implementando soluções para o desenvolvimento de um repositório de informações e conhecimentos relevantes.

A ideia do sistema é possibilitar o monitoramento ambiente em tempo real para captura, divulgação e intercâmbio de todas informações presentes em fontes de diversas naturezas, como leis, relatórios de análise de fiscalização, informações governamentais, *web*, mídia social, notícias, academia, organizações não governamentais e internacionais ou opiniões de especialistas, tudo de maneira a oferecer ao analista uma visão ampla do *ao redor* para apreciar, avaliar e antecipar a prática de um crime emergente. O propósito: aumentar a eficácia das Polícias Nacionais, institutos criminológicos e empresas privadas, além de permitir a identificação e a qualificação de novas ameaças no ambiente de policiamento e a

---

antecipar um crime emergente, monitorando o ambiente e capturando em tempo real informações relevantes presentes em fontes heterogêneas, incluindo relatórios de análise de aplicação da lei, informações governamentais, web, mídia social, notícias, academia, organizações não governamentais e internacionais e especialistas no assunto" (EARLY Pursuit Against Organized Crime Using EnvirOnmental Scanning, the Law and IntelligenCE Systems (ePoolice). **Unicri**. Disponível em: http://www.unicri.eu/topics/organized_crime_corruption/epoolice/. Acesso em: 11 ago. 2022).

[305] O objetivo da Caper é construir uma plataforma comum de colaboração e compartilhamento de informações para a detecção e prevenção do crime organizado em que a internet é usada (por exemplo, venda de produtos falsificados ou roubados, crimes cibernéticos) e que explora a Inteligência de Código Aberto. As agências de inteligência do Estado estão cada vez mais inclinadas a usar o Open Source Intelligence (OSI) e, particularmente, as ferramentas normalmente associadas a Internet Social ou Semântica. As técnicas e tecnologias aplicadas pela Caper ao Open Source Intelligence também serão aplicadas ao "Closed Source Intelligence", ou seja, sistemas de informação existentes em uso pelas LEAs. Ambos os conjuntos de informações serão processados e explorados igualmente, permitindo que um infira no outro. Os módulos de análise construídos no projeto Caper também darão um novo valor à inteligência existente por meio de imagem, vídeo, fala e análise biométrica. A Caper fornecerá às Agências de Aplicação da Lei (LEA) uma plataforma operacional comum para Inteligência de Código Aberto complementada por conjuntos de interfaces baseadas em padrões. Permitirá fácil integração com sistemas legados e aplicações futuras. Módulos de análise para conteúdo multilíngue e multimídia (vários idiomas, voz, texto, áudio, imagem, vídeo e biometria) e aplicação das tecnologias de análise em sistemas de informação existentes (Fontes Fechadas) serão incluídos para ganhar novo valor e detectar pistas perdidas. A Caper agrupa parceiros europeus que trazem os seus conhecimentos tecnológicos para vídeo, voz, imagem, análise biométrica, aquisição de informação Open Source e tecnologias ETL, mas também Agências de Aplicação da Lei para a definição das suas necessidades e a integração do sistema, que garantirá o sucesso do projeto (COMISSÃO EUROPEIA. Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime. EU research Results. Disponível em: https://cordis.europa.eu/project/id/261712. Acesso em: 11 ago. 2022).

aplicação da lei e subsidiar com precisão o ambiente externo pelo uso de tecnologias avançadas, informações de prospecção para combate a todo tipo de crime organizado[306].

Por sua vez, reconhecendo a inclinação das agências para o uso de ferramentas de fontes abertas, sobretudo aquelas capazes de gerenciar dados de redes sociais, o projeto "Informações colaborativas, aquisição, processamento, exploração e relatórios para a prevenção do crime organizado" foi criado em cooperação entre a Caper e as agências de aplicação da lei, com o intuito de construir uma plataforma de colaboração e compartilhamento de informações para detecção e prevenção do crime organizado explorando ferramentas de inteligência de fontes abertas. A partir do subsistema de rastreamento e análise do Facebook, algoritmos exploradores foram implementados para extrair propriedades específicas do gráfico social, em particular interações dos usuários. Grande esforço foi empenhado para analisar o conteúdo textual gerado pelos usuários e no reconhecimento de entidades nomeadas (nomes de pessoas, locais e organizações) para, a partir da mescla da relação entre usuários e entidades, extrair um gráfico social onde todos os relacionamentos são visualizados em redes amigáveis[307].

4.4. Inteligência de fontes abertas e Ministérios Públicos

Reconhecendo o contexto universal e de transversalidade dos dispositivos tecnológicos nos mais diversos âmbitos de aplicação (comunicação, redes sociais, comércio, geolocalização, consumo de informação), a necessidade de adaptação a esses recursos tecnológicos e do bom emprego dos recursos disponíveis pelas plataformas para a investigação criminal, por intermédio da Subsecretaria de Planejamento e Inteligência Criminal, a Direção do Departamento de Investigações Criminais do Governo da Província de Buenos Aires promoveu, em abril 2021, "para prevenir situações indesejadas no ciberespaço", o seminário *Inteligencia en Fuentes Abiertas OSINT* (*Open Source Intelligence*), atividade voltada às polícias de segurança, aos departamentos de investigação, departamentos de narcóticos, departamentos do Comando de Prevenção Rural, além de promotores e peritos do

[306] COMMUNITY Research and Development Information Service (Cordis). **Early pursuit against organized crime using environmental scanning, the Law and IntelligenCE systems.** Disponível em: https://cordis.europa.eu/project/id/312651/reporting. Acesso em: 26 fev. 2022.

[307] ALIPRANDI, Carlo; DE LUCA, Antonio E.; DI PIETRO, Giulia; RAFFAELLI, Matteo; GAZZÉ, Davide; LA POLLA, Mariantonietta; MARCHETTI, Andrea; TESCONI, Maurizio. CAPER: Crawling and analysing Facebook for intelligence purposes. **IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)**, Beijing, China, p. 665-669, outubro 2014. DOI: 10.1109/ASONAM.2014.6921656. Disponível em: https://ieeexplore.ieee.org/document/6921656. Acesso em: 26 fev. 2022.

Ministério Público da Província de Buenos Aires. Com o objetivo de apresentar conteúdos, técnicas, ferramentas e abordagens diferenciadas de critérios de busca para que os operadores incorporem em suas atividades nessas plataformas, conhecer com profundidade as bases de uma cultura digital e orientar as atividades com respeito ao caráter legal investigações nas redes, o curso concentrou-se nos avanços ocorridos em matéria de investigação judicial com ferramentas de inteligência de fontes abertas[308].

Organizada no âmbito do Projeto de Parceria UE/CoE para a Boa Governança II sobre "Fortalecimento do combate ao branqueamento de capitais e recuperação de ativos no Azerbaijão", financiado pela União Europeia e pelo Conselho da Europa e implementado pelo Conselho da Europa, ocorreu, entre 25 e 29 de novembro de 2019, o *Open Source Intelligence (OSINT) Training*, em Baku, Azerbaijão, treinamento que reuniu analistas do Serviço de Monitoramento Financeiro e profissionais de investigação da Direção Anticorrupção do Gabinete do Procurador-Geral para apresentar técnicas e estratégias avançadas necessárias para coletar, de forma eficaz, e alavancar com segurança a inteligência de código aberto, aprimorando as

[308] "*6. Intenciones Educativas- Propósitos. La OSINT o inteligencia en fuentes abiertas es exactamente lo contrario que las fuentes de información clasificadas o cerradas o de pago. Cualquier página web, blog, diario digital, red social, etc., constituyen el grueso de estas fuentes de información. La cantidad de información disponible atenta contra el investigado, hay que saber buscar. El profesional deberá conocer: – cómo debe darse la relación con los proveedores de contenidos (empresas) durante las etapas de investigación. – qué información pueden obtener de cada uno de ellos y cómo solicitarla. - qué acciones llevar adelante con esa información. – cómo relacionar la información para obtener un modelo integral de investigación.*
7. Objetivos. En relación con los contenidos del presente proyecto, pretenderemos que el asistente incorpore los saberes necesarios para: – Recolectar información desde fuentes lícitas de datos. – Realizar inteligencia preventiva. - Dar a las investigaciones un carácter proactivo con OSINT. – Detectar conductas sospechosas en perfiles, blogs y páginas. – Optimizar búsquedas en la web. - Generar la integralidad de los datos necesaria para mejorar las investigaciones. 8. Contenidos: Introducción a OSINT: definición. Objetivos del OSINT. Metodología OSINT: integralidad de las investigaciones. Conceptos básicos. Importancia y utilidad. El proceso de OSINT. Tipos de OSINT. Buscadores de personas. Pipl.com. Sitios de tarjetas. Herramientas y plataformas OSINT: inteligencia y contrainteligencia. Motores de búsquedas y otras fuentes de investigación. Google Dork. Fuentes de Datos. Búsqueda en navegadores. User Agent. Metadatos: textos e imágenes. Software. Búsquedas inversas. Geolocalización. Curación de contenidos. Google Analytics. Análisis de redes sociales: scripts y herramientas. Definición de API. APIs de redes sociales. Twitter, Facebook, Instagram y otras. Facebook ID, Facebook Search. Aplicaciones Facebook. Software específico para obtener información: FOCA, Cree.py y Maltego. LinkedIn. Borrar identidades sociales. Preservación de cuentas sociales. Snapchat: visual search. Twitter Map. One Million Tweet. Trackeo de IP: la Dirección IP. Concepto. Redes e Internet. Identificación de los dispositivos en las redes. Características. Dominios de Internet. Estructura de dominios y subdominios. Dispositivos conectados. Internet de las Cosas. Anonimato del analista. Animación de la computadora. Borrar identidad. Geoposición. GEOINT: Geospacial Intelligence. Inteligencia electrónica. Máquinas virtuales. Redes VPN. Sistemas operativos anónimos. WhoIs. Grabify. Procedimientos jurídicos con proveedores locales de internet. LACNIC. Proveedores. Mail: concepto de correo-e. Cabeceras. Mail anónimo. Mail temporal. Preservación de correo-e. Parámetros necesarios para identificar un mail. Comprobar si existe. Google Mail. Software. DNS: definición de DNS (Domain Name Server). Jerarquía de servicios. Uso del DNS en las investigaciones. ICANN. TLDs. Registradores. Registros de dominios. Información de zona de los TLDs. Software. Deep Web & Dark Web: definición. Funcionamiento. Software. TOR. Desafíos en las investigaciones de delitos informáticos. Criptomonedas. Bitcoin. Funcionamiento de las billeteras virtuales. Delitos económicos. Fraudes" (ARGENTINA. Governo da Província de Buenos Aires. **Anexo nº IF-2021-06806836-GDBA-DPFCEMSGP**. La Plata, Buenos Aires. 22 de março de 2021.Disponível em: https://www.mseg.gba.gov.ar/areas/boletin_informativo/14IF-2021-06806836-GDEBA-DPFCEMSGP.pdf. Acesso em: 26 fev. 2022).

medidas de combate à lavagem de dinheiro e ao financiamento do terrorismo. O treinamento desenvolveu conscientização sobre como analisar e avaliar dados com sucesso, de forma a aumentar a eficácia das conclusões analíticas e recomendações fornecidas aos tomadores de decisão, além de aprimorar as atividades de *due diligence* e investigações conduzidas por inteligência.[309] Na Espanha, durante o recesso da pandemia, a Secretaria Técnica do Ministério Público avaliou como urgente a necessidade de pôr em andamento mudanças metodológicas na formação dos promotores para o desempenho de suas funções e aquisição de conhecimento para os anos vindouros, razão pela qual, no plano de formação continuada 2020 da carreira de Promotoria, incluiu a disciplina de técnicas de *Open Source Intelligence*.[310]

E, assim, desenha-se uma tendência de emprego massivo da inteligência em fontes abertas não apenas em território europeu, mas também da América Latina.

Na Argentina, a Procuradoria Regional da Província de Santa-Fé ofertou a promotores, funcionários e empregados das promotorias e membros da *Policia de Investigaciones* (*DPI*) curso de capacitação em torno de novas tecnologias digitais para investigações de delitos, incluindo disciplina específica de Inteligência de Fontes Abertas.[311] Ainda na Argentina, o Procurador Geral editou a Resolução P.G. n° 194/20, determinando aos membros do Ministério Público o aproveitamento de recursos tecnológicos para a investigação de delitos informáticos e aqueles cometidos com base em suportes tecnológicos, destacando-se como uma das primeiras ações da Secretaria de Política Criminal daquela instituição a criação de uma rede de orientações em investigação digital para compartilhar e delinear linhas de atuação, já que suas particularidades demandam sistematização de saberes e procedimentos apurados para transformar evidência digital em prova válida a ser incorporada e reproduzida em juízo. Na mesma linha, o *Informe de Gestión 2020*, do Ministério Público da Província de Buenos Aires, ressaltou a importância e os desafios da incorporação de evidências digitais ao processo penal como prova fundamental da investigação de qualquer delito, apontando como necessária a regulamentação adequada para permitir uma utilização eficiente das mesmas.

---

[309] UNIÃO EUROPEIA. Council of Europe. **Strengthening the rule of law and anti-corruption mechanisms**. Disponível em: https://pjp-eu.coe.int/en/web/pgg2/anti-corruption/-/asset_publisher/6W7G8ke6G0qc/content/open-source-intelligence-osint-training-in-azerbaijan?_101_INSTANCE_6W7G8ke6G0qc_viewMode=view/. Acesso em: 23 abr. 2022.

[310] FISCALÍA GENERAL DEL ESTADO. Secretaría Técnica. **7.3 Formacíon Continuada**. p. 74-84. Disponível em: https://www.fiscal.es/memorias/memoria2021/FISCALIA_SITE/capitulo_I/cap_I_7_3.html. Acesso em: 23 abr. 2022.

[311] PROVINCIA DE SANTA FE (Argentina). **Poder Judicial – Ministerio Público de la Acusacíon**. Disponível em: https://mpa.santafe.gov.ar/news/view/se_realizar_en_rosario_el_ curso_nuevas_tecnolog_as_digitales_ para_la_investigaci_n_de_delitos. Acesso em: 23 abr. 2022.

O relatório saúda a elaboração e a consolidação de *guias interativas, intuitivas e de fácil acesso* colocadas à disposição dos membros da instituição que exercem funções de investigação, destacando-se inteligência em fontes abertas, através de uma metodologia própria de investigação na rede, que comporta a conservação forense dos dados e sua análise a partir de motores de busca para acessar elementos de prova oportunos e *workshops de capacitação*, objetivando capacitar membros do Ministério Público argentino – e aqueles profissionais que provisoriamente exercem funções de detetive – com conhecimentos para conduzir de forma eficiente e eficaz *investigações de entornos digitais*[312]; o curso foi dividido em cinco módulos: análise de informação digital, a importância de formar analistas digitais, como potencializar investigações a partir de um dado, metodologia específica para coletar evidência digital e fontes de informação digital, com especial destaque para fontes abertas e Osint[313].

No Brasil, em setembro de 2019, por intermédio de sua Coordenadoria de Tecnologia da Informação e Comunicação – Assessoria de Pesquisa e Análise, a Procuradoria da República no Estado do Pará editou seu *Catálogo de Fontes Abertas*, acervo informacional que surgiu com o objetivo de apoiar as atividades finalísticas da instituição e incrementar a eficiência na utilização das fontes abertas, organizadas de forma temática, por servidores e público em geral. O documento situa as instituições do poder público "vezes como fornecedor, em outras como consumidor de dados", reverenciando a atuação do Estado-consumidor pela utilização de fontes de livre acesso por parte de órgãos responsáveis por investigações, "que não deveriam ficar restritas aos depoimentos e às tradicionais pesquisas [...] na busca da verdade real": incontáveis dados e informações, organizados ou não, estão disponíveis na rede mundial dos computadores e não são utilizados da forma devida em atividades investigativas, qualquer que seja esfera.[314]

Em dezembro de 2020, de forma a automatizar, aprofundar as coletas e analisar as relações do mundo real entre as informações que são acessíveis publicamente na internet, a

---

[312] "[...] *se diseñaron una serie de talleres, que se llevaron adelante de manera virtual, por la plataforma Microsoft Teams, en los que se inscribieron más de 450 agentes. Los disertantes y capacitadores resultaron agentes del Ministerio Público especializados en la temática, a saber: peritos y técnicos Informáticos, operadores especializados en UFED e I2 así como referentes en investigación digital. Los mismos, se llevaron adelante con la asistencia del Centro de Capacitación, y la producción de los diferentes eventos con la colaboración de personal de la Subsecretaría de Informática*" (MINISTERIO PÚBLICO DE LA PROVINCIA DE BUENOS AIRES. **Informe de Gestión 2020**. Disponível em: https://www.mpba.gob.ar/files/content/Informe% 20de%20 Gestion%202020.pdf. Acesso em: 23 abr. 2022).

[313] MINISTERIO PÚBLICO DE LA PROVINCIA DE BUENOS AIRES. **Informe de Gestión 2020**. Disponível em: https://www.mpba.gob.ar/files/content/Informe%20de%20Gestion%202020.pdf. Acesso em: 23 abr. 2022.

[314] Disponível em: http://bibliotecadigital.mpf.mp.br/bdmpf/handle/11549/188193?show=full. Acesso em: 29 dez. 2021.

Comissão de Licitação da Procuradoria-Geral de Justiça do Estado de Goiás tornou público o Edital de Licitação nº 158/2020, com objeto na aquisição de *software* Maltego-Pro – ferramenta com capacidade de entregar uma figura clara de relacionamento de organizações; classificar entidades como pessoas, grupos, companhias, organizações, páginas *web*, infraestrutura de internet, frases, documentos e arquivos em diversas extensões; utilizar fontes abertas de inteligência do que estiver indexado na internet; viabilizar a busca de informações em redes sociais e *sites* de busca – para utilização no Centro de Inteligência do Ministério Público de Goiás (CI-MPGO). Justificou-se a contratação "para a automatização de tarefas, buscas na *web* e visualização de resultados em um ambiente único, redução da complexidade de trabalho, redução da complexidade para interpretação e entrega de resultados", tudo de forma a "reduzir tempo-resposta de uma investigação"[315].

Na mesma época, por intermédio do Pregão Eletrônico nº 046/2020-MPAP – Processo nº 20.06.0000.0003919/2020-65/MPAP, a Procuradoria-Geral de Justiça do Estado do Amapá também licitou uma cessão anual de direito de uso sobre programas de computador para coleta de dados em fontes abertas com o objetivo de subsidiar tecnicamente as atividades da Assessoria de Investigação em Tecnologia da Informação na prestação de serviço de identificação, coleta, preservação e correlacionamento de dados dessa natureza. A aquisição de programas com características para automatização de tarefas, buscas na *web* e visualização de resultados em um ambiente único e redução da complexidade para interpretação de resultados também se deu com o propósito de reduzir o tempo-resposta de pesquisa inteligente em fontes abertas e reduzir a complexidade do trabalho feito por humanos.[316]

Capacitações também estão ocorrendo no Brasil. Entre os dias 12 e 15 de março de 2022, sete membros e 14 servidores do Ministério Público Federal (MPF) participaram de curso da Organização dos Estados Americanos (OEA) sobre Inteligência de Fonte Aberta (Osint), no qual foram treinados para investigarem pessoas e empresas utilizando informações públicas, como redes sociais, publicações e notícias.[317] Outra edição do curso já havia

---

[315] Disponível em: https://intranet.mpgo.mp.br/sgoc/upload/edital/SGOC_CPL_Edital_Ed.158-2020_PE_SRP%20-%20Aquisicao%20de%20software%20de%20analise%20em%20fontes%20%20-Processo%20n.%202020-375697_Regra%20Geral%20e%20Exclusividade%20ME%20EPP.pdf. Acesso em: 29 dez. 2021.

[316] MINISTÉRIO PÚBLICO DO ESTADO DO AMAPÁ. Edital de licitação. Pregão nº 046/2020. Processo nº 20.06.0000.0003919/2020-65/MPAP. [OBJETO: Cessão anual de direito de uso sobre programas de computador para coleta de dados em fontes abertas, de acordo com as especificações e exigências dispostas no Termo de Referência]. **Procuradoria-Geral de Justiça.** Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/noticias/noticias-1-1/membros-e-servidores-participam-de-curso-da-oea-sobre-pesquisa-em-dados-abertos. Acesso em: 23 abr. 2022.

[317] BRASIL. Ministério Público Federal. **Membros e servidores participam de curso da OEA sobre pesquisa em dados abertos**. 2 de abril [20--]. Disponível em: http://www.mpf.mp.br/atuacao-

ocorrido no Instituto Nacional de Criminalística, em Brasília, entre os dias 15 e 16 de março de 2018.[318]

Entre 29 de novembro e 3 de dezembro de 2021, a Escola Superior do Ministério Público de Pernambuco ofertou a seus membros e servidores, prioritariamente aqueles que executam atividades de inteligência e combate ao crime organizado, o Curso de Inteligência e Investigação em Fontes Abertas – Osint, com o objetivo de capacitá-los a coletar e analisar dados e informações em fontes abertas no contexto da *surface web* e da *deep web*[319]. Parte do curso "Investigação Criminal na Era Tecnológica", o *workshop* "Técnicas de Open Source Intelligence (OSINT)" promoveu para membros e servidores do Ministério Público de Sergipe um exercício prático de investigação digital em fontes abertas para rastreamento de ativos, com a apresentação de ferramentas e "metodologia essencial"[320].

4.5. Inteligência de fontes abertas e o Tribunal Penal Internacional

Um dos problemas do Tribunal Penal Internacional, a efetividade da cooperação internacional nas diligências penais, é apontada como causa para que processos não se desenvolvam da forma como espera a comunidade internacional ou que se encerre as investigações por falta de elementos.[321] Considerando a função institucional do procurador do Tribunal Penal Internacional em conduzir investigações de forma que consiga judicializar

---

tematica/sci/noticias/noticias-1-1/membros-e-servidores-participam-de-curso-da-oea-sobre-pesquisa-em-dados-abertos. Acesso em: 23 abr. 2022.

[318] BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão Criminal. Edital 2CCR nº 7, de 6 de março de 2018. [Seleção de Participantes do Curso]. Brasília: 2ª Câmara de Coordenação e Revisão Criminal, 6 de março de 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/comunicados-da-2a-ccr-1/2018/ comunicado_17_edital_curso_oea_brasilia.pdf. Acesso em: 23 abr. 2022.

[319] MINISTÉRIO PÚBLICO DE PERNAMBUCO. **Curso de Inteligência e Investigação em Fontes Abertas – OSINT**. [2021]. Disponível em: https://www.mppe.mp.br/mppe/institucional/escola-superior/ultimas-noticias-escola-superior/15370-curso-de-inteligencia-e-investigacao-em-fontes-abertas-osint. Acesso em: 23 abr. 2022.

[320] MINISTÉRIO PÚBLICO DE SERGIPE. **Membros e servidores do MPSE participam de workshop presencial sobre investigação digital em fontes abertas**. Aracaju, Sergipe. Disponível em: https://www.mpse.mp.br/index.php/2021/11/16/membros-e-servidores-do-mpse-participam-de-workshop-presencial-sobre-investigacao-digital-em-fontes-abertas/. Acesso em: 23 abr. 2022.

[321] "E eles representam um desafio aos tribunais sobre a natureza da confiabilidade e dos padrões probatórios. Tribunais internacionais de direitos humanos, como o TPI, estão apenas começando a decidir o que fazer com as evidências obtidas de fontes abertas como Facebook e YouTube.Mas os defensores dos direitos humanos devem mudar com um mundo em mudança. A adoção generalizada de dispositivos móveis conectados à Internet e mídias sociais resultou em fontes de evidências ricas, mas não tradicionais. As investigações de código aberto oferecem uma maneira de entender a grande quantidade de informações disponíveis *online*. Eles vão economizar dinheiro. Mais importante, eles vão salvar vidas. Por essas razões, os tribunais internacionais de direitos humanos devem adotar investigações de código aberto e devem esclarecer as regras probatórias para permitir a admissão e uma ponderação mais clara desse novo e poderoso tipo de evidência" (HIATT, Keith. **Open Source Evidence on Trial**. 125 Yale LJF 323 (2016). Disponível em: http://www.yalelawjournal.org/forum/open-source-evidence-on-trial. Acesso em: 23 abr. 2022).

demandas por conta das violações aos Direitos Humanos e Direito Internacional Humanitário, defende-se o uso do produto derivado de Osint como forma de adiantar investigações sem que a promotoria dependa da assistência dos Estados-parte.

Ao menos essa foi a direção da decisão no caso contra Mahmoud Mustafa Busayf Al-Werfalli, nos casos dos episódios de violência na Líbia, em razão de a Corte ter aceito como suficiente para decretar ordem de arresto material probatório derivado Osint, encontrados em redes sociais como Facebook e Twitter, o que fez denotar que o Tribunal Penal Internacional reconheceu que o material cumpriu com o estândar probatório estabelecido no artigo 58 do Estatuto de Roma[322]: considera-se que, ao menos naquela fase, elementos apresentados baseados em inteligência em fontes abertas foram suficientes para provar a prática de um crime de competência da Corte. A propósito, em seu Planejamento Estratégico 2016/2018, o Tribunal Penal Internacional apontou a necessidade de estabelecer cooperação com agências de inteligência capazes de processar dados de Osint, assim como o desenvolvimento e a sistematização de uma base de dados sobre crimes que permita rápido acesso a informações de interesse das atividades do Tribunal[323].

---

[322] ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. **Estatuto de Roma de la Corte Penal Internacional**. Disponível em: https://www.ohchr.org/es/instruments-mechanisms/instruments/rome-statute-international-criminal-court. Acesso em: 15 ago. 2022.

[323] "[...] *o régimen de cooperación establecido a partir de una relación mixta entre la CPI y los Estados parte del ER ha dificultado aún más la relación entre estos, teniendo en cuenta que la Corte no tiene capacidad sancionatoria frente al Estado que incumple con las obligaciones establecidas en el tratado de Roma, y que la Asamblea de Estados Parte, que es la entidad capaz de eventualmente sancionar por dicho incumplimiento, tampoco cuenta con una forma de coerción suficiente para materializar las sanciones que pudiera imponer*
[...]
No obstante, no se han logrado pronunciamientos donde una eventual confirmación de cargos se base en dicho material probatorio y cumpla así con el estándar contenido en el artículo 61(7) y misma situación se aprecia en lo relativo a una condena y el respeto al estándar contenido en el artículo 66(3), por lo que no hay certeza de cuál será el tratamiento que se le dé a las pruebas ya recopiladas en el caso antes mencionado. No obstante lo anterior, debe decirse que el material probatorio OSINT, una vez ha sido validado frente a su confiabilidad, esto es, el cómo, cuándo, por qué, por quién y dónde fue producido, si representa a todas luces una prueba admisible ante la CPI y lo que se estudiará en juicio será, dependiendo de cada elemento, el peso que cada uno de ellos pudiera tener frente a los hechos que se pretenden probar. La potencialidad es enorme y desarrollo de esta herramienta está apenas empezando y los retos para dotarla de confiabilidad, peso y pertinencia son enormes, no obstante, debe recordarse que similares ejercicios se están dando en Suecia y Alemania, donde Cortes nacionales están optando por dotar probatoriamente sus casos con elementos derivados de OSINT y así terminar con la situación de impunidad en la situación actual de Siria. El reto que tiene la CPI es enorme sin lugar a dudas, por las implicaciones de cooperación con agencias internacionales, por los retos tecnológicos que supone validar el material probatorio que se pretende hacer valer en juicio, por el desafío jurídico de introducir una forma relativamente nueva de prueba en juicio de forma que respete los estándares del ER y los derechos del acusado. Sin embargo, es la oportunidad para que se genere una forma investigativa en la que la CPI saldrá fortalecida ante la nueva capacidad de adelantar pesquisas sin depender cómo lo hace en la actualidad de la cooperación internacional en asistencia judicial" (DIAZ MANILLA, Luis Felipe. **Open Source Intelligence en la CPI**: hacia un nuevo paradigma de investigación más allá de la cooperación internacional. Colômbia*:* Uniandes, 2018).

5. O TRATAMENTO DE DADOS E A GARANTIA DO DIREITO DE DEFESA

5.1. Ainda sobre a participação ativa da defesa e a paridade de armas na fase preliminar

O emprego da mentalidade disruptiva e do pensamento não linear a partir da modificação promovida pela experiência interativa compreende a invasão tecnológica como um novo modo de engajamento no processo penal e que oferece suporte para uma nova forma de enfrentamento das adversidades. Tecnologia passa a ser pressuposto de atuação alinhada à complexidade e à velocidade de novas dinâmicas decorrentes do incremento de aplicações que produzem dados e elementos informacionais a todo momento, e a capacidade de avaliação e emprego dessas novas ferramentas, além de incremento em performance, oferece vantagens pelo alcance em informações qualificadas em apoio às decisões; não apenas decisões judiciais, mas todas aquelas que devem ser tomadas pelos agentes processuais[324].

Enquanto Polícias e Ministérios Públicos, sempre que possível, trabalharam a partir de uma lógica de acesso e compartilhamento ilimitado – e, agora, transnacional de dados fechados e abertos –, a razão inquisitorial reservou às defesas relativa incapacidade de interlocução e absoluta ausência de protocolos de compartilhamento de dados e informações relevantes, implicando a fragmentação de elementos, muitas vezes úteis. Se não houver mudança do *mind set* defensivo, o ambiente tecnológico alargará ainda mais o abismo entre investigação/acusação e defesa.

Não é de hoje que as pesquisas promovidas no campo da Sociologia[325] e da

---

[324] "Os agentes processuais trazem consigo um conjunto de convicções robusto e entrincheirado. A posição analógica pode gerar a falsa sensação de segurança, mas no mundo digital, significa defasagem. O agente processual analógico corre sérios riscos porque a aceleração tecnológica é silenciosa e avassaladora, sem que, talvez, tenha sequer tempo suficiente para recuperar a desvantagem tecnológica atual, além de, depois de se dar conta, perceber que sua resistência pode ter lhe custado erros crassos. É do constante trabalho de atualização das antigas convicções em face dos avanços tecnológicos que surge a capacidade de compreender melhor o ambiente processual penal invadido pela tecnologia. Será preciso reconhecer que alguns comportamentos simplesmente ficaram obsoletos/ultrapassados. O futuro do direito depende de uma decisão pessoal. De uma atitude. O ambiente digital do processo penal modificou-se e os agentes processuais precisam assumir as evidências: ou se atualizam tecnologicamente, ou continuarão em flagrante desvantagem competitiva.
[...]
O trabalho dos agentes processuais (com tecnologia) será cada vez mais artesanal, de um modo diverso. A capacidade de customização do Caso Penal, diante das potencialidades cognitivas das máquinas, amplia os horizontes, mas depende dos parâmetros, da seleção dos dados, das fontes, realizadas sob a nossa supervisão. O que faremos é mostrar como a máquina, sempre supervisionada por humanos, pode melhorar (muito) o nosso desempenho, em alguns casos, conferir condições mínimas de paridade de armas (matéria probatória, principalmente). A nossa capacidade de singularizar/individualizar o Caso Penal será a alavanca capaz de conferir 'ração cognitiva' aos sistemas de apoio à decisão" (ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico**: de acordo com a teoria dos jogos e MCDA-A. Florianópolis: Emais, 2021. 42-49).

[325] AZEVEDO, Rodrigo Ghiringhelli de. Elementos para a Modernização das Polícias no Brasil. **Revista**

Criminologia apontam para a insuficiência do dispositivo inquérito policial[326]: denunciam que, em favor do bom funcionamento do sistema, a gestão do inquérito acaba virando palco de acordos e pactos informais, o que propicia desvios da lei geridos institucionalmente[327] e fixa a passagem entre a polícia e o Ministério Público como o *locus* em que ocorre o principal gargalo de todo sistema, já que é o inquérito que forma culpa e, na prática, toma forma de uma pré-instrução criminal dominante na etapa judiciária e que se reproduz nesses sistema de crença de perfil bacharelesco, baseado no dogma de uma verdade real obtida pela lógica do expediente cartorário, burocrático e chancelada por uma autoridade que detenha fé-pública[328], o que permite sustentar que efeitos probatórios decorrentes da manutenção dos atos praticados durante o inquérito policial no processo penal produzem "abalos indestrutíveis à presunção de inocência", pois o que se está produzindo são elementos decisivos em plena investigação preliminar[329]. O modelo sob presidência do juiz instrutor propiciou relações mais próximas entre o Judiciário e a Polícia, papéis não desempenhados em outras tradições judiciais, em que arranjos organizacionais orientados de maneira distinta esculpiram diferentes possibilidades de interação, papéis e conflitos pela distribuição dos saberes/poderes[330].

Essa estrutura histórica e culturalmente comprometida com matrizes inquisitoriais inviabiliza o exercício do contraditório como estabelecido no marco constitucional. Ao contrário, ela rompe com qualquer possibilidade de paridade de forças, inverte e mescla funções, põe o Estado-jurisdição a serviço do Estado-acusação e chancela de forma imodificável os elementos, muitas vezes produzidos por meio de práticas não discursivas[331]. A intersecção entre essa fase – reconhecidamente uma faixa de tensão entre a eficiência da persecução penal e direitos fundamentais – e o advento da realidade tecnológica já atraiu a atenção em busca de regulação específica no âmbito europeu, objetivo de difícil alcance em razão dos tantos desafios impostos pelo vertiginoso progresso tecnológico.

Dentre outros tantos princípios afetados, emerge de forma intensa a *igualdade de armas no processo penal*: a acusação goza de maiores recursos e acesso a melhores

---

Brasileira de Segurança Pública, São Paulo, v. 10, p. 8-20, mar. 2016.

[326] SAMPAIO, André. Profanando o dispositivo Inquérito Policial e seu Ritual de Produção de Verdades. **Revista Brasileira de Ciências Criminais**, São Paulo, ano 25, v. 134, p. 351-383, 2017. p. 353.

[327] SUTHERLAND, Edwin. White-collar criminality, *in* **American Sociological Review**, v. 5, n. 1, 1940, p. 01-12.

[328] AZEVEDO, Rodrigo Ghiringhelli de. Elementos para a Modernização das Polícias no Brasil. **Revista Brasileira de Segurança Pública**, São Paulo, v. 10, p. 8-20, mar. 2016.

[329] GLOECKNER, Ricardo Jacobsen. **Autoritarismo e Processo Penal: uma genealogia das ideias autoritárias do processo penal brasileiro**. Florianópolis: Tirant lo Blanch, 2018. p. 397.

[330] MACHADO, Bruno Amaral. O inquérito policial e a divisão do trabalho jurídico-penal no Brasil: discursos e práticas. **Revista Brasileira de Segurança Pública**, São Paulo, v. 9, n. 1, p. 12-33, fev./mar. 2015. p. 13.

[331] GARLAND, David. **La Cultura del Control**: crimen y orden social en la sociedad contemporánea. Barcelona: Gedisa, 2005. p. 67.

tecnologias para obter resultados para propor como meios de prova; a defesa, desprovida de elementos para contrariar, ainda é onerada pela dificuldade de contrapor e colocar em questão a credibilidade da prova[332].

Por outro lado, é recorrente a crítica de que os órgãos do sistema de Justiça criminal brasileiro operam com cifras ocultas[333], sendo o modelo baseado na atribuição de poderes de investigação concentrados preponderantemente nas mãos das autoridades policiais totalmente fracassado. Os seus dogmas de verdade – de que é a investigação policial a responsável por colher *todas* as provas que servem para o esclarecimento do fato e de suas circunstâncias (inciso III do art. 6º do Código de Processo Penal), além de fornecer às autoridades judiciárias as informações *necessárias* à instrução e julgamento do processo (art. 13, I, do Código de Processo Penal) – absolutamente questionáveis.[334]

Admitindo que o nosso sistema atual possibilita de forma legal a intromissão do conteúdo do inquérito policial na formação da decisão judicial, a investigação policial com plenitude contraditória poderia inserir a atividade definitivamente dentro do marco democrático, legitimando o conteúdo das decisões judiciais amparadas nos elementos lá produzidos[335], superando uma das premissas basilares de um sistema inquisitório, que é o de que a defesa – leia-se o contraditório – só atrapalha na busca pela verdade[336].

O conteúdo da atuação dos órgãos responsáveis pela investigação do crime é relativamente amplo, não se restringindo ao conhecimento e à aplicação de normas de natureza constitucional ou processual penal; também, está relacionado ao domínio de tantas técnicas de investigação e de inteligência possíveis e necessárias para apuração de uma criminalidade que se reinventa na mesma velocidade e com a mesma complexidade que

---

[332] RODRIGUES. Anabela Miranda. Inteligência artificial e Direito Penal – a justiça preditiva entre a Americanização e a Europeização. *In*: RODRIGUES. Anabela Miranda (coord.). **A Inteligência Artificial no Direito Penal**. Coimbra: Edições Almedina, 2020. p. 14-17.

[333] A discricionariedade policial para decidir que ocorrência gerará ou não um inquérito e o que ali constará ou não, é apontada por alguns operadores do sistema de Justiça criminal como um elemento que gera consequências em todo o fluxo da Justiça. Diante do aumento da demanda, é cada vez maior a distância entre os delitos registrados e os que são efetivamente investigados, obrigando os policiais a desenvolverem critérios informais para selecionar os casos que serão priorizados (AZEVEDO, Rodrigo Ghiringhelli de. Elementos para a Modernização das Polícias no Brasil. **Revista Brasileira de Segurança Pública**, São Paulo, v. 10, p. 8-20, mar. 2016).

[334] MENDES, Carlos Hélder Carvalho Furtado; MELO, Marcos Eugenio Vieira; MENDES, Tiago Bunning. A lei 13.245/2016 e a efetivação das prerrogativas do advogado na investigação criminal: garantia constitucional ao direito de defesa na fase preliminar. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 159, n. 0, p. 261-296, set. 2019.

[335] SAMPAIO, André. Profanando o dispositivo Inquérito Policial e seu Ritual de Produção de Verdades. **Revista Brasileira de Ciências Criminais**, São Paulo, ano 25, v. 134, p. 351-383, 2017. p. 361-362.

[336] SAMPAIO, André Rocha. Polícia para quê (quem), ou o ataque do coiote fracote ao poder disciplinar do soberano. *In*: **Biopolíticas**: estudos sobre Política, Governamentalidade e Violência. Curitiba: Iea academia, 2015. p. 327.

andam todas as nossas relações sociais.

Partindo do pressuposto de que, em uma República democrática, os poderes sem controle não devem ser tolerados – poder sem freio vira abuso[337] – e que o exercício do poder digital varia de acordo com os consórcios que se estabelecem no contexto do seu exercício, cabe papel importante ao Legislativo para coibir os excessos decorrentes do "encantamento digital". Em ensaio contemplando considerações oferecidas à Comissão de Juristas no painel "Proteção de dados pessoais na segurança pública e investigação criminal", promovido pela Câmara dos Deputados do Congresso Nacional Brasileiro durante o VI do Seminário Internacional da Comissão de Juristas, defendeu-se, na busca por domesticar o "poder digital", a necessidade de uma redefinição dos limites da disciplina Processo Penal através do uso de elementos como controle, transparência, equilíbrio e prestação pública de contas. Essa redefinição implica considerar três aspectos a serem avaliados em conjunto com os temas estruturantes tradicionais: (i) policiamento preditivo; (ii) extraterritorialidade das normativas[338]; (iii) sujeitos processuais[339], dos quais nos interessa especificamente este último.

A partir da consideração de que, no "mundo digital", a tutela do interesse público que envolve a apuração do fato controvertido poderá estar condicionada pelo domínio de ferramentas, acesso a plataformas e emprego de linguagem digitais a reclamar uma metalinguagem que faça a mediação entre as narrativas cibernética e jurídica, existe a necessidade urgente de se enxergar corporações digitais como sujeitos processuais que

---

[337] "A democracia e a aristocracia não são Estados livres por natureza. A liberdade política só se encontra nos governos moderados. Mas ela nem sempre existe nos Estados moderados; só existe quando não se abusa do poder; mas trata-se de uma experiência eterna que todo homem que possui poder é levado a dele abusar; ele vai até onde encontra limites. Quem diria! Até a virtude precisa de limites. Para que não se possa abusar do poder, é preciso que, pela disposição das coisas, o poder limite o poder. Uma constituição pode ser tal que ninguém seja obrigado a fazer as coisas a que a lei não obriga e a não fazer aquelas que a lei permite" (MONTESQUIEU, Charles de Secondat, Baron de. **O espírito das leis**. São Paulo: Martins Fontes, 1996. p. 166-167).

[338] A característica evidentemente transfronteiriça do uso trivial das Tecnologias de Informação e Comunicação (TICs) provoca reações normativas, ora de defesa das soberanias estatais, no âmbito das quais situam-se os Poderes Judiciários, MPs e Polícias — como na hipótese do Cloud Act —, ora de harmonização multinível, como na Proposta de Regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrônicas em matéria penal (PRADO, Geraldo. Proteção de dados, prova digital e devido processo legal. **VI Seminário Internacional "Proteção de dados pessoais na segurança pública e investigação criminal"**. Câmara dos Deputados do Congresso Nacional Brasileiro: Brasília, jul-2020. Disponível em: https://www.youtube.com/watch?v=J4m5yiQnLbI&feature=youtu.be. Acesso em: 20 abr. 2022).

[339] O papel desempenhado pelos sujeitos privados no processo penal – ao lado de polícia, MP, defesa e juiz – com as grandes corporações de mídia social convertendo-se em players decisivos na gestão das condições concretas de autodeterminação informativa, proteção da segurança e cooperação nas investigações e processos criminais, altera sobremaneira a lógica de funcionamento do sistema e afeta a capacidade de intervenção dos agentes públicos (PRADO, Geraldo. Proteção de dados, prova digital e devido processo legal. **VI Seminário Internacional "Proteção de dados pessoais na segurança pública e investigação criminal"**. Câmara dos Deputados do Congresso Nacional Brasileiro: Brasília. jul-2020. Disponível em: https://www.youtube.com/watch?v=J4m5yiQnLbI&feature=youtu.be. Acesso em: 20 abr. 2022).

exercem, concretamente, poderes que interferem no arbitramento da responsabilidade penal: elas podem ditar o ritmo das investigações e o acesso a informações essenciais à apuração dos fatos. A consecução de diligências de investigação eletrônica para a aquisição, preservação de informações, tratamento e análise de dados no âmbito de empresas privadas pode ser definida como *externalização da investigação*, colaboração muitas vezes essencial para o acesso a informações penalmente relevantes. No acelerado processo de desenvolvimento do mundo digital, também as perícias digitais assumem papel relevante: ainda que não venham a ser protagonistas, assistentes e técnicos vão ocupar espaço de destaque no processo criminal, cada vez mais aproximando-se da centralidade das questões penais controvertidas[340]. Esse aparato tecnológico, antes concentrado exclusivamente nas mãos das autoridades públicas e amplamente utilizadas para o exercício do controle, hoje torna-se disponível para todos os tipos de finalidade e de interesses na obtenção de informações[341].

Com o acelerado cenário que se apresenta por conta do salto da indústria das tecnologias 4.0 para as tecnologias 5.0, haverá uma profunda ressignificação do papel do ser humano ante as tecnologias disruptivas que estão a moldar as sociedades e a forma como pessoas e instituições se estruturam e relacionam: como última fase do desenvolvimento baseado em novas soluções, a indústria 5.0 se caracteriza por ser um período que equilibra a participação de pessoas e máquinas no ambiente de trabalho, obtendo o melhor dos diferenciais de cada um em prol dos resultados. Alia tecnologia ao potencial humano, em uma abordagem centrada na participação das pessoas e colaboração entre equipe e sistemas como fator de vantagem competitiva e rapidez na tomada de decisão, atingindo mercado, instituições e suas estruturas, modificando a forma como produzimos, trabalhamos, vivemos e nos relacionamos e criando como tendência uma nova visão do mundo do trabalho e instituições. Integrar essas soluções à mudança de postura passará a ser um predicado necessário ao desempenho das atividades humanas: a realidade 5.0 passou a exigir, dentre outros: (i) adesão a novas tecnologias em todos os processos, aliada à adaptações culturais dos sujeitos aos novos valores; (ii) mudança de *mindset*, orientada à formação e ao treinamento da equipe com investimentos em letramento digital; (iii) adoção de decisões baseadas em dados; (iv) investimento em cibersegurança.

---

[340] PRADO, Geraldo. Proteção de dados, prova digital e devido processo legal. **VI Seminário Internacional "Proteção de dados pessoais na segurança pública e investigação criminal"**. Câmara dos Deputados do Congresso Nacional Brasileiro: Brasília, jul-2020. Disponível em: https://www.youtube.com/watch?v=J4m5yiQnLbI&feature=youtu.be. Acesso em: 20 abr. 2022.

[341] COLOMER, Juan-Luis Gómez. Estado democrático y modelo policial: Una propuesta de diseño de cara a lograr una investigación eficaz del crimen. *In*: AMBOS, Kai; COLOMER, Juan-Luis Gómez; VOGLER, Righard. **La Policía en los Estados de Derecho Latinoamericanos**: un proyecto internacional de investigación. Chile: Ediciones Jurídicas Gustavo Ibáñez G., 2003.

A teoria da gestão distingue tecnologias entre *de sustentação* e *disruptivas*. As primeiras apoiam e melhoram a forma como um negócio, um mercado, empresa ou setor funcionam; as segundas alteraram o seu funcionamento. Em relação aos profissionais do mundo jurídico, existem ao menos muitas tecnologias disruptivas a desafiar e alterar a forma como os serviços serão prestados, dentre as quais, aqui, destacaremos: (i) conectividade implacável; (ii) *e-learning*; (iii) fornecimento aberto legal; (iv) comunidades jurídicas fechadas; (v) previsão da máquina; (vi) *analytics*; (vii) redição da máquina[342].

A conectividade implacável da tecnologia impede que advogados se desliguem de clientes e local de trabalho, e a tendência é de que isso se intensifique bastante; o *e-learning* transformará como escritórios de advocacia fornecem e integram suas funções de formação e *know-how*, alterando disciplinas de formação expositivas em sala de aula para aprendizagem prática baseada em ferramentas interativas. Prevê-se uma massiva colaboração *online* pela troca de dados provenientes de fontes abertas em geral, e, no campo do Direito, isso pode significar a construção de grandes bancos de materiais jurídicos públicos e, por consequência, uma forma de comoditização.[343]

Formam-se consórcios de advogados com interesses comuns e que cooperam entre si, compartilhando até mesmo inteligência, em redes privadas, muitos deles equipados com acesso a sistemas preparados para analisar grande quantidade de documentos e capacitados em *big data* e *analytics*, sistemas emergentes que analisam conjuntos de documentos e deles extraem inteligência. Essas capacidades de pesquisa e aprendizagem de máquinas não suportam apenas escritórios de advocacia, mas fomenta o surgimento de novos sujeitos que colaboram decisivamente no serviço jurídico, inclusive na investigação ou no processo penal[344].

Combinados, dados obtidos pelas atividades inerentes à advocacia àqueles acessíveis ao público permitem a produção de previsões ou hipóteses em relação às causas; conhecimentos cruciais à prática jurídica e à gestão do risco jurídico poderá ser gerada de algoritmos que operam em dados e que podem ser desenvolvidas exclusivamente por cientistas de dados. À medida que novas tecnologias são implantadas, inevitável deixar de

---

[342] SUSSKIND, Richard E**. Tomorrow's lawyers:** An introduction to your future. USA: Oxford University Press, 2017. p. 32-58.
[343] SUSSKIND, Richard E. **Tomorrow's lawyers**: An introduction to your future. USA: Oxford University Press, 2017. p. 32-58.
[344] SUSSKIND, Richard E. **Tomorrow's lawyers**: An introduction to your future. USA: Oxford University Press, 2017. p. 32-58.

pensar em trabalhar de forma diferente, adotar métodos alternativos de trabalho, o que exige gestão de mudança e preparação estrutural para o emprego de métodos alternativos.[345]

A aparente *inevitabilidade*[346] no emprego dessas tecnologias demandará esforços de todas as ordens para que pessoas e grupos totalitários não se apropriem delas para emprego na ampliação do exercício do poder punitivo, havendo de se reconhecer limites válidos ao emprego dessas técnicas, sobretudo diante da aparente expansão que possibilita a utilização desses mecanismos por outros sujeitos interessados na investigação[347].

Garantias judiciais impõem que pessoas suspeitas ou acusadas tenham acesso a uma *defesa penal efetiva*, da qual emana uma série de direitos processuais, dentre os quais merecem especial destaque o direito de investigar o caso, no qual o exercício do contraditório se mostra essencial de forma a assegurar que imputado e seu defensor tenham possibilidades reais de investigar o caso e propor a produção de elementos, exercício que não deve se dar exclusivamente na fase judicial através de postulação, admissão, produção e valoração da prova, senão também de forma em que se outorgue poderes para que imputado e defensor realizem investigações para localizar elementos de interesse probatório.[348] Ainda que a investigação preliminar esteja a cargo do Estado, admite-se a defensiva. Se o escopo é a apuração na maior amplitude possível do fato, os valores democráticos autorizam a colaboração dos envolvidos em seu esclarecimento em todas as etapas procedimentais da persecução penal. Em espaços de consenso, a situação é ainda mais sensível: ou a defesa investiga, ou sequer terá chances de produzir elementos nas etapas antecedentes ao julgamento, uma vez que as evidências apresentadas ao processo serão restritas àquelas apuradas pelos órgãos encarregados pela persecução penal, tornando equivocada a postura daquele que aguarda a coleta de elementos pelo Estado para dar início ao exercício da defesa.[349]

---

[345] SUSSKIND, Richard E. **Tomorrow's lawyers**: An introduction to your future. USA: Oxford University Press, 2017. p. 32-58.

[346] ZUBOFF. Shoshana. **A era do capitalismo da vigilância: a luta por um futuro humano na nova fronteira do poder**. Rio de Janeiro: Intrínseca, 2020.

[347] FRANÇA JÚNIOR, Francisco de Assis; LEITÃO SANTOS, Bruno Cavalcanti; NASCIMENTO, Felipe Costa Laurindo do. Aspectos críticos da expansão das possibilidades de recursos tecnológicos na investigação criminal: a inteligência artificial no âmbito do sistema de controle e de punição. **Revista Brasileira De Direito Processual Penal**, v. 6, n. 1, p. 211–246, 2020. DOI: https://doi.org/10.22197/rbdpp.v6i1.334.

[348] BINDER, Alberto; CAPE, Ed; NAMORADZE. **Defesa Penal Efectiva em America Latina**: Argentina, Brasil, Colômbia, Guatemala, México, Peru. [*S. l.*]: ADC, Cerjusc, Conectas, Dejusticia, ICCPG, IDDD, IJPP, Inecip, 2015. p. 90-92.

[349] ROSA, Alexandre Morais da; CAMARGO, Rodrigo Oliveira de. O desafio de qualificar a prática da investigação defensiva. **Revista Consultor Jurídico**, 23 set. 2022. Disponível em: https://www.conjur.com.br/2022-set-23/limite-penal-desafio-qualificar-pratica-investigacao-defensiva. Acesso em: 23 set. 2022.

Daí a emergência no debate sobre a descentralização do poder de investigar[350], sobretudo porque informação é coisa pública, investigação significa acesso ao poder de saber e por que existe uma modificação significativa na sociedade a partir do advento das experiências tecnológicas e a ampliação de métodos de acesso à informação, circunstâncias que fundamentam, ainda mais, o direito à participação e à ampliação do direito à informação nos atos que levam a essas decisões de poder. A paridade de armas reacende com o fim do monopólio probatório do Estado, possibilita a mitigação de investigações enviesadas ou alinhadas a um único propósito e permite inventariar e investigar os elementos úteis ao exercício pleno da ampla defesa. Negar à defesa a atividade investigatória não apenas aniquila as chances de produção de elementos úteis como também a chance de descoberta de comportamentos oportunistas por parte dos agentes da investigação oficial, ampliados pelo poder digital[351].

Em um sistema baseado na perspectiva acusatória, são comuns as atividades de investigações levadas a efeito por unidades privadas que oferecem suporte integral ao advogado durante a defesa criminal. O contraditório exige que as partes tenham um acesso legal e concomitante a toda informação pertinente para o processo, ao passo que só aparece no direito continental como uma etapa da instância, seu momento público mais secundário em relação à fase preparatória amplamente controlada pelo juiz. O acesso à pré-construção da causa tem por função colocar os fatos em situação de serem julgados e constituirá, durante toda a duração do processo, a referência dos debates. O modelo de acusação, dada a sua desvinculação com a verdade, não garante que todas as informações pertinentes sejam apresentadas no debate, mas a igualdade de oportunidades consiste em dispor de meios idênticos para que as partes proponham sua própria argumentação[352].

No âmbito da investigação dos fatos, isso implica que as partes e seus advogados tenham condições de ir à busca de elementos do material probatório, preparando-o para sua utilização em juízo, o que transforma inerentes ao sistema poderes para que advogados busquem, selecionem e apresentem em juízo da maneira mais favorável. O conceito de *propriedade de prova* é uma expressão que claramente se associa a essa atividade:

---

[350] CAMARGO, Rodrigo Oliveira de; BULHÕES, Gabriel. Defesa Penal Efetiva no Brasil: desafios da atuação defensiva na investigação preliminar em meio ao sistema acusatório. *In*: GONZÁLEZ, Leonel; BALLESTREROS, Paula. **Desafiando a Inquisição**: ideias e propostas para a reforma processual no Brasil. Santiago: Ceja-JSCA. 2019.

[351] ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico**: de acordo com a teoria dos jogos e MCDA-A. Florianópolis: Emais, 2021. p. 557-567.

[352] GARAPON, Antonie; PAPAPOULOS, Ioannis. **Julgar nos Estados Unidos e na França**: cultura jurídica francesa e *Common law* em uma perspectiva comparada. Rio de Janeiro: Lumen Juris Editora, 2008. p. 88.

testemunhas pertencem à parte proponente e, quando atestam algo para ela, somente situações extremas podem macular sua credibilidade. Por isso é de suma importância a oportunidade de atacar imediatamente fontes de informação apresentadas pela parte contrária, decorrência de um princípio geral de justiça estruturado sob um esquema competitivo de determinação dos fatos.[353]

Integradas por investigadores particulares com formação e capacidade de encontrar evidências negligenciadas ou ignoradas pelos órgãos de aplicação da lei, como testemunhas desconhecidas ou provas físicas, e que atuam orientados por métodos de investigação empregados desde a investigação de campo até análises avançadas baseadas em suporte tecnológico, empresas entregam assistência em áreas como revisão e análise dos dados da notícia crime e da investigação ou processo, entrevista com o réu ou testemunha, revisão e análise do local dos fatos, revisão e exame de evidências, verificação de antecedentes de sujeitos que envolvem o caso penal e/ou descoberta de novas evidências. A adoção do sistema acusatório confere às próprias partes responsabilização pelo material probatório a ser introduzido no processo, sendo ele totalmente dependente das informações aprovisionadas pelas próprias partes[354]. A atitude da defesa é muito diferente daquela dos países de *Civil Law*, em que só pode apresentar um discurso de oposição radical, ironizar, lançar confusão sobre a versão da inicial da acusação e raramente propor, desde o início, uma outra versão dos fatos, uma outra forma de relatar, já que não dispõe de meios amplos para tanto: não há escolha a não ser a de atacar o relatório da autoridade policial e a acusação formalizada, mais destinadas a desestabilizar do que a fazer mudar de opinião[355].

A 6ª Emenda à Constituição dos Estados Unidos apresenta-se como fundamento constitucional do *duty to investigate*[356], um poder-dever atribuído ao defensor e um direito para o cidadão americano, que determina e até mesmo exige do profissional um perfil proativo, autônomo, no sentido de produção probatória unilateral e/ou antecipada e que não se

---

[353] DAMASKA, Mirjan R. **El derecho probatorio a la deriva.** Madri: Marcial Pons, 2015. p. 87-89.
[354] DAMASKA, Mirjan R. **El derecho probatorio a la deriva.** Madri: Marcial Pons, 2015. p. 87-97.
[355] GARAPON, Antonie; PAPAPOULOS, Ioannis. **Julgar nos Estados Unidos e na França**: cultura jurídica francesa e *Common law* em uma perspectiva comparada. Rio de Janeiro: Lumen Juris Editora, 2008. p. 88.
[356] "*In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense*" (ESTADOS UNIDOS DA AMÉRICA. Constitution of the United States – Sixth Amendment Explained. **Constitution Annotated – Analysis and Interpretation of the U.S. Constitution**. Disponível em: https://constitution.congress.gov/constitution/amendment-6/#:~:text=In%20all%20criminal%20 prosecutions%2C%20the,of%20the%20accusation%3B%20to%20be. Acesso em: 20 fev. 2022).

restringe à esfera criminal[357]. O tema dos poderes de investigação nas mãos da advocacia não é algo dissociado de sua atuação em geral e decorre do modelo processual que opera nos Estados Unidos, desde o âmbito cível *lato sensu* até mesmo às questões criminais. Isso ganha singular relevância quando o próprio sistema se estrutura sob o conceito de justiça penal negociada, em que bens jurídicos penalmente relevantes passam à esfera da disponibilidade e integram um verdadeiro "balcão de negócios", no qual a *moeda é informação* – saber-poder – e o objetivo do processo não é a realização de justiça, mas sim conferir celeridade e eficiência ao organismo judicial, ainda que em detrimento de direitos e garantias materiais e processuais.

Nesse contexto, a *American Bar Association* (ABA), órgão equivalente à Ordem dos Advogados do Brasil, estabelece alguns diplomas com instruções que orientam o advogado criminal a uma forma habitual de agir, que inclui um dever de busca incessante pelo esgotamento das formas e dos meios privados de obtenção das informações, ganhando especial destaque o *Criminal Justice Standards for the Defense Function* e *Guidelines for the Appointment and Performance of Defense Counsel in Death Penalty Cases*, este último aplicável exclusivamente aos casos em que há previsão de pena capital. Igualmente, o livro dos *Standards for The Administration of Criminal Justice* aponta prescrições à advocacia criminal e se debruça pontualmente sob o dever de investigar (*duty to investigate*), instituto que equipara a prescrição a um verdadeiro dever geral de agir ao advogado do investigado para apurar as circunstâncias do fato, explorando em sua integralidade as hipóteses disponíveis, técnicas de investigação e recursos tecnológicos para apurar todo e qualquer dado que possa exercer influência sobre o julgamento; estabelece deveres genéricos que incluem a vedação do advogado violar a cláusula geral sobre a inadmissibilidade de obtenção de elementos de prova ou informações de forma ilícita, ou de instruir e encorajar terceiras pessoas a fazê-lo; também, disciplina as relações entre o advogado de defesa e potenciais testemunhas, entre o advogado e peritos, assim como o dever de cooperar com os procedimentos de compartilhamento de provas (*Discovery)*, devendo fazer esforço para atender pedido legal de revelação dos elementos de prova que estejam na sua posse *(discover*

[357] *"*Entende-se, pois, que as expressões 'o acusado terá direito [...] de ser acareado com as testemunhas de acusação, de fazer comparecer por meios legais testemunhas da defesa, e de ser defendido por um advogado', constituem o arcabouço sistêmico do qual decorre a investigação defensiva, do plano constitucional do modelo americano. A Suprema Corte Americana já se manifestou algumas vezes sobre o assunto, de forma direta ou colateral, principalmente nos casos que ficaram conhecidos como: (i) Caso Strickland vs. Washington; ii) Caso United States vs. Cronic (ambos em 1984); iii) Caso Wiggins vs. Smith (2003); iv) Caso Bobby vs. Van Hook (2009) e v) Caso Padilla vs. Kentucky (2010)" (DIAS, Gabriel Bulhões Nóbrega. **Manual prático de investigação defensiva**: um novo paradigma na advocacia criminal brasileira. Florianópolis: Emais, 2019. p. 38).

request)[358].

As partes são dotadas de poderes destinados a controlar a investigação sobre os fatos antes do julgamento, chamados de *pre trial* ou *Discovery*, ferramentas processuais com as quais os advogados dos litigantes podem buscar provas fora do Tribunal, respaldados pela autoridade da Corte em exigir a cooperação dos adversários e de terceiros; elas têm o poder de exigir que o adversário e outras testemunhas em potencial se sujeitem a questionamentos orais sob juramento sem a presença do juiz (*deposition*), respondam sob juramento perguntas escritas (*interrogatories*), ofereçam seus documentos para exame pelo adversário (*document Discovery*) e, quando suas condições físicas e mentais estejam em discussão, submetam-se a exames médicos realizados por um profissional da escolha do interessado[359]. Nada semelhante a esse sistema de determinação dos fatos fora do tribunal é admitido no âmbito de *civil law*.

O igualitarismo norte-americano é expresso pelo *Discovery*, tendo em conta que esta alternativa assegura a igualdade de oportunidades, mas não de resultados: a condução do *discovery* pelas partes também engloba sua responsabilidade por arcar com os custos inerentes à coleta de dados. *Discovery* reflete o individualismo competitivo, já que permite a cada advogado criar e seguir um programa de instrução processual concebido para lograr a melhor maneira de agir no caso concreto, sem qualquer supervisão judicial ampla e com limitações vagamente ditadas pelas regras processuais[360]. Representa um ponto de fundamental compreensão para aproximação dos sistemas norte-americano e aqueles tradicionalmente denominados inquisitórios: significa uma ferramenta do *fair-play* processual que impõe às partes envolvidas no conflito em apresentar as provas que possuem e conceder, à outra, tempo para que se prepare para o enfrentamento[361].

No *pretrial discovery*, o sistema processual americano confere poder às partes para que exerçam, antes do julgamento, controle sobre investigações dos fatos. O igualitarismo norte-americano, sustentado sob a ideia de sujeitos detentores de iguais direitos[362], inclusive quanto à possibilidade de reivindicá-los, prevê a concessão de amplas ferramentas aos advogados para que, respaldados pela autoridade da Corte, exijam cooperação dos adversários

---

[358] DIAS, Gabriel Bulhões Nóbrega. **Manual prático de investigação defensiva**: um novo paradigma na advocacia criminal brasileira. Florianópolis: Emais, 2019. p. 34-38.
[359] CHASE, Oscar G. **Direito Cultura e Ritual**: Sistemas de resolução de conflitos da cultura comparada. São Paulo: Marcial Pons, 2014. p. 91-92.
[360] CHASE, Oscar G. **Direito Cultura e Ritual**: Sistemas de resolução de conflitos da cultura comparada. São Paulo: Marcial Pons, 2014 p. 91-92.
[361] GÓMEZ COLOMER, Juan Luis. **El proceso penal adversarial**: una crítica constructiva sobre el llamado sistema acusatorio. Editorial Ubijus: México-DF, 2012. p. 50.
[362] DAMASKA, Mirjan R. **El derecho probatorio a la deriva**. Madri: Marcial Pons, 2015. p. 97.

e de terceiros e para que busquem provas fora do Tribunal. Com esse poder, adversário e outras testemunhas em potencial devem se sujeitar: (i) a questionamentos orais sob juramento sem a presença do juiz (*deposition*); (ii) a responder, sob juramento, perguntas escritas (*interrogatories*); (iii) a oferecer documentos para exame pelo adversário (*document discovery*); (iv) a se submeter a exames médicos realizados por um profissional da escolha do interessado, poderes importantes na litigância norte-americana, porque criar um atraso substancial no julgamento devido à colheita de novas provas é inconveniente. Assegura-se a igualdade de oportunidades, mas não de resultados. A condução do *discovery* engloba a responsabilidade por arcar com os custos inerentes à coleta dos dados[363].

O tecnicismo utilizado pelos advogados auxiliou a moldar o sistema. Enquanto no período do jurado autoinformado – o que tinha conhecimentos sobre fatos relevantes ou que desenvolvia investigações por conta própria – a participação do advogado se resumia à formulação de estratégias, por meio do mecanismo de alegatos, para promover as perguntas em busca do convencimento do órgão decisório; quando os jurados deixam de ser autoinformados e os fatos devem ser provados ante um tribunal, advogados podem participar do processo judicial, são dotados da capacidade de controlar o fluxo de informações apresentadas e assegurar que as provas apresentadas sejam suficientes para iniciar uma discussão perante a Corte.[364]

Se de um lado o *discovery* reflete o individualismo competitivo que permite a cada parte criar e seguir uma estratégia processual concebida para, sem ampla supervisão judicial e com limitações vagamente ditadas pelas regras processuais, encontrar a melhor maneira de agir, sob o ponto de vista de quem é exigida a providência, intromissões de qualquer natureza podem ser encaradas como uma violação pessoal. De qualquer sorte, a ênfase do modelo está voltada ao poder dado à parte para a obtenção de seus anseios durante a instrução, e não no fato de estar também sujeita à produção probatória[365]. Estruturas paritárias definem-se pela organização de pessoas não profissionais em um único nível de poder[366].

Um importante precedente brasileiro, talvez o maior nesse sentido, vem do Tribunal Regional Federal da 3ª Região no caso da Operação Lava Jato, que envolve o ex-presidente Luiz Inácio Lula da Silva, que propôs ação de obrigação de fazer em face da Odebrecht para,

---

[363] CHASE, Oscar G. **Direito Cultura e Ritual**: Sistemas de resolução de conflitos da cultura comparada. São Paulo: Marcial Pons, 2014.
[364] DAMASKA, Mirjan. **Las Caras de La Justicia y el Poder del Estado**: análisis comparado del proceso legal. Santiago: Editora Juridica de Chile, 2000. p. 73-75.
[365] CHASE, Oscar G. **Direito Cultura e Ritual:** Sistemas de resolução de conflitos da cultura comparada. São Paulo: Marcial Pons, 2014.
[366] DAMASKA, Mirjan. **Las Caras de La Justicia y el Poder del Estado**: análisis comparado del proceso legal. Santiago: Editorial Juridica de Chile, 2000. p. 34-35.

com fundamento no direito à investigação defensiva e com o intuito de constituir acervo probatório lícito para combater constrangimentos sofridos nos processos criminais decorrentes da operação, a ele garantir acesso aos procedimentos e documentos apresentados internamente para apuração do setor de integridade da empresa no âmbito da Operação Lava Jato. Baseada em dados proveninentes de fontes abertas, a defesa do ex-presidente alegou que o presidente da companhia teria confidenciado a pessoas próximas que os elementos angariados na investigação interna não comprovaram os benefícios atribuídos a Lula pelos desvios da Petrobrás e que a maioria das delações foram lastreadas em "colaborações incentivadas" entre o Ministério Público Federal (MPF) e os acionistas e ex-colaboradores da empresa, razão pela qual, com fundamento no Provimento nº 188/2018 do Conselho Federal da Ordem dos Advogados do Brasil (Cfoab), encaminhou requerimento, não respondido, à Odebrecht para ter acesso aos documentos. Em primeira instância, sobreveio decisão que extinguiu liminarmente o feito sem julgamento de mérito em razão de alegada incompetência absoluta do juízo e ausência de pressuposto de constituição e desenvolvimento válido e regular do processo, sob fundamento de que a medida apresentada perante a jurisdição criminal se assemelhava a pleito cível de exibição de documentos ou coisas.

Manejado apelo defensivo contra a decisão de primeira instância, o Tribunal Regional Federal da 3º Região discordou dos fundamentos sentenciais, salientando que o inquérito criminal defensivo é expediente que tem como principal objetivo assegurar ao advogado a reunião de evidências que permitam fundamentar teses favoráveis ao seu assistido, atividade não proibida pelo sistema jurídico brasileiro, e que, se o modelo constitucional vigente confere, além do controle externo da atividade policial, poderes investigatórios ao Ministério Público[367] – o que lhe atribui ampla atividade investigatória –, isso o torna um ator com função significativamente diferente daquela que exercia no processo penal brasileiro. Assim, a investigação defensiva, que encontra amparo não somente em razão da ausência de norma proibitiva, mas também em razão de interpretação extensiva dos princípios da igualdade e do devido processo legal, surge como materialização da paridade de armas para que a defesa também tenha condições de influenciar o julgador[368] com as mesmas oportunidades entre sujeitos processuais que se encontram em diferentes posições, o que somente ocorre se lhe

[367] BRASIL. Supremo Tribunal Federal. **RE 593.727 -MG**. Relator: Min. Gilmar Mendes, 3 de outubro de 2017. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2641697. Acesso em: 20 abr. 2022.

[368] CAMARGO, Rodrigo Oliveira de; BULHÕES, Gabriel. Defesa Penal Efetiva no Brasil: desafios da atuação defensiva na investigação preliminar em meio ao sistema acusatório. *In*. GONZÁLEZ, Leonel; BALLESTREROS, Paula. **Desafiando a Inquisição**: ideias e propostas para a reforma processual no Brasil. Santiago: Ceja-JSCA. 2019.

forem oferecidas condições de acessar todos os recursos necessários para se defender antes, durante ou depois do processo, em juízo ou fora dele. Ademais, se o Provimento nº 188/2018 discorre sobre prerrogativas profissionais do advogado na realização de diligências investigatórias, entendeu a Corte que a atuação do particular no curso da investigação defensiva não pode sofrer limitações que a investigação policial ou a investigação administrativa realizada pelo Ministério Público não suportam e que, se ela não goza da mesma imperatividade que investigações levadas a efeito por agentes públicos, é legítimo que acione o Poder Judiciário para a tutela de seus interesses[369].

5.2. Da ilicitude à paridade de armas

Durante o julgamento dos recursos do Caso da boate Kiss, dois precedentes do Órgão Especial do Tribunal de Justiça do Estado do Rio Grande do Sul foram analisados no voto divergente do Desembargador Jayme Weingartner Neto a respeito do tema e, ainda que não tenham avançado quanto à eventual utilização indevida do Sistema Consultas Integradas pelo órgão da acusação, manifestaram intensa preocupação quanto à paridade de armas.

O primeiro, um agravo regimental interposto contra a decisão liminar que indeferiu um pedido de suspensão do uso do Sistema Consultas Integradas por promotores de Justiça atuantes na Vara do Júri da Comarca de Porto Alegre, alegando a violação ao direito a um julgamento justo na medida em que, enquanto a acusação se utiliza de informações privilegiadas sobre cidadãos convocados ao Tribunal do Júri e que são informações valiosas não só para aferir a idoneidade dos jurados, mas também para a eventual recusa imotivada dos jurados sorteados, colhidas através do Sistema Consultas Integradas, se está violando os princípios da ampla defesa, do contraditório e da paridade de armas, já que o acesso ao conteúdo do banco de dados das Consultas Integradas significa um *handicap* para a acusação, impactando o princípio da igualdade quando a defesa não possui o mesmo direito que o MPRS [370].

O segundo precedente abordado também se referia a alegações formuladas contra abusos dos agentes ministeriais por buscarem informações privilegiadas sobre a vida dos jurados inseridos na listagem anual do Tribunal do Júri, afrontando o princípio da paridade de armas. Em razão disso, foi interposto mandado de segurança de forma a que se abstivesse o

[369] BRASIL. Tribunal Regional Federal da 3ª Região. 5ª Turma. **Apelação Criminal 5001789-10.2020.4.03.6181**. Relator Desembargador Federal Maurício Kato.
[370] BRASIL. Tribunal de Justiça do Estado do Rio Grande do Sul. **AgRg em MS n.º 70056759152**, Órgão Especial. Relator Desembargador Gaspar Marques Batista.

MPRS de utilizar os mecanismos previstos no convênio celebrado com o Poder Executivo do Estado do Rio Grande do Sul, por intermédio da Secretaria de Segurança Pública, que disponibiliza "acesso à base do Sistema Consultas Integradas, para integração com o Sistema de Inteligência do MPRS, visando a agilização e a otimização das operações de inteligência". Em um julgamento complexo, que também se debruçou sobre uma série de outras questões processuais de cabimento e legitimidade do *mandamus*, mas que teve encaminhamento final pela denegação da segurança, extraiu-se uma série de considerações que aqui nos cabem para dar encaminhamento às nossas propostas[371].

A peça inicial encaminha três pedidos, um deles alternativo, no caso de indeferimento do primeiro: (i) determinar a "cessação do uso indevido do Sistema Consultas Integradas, com o cancelamento das senhas, cabendo apenas ao gabinete do procurador-geral de Justiça o acesso ao sistema, com o fornecimento dos dados mediante pedido devidamente justificado; (ii) ser realizado novo alistamento dos jurados que tiveram suas informações devassadas; (iii) alternativo ao primeiro pedido, que a defesa tivesse o direito de acessar as mesmas informações obtidas pelo MPRS. Afastados os pedidos (i) e (ii) pelo voto que encaminhou a divergência, o pedido que buscava a concretização do princípio da ampla defesa acabou sendo apreciado a partir de uma proposta de "olhar diferenciado".

As divergências encaminhadas consideraram que, no caso do acesso ao Sistema Consultas Integrado por membros do MPRS, a solução da controvérsia deveria partir da interpretação e ponderação criteriosa de colisão, ou aparente colisão, entre princípios constitucionais que se caracterizam direitos fundamentais da cidadania[372]: (i) a proteção da privacidade, a proteção da intimidade, a proteção de dados arquivados digitalmente por órgãos do Estado; (ii) a garantia da imparcialidade da magistratura e de outras decorrências do princípio do devido processo legal e do juiz natural que prevê que também estabelece a vedação aos tribunais de exceção e tudo o que possa macular a jurisdição, imparcial e independente; (iii) o da ampla defesa e o do contraditório.

Inerente ao poder de acusar, o MPRS não pode ser inibido do seu poder de investigar, mas torna-se responsável por eventuais abusos: apesar de terem acesso privilegiado a uma série de dados contidos em bancos públicos e privados, os órgãos da *persecutio criminis* não podem realizar devassas indiscriminadas sobre as pessoas. A defesa, da mesma forma, não

---

[371] BRASIL. Tribunal de Justiça do Estado do Rio Grande do Sul. **AgRg no RMS nº 62.562**, Órgão Especial. Relator Desembargador Manuel Jose Martinez Lucas.

[372] DWORKIN, Ronald. **Levando os direitos a sério**. São Paulo: Editora WMF Martins Fontes, 2010; ALEXY, Robert. **Teoría de los derechos fundamentales**. Madrid: Centro de Estúdios Políticos e Constitucionales, 2008; CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da constituição**. 9. ed., 7. reimpressão. Coimbra: Almedina, [20--].

tem contra si qualquer proibição de realizar a investigação, encontrando limites nos direitos constitucionais da intimidade, privacidade, da proibição de violação de sigilos e na cláusula geral da proibição de provas ilícitas, o que pode ser violado por ordem judicial. Mas, historicamente, a grande dificuldade da defesa sempre foi a de que não tinha meios eficazes para fazer investigações, o que a colocava em condição de submissão do produto do trabalho realizado pelos órgãos da persecução, que deveriam zelar para não aumentar o desequilíbrio, já que a informação qualificada de uma das partes representa, sem sombra de dúvidas, uma vantagem.

Quanto à possibilidade de que defensores tivessem acesso às mesmas informações como decorrência do princípio da paridade de armas, as divergências reconheceram tratar-se de pleito absolutamente factível e que deveria ser permitido, sob pena de violação da ampla defesa, já que o acesso ao Sistema de Consultas Integradas por membros do MPRS, para fins de afastamento de nomes da lista geral de jurados inseridos na listagem anual, cria injustificável disparidade entre o MPRS e a defesa no Tribunal do Júri: ainda que se sustente que a defesa possa, de outras formas, acessar esses dados que por convênio estão à disposição do MPRS, fato é que o caminho percorrido entre partes supostamente iguais são, na verdade, bastante diferentes.

Assim, se inexiste princípio da ampla acusação, mas tão somente princípio da ampla defesa expressamente previsto na Constituição Federal de 1988 no art. 5º, inciso XXXVIII, não é possível que o Estado permita o acesso privilegiado a dados arquivados em sistema do governo e da Secretaria de Justiça e Segurança sem que permita o mesmo acesso aos defensores, motivo pelo qual a vencida divergência encaminhou-se no sentido de que a defesa tivesse o direito de acessar as mesmas informações obtidas pelo MPRS, propondo, inclusive, repercussão administrativa da decisão jurisdicional para que fosse facultado o acesso aos defensores às informações no arquivo digital de dados do Sistema Consultas Integradas do Estado, compromissando-se estes, sob pena de responsabilidade penal e ética, a manterem o sigilo das informações, vedadas, ainda, cópias de documentos e informações.

O tratamento de dados pessoais dos jurados pelo manejo do Sistema Consultas Integradas pelo MPRS demonstrou a emergência do debate sobre a disparidade de armas e substancial assimetria no que guarda relação com o tratamento de dados pessoais, pois a disposição de informação privilegiada sobre cada um dos jurados evidencia a disparidade de armas e que assegurar à defesa o mesmo tipo de informação que detém o MPRS é algo inafastável, pois, se informação é poder, uma parte controlar informações sobre os jurados

não serve só para recusá-los, mas para abordar certas temáticas que lhes interessam e que lhes sejam mais sensíveis.

5.3. *E-discovery*, a coleta estratégica de elementos de elementos de informação e os desafios da garantia da defesa

Acessíveis por escritórios de advocacia de qualquer dimensão, grandes, pequenas ou médias empresas e até mesmo meros consumidores com níveis não tão avançados de letramento digital, ferramentas (jurídicas ou não) fomentam o surgimento de novos atores que oferecem serviços com base em elementos inteligentes e acessíveis em formato digital. Uma das funcionalidades oferecidas por essas empresas de inteligência e *contrainteligência* vem sendo classificada como *e-discovery*, responsável pela seleção do material probatório para demandas judiciais[373]. Essa ampliação do controle, da qualidade e da quantidade de evidências abrem horizontes cognitivos, favorecendo a precisão e a acurácia da decisão de um lado e, do outro, criando novos desafios, já que novas habilidades estratégicas, ainda pouco exploradas, serão exigidas[374].

O advogado não mais se limita em apenas dar respostas a questões legais: pode ir além para melhor atender aos interesses do seu constituinte. Tem à disposição ferramentas que ampliam seu poder de análise pela possibilidade de multiplicação dos elementos e das informações para melhor decidir sobre o tema em questão. Assessoria legal e prestação de informações parecem se confundir; o que as diferencia é a circunstância de que assessoria legal pressupõe a aplicação do conhecimento jurídico às especificidades do caso individualizado, o que não ocorre na mera transmissão de informações. O serviço jurídico agregará em sua classificação "informação" como *commodity*. O *serviço* será reservado para a atividades em que será necessária a intervenção humana; *bem de informação jurídica gerado através de máquinas inteligentes* é produto, o que origina a celebração de contratos atípicos que compreendem prestações que se subsumem a diversos tipos contratuais, que incluem serviços de advocacia, serviços digitais e *bem de informação jurídica*[375].

---

[373] NAVARRO; Susana Navas. Da assistência à substituição dos advogados – a repercussão da Proposta europeia de Regulamento sobre a Inteligência Artificial no Legal Tech. *In*: ABREU, Joana Covelo de; COELHO, Larissa; CABRAL, Tiago Sérgio. **O Contencioso da União Europeia e a cobrança transfronteiriça de créditos**: compreendendo as soluções digitais à luz do paradigma da Justiça electrónica europeia (e-Justice). Braga: UNIO EU Law Journal, 2021. v. 3. p. 107-121.

[374] ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico**: de acordo com a teoria dos jogos e MCDA-A. Florianópolis: Emais, 2021.p. 557-568.

[375] NAVARRO; Susana Navas. Da assistência à substituição dos advogados – a repercussão da Proposta europeia de Regulamento sobre a Inteligência Artificial no Legal Tech. *In*: ABREU, Joana Covelo de; COELHO, Larissa; CABRAL, Tiago Sérgio. **O Contencioso da União Europeia e a cobrança**

Essas verdadeiras empresas de terceirização jurídica apresentam suporte personalizado, com soluções integradas e econômicas para advogados, escritórios de advocacia e empresas e que agregam valor, produtividade e tecnologia atualizada à atuação dos tomadores de decisão, prometendo – e aparentemente entregando – eficiência e vantagem competitiva em relação à qualidade da informação e ao tempo de resposta no curso do processo. Um verdadeiro ciclo de investigação, agora orientado sob a perspectiva defensiva, sem perder de vista a necessidade de imposição de limites a quem exerce esse tipo de poder[376] – sem freios, poder é abuso.

Também denominadas como *Electronically Stored Information* (ESI), essas informações coletadas e utilizadas podem ter origem e estar organizadas em formatos digitais diversificados, ainda que seja patente o risco de que, se não tratados da forma adequada, esses elementos não sejam admitidos no processo judicial[377]. Proliferam-se poderosos mecanismos para pesquisas em larga escala, orientadas por dados, auxiliando todos os tipos de organizações a identificar elementos que permitam a tomada de decisões mais informadas e com menores riscos. Por outro lado, não se identificam, ainda, procedimentos estipulados para identificação, coleta e apresentação dessas informações, a não ser remissões genéricas às normas vigentes e ao emprego de práticas técnicas.

No exterior, organizações como o *Scientific Working Group on Digital Evidence* (*SWGDE*) ou a *Internet Engineering Task Force* (*IETF*) buscam descrever e orientar as melhores práticas para a coleta de itens que podem conter evidências digitais, projetando processos para manter a integridade de seus resultados. No plano legal, para garantir validade científica, confiabilidade e precisão em testes, fortalecendo e promovendo a confiança no sistema de Justiça criminal, o *Criminal Justice and Forensic Science Reform Act* busca estabelecer, nos Estados Unidos, estruturas relacionadas às Ciências Forenses, além da *Forensics Science and Standards Act*, que indica estratégias de pesquisa unificada e revisão

---

transfronteiriça de créditos: compreendendo as soluções digitais à luz do paradigma da Justiça electrónica europeia (e-Justice). Braga: UNIO EU Law Journal, 2021. v. III. p. 107-121.

376 "Quanto aos deveres do advogado condutor da investigação defensiva, transpondo a leitura das obrigações (constitucionais, legais, administrativas e éticas) que norteiam a advocacia para o campo dessa atividade, entende-se que se deva: 1) preservar o sigilo das fontes de informação; 2) respeitar o direito à intimidade, à privacidade, à honra e à imagem das pessoas; 3) exercer a atividade com zelo e probidade; 4) defender, com isenção, os direitos e as prerrogativas profissionais, zelando pela própria reputação e a da classe; 5) zelar pela conservação e proteção de documentos, objetos, dados ou informações que lhe forem confiados pelo constituinte ou em defesa dos seus interesses; 6) restituir, íntegro, ao constituinte, findo o contrato ou a pedido, documento ou objeto que lhe tenha sido confiado; e 7) prestar contas ao constituinte" (DIAS, Gabriel Bulhões Nóbrega. **Manual prático de investigação defensiva**: um novo paradigma na advocacia criminal brasileira. Florianópolis: Emais, 2019).

377 IBPTECH. **E-Discovery**. Disponível em: https://ediscovery.com.br/. Acesso em: 20 abr. 2022.

sobre as orientações de desenvolvimento de padrões em ciência forense, além do RFC nº 3227, memorando que estabelece diretrizes e procedimentos de boas práticas para a coleta e arquivamento de evidências digitais e que especifica as Melhores Práticas Atuais da Internet para a Comunidade da Internet, e da ABNT NBR ISO/IEC nº 27037, norma reconhecida internacionalmente e que estipula diretrizes técnicas para identificação, coleta, aquisição e preservação de evidências digitais[378].

Por isso, no âmbito da investigação criminal em ambiente digital, tais características impõem a intervenção de agentes com conhecimento específico em informática, Ciência de Dados ou Ciência Forense Digital, sujeitos encarregados pelo manejo de ferramentas e desenvolvimento de procedimentos e métodos adequados para recuperação de arquivos, registros ou outros dados úteis para a reconstrução do cenário da atividade delituosa, sempre observando o marco legal aplicável. Evidência-Digital (*E-Evidência*) pressupõe a compreensão da leitura da categoria *prova documental* a partir do desenvolvimento tecnológico, havendo uma relação muito próxima com técnicas de inteligência baseadas em tratamentos de dados, como visto, disciplina e atividade em franca evolução dentro dos órgãos encarregados pela persecução penal, mas pouco exploradas por instituições e agentes processuais responsáveis pela tutela da defesa e da liberdade. Letramento digital combinado com segurança cibernética ampliam a disponibilidade de dados e informações para a tomada de decisões estratégicas na investigação ou no processo, já que o *input* de um único dado ou elemento disponível na ferramenta tecnológica adequada pode ofertar ao agente *output* com dois ou mais novos dados[379].

A relação dos órgãos de aplicação da lei com *machine learning* e análise preditiva corresponderá a uma crescente necessidade de peritos em dados, especialistas nas ferramentas e técnicas necessárias para capturar, analisar e manipular grandes quantidades de informação; o sujeito responsável por identificar correlações, tendências, padrões e percepções, especialistas interdisciplinares com conhecimento não apenas em sistemas, mas também do Direito, do serviço jurídico e, no campo das Ciências Criminais, em Antropologia, Criminologia, Criminalística e, por que não, Direito e Processo Penal. O enfoque em desenvolver novas capacidades, técnicas e tecnologias para a prestação de serviços e

[378] CAMARGO, Rodrigo Oliveira de; MONTANARO, Domingo. A Cadeia de Custódia de Evidências Digitais: mais um desafio da intersecção entre Direito e Tecnologia. *In*: ARAÚJO, Guilherme Silva; CARDOSO, Luis Eduardo Dias; PRADO, Rodolfo Macedo. **Advocacia Criminal**: temas atuais. Florianópolis: Tirant Lo Blanch, 2022. p. 265-273.

[379] ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico**: de acordo com a teoria dos jogos e MCDA-A. Florianópolis: Emais, 2021. p. 437-443.

fornecimento de soluções jurídicas também fomenta o empreendimento para a produção de novos serviços e soluções[380].

Sujeitos capacitados a promover varreduras digitais e a coleta de todo e qualquer dado disponível em diversas fontes e que possam interessar à investigação ou ao processo já são uma realidade. Equipes multidisciplinares voltadas ao apoio de escritórios e profissionais liberais prestam serviços de tecnologia, consultoria e assistência técnica para suportar decisões estratégicas nos âmbitos de Investigações Internas ou Investigações Defensivas; utilizando-se de ferramentas específicas, promovem a coleta e a preservação de dados eletrônicos, o processamento e a organização de evidências, a revisão e a classificação de documentos eletrônicos, tudo materializado em relatórios de captura aptos para apresentação em juízo como evidência digital.[381]

No âmbito corporativo, em razão das atribuições conferidas às empresas para a investigação de condutas ilícitas praticadas pelas pessoas físicas sob sua supervisão e que podem causar repercussões em diversos âmbitos (criminal, laboral, propriedade industrial, propriedade intelectual, concorrencial…), a investigação para a obtenção de evidências surge como pretensão legítima para a proteção de bens jurídicos das empresas. A utilização de equipamentos informáticos, dispositivos eletrônicos ou instrumentos digitais de comunicação para organização e funcionamento da corporação também se apresentam como fonte de conhecimento sobre padrões e comportamentos de seus subordinados, já que a prestação laboral por intermédio desses aparelhos registra e toma a métrica das atividades desenvolvidas. A investigação levada a efeito pela empresa, para além de oferecer dados e informações para justificar a comunicação de um fato delituoso, produzirá fontes que, posteriormente, poderão ser propostas como prova em juízo, seja ela testemunhal, documental, seja pericial, e não estão, em um primeiro momento, submetidas ao regramento, porque se estaria diante de tratamento necessário para o cumprimento de obrigação legal aplicável ao responsável pelo tratamento.

---

[380] SUSSKIND, Richard E. **Tomorrow's lawyers**: An introduction to your future. USA: Oxford University Press, 2017. p. 133-145.

[381] Por exemplo, segundo a Verifact, a validade jurídica de sua solução de captura de evidências digitais está ancorada nos princípios da cadeia de custódia relativos à coleta e preservação de evidências definidos pelo Pacote Anticrime, bem como em relação aos meios regulamentados para autenticação de documentos, com o uso da Certificação Digital ICP/Brasil – gerida pelo Instituto Nacional de Tecnologia da Informação/Casa Civil da Presidência da República, regulamentada pela MP nº 2.200-2/2001, e capaz de autenticar documentos segundo o inciso II do artigo 411 do CPC. Ainda que do ponto de vista técnico a ferramenta tenha sido elaborada com base em recomendações forenses em conformidade com normas internacionais, como a ABNT NBR ISO/IEC 27037:2013, referentes aos métodos necessários para a confiança na coleta e preservação de provas digitais, verificadas para a situação de coleta de conteúdos remotos sem acesso direto ao dispositivo (VALIDADE Jurídica. **Verifact**. Disponível em: https://www.verifact.com.br/validadejuridica/. Acesso em: 25 jun. 2022).

No âmbito da investigação defensiva propriamente dita, tanto o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal quanto o Projeto nº 1515/2022 afastam expressamente o tratamento de dados por pessoas de direito privado – submetendo-os ao escrutínio da autoridade pública –, o que cria importante lacuna a ser suprida para o tratamento de dados pela defesa no que guarda relação às atividades de persecução e repressão de infrações penais no Brasil, já que uma vedação nesse sentido, a nosso sentir, encontra óbice na paridade de armas. O dispositivo apontado faz vedação expressa ao tratamento de dados pessoais para atividades de segurança pública e persecução penal por pessoa de direito privado, desconsiderando a importância da participação da defesa para a investigação, a apuração, a persecução e a repressão de infrações penais e execução de penas.

A paridade de armas exige pensar o novo sob a perspectiva da defesa dos direitos individuais: dados pessoais e abertos à disposição da Defensoria Pública ou da advocacia também têm o condão de ser tratados quando o tratamento tiver por escopo o cumprimento de atribuições legais, observados, assim como cabe aos órgão de persecução penal, os princípios da finalidade, adequação e necessidade, e houver (i) respaldo na garantia da liberdade e do direito de uma *defesa penal efetiva*[382] para o exercício das garantias individuais e/ou (ii) amparo em previsão legal específica. A nova geometria de poder que entrega a iniciativa da investigação a entes privados, aliada ao desenvolvimento tecnológico que entrega ao indivíduo capacidade de coleta de dados acessíveis a um clique, enseja novas problematizações no fator tradição defensiva e sua estruturação, sobretudo em razão da ampliação dos campos de atuação.

Qualquer investigação unilateral, desprovida de controle, amplia os incentivos do comportamento desleal[383], sendo o temor da informação potencialmente enganosa uma preocupação que aumenta a importância de se conferir à parte adversa a oportunidade de atacar fontes apresentadas pelo oponente[384]. A crença no mito da suficiência dos elementos angariados pelos agentes administrativos, sustentados pela presunção de legitimidade de seus atos[385] e pela discricionariedade, não podem, no que diz respeito à investigação por legítimos interessados, sobrepor-se em relação ao direito de prova e ao direito de defesa. Em qualquer

[382] BINDER, Alberto; CAPE, Ed; NAMORADZE. **Defesa Penal Efectiva em America Latina**: Argentina, Brasil, Colômbia, Guatemala, México, Peru. [*S. l.*]: ADC, CERJUSC, CONECTAS, DE JUSTICIA, ICCPG, IDDD, IJPP, Inecip, 2015. p. 90-91.
[383] ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico: de acordo com a teoria dos jogos e MCDA-A**. Florianópolis: Emais, 2021. p. 557-568.
[384] DAMASKA, Mirjan R. **El derecho probatorio a la deriva**. Madri: Marcial Pons, 2015. p. 87.
[385] ROSA, Alexandre Morais; CANI, Luis Eduardo. Gravações com Câmeras Individuais em Policiais Geram Outros Problemas. *In*: CUNHA, Rogério Sanchez. **Atualidades do Direito**: obra em homenagem ao professor Luis Flávio Gomes. Salvador: Editora JusPodivm, 2020. p. 76-79.

esfera, a *supressão do direito* ou a *frustração da possibilidade* de buscar produzir a prova que interesse às suas alegações em relação àquele que sofre a persecução penal viola a regra do *due process of law* por manifesto desrespeito ao estatuto constitucional do direito de defesa: é direito fundamental do sujeito produzir elementos de informação considerados imprescindíveis, ainda que para infirmar a persecução penal[386].

Nesse sentido, no julgamento do Mandado de Segurança nº 26.627/DF, com assento nos princípios da igualdade, do devido processo legal, do contraditório e da ampla defesa, da segurança pública como direito e responsabilidade de todos, bem como no Provimento nº 188 do Cfoab, o Superior Tribunal de Justiça reconheceu, pela primeira vez, a prática da investigação defensiva e determinou que fosse ao impetrante franqueado acesso a elementos produzidos no âmbito de cooperações jurídicas internacionais, reconhecendo que a autoridade condutora não se erigia como destinatária final ou guardiã definitiva do "produto investigativo" gerado pela cooperação. No caso, a partir de uma série de informações de fontes abertas que dariam conta de um intercâmbio ilegal de informações e de documentos[387], encontros e diligências entre autoridades judiciárias nacionais e norte-americanas no âmbito da Operação Lava Jato, o impetrante instrumentalizou, a partir do levantamento de dados com a prática de investigação defensiva, pleito para que fosse conferido acesso à cópia integral de todos os eventuais registros relativos ao intercâmbio de informações, contatos, encontros, provas, procedimentos e investigações entre as autoridades locais e norte-americanas no âmbito da Operação Lava Jato. Ou, ainda, para que fosse esclarecido e certificado que a autoridade coatora não havia participado dessa cooperação internacional com os Estados Unidos da América na condição de autoridade central, na forma prevista no Decreto nº 3.810/2001[388].

Se a finalidade da fase anterior é a de produzir material capaz de suportar, a partir das regras democráticas, pontos de vista para o fim de justificar ou não o processo, a atividade defensiva não mais deve se conformar com uma postura passiva, em "correr atrás do prejuízo"[389]; a antecipação temporal para a coleta de fontes de prova pode determinar o êxito

---

[386] BRASIL. Supremo Tribunal Federal. **Inq. 4.831-DF**. Relator: Min. Celso de Mello, 05 de dezembro de 2020. Acesso em: 31 agosto de 2022. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15345201506&ext=.pdf. Acesso em: 20 abr. 2022.

[387] MARTINS, Rafael Moro; SANTI, Alexandre de; GREENWALD, Glenn. Não é muito tempo sem Operação? **The Intercept_Brasil**, 9 de junho de 2019. Disponível em: https://theintercept.com/2019/06/09/chat-moro-deltan-telegram-lava-jato/. Acesso em: 20 abr. 2022.

[388] BRASIL. Superior Tribunal de Justiça. Mandado de Segurança nº 26.627/DF.

[389] MACHADO, Leonardo Marcondes. **Introdução Crítica à Investigação Preliminar**. Belo Horizonte: Editora d' Plácido, 2018. p. 162-166.

do papel defensivo, devendo iniciar assim que for possível[390]. A advocacia não é dogmática; advocacia é arte, cética, investigadora e crítica. O profissional da advocacia investiga fatos, decide livremente por sua própria conduta e argumenta com base em dados que a realidade lhe oferece[391].

Isso ganha maiores contornos diante dos espaços de negociação e consenso[392] e em função da aceleração tecnológica. A proatividade decorre não apenas do direito assegurado em razão da garantia constitucional da defesa penal efetiva, senão também em dever de diligência que se origina na indispensabilidade do advogado para a administração da Justiça e a consequente necessidade de criar mecanismos para seu controle sob a investigação preliminar e do dever de identificar provas ou meios para sua obtenção.

A atividade do defensor, que deve ser orientada por limites, demanda novas habilidades em decorrência da profusão de instrumentos capazes de melhorar o desempenho, já que favorecem um agir estratégico e o uso de ações que podem ampliar a qualidade e a quantidade de elementos disponíveis. Ainda que marcada pela unilateralidade e com eficácia probatória limitada, a apuração defensiva inserida no espectro da ampla defesa, da paridade de armas, das ações neutras e do sigilo do advogado traz profundidade à investigação e permite o contraponto.[393]

Emancipar o arguido e seu defensor como sujeitos processuais liga-se ao interesse em dotar-lhes de um estatuto processual próprio que assegure, mediante exercício dos direitos, liberdades e garantias, efetivar a defesa no processo. Constitui pedra fundamental para avaliar o ordenamento jurídico processual penal, de forma a conceber relações entre Estado e indivíduo e sua posição na comunidade. Sob a perspetiva da evolução civilizacional do processo penal que dá sentido às determinações constitucionais que atribuem estrutura acusatória ao processo penal, um estatuto atribuído ao arguido e seu defensor teria um efeito

---

[390] SILVA, Franklyn Roger Alves da. **Investigação Direta pela Defesa**. 2. ed. Salvador: Editora Juspodivm, 2020.

[391] COUTURE, Eduardo Juan. Os Mandamentos do Advogado. Tradução de Ovídio A. Baptista e Carlos Otávio Athayde. Porto Alegre: Fabris. 1979, p. 45-49.

[392] POZZEBON, Fabrício Dreyer de Ávila; CAMARGO, Rodrigo Oliveira de. A relevância do Juiz das Garantias para investigação defensiva na fase preliminar. **Boletim do IBCCRIM**, São Paulo, ano 28, n. 334, p. 21-23, set/2020. p. 21-23.

[393] "No campo de investigações 4.0., com alto poder tecnológico, bem assim de casos de Alta Complexidade (Megaprocessos), a antecipação defensiva é condição para que se possa ao menos confrontar a acusação, em flagrante vantagem competitiva (O Estado dispõe de meios, tempo e preparação, enquanto o exíguo prazo da resposta à acusação impede, em geral, robustez dos meios de resistência). É que o palco da culpa deixou de ser somente a audiência de instrução e julgamento, para coadjuvar com a investigação preliminar, já que em boa parte dos casos o julgamento sequer ocorrerá (colaboração, ANPP, etc.). A defesa não pode mais ficar observando a movimentação estatal, sem armas adequadas para se opor, já que o fator tempo será decisivo e opera contra" (ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico**: de acordo com a teoria dos jogos e MCDA-A. Florianópolis: Emais, 2021. p. 557-567).

decisivo na materialização dessa estrutura: ela se cumpre fundamentalmente através de uma consideração do arguido por todos os poderes públicos (legislador, autoridades judiciárias e órgãos de polícia criminal) como autêntico sujeito processual. Isso significa ter de assegurar-lhe (i) posição que permita participação constitutiva na declaração do seu direito e (ii) direitos processuais definidos em lei, respeitados pelos intervenientes no processo penal[394].

Uma proposta de *estatuto processual do arguido*[395] radica em três eixos fundamentais: *direito de defesa, direito à presunção de inocência* e o *respeito pela decisão de vontade do arguido*. Interessa-nos em especial aquele que diz respeito ao direito de defesa, *categoria aberta* à qual devem ser imputados direitos concretos, disponíveis ao arguido, para determinar a decisão final do processo, incidindo sobre questões de fato e questões de direito que se discutem. Esse direito de defesa densifica-se pela consagração expressa do direito à prova e, mais em especial, do direito ao contraditório, prerrogativas que poderão ser exercidas em relação a tudo que tenha importância na apuração da culpabilidade e para a determinação da sanção.

Uma formulação mais ampla do que a simples oportunidade conferida a todo o participante processual de influir, através da sua audição pelo Tribunal, no decurso do processo, o contraditório representa um *direito à concessão de justiça*

---

[394] "As afirmações feitas são amplamente confirmadas por uma análise, mesmo perfunctória, da *evolução histórica* – não só entre nós, aliás, mas em todas os outros países de idênticos níveis de civilização e de cultura[5] – do estatuto jurídico do arguido no processo penal: ele esteve sempre em correspondência *direta* com os fundamentos políticos da respetiva ideia do Estado. Assim, compreende-se que – dentro dos limites consentidos pelo primitivismo das instituições processuais penais – o estatuto do arguido no nosso direito processual penal do tempo da reconquista lhe fosse favorável, até ao ponto de permitir a Dias da Silva afirmar que, nesse período, 'a autoridade defendia menos os particulares contra os delinquentes, do que os delinquentes contra os particulares ofendidos'. Igualmente se compreende a rápida e progressiva deterioração daquele estatuto com o advento das ideias inquisitórias – como se mostra pela autorização, dada pelas Ordenações Filipinas, ao uso da tortura e, exemplarmente, pelo simulacro de direito de defesa do arguido contido nos diversos regimentos do Santo Ofício da Inquisição dos Reinos de Portugal (*maxime* no de 1640)[7]. No processo inquisitório, com efeito, é toda a força de um Estado fundado em um princípio totalitário que se põe ao serviço da investigação da verdade material; com uma tal desconsideração, porém, pelas liberdades fundamentais do arguido e pela sua dignidade de pessoa, que o direito de defesa se torna de real em aparente e o arguido se transforma em mero 'objeto' de um processo que nada mais visa do que obter a sua 'confissão'; tudo a justificar completamente a afirmação de um documento coevo: 'Evidente é que saírem tantos confessos não é realidade da culpa, mas culpa do processo'. Foi intenção primordial das reformas processuais do séc. XIX, operadas sob o influxo das ideias revolucionárias, ligar a investigação da verdade material aos pressupostos do Estado de Direito, limitando-a assim pela observância escrupulosa dos direitos, liberdades e garantias do cidadão. Daí, justamente, que importasse assegurar ao arguido, no processo penal, a posição de *sujeito* dotado de um real e efetivo *direito de defesa.* Com isto não se pretendeu apenas – ou nem tanto – limitar o poder do Estado e o arbítrio dos seus representantes, mas corresponder à ideia, finalmente adquirida por uma consciência jurídica mais desperta, de que *não há verdade material onde não tenha sido dada ao arguido a mais ampla e efetiva possibilidade de se defender da suspeita que sobre ele pesa,* onde, numa palavra, não tenha sido conferida ao arguido a *proteção do direito*" *(*FIGUEIREDO DIAS, Jorge de; BRANDÃO, Nuno. **Sujeitos Processuais Penais**: o Arguido e o Defensor. Coimbra: [*s.n.*], 2020).

[395] FIGUEIREDO DIAS, Jorge de; BRANDÃO, Nuno. **Sujeitos Processuais Penais**: o Arguido e o Defensor. Coimbra: [*s.n.*], 2020.

(*Justizgewährungsanspruch*), direito de caráter público que conduz à consideração processual das pessoas como partícipes da criação: a administração da Justiça pelos tribunais também se relaciona com a posição processual dos afetados pela decisão. A responsabilidade sobre a tarefa de declaração do direito do caso penal concreto deixa de ser *apenas* tarefa do juiz ou tribunal e passa a ser de *todos* os que participam e se encontram em condição de influir na declaração final, na medida de sua posição ou função processual. O esclarecimento da situação em conflito supõe não apenas garantia formal da preservação do direito de cada um, mas a comprovação objetiva de todas as circunstâncias, inalcançável sem uma audiência esgotante de todos os participantes processuais – e com o emprego de recursos em idênticas condições.

O respeito pelo direito de audiência implica dar ao interessado oportunidade *efetiva* e *eficaz* mediante: (i) conhecimento tempestivo do lugar, tempo e objeto do debate; (ii) concreta possibilidade de se preparar para a intervenção; (iii) efetiva possibilidade de intervir no debate e se pronunciar sobre a decisão que possa afetá-lo juridicamente, antes de sua ocorrência.

Já a proposta de *estatuto processual do defensor*[396] parte da negação da tese de que sua posição jurídica se resume à assistência judicial do arguido. Está vinculado ao poder-dever que a lei confere ao exercício da defesa: uma função pública, com assento no Direito Público, alheia ao instituto da representação ligada às instruções ou à vontade do arguido, esta de natureza essencialmente privada. O defensor é órgão autônomo de administração da Justiça, cabendo-lhe a tarefa de colaborar com o tribunal na descoberta da "verdade" e na realização do Direito; uma de suas funções é justamente contrariar qualquer possibilidade de visão unilateral ou parcial que tenda a formar-se em desfavor do arguido. O exercício da função de defesa é admissível em qualquer processo e em qualquer altura do processo, cabendo ao defensor, no desempenho dessa função, guardar independência tanto em relação aos demais sujeitos e participantes processuais como em relação ao arguido, condição fundamental para que atue em seu interesse, mas com independência.

Para além do aconselhamento jurídico, do acompanhamento do arguido em quaisquer atos processuais que envolvam a sua presença e das intervenções que no processo realiza em nome e no interesse do *arguido*, cumpre ao defensor expor toda a verdade favorável ao arguido, do que decorre um dever de trazer todo o material capaz de convencer da inocência

[396] FIGUEIREDO DIAS, Jorge de; BRANDÃO, Nuno. **Sujeitos Processuais Penais**: o Arguido e o Defensor. Coimbra: [*s.n.*], 2020.

ou da menor culpa. Contudo, diferentemente do que se dá no processo penal de matriz anglo-saxã, não nos é comum ao defensor proceder a investigações autônomas, paralelas àquelas levadas a efeito pelo Ministério Público e auxiliares, o que de forma alguma representa proibição para que o defensor proceda às suas próprias averiguações complementares, ainda que não tenha ao seu dispor meios coercivos de obtenção de provas que lhe poderão ser úteis[397].

5.4. Prerrogativa de defesa digital: o tratamento de dados na garantia do direito de defesa

Práticas tecnológicas produzem efeitos dentro e fora dos limites estabelecidos pela organização tradicional do Direito, já que o ciberespaço se desenvolve de forma absolutamente indiferente à demarcação geográfica pensada nos séculos passados, exigindo que a resposta adotada pelo ordenamento jurídico diante da ciberdelinquência e do ciberterrorismo se articule em torno de parâmetros compatíveis a essa nova realidade. O desafio das agendas dos governos mundiais é garantir o uso do ciberespaço e estabelecer regulamentações mínimas que aproveitem as máximas potencialidades e capacidades dessas tecnologias, sem perder de vista princípios e valores que orientam o Estado de Direito[398].

Eventos e atividades gerados no ciberespaço sofrem mudanças dinâmicas, tanto em componentes tangíveis quanto intangíveis; informação é gerada em velocidade jamais experimentada devido às diferentes fontes que interagem constantemente nesse domínio, o que obriga os analistas a atualizarem constantemente os dados e informações, gerados ou transmitidos quase em tempo real, constantemente atualizados e, portanto, também tendem a desaparecer ou a se transformar muito rapidamente, o que significa que dados associados possam ser renovados rapidamente. Ainda há novos cenários a serem explorados: alguns, semelhantes a outros existentes, outros, ilustres desconhecidos e cujas implicações terão de ser examinadas em profundidade e a longo prazo. O ciberespaço é apresentado como oportunidade para analisar ameaças cibernéticas e como um espaço que oferece recursos para coletar todos os tipos de informações, além de local em que ferramentas podem ser obtidas e utilizadas para fazer análises com maior abrangência, de forma que conhecer essas interações

---

[397] FIGUEIREDO DIAS, Jorge de; BRANDÃO, Nuno. **Sujeitos Processuais Penais**: o Arguido e o Defensor. Coimbra: [*s.n.*], 2020.

[398] LA FUENTE; Elvira Tejada de. Introducción: Ciberseguridad y Ciberdelincuencia: respuestas desde el Estado de Derecho. La Armonización Legislativa Transnacional, en particular: las medidas de investigación criminal en la Convención de Budapest. *In*: ZARAGOZA TEJADA, Javier Ignácio. **Investigación Tecnológica y Derechos Fundamentales**: comentarios a las modificaciones introducidas por la Ley 13/2015. Navarra: Editorial Aranzadi, 2017. p. 25-72.

que ocorrem e os dados compartilhados oferece oportunidades para os atores com necessidade de informação e conhecimento, sobremaneira no campo da inteligência criminal[399].

A policialização do Direito aparece como solução possível em meio a essa *sociedade sinóptica e internético-personocênctrica*, com a consequente securitização dos instrumentos do Direito Penal e Processual através do implemento dessas novas tecnologias a serviço de vigilância e controle da sociedade. Ao se reclamar um novo sistema processual penal, surgem alternativas que defendem desde o aumento das prerrogativas dos poderes de polícia até a ampliação das atividades de investigação com a dispensa do controle jurisdicional para a obtenção de provas. Admite-se uma maior discricionariedade do Estado baseada no princípio de sua autoproteção, resultado da eleição do caminho mais fácil para tratar de um fenômeno complexo que envolve técnicas e velocidades antes impensadas quando da constituição do regime democrático.[400]

Por um lado, é imprescindível que as normas produzidas para a prevenção e a repressão à criminalidade digital tenham a capacidade de oferecer soluções ágeis a essas situações geradas pelo progressivo desenvolvimento tecnológico, inclusive exigindo cooperação mútua da comunidade internacional e de organismos do setor privado (leia-se operadoras de comunicações e provedores de internet e outros serviços ligados ao gerenciamento das comunicações sociais) diante das características desse tipo de delito[401]. De outro, toda e qualquer atuação estratégica e operativa para o combate à criminalidade cibernética deve se ajustar de forma plena aos vetores que orientam a proteção dos direitos e liberdades pessoais, assim como a todo e qualquer valor que oriente o desenvolvimento da

---

[399] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**, Bogotá, v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.

[400] VALENTE. Manuel Guedes. **Os Desafios do Processo Penal do Estado Democrático de Direito**: A Sociedade Internético-Personocêntrica. 2014. p. 3-4. Disponível em: http://www.ibadpp.com.br/1773/. Acesso em: 17 jun. 2019.

[401] "É cada vez mais frequente que as provas digitais relevantes para um processo penal não sejam localizadas no Estado em que ocorreu o cometimento de um crime, e que se encontrem dispersas no *cloud*, tornando-se dessa forma acessíveis somente por meio da intervenção do *service provider* que realiza o armazenamento. Nesses casos, os tradicionais instrumentos de cooperação judiciária entram em crise, porque pode tornar-se muito difícil especificar um Estado de execução ao qual direcionar pedidos de cooperação. Nesse quadro delineado, nasce a ideia, acolhida em uma proposta de regulamentação da União Europeia, de criar um canal de cooperação direta entre as autoridades judiciarias interessadas na colheita da prova e o *provider*, ao qual caberia verificar se os pedidos instrutórios respeitam a Carta de Nice. No entanto, trata-se de tendência de privatização de uma atividade tradicionalmente reservada aos órgãos públicos: uma preocupante mudança de paradigma capaz de fragilizar os direitos fundamentais" (DANIELE, M. Obtenção de provas digitais por servidores: uma preocupante mudança de paradigma na cooperação internacional. **Revista Brasileira de Direito Processual Penal**, [*S. l.*], v. 5, n. 3, p. 1277–1296, 2019. DOI: 10.22197/rbdpp.v5i3.288. Disponível em: https://revista.ibraspp.com.br/ RBDPP/article/view/288. Acesso em: 27 abr. 2022).

ordem jurídica e social de cada nação[402].

Sabedores da premente necessidade de que o Direito moderno se preste à prevenção e à repressão de ofensa a bens jurídicos carentes de tutela penal, essa atividade jamais pode se descolar da observância estrita aos princípios constitucionais que limitam as atividades de restrição de direitos, liberdades e garantias fundamentais promovidas pelo Estado no combate à criminalidade. Mesmo no âmbito digital, não se pode admitir, em nome de uma maior eficácia processual na coleta de elementos para a construção de uma verdade, o arrefecimento de tutelas jurisdicionais para a obtenção da prova[403]. É necessário que se estabeleçam limites jurídicos orientados pelo paradigma estabelecido pela Constituição Federal, não apenas para evitar a ocorrência de graves violações às garantias individuais como também para evitarmos o risco de transformar a pessoa em objeto[404].

A prevenção e a repressão da criminalidade, ainda que tecnológica, não pode se afastar da ordem estabelecida pelos princípios constitucionais, mesmo que os quadros normativos por enquanto existentes se apresentem como absolutamente frágeis para o combate efetivo desse tipo de delinquência. Existe um sistema que estrutura e limita o uso do poder estatal que não pode ser relativizado, ainda que leve em consideração a transformação de uma sociedade antes panóptica para uma sociedade sinóptica, caracterizada pelas transformações sociais decorrente da liquidez e do controle dos riscos em direção a uma sociedade tecnológica, em que seres humanos se autoisolam e se autocoisificam, vivendo em um regime de servidão absoluta a uma extensa gama de redes virtuais e dispositivos tecnológicos que se multiplicam assustadoramente na sociedade do século XXI.

Como foi possível até aqui verificar, subsistemas têm se desenvolvido muito mais em favor da policialização do Judiciário e dos órgãos administrativos em matéria penal, com uma consequente admissibilidade de meios de provas com base em autorizações carentes de jurisdição, reforçando a produção de elementos sob o manto de autorizações administrativas e policiais, o que reforça uma atuação antecipada do Judiciário[405]. Esses novos modelos

---

[402] LA FUENTE. Elvira Tajeda de. Ciberseguridad y ciberdelincuencia: respuestas desde el Estado de Derecho. La armonización legislativa transnacional, en particular: las medidas de investigación criminal en la convención de Budapest. *In*: ZARAGOZA TEJADA, Javier Ignácio. **Investigación Tecnológica y Derechos Fundamentales**: comentarios a las modificaciones introducidas por la Ley 13/2015. Navarra: Editorial Aranzadi, 2017. p. 38.

[403] VALENTE. Manuel Monteiro Guedes. O reforço dos Princípios Constitucionais na obtenção da prova no mundo digital. RDPJ, Brasília, ano 2, n. 3, p. 11-25, jan/jun 2018. p. 12-13.

[404] GIACOMOLLI. Nereu José. **A Fase Preliminar do Processo Penal**: crises, misérias e novas metodologias investigatórias. Rio de Janeiro: Lumen Juris Editora, 2011. p. 165.

[405] VALENTE. Manuel Monteiro Guedes. **Os Desafios do Processo Penal do Estado Democrático de Direito**: A Sociedade Internético-Personocêntrica. 2014. p. 7-8. Disponível em: http://www.ibadpp.com.br/1773/. Acesso em: 17 jun. 2019.

legislativos construídos a partir da intervenção do fenômeno da tecnologia no Direito têm se demonstrado capazes de relativizar e até mesmo suprimir a observância das garantias constitucionais que regem a intervenção do Estado a partir da suspeita ou cometimento de atividades ilícitas no mundo digital, sobretudo se consideradas as aparentes incapacidades de ação e prevenção do poder público para a repressão dessas condutas. Isso jamais pode servir como elemento fundante de retorno às práticas autoritárias desenvolvidas antes das conquistas democráticas consagradas nas constituições modernas.

Inovação tecnológica e a difusão estão se acelerando, demandando uma postura reflexiva sobre seu desenvolvimento, incorporação em nossas vidas e utilização, bem como de como estabelecer estruturas e recursos compatíveis com essas tecnologias emergentes; pensar ética e políticas para elas, já que conferem poder àqueles que a ela têm acesso, é tema de destaque na ética das tecnologias emergentes, que está centrada justamente na necessidade de se assumir a responsabilidade pelo poder que a tecnologia moderna proporciona e de desenvolver uma ética apropriada para esse poder. O objetivo de uma análise a partir de poder é identificar a projeção de tecnologias e abordar aspectos de seu contexto social e ecológico, contribuindo, assim, para a justiça, a autonomia e a sustentabilidade. As tecnologias reestruturam continuamente as condições da experiência humana, molda relações, valores, paisagens e expectativas; alteram as relações de poder e torna possíveis novas formas de vida e desloca as anteriores. Mas enquanto não estiverem integralmente desenvolvidas, não se saberá quais as características ou como funcionam; enquanto não difundidas, desconheceremos seus impactos.

Mídia digital pode ser copiada e disseminada, de forma barata, sem perda de qualidade. Consumidores compartilham, aumentando seu poder social ou político, causando mudanças nas relações: o aumento do poder social e político proporcionado por uma nova tecnologia muitas vezes vem com uma diminuição correlativa do poder de outros. Como a tecnologia fornece um poder material que muitas vezes se traduz em poder social e político difuso, uma avaliação abrangente das dimensões social e ética de uma tecnologia emergente requer a realização de uma análise de poder da tecnologia, sobretudo porque a tecnologia, em termos de valor, não é neutra: distribui-se de forma desigual; dá poder a pessoas ou instituições enquanto desarma outras, o que desvenda preocupações sobre a distribuição da justiça em uma ampla gama de domínios, sobretudo quando introduzida em contextos já desiguais e quando favorece o acesso dos já favorecidos. A análise ética de uma tecnologia emergente pode ser conduzida por vários eixos, dentre os quais interessam (i) uma análise para identificar *quem tem* e *quem é destituído* ou *como têm* ou *são destituídos* de poder pela

tecnologia ou (ii) para identificar como a tecnologia pode reestruturar as atividades, as condições pessoais, sociais e ecológicas em que está envolvida. Essas análises e identificações devem ser feitas ao longo do ciclo de vida tecnológico, atentando para como se difere de tecnologias anteriores e as características dos contextos sociais e ecológicos em que está emergindo[406].

Interessa-nos, em especial, o tratamento de dados – pessoais e provenientes de fontes abertas – através da iniciativa privada para uma investigação legítima levada a efeito com fundamento na Investigação Defensiva (Provimento nº 188/2018 do Cfoab), Investigações Internas (Lei nº 12.846 e Decreto nº 11.129/2022), aquelas que, por orientação da defesa, são realizadas por detetives particulares (art. 2º c/c art. 5º da Lei nº 13.432/2017) ou até mesmo de investigações atinentes a outras jurisdições (laboral, propriedade industrial e/ou intelectual), mas que igualmente podem apontar para a prática de ilícitos penais, o que perpassa por refletir sobre o enquadramento do advogado como controlador ou operador de dados para poder definir os limites de suas responsabilidades e prerrogativas: ao controlador competem as decisões referentes ao tratamento, em nome de quem o operador deverá realizar, dentro dos estreitos limites estabelecidos, o tratamento[407].

No caso dos dados coletados fora do exercício do objeto do escritório, parece não haver dúvida: dados são tratados pelo advogado na condição de controlador[408], onde sua responsabilidade é mais abrangente, cabendo-lhe definir os aspectos relacionados aos dados recebidos para tratamento. O Guia 7/20, editado pelo Conselho Europeu de Proteção de Dados, estabeleceu em seu item 33, sem apontar uma diretiva específica sobre o papel de advogados, que o controlador é aquele que determina qual a finalidade do tratamento do dado e como esta será atingida.

A questão sensível diz respeito àqueles dados tratados no próprio exercício da profissão, já que, com a LGPD, para definir os limites da responsabilidade o advogado deverá, ante seu representado, ter cuidado com os dados que está recebendo, se serão úteis ou se está claro como serão tratados. Os princípios da adequação, da necessidade e da transparência exigem do advogado identificar os dados necessários, orientar para a

---

[406] SANDLER, Ronald L. **Ethics and Emerging Technologies**. London: Palgrave Macmillan, 2014. p. 9-23.
[407] GUARIENTO, Daniel Bitencourt; MAFFEIS, Ricardo. **Qual o Papel dos advogados enquanto agentes de tratamento de dados**: controladores ou operadores? Disponível em: https://www.migalhas.com.br/coluna/impressoes-digitais/336001/qual-o-papel-dos-advogados-enquanto-agentes-de-tratamento-de-dados--controladores-ou-operadores. Acesso em: 7 ago. 2022.
[408] Dados recebidos, por exemplo, para a execução de contratos com fornecedores, na relação de trabalho com colaboradores ou para controle de acesso às suas dependências, são tratados na condição de controlador.

minimização de dados e eliminar aqueles dispensáveis.[409] Como a proteção do dado pessoal não está na cultura do brasileiro, enquadrar os tratados no próprio exercício da profissão vem sendo encarado como um desafio. No geral, advogados devem ser encarados como controladores, já que boa parte da própria execução do trabalho e da *expertise* do advogado estará na definição de como tratar o dado.

Na Comunidade Europeia, onde já é sedimentada a consciência da importância na preservação do dado pessoal, a tendência tem sido em considerar, de regra, escritórios como controladores. Lá, o Grupo de Trabalho do Artigo 29 (Art. 29 WP)[410] posicionou-se em favor de que se o prestador do serviço exerça atividade tradicional e de *expertise* profissional que lhe imponha definir o propósito e os meios de tratamento, e aquela determinada *expertise*, em geral, o define como um controlador. A Opinião 1/2010 analisou advogados atuando em juízo e, sob a justificativa de que a instrução que o cliente lhe dá não é para tratar o dado, mas para representar seus interesses em juízo, concluiu que advogados devem ser encarados como controladores[411], já que o tratamento do dado seria uma atividade auxiliar, a ser total ou parcialmente determinada pelo advogado, dentro da sua independência profissional e funcional, portanto, sem ingerência do cliente[412].

Conclusão similar foi apontada pela Agência de Informações do Reino Unido e de outros órgãos, inclusive de ordens de advogados de países da Comunidade Europeia, como França, Alemanha e Itália. Para a *United Kingdom Information Commissioner's Office*, o advogado deve ser considerado controlador em duas circunstâncias: (i) quando receber dados pessoais sobre terceiros para assessorar o cliente em relação a seus direitos e (ii) quando o cliente tiver pouco discernimento acerca de como os dados serão tratados no curso da representação profissional pelo advogado. Esses órgãos, entretanto, ressalvam eventualidades em que advogados podem ser considerados operadores conforme recebam objetivos/premissas específicas para que, com base em métodos/formas também específicas, realizam o tratamento

---

[409] GUARIENTO, Daniel Bitencourt; MAFFEIS, Ricardo. **Qual o Papel dos advogados enquanto agentes de tratamento de dados**: controladores ou operadores? Disponível em: https://www.migalhas.com.br/coluna/impressoes-digitais/336001/qual-o-papel-dos-advogados-enquanto-agentes-de-tratamento-de-dados--controladores-ou-operadores. Acesso em: 7 ago. 2022.

[410] Grupo de trabalho europeu independente formado a partir do art. 29 da Directiva 95/46 de 1996, que tratou de questões relacionadas à proteção da privacidade e dos dados pessoais e atuou por mais de 20 anos lidando com as questões relacionadas à proteção de dados pessoais e privacidade até a entrada em aplicação do *General Data Protection Regulation*.

[411] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 1/2010 on the concepts of "controller" and "processor". Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Acesso em: 7 ago. 2022.

[412] GUARIENTO, Daniel Bitencourt; MAFFEIS, Ricardo. **Qual o Papel dos advogados enquanto agentes de tratamento de dados**: controladores ou operadores? Disponível em: https://www.migalhas.com.br/coluna/impressoes-digitais/336001/qual-o-papel-dos-advogados-enquanto-agentes-de-tratamento-de-dados--controladores-ou-operadores. Acesso em: 7 ago. 2022.

dos dados na execução de trabalhos como análise de contratos, revisão de documentos ou *due diligences*[413]. Aqui, parece-nos, se inserem as atividades de investigação defensiva e investigações internas, de forma que os advogados também poderiam ser considerados como operadores de dados.

Sob a perspectiva da eficácia horizontal dos direitos fundamentais[414], a atividade de obtenção da evidência digital possibilita a proposição de dado como prova, justificada na satisfação de interesses legítimos do responsável pelo tratamento ou de terceiro, ferramenta de concretização do exercício do direito de defesa. Por sua vez, a atividade de admissão e incorporação do dado como prova, feita pelo juiz, é legitimada pelo cumprimento de missão realizada em interesse público ou de poderes públicos no exercício de sua função jurisdicional[415].

Quando o particular apresenta dados de sua titularidade não existe qualquer ilegalidade, pois estar-se-á diante da hipótese de *consentimento* do titular dos dados, o que afasta a proteção da garantia fundamental. Tormentosa é a situação de quando os dados pessoais à disposição ou que se encontram em seu poder são da parte contrária ou de terceiros que não ostentam a condição de parte, casos em que será necessário o consentimento do interessado ou, ante sua ausência, verificar se o tratamento está justificado sob uma base jurídica legítima. A incorporação de dados pessoais da parte contrária licitamente obtidos coloca em colisão a existência de dois direitos fundamentais: de um lado, o direito fundamental de proteção de dados pessoais e, de outro, a garantia judicial efetiva, em especial os direitos de defesa e à prova; estes relativizam a eficácia do primeiro, de forma que os dados possam ser incorporados ao processo com fundamento na existência de interesse legítimo, sempre que realizada com fins explícitos e legítimos – exercício de defesa – e atendendo aos princípios de proteção de dados[416].

A análise das relações entre proteção de dados pessoais e o regime de prova parte do pressuposto de que tanto a obtenção do dado quanto a sua incorporação ao processo penal por seus sujeitos constitui forma de tratamento de dados. Assim como também o é a admissão do

---

[413] GUARIENTO, Daniel Bitencourt; MAFFEIS, Ricardo. **Qual o Papel dos advogados enquanto agentes de tratamento de dados**: controladores ou operadores? Disponível em: https://www.migalhas.com.br/coluna/impressoes-digitais/336001/qual-o-papel-dos-advogados-enquanto-agentes-de-tratamento-de-dados--controladores-ou-operadores. Acesso em: 7 ago. 2022.

[414] ALEXY, Robert. **Teoría de los Derechos Fundamentales**. Centro de Estudios Políticos y Constitucionales: Madrid, 2012. p. 506-524.

[415] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 413-414.

[416] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 415.

dado, pelo juiz, como prova, de forma que, como *corresponsável pelo tratamento de dados*, também estará suscetível ao regime jurídico e à aplicação dos princípios de tratamento de dados pessoais especialmente aplicáveis em matéria probatória.[417]

A incorporação de dados pessoais ao processo com finalidade de constituir prova pode ocorrer ante uma base jurídica que a legitime e assegure a licitude do tratamento: consentimento do interessado; tratamento necessário para a execução de um contrato em que o interessado é parte; tratamento necessário para o cumprimento de obrigação legal aplicável ao responsável pelo tratamento; tratamento necessário para proteger interesses vitais do interessado ou de outra pessoa física; tratamento para o cumprimento de missão realizada em interesse público ou de poderes públicos conferidos ao responsável pelo tratamento e o tratamento necessário para a satisfação de interesses legítimos do responsável pelo tratamento ou de terceiro – que não se confunde àquele realizado por autoridades públicas.

Ou seja, ainda que não ocorra o consentimento do interessado, pode ser lícita a incorporação de dados pessoais ao processo com finalidade de constituir prova.[418] Nesse sentido, a reforma da Lei Orgânica do Poder Judiciário espanhol, ocorrida no ano de 2015, estabeleceu não ser necessário o consentimento do interessado para tratamento de seus dados pessoais no âmbito do processo judicial, independentemente se apresentados pelas partes ou obtidos por solicitação do próprio órgão judicial.[419] Esse novo cenário da prática jurídica permitirá que outros atores dela participem, e isso invariavelmente determinará uma completa revisão do estatuto geral da advocacia e de seu código deontológico; surgirão novos trabalhos e desafios para a advocacia, a qual será demandada a acumular, aos conhecimentos jurídicos, saber tecnológico.[420]

As normas brasileiras que dizem respeito ao tratamento de dados não são explícitas quanto à possibilidade ou à impossibilidade de tratamento de dados pelo advogado para o exercício de defesa. Aparentemente, tanto o Anteprojeto da Comissão de Juristas como o Projeto nº 1515/2022 destinam-se ao tratamento de dados para fins de persecução penal realizados por autoridades públicas; por outro lado, ainda que não exista qualquer negativa ou

---

[417] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 403-404.
[418] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 408.
[419] DELGADO MARTÍN, Joaquín. **Investigación tecnológica y prueba digital en todas las jurisdicciones**. Madrid: España, 2018. p. 138.
[420] NAVARRO; Susana Navas. Da assistência à substituição dos advogados – a repercussão da Proposta europeia de Regulamento sobre a Inteligência Artificial no Legal Tech. *In*: ABREU, Joana Covelo de; COELHO, Larissa; CABRAL, Tiago Sérgio. **O Contencioso da União Europeia e a cobrança transfronteiriça de créditos**: compreendendo as soluções digitais à luz do paradigma da Justiça electrónica europeia (e-Justice). Braga: UNIO EU Law Journal, 2021. v. III. p. 107-121.

proibição explícita, ambos vedam o tratamento de dados por pessoas jurídicas de direito privado, a não ser que submetidos ao escrutínio da autoridade pública, o que deixa uma perigosa margem para interpretações restritivas aos direitos e às garantias fundamentais, notadamente, no caso de persecução penal, o devido processo legal e a paridade de armas dele decorrente, assim como o direito à prova.

O cerne da investigação defensiva se baseia na ideia de coleta e tratamento de dados pelo advogado, que evidentemente tem interesse na investigação, persecução e também na execução da pena, é sujeito imprescindível à administração da justiça, de forma que, se – conforme os projetos de LGPD Penal propostos a partir da Convenção de Budapeste –, Ministérios Públicos e Polícias em geral poderão tratar dados de suspeitos, testemunhas e outros envolvidos no processo, a paridade de armas impõe que advogados, atuando no exercício do direito de defesa, tenham a mesma prerrogativa. Leis de proteção de dados devem ser cotejadas com os direitos e as garantias individuais previstos na Constituição Federal, os quais, na garantia do direito de defesa, asseguram direitos como o devido processo legal, o direito à prova e a paridade de armas, o que não pode ser-lhes negado diante de sua imprescindibilidade à administração da Justiça e a quem devem ser outorgadas as prerrogativas necessárias para que cumpram com seu papel constitucional.

Quanto ao tratamento de dados por advogados e outros sujeitos investidos desse poder, como é o caso do detetive particular[421], a análise pode ser proposta a partir de três diferentes categorias: *dados do representado e do ofendido* – advogados e procuradores são responsáveis pelo tratamento dos dados pessoais de seu representado, de modo que são integralmente aplicáveis os princípios e normas de tutela para a proteção de dados pessoais –, *dados pessoais disponíveis no processo* – quando advogados e procuradores têm acesso aos dados pessoais em razão da representação processual, o acesso se legitima com fundamento no direito à tutela judicial efetiva e passa o profissional a ser responsável pelo tratamento dos dados conhecidos – e *dados da parte contrária* – igualmente com fundamento na tutela judicial efetiva, e agora também no acesso à defesa e no uso de todos os meios de prova para

[421] "Art. 2º Para os fins desta Lei, considera-se detetive particular o profissional que, habitualmente, por conta própria ou na forma de sociedade civil ou empresarial, planeje e execute coleta de dados e informações de natureza não criminal, com conhecimento técnico e utilizando recursos e meios tecnológicos permitidos, visando ao esclarecimento de assuntos de interesse privado do contratante.
[...]
Art. 5º O detetive particular pode colaborar com investigação policial em curso, desde que expressamente autorizado pelo contratante. Parágrafo único. O aceite da colaboração ficará a critério do delegado de polícia, que poderá admiti-la ou rejeitá-la a qualquer tempo" (BRASIL. **Lei nº 13.432, de 11 de abril de 2017**. Dispõe sobre o exercício da profissão de detetive particular. Brasília, DF: Presidência da República – Secretaria-Geral – Subchefia para Assuntos Jurídicos, 11 de abril de 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13432.htm. Acesso em: 12 abr. 2022).

a defesa dos direitos individuais, esses mesmos profissionais encontram-se legitimados ao tratamento dos dados da parte contrária, desde que isso não configure infração a algum direito fundamental[422].

Via de regra, o aporte de dados pessoais obtido por particular no âmbito da investigação criminal ou do processo penal deve ser considerado como violação ao direito fundamental à proteção de dados pessoais, na medida em que direitos fundamentais igualmente são aplicáveis entre as relações privadas, atendendo ao critério da eficácia horizontal desses direitos fundamentais[423]. Trata-se, portanto, de prova ilícita obtida por particular, incide a regra geral de ilicitude probatória, de forma que se algum dado é obtido por particular a partir da violação do direito fundamental à proteção de dados pessoais ou outro direito fundamental, haverá de ser reconhecida a nulidade desse elemento, dado que a eficácia horizontal dos direitos fundamentais impõe o mesmo tratamento às relações privadas, sem distinção.

Entretanto, a jurisprudência[424] da Sala Penal do Tribunal Supremo espanhol considera que as provas obtidas por particulares com vulneração de direito fundamental nem sempre são nulas. Para a Corte, em cada caso cabe valorar de maneira exaustiva as concretas circunstâncias concorrentes, não se aplicando a regra de exclusão probatória quando ficar demonstrado: a) que existe desconexão entre a conduta do particular e a atividade do Estado; b) que a vontade do particular, em sua origem, tenha sido alheia à vontade de pré-constituir prova, o que significa dizer, ao fim e ao cabo, que, quando a atuação do particular deu-se sem o objetivo de obter a prova mediante vulneração de garantia fundamental para sua juntada no processo, ela não pode ser considerada ilícita, ainda que possa o agente responder civil ou penalmente[425].

A simples alusão aos princípios constitucionais, entretanto, parece ser absolutamente insuficiente para assegurar os direitos. Assegurar ao defensor ou a quem esteja conduzindo investigações defensivas ou internas prerrogativas para poder transformar dados brutos em inteligência e dotar-lhes de estruturas tecnológicas é uma nova realidade que deve ser pensada em instituições como as Defensorias Públicas e a Organização dos Advogados do Brasil (OAB). Prerrogativas digitais aos defensores, baseadas na lógica do tratamento de dados

---

[422] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 446-447.
[423] DELGADO MARTÍN, Joaquín. **Investigación tecnológica y prueba digital en todas las jurisdicciones.** Madrid: España, 2018. p. 139.
[424] SSTS 508/2017, 287/2017, 116,2017, 54/2014 e 793/2013.
[425] MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020. p. 225-228.

pessoais pelas defesas e da inteligência em fontes abertas no âmbito das Defensorias Públicas e da advocacia surgem como estruturas fundamentais para, em igualdade de condições, a promoção de suas funções constitucionais relacionadas à garantia efetiva da liberdade, do direito de defesa e à prova.

Parece-nos ser possível, sustentar, portanto, uma prerrogativa de tratamento de dados pessoais por advogados e procuradores, destinados a recolher informações para o exercício de suas funções, assim como se extrai do art. 8 da *Ley Orgánica* 3/2018, que impõe proteção de dados pessoais e garantias aos direitos digitais na Espanha, estabelece para que o tratamento de dados pessoais possa ser considerado como tendo por base o cumprimento de uma obrigação legal a cargo do responsável pelo tratamento, que ele deve estar previsto por norma de direito da União Europeia ou com *status* de lei, que pode determinar as condições gerais do tratamento e os tipos de dados tratados, bem como as transferências necessárias como resultado do cumprimento da obrigação legal. Em complemento, o artigo 19.3, também da *Ley Orgánica* 3/2018, regula de forma tópica o tratamento de dados de contato, de empresários individuais e profissionais liberais, estipulando que controladores de dados podem efetivar tratamento de dados quando isso surgir de uma obrigação legal ou for necessário para o exercício de seus poderes[426].

Veja-se que não se trata, apenas, do direito de requisitar dados públicos ou de ter acesso aos dados que estão sendo tratados, mas do direito de tratar dados, não apenas aqueles que estão sendo objeto de tratamento por uma parte – e têm que estar acessíveis ao tratamento pela outra –, mas também aqueles disponíveis em investigação criminal ou processo a que tenham acesso em razão de sua função. Evidentemente, ao outorgar às instâncias de defesa tal prerrogativa, também surgirá a necessidade de promover a estruturação de autoridade de controle de tratamento de dados nas defensorias públicas e na OAB, de forma a que comuniquem e registrem as operações de tratamento de dados levadas a efeito por advogados ou defensores nos cursos de suas investigações defensivas, evidentemente cumprindo com todas as exigências relativas à proteção de dados pessoais.

Por outro lado, a realidade financeira da Defensoria Pública não permite esse tipo de investimento, o que se dirá para advogados privados, a imensa maioria de questionável disponibilidade orçamentária e, nesse aspecto tecnológico, ainda sem maior suporte da Ordem ou das associações de classe. O abismo tecnológico tende a aumentar ainda mais: para

[426] ESPANHA. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. **Agência Estatal Boletín Oficial del Estado**: Espanha, seção I – Disposiciones generales, n. 294, p. 119788-119857, 6 de dezembro de 2018. Disponível em: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673. Acesso em: 11 abr. 2022.

tratamento de dados pessoais, incluindo o uso da inteligência de fontes abertas, ao passo que Polícia e Ministério Públicos se estruturam com Unidades de Inteligência, as defesas sequer possuem condições de rodar programas[427]. Esse novo domínio, em franca expansão, cria um espaço que exige analistas bem treinados e com as ferramentas tecnológicas avançadas para analisar os componentes do ciberespaço[428]. Suas estruturas e seu *mind set* carecem, ainda, de agentes neutros de compartilhamento de dados e informações relevantes, Unidades de Inteligência, orçamento e estrutura para o desempenho de atividades tecnológicas em igualdade.

O que poderia ser considerado o embrião do modelo baseado em Unidades de Inteligência Defensiva nasce a partir da Lei Estadual nº 10.779/2018, junto com a própria Defensoria Pública do Estado do Mato Grosso, que dispõe sobre a estrutura organizacional, o quadro de pessoal e o plano de carreiras de apoio administrativo da instituição. Vinculada ao gabinete do defensor público-geral, a norma local criou a Unidade de Inteligência e Segurança Institucional (art. 5º, parágrafo 1º, inciso I, alínea "i"), a qual, regulamentada pela Portaria nº 0486/2019, é classificada como um órgão de administração sistêmica orientado ao atendimento de demandas específicas nas áreas de inteligência e segurança institucional que contempla ações de inteligência, contra inteligência, operações de inteligência, segurança de pessoas, materiais, áreas, instalações e as demais relacionadas ao tema (art. 18), a quem compete, dentre outras atribuições: (i) Planejar, organizar, dirigir, executar, coordenar, monitorar e orientar as atividades de inteligência da Defensoria Pública; (ii) propor a celebração de convênios, acordos, parcerias, programas de capacitação técnica e treinamento de servidores da Defensoria Pública em inteligência; (iii) exercer outras atividades compatíveis com as suas finalidades que forem determinadas pelo Defensor Público-Geral (art. 19) e é também utilizada no âmbito das atividades de sua própria Corregedoria para a obtenção e análise de dados e informações e para a produção e difusão de conhecimentos, relativos a fatos e situações de imediata ou potencial influência sobre a atividade correcional da Instituição.

Outro modelo – agora não apenas no plano normativo, mas que finalmente busca concretizar estrutura para efetivar a transição de uma cultura defensiva que sempre ocupou posição de resistência para uma defesa ativa no que guarda relação com a reunião de

---

[427] ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico**: de acordo com a teoria dos jogos e MCDA-A. Florianópolis: Emais, 2021. 42-49.

[428] PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**, Bogotá: v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.

elementos e informações – foi anunciado em 2022 pela Defensoria Pública do Estado do Rio de Janeiro (DPRJ), que está implantando um Núcleo de Investigação Defensiva ligado à área de Defesa Criminal e que, em busca de efetivação da paridade de armas, propõe-se a satisfazer seus objetivos institucionais oferecendo apoio técnico-científico e a possível criação de um laboratório de ciências forenses para dar apoio prático e técnico nas atividades de investigação e consultas pelo defensor público. Através de convênios ou até se admitindo a busca de profissionais em áreas técnico-científicas, a efetivação de um núcleo de inteligência pode suportar o profissional responsável pela defesa com informações que podem ser advindas de elaboração de laudos, contralaudos, análises de provas periciais e, por que não, por intermédio de tratamento de dados pessoais disponíveis no processo ou em fontes abertas, tudo em apoio à concretização da defesa no processo criminal[429]. Na mesma linha, por meio da Portaria nº 1.165/2022/DPG, a Defensoria Pública de Mato Grosso instituiu, em setembro de 2022, uma Comissão para o estudo da criação e normatização do Núcleo especializado na Investigação Criminal Defensiva, na atuação em interrogatórios, em inquéritos policiais e junto ao Núcleo de Inquéritos Policiais do Poder Judiciário de Mato Grosso[430].

As prerrogativas da defesa surgem para assegurar a plena liberdade do exercício profissional, especialmente no momento de defender os clientes, de forma com que o faça com independência e autonomia, sem temor ou constragimento por parte daqueles agentes que integram os órgãos da persecução penal. Apontadas no art. 6º e 7º da Lei nº 8.906/1994, foram pensadas para o exercício de uma advocacia analógica, que não tinha, diante de si, os enormes desafios gerados pelos impactos das tecnologias emergentes, sobretudo pela multiplicação e pelo fácil acesso à informação advindos do contexto tecnológico. Está nítido que a nova racionalidade de trazer sentido aos dados através de computadores e *softwares* passará a permear cada vez mais as atividades das agências do controle punitivo, fato evidenciado não apenas pelas orientações internacionais e projetos e anteprojetos de lei aqui analisados, no que dizem respeito ao tratamento de dados pessoais para fins de investigação e persecução penal, como também pelas evidências que demonstram uma corrida dessas mesmas agências à capacitação para a coleta e tratamento de dados abertos.

De forma a superar as lacunas decorrentes, parece-nos imprescindível assegurar à Lei 8.906/96 uma prerrogativa à advocacia para que possa promover o tratamento de dados

[429] RIO DE JANEIRO (Estado). Defensoria Pública do Estado do Rio de Janeiro. **Defensoria do Rio terá novo Núcleo de Investigação Defensiva**. Rio de Janeiro: Defensoria Pública do Estado do Rio de Janeiro, 24 de agosto de 2022. Disponível em: https://www.defensoria.rj.def.br/noticia/detalhes/20445-Defensoria-do-Rio-tera-novo-nucleo-de-Investigacao-defensiva. Acesso em: 20 abr. 2022.

[430] IOMAT. **Diário Oficial do Estado do Mato Grosso**. Disponível em: https://www.iomat.mt.gov.br/ver-html/16950/#/e:16950. Acesso em: 20 abr. 2022.

pessoais e de dados disponíveis em fontes abertas – assim compreendidas como dados governamentais em formato aberto e dados manifestamente tornados públicos pelo seu titular por qualquer meio –, do seu representado, do ofendido, de dados disponíveis em procedimentos administrativos ou processo que esteja constituído e de dados da parte contrária, quando, sempre que realizado com fins explícitos e atendendo os princípios gerais das LGPDs, ocorrer: (i) o consentimento do interessado; (ii) o tratamento necessário para a execução de um contrato em que o interessado é parte; (iii) for o tratamento necessário para o cumprimento de obrigação legal aplicável ao responsável pelo tratamento; (iv) for o tratamento necessário para proteger interesses vitais do interessado ou de outra pessoa ou (v) for o tratamento necessário para a satisfação de interesses legítimos do responsável pelo tratamento ou de terceiro, ou seja, surgir de uma obrigação legal ou for necessário para o exercício de seus poderes.

Esta nossa proposta foi encaminhada objetivamente à Associação Brasileira de Advogados Criminalistas, que, em meio ao XI Encontro Brasileiro da Advocacia Criminal, realizado na cidade Florianópolis (SC) no ano de 2022, lançou, por intermédio de sua Comissão de Investigação Defensiva e Novas Tecnologias, o Código Deontológico de Boas Práticas da Investigação Defensiva, diante da necessidade de se estruturarem normas de conduta ético-profissionais para o exercício da atividade e propor parâmetros para a conduta da advocacia no curso da Investigação Defensiva[431].

Tendo como hipótese que a qualificação da inteligência defensiva como atividade levada a efeito pelo defensor para coletar, estruturar e analisar elementos de informação de interesse do sujeito passivo tende a promover paridade de armas, *fair trial* e mitigação dos erros, o Código Deontológico de Boas Práticas da Investigação Defensiva surge como instrumento de consolidação democrática, superando o desafio de estabelecer regras de conformidade a serem seguidas, uma espécie de *compliance* da investigação defensiva. Como a questão sensível ainda é a produção de regras e procedimentos éticos, técnicos e normativos associados à função defensiva, demandando a estruturação para o exercício da atividade, o instrumento propõe parâmetros de atuação para auxiliar ações próprias da investigação defensiva e a todos aqueles dispostos à aquisição de novas habilidades, inclusive observando regras para o bom domínio de ferramentas digitais disponíveis, sempre mantido o mínimo dever de conformidade: a ausência de cuidados no tratamento dos elementos disponíveis e na apresentação do produto da investigação defensiva pode invalidar o esforço defensivo, de

[431] COMISSÃO DE INVESTIGAÇÃO DEFENSIVA E NOVAS TECNOLOGIAS DA ABRACRIM. **Código Deontológico de Boas Práticas da Investigação Defensiva.** Florianópolis: Emais Editora, 2022.

forma que o emprego de boas práticas surge como importante passo à democratização do Processo Penal brasileiro[432].

As novas realidade e complexidade que se põem diante da nossa sociedade não podem ser enfrentadas com retrocessos que se fundamentam no direito à eficiência do Estado para a apuração de condutas ilícitas em detrimento do reconhecimento da necessidade, por parte desse mesmo Estado, na busca de maior e melhor cientificidade de atuação nesse campo. As técnicas de apuração de ilícitos – fase de investigação – e de obtenção e produção de provas – fase judicial – na Era Digital devem se adequar à dinâmica dos tempos modernos e ao próprio Direito, dadas suas elevadas potencialidades na produção de danos sociais e lesões às garantias fundamentais, ressaltando a importância de que a orientação dessas atividades estejam ancoradas, se não na observância estrita das normas de processo penal, na observância dos princípios constitucionais que as regem.

Existem limites intransponíveis às pretensões de alteração de sistemas processuais penais, criação de novos modelos de intervenção penal ou de subsistemas de intervenção dentro do sistema processual penal. Ainda que em uma sociedade internético-personocêntrica a investigação e a produção de provas encontrem limites nas liberdades e garantias fundamentais individuais, conceito atribuído a uma sociedade que vive em permanente estado de ligação promovido, sobretudo, pelas redes sociais e pela virtualização do ser, em que as relações se assentam no espaço global e em redes extraterritoriais, cuja principal dimensão é o ciberespaço, local dotado de vigilância indeterminada e invisível, mas que exige do Direito que o seu cientista pense nessa complexidade sem esquecer do indivíduo como ser humano[433].

---

[432] ROSA, Alexandre Morais da; CAMARGO, Rodrigo Oliveira de. O desafio de qualificar a prática da investigação defensiva. **Revista Consultor Jurídico**, 23 de setembro de 2022. Disponível em: https://www.conjur.com.br/2022-set-23/limite-penal-desafio-qualificar-pratica-investigacao-defensiva. Acesso em: 23 set. 2022.

[433] VALENTE. Manuel Monteiro Guedes. **Os Desafios do Processo Penal do Estado Democrático de Direito**: A Sociedade Internético-Personocêntrica. 2014. p. 15-20. Disponível em: http://www.ibadpp.com.br/1773/. Acesso em: 17 jun. 2019.

CONSIDERAÇÕES FINAIS

Já que no Brasil há opção expressa do legislador em não contemplar o tratamento de dados pessoais para fins de segurança pública e persecução penal no âmbito de aplicação da Lei Geral de Proteção de Dados, e como ainda paira uma imensa lacuna sobre a matéria para identificar como garantir o exercício do direito de defesa na atividade de tratamento de dados pessoais, foram analisadas a Convenção de Budapeste (Diretiva nº 2.016/680), o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, ofertado pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados, e o Projeto de Lei nº 1.515/2022. Tanto a Convenção de Budapeste quanto o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal aliam o dever de conferir transparência a modalidades de tratamento de dados pessoais realizadas pela autoridade competente e operações que pretendam gerar confiança em sua legitimidade e integridade a mecanismos de supervisão e controle institucional, tudo de forma a assegurar garantia de publicidade aos tipos, ao escopo e às finalidades de usos de dados.

Preveem direitos aos titulares e obrigações aos agentes de tratamento: aos primeiros, assegura *direitos de acesso aos dados, de retificação, à proteção contra a discriminação* e o *direito à explicação de processos automatizados*; aos segundos, impõem como obrigações a necessidade de elaboração de relatórios de impacto à proteção de dados pessoais em casos de tratamento de dados pessoais sensíveis, sigilosos, ou operações que apresentem elevado risco aos direitos, às liberdades e às garantias dos titulares de dados e à manutenção de registros detalhados das atividades de tratamento.

Já o Projeto de Lei nº 1.515/2022 amplia poderes de acesso, tratamento e compartilhamento de dados por agentes públicos, não deixando maiores espaços para que outras propostas se desenvolvam de forma compatível com garantias processuais e direitos fundamentais. Ao contrário, a proposta está orientada a aumentar prerrogativas às autoridades públicas para o tratamento de dados pessoais e sensíveis, garantindo acesso, tratamento e compartilhamento entre autoridades competentes a esses tipos de dados, assim como a bancos de dados controlados por órgãos e entidades da administração pública ou por pessoas jurídicas de direito privado para diversas finalidades, como inteligência de segurança pública, investigação e repressão de infrações penais.

Diante da opção em não contemplar o tratamento de dados pessoais, e tampouco aqueles provenientes de fontes abertas, para fins de segurança pública e persecução penal no

âmbito de aplicação da Lei Geral de Proteção de Dados e da análise dos referidos instrumentos, constatou-se que a garantia da defesa nas atividades de tratamento de dados pessoais limita-se à prerrogativa exclusiva do titular em ter acesso aos dados pessoais que estão sendo tratados, de retificação, à proteção contra a discriminação e o direito à explicação de processos automatizados. Não se trata de direito atribuído à defesa de tratar os mesmos conjuntos de dados que estão sendo tratados pelos órgãos da persecução penal, ainda que os textos se refiram, ao menos na Convenção de Budapeste e o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, orientados pelo respeito ao direito de defesa e ao devido processo legal.

Para identificar como garantir o exercício do direito de defesa na atividade de tratamento de dados abertos, a análise foi subdividida entre dados publicados por usuários e dados governamentais em formato aberto.

Em relação aos dados publicados por usuários, os quais têm caráter público e sob os quais ao acesso se presume o consentimento, verificou-se que a inserção de conteúdo em canais abertos proporciona que estes sejam acessados por qualquer usuário, inclusive permitindo, sem restrições, a busca de elementos por quaisquer alvos envolvidos, sem que afete direitos fundamentais. Importante lembrar que a LGPD regula o tratamento de dados pessoais cujo acesso é público; não proíbe a atividade, mas aponta o dever em considerar-se a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização, razão pela qual podemos concluir não apenas que se trata de atividade inerente e possível dentro da esfera do exercício do direito de defesa, assim como parece ser necessário assegurar formas para garantir maior transparência e responsabilização sobre o uso dessas tecnologias, tanto pelo setor público quanto pelo privado.

Já os dados governamentais em formato aberto pressupõem um regime jurídico e global de acesso à informação que determine que governos mantenham sistemas de gerenciamento e preservação de documentos públicos, de forma a facilitar o seu acesso futuro, na medida em que documentos e informações produzidas por agentes públicos, governantes ou políticos não pertencem a ele nem ao Estado, mas ao cidadão. Em se tratando da garantia do direito de defesa, a Lei de Acesso à Informação surge como instrumento de resistência ao *poder de requisição* de documentos pelos agentes públicos, já que tem como principal finalidade assegurar ao indivíduo, em face do poder público e seus agentes, transparência, publicidade, controle social e dever de *accountability*, essenciais à eficácia do acesso à informação, fornecendo direitos que podem ser exercidos por intermédio de pedidos de acesso

à informação, o que a pesquisa demonstrou ser verdadeiro instrumento de garantia da defesa no que guarda relação com os dados governamentais em formato aberto.

O surgimento de tecnologias e ferramentas *open source* auxiliam os atores privados ao tratamento dessas informações, de forma que aparecem como importantes recursos que podem ser utilizados para o exercício de uma defesa penal efetiva. Em ambos os casos, mas sobretudo em se tratando de dados publicados por usuários, de forma a garantir o pleno funcionamento das democracias, é necessário que responsáveis pela governança de inteligência em fontes abertas também zelem pelo uso apropriado e profissional das técnicas de tratamento de dados, assim como cumpram com deveres legais para disponibilizar e compartilhar informações, sobretudo se o propósito é voltado para que a informação seja utilizada como evidência em procedimentos de natureza criminal. Em se tratando do uso de aplicações tecnológicas, para que o produto do tratamento de dados seja utilizado para suportar investigações, como elemento de assistência à prova ou como meio de prova no processo, é impositivo que possam, em relação ao seu conteúdo, dados inseridos, automatização e configuração algorítmica ser explicados, conhecíveis e entendíveis pelos sujeitos do processo. Só assim estar-se-á respeitando o direito de defesa e ao devido processo legal.

Essas práticas investigativas voltadas a conhecer o ambiente criminoso, como se viu, agregam não apenas a atividade policial, mas também já se inserem nas atribuições do Ministério Público, apontando para a incursão desses órgãos, acostumados à função repressiva, ao exercício de atividades preventivas. Esse alinhamento aos investimentos em procedimentos de prevenção cria um novo campo de atuação das instâncias responsáveis pela persecução penal. Muitas vezes, são antecedentes à própria investigação preliminar.

O desequilíbrio material entre a igualdade de partes e o direito de defesa não pode ser ignorado. O manejo dessas técnicas oferece vantagens indiscutíveis, sobretudo como analisar expressivas quantidades de dados, provenientes de fontes fechadas ou abertas, de forma muito rápida e intuitiva, tudo com o objetivo de criar valor. A pesquisa realizada demonstrou que, enquanto apenas agentes públicos se valem amplamente desse recurso e ainda demandam maiores prerrogativas, as defesas, acostumadas à razão inquisitorial e sem condições financeiras e materiais, não possuem acesso ou encontram severas dificuldades para ter esse mesmo tipo de acesso, justificando a emergência de discussão sobre a necessidade de novas estruturas, direitos e prerrogativas para suportar, com segurança, o exercício de suas atribuições dentro desta nova realidade.

A partir daí, sob a perspectiva da defesa penal efetiva e de que não é possível que o Estado tenha acesso privilegiado a dados sem que a defesa tenha o direito de acessar as mesmas informações, passou a fazer parte do trabalho cumprir com o objetivo de encontrar alternativas para assegurar os princípios constitucionais relacionados ao processo penal em meio às atividades de tratamento de dados, mormente o devido processo legal e suas principais ramificações: contraditório, ampla defesa e paridade de armas. O desenvolvimento das capacidades de pesquisa e aprendizagem de máquinas fomenta o surgimento de novos sujeitos que colaborem decisivamente na investigação ou no processo penal, e cabe às defesas ter ampla participação nessas fases e no desenvolvimento de tais atividades.

As alternativas encontradas, e que possibilitam novas pesquisas a respeito dessa temática, podem ser categorizadas como estruturais, normativas e deontológicas.

As primeiras, dizem respeito à criação de unidades ou centros de inteligência para o tratamento de dados pessoais ou provenientes de fontes abertas, orientados à razão defensiva, com suporte institucional. Essa proposta que vinha sendo delineada acabou, inclusive, se tornando uma realidade próxima, com a recentíssima criação do Núcleo de Investigação Defensiva da Defensoria Pública do Estado do Rio de Janeiro, onde se estrutura um ambiente em que esta tese pode ser empregada como orientação no que guarda relação, ao menos, com as atividades de tratamento de dados pessoais e abertos no âmbito das atribuições deste Núcleo.

A segunda, demanda espaço para o comprometimento normativo das leis de proteção de dados no âmbito criminal e das normas processuais penais para que seja assegurada a garantia da defesa no que guarda relação com o tratamento de dados, admitindo-se que, nas atividades relacionadas à persecução penal, podem as defesas efetivar tratamento de dados quando isso surgir de uma obrigação legal ou for necessário para o exercício de seus poderes. É imperioso que instrumentos que se destinam a regulamentar as atividades de tratamento de dados pessoais para fins de segurança pública e persecução penal reconheçam a necessidade de assegurar o exercício da defesa: se, de um lado, a LGPD cria hipóteses que justificam atuações de sujeitos como advogados, de outro os projetos de LGPD Penal, ao colocarem as atividades de tratamento de dados exclusivamente nas mãos das autoridades públicas, excluem tal possibilidade quando se trata de tratamento de dados que tenham por objeto o resguardo da segurança pública e persecução penal, o que ainda é reforçado quando os projetos expressamente afastam a possibilidade de tratamento de dados pessoais por entes privados para essas finalidades.

Por fim, parece ser necessária uma alteração nos códigos deontológicos da advocacia e da defensoria para assegurar o tratamento de dados como direito inerente às atividades de defesa, estabelecendo-se regras de conformidade a serem seguidas, uma espécie de *compliance* do tratamento de dados realizado. Na linha da primeira alternativa apontada, isso demanda que OABs e Defensorias Públicas estruturem-se em torno de práticas de governança de informações, agindo como autoridades de controle das atividades de tratamento de dados realizadas por seus agentes.

No plano deontológico, a proposta produzida nesta tese acabou sendo incorporada ao Código Deontológico de Boas Práticas da Investigação Defensiva, publicação orientada pelo reconhecimento da necessidade da estruturação de normas de conduta ético-profissionais para o exercício da atividade de investigação defensiva, lançado no final de setembro de 2022 pela Associação Brasileira dos Advogados Criminalistas. Considerando que a Constituição Federal assegura os princípios da igualdade, do contraditório, do devido processo legal, da ampla defesa e do livre exercício das profissões; que a lógica acusatória trazida pela Constituição Federal assegura a noção de paridade de armas e a necessidade da valorização da advocacia para diminuição do desequilíbrio real de possibilidades dadas entre acusação e defesa no âmbito da persecução penal; a edição do Provimento n.º 188/2018 CFOAB e que a Lei Geral de Proteção de Dados dispõe sobre tratamento de dados pessoais, o instrumento reconhece a necessidade de orientar advogados quanto às possibilidades inerentes à investigação de dados em fontes abertas e fechadas em favor da investigação defensiva.

Nesse sentido, em meio às técnicas de investigação defensiva, a publicação destina um capítulo para, atendendo os princípios constitucionais e aqueles referentes às Leis Gerais de Proteção de Dados (art. 36), conceituar e orientar as atividades de tratamentos de dados pessoais e dados abertos levadas a efeito no curso deste tipo de apuração. O art. 35 do Código Deontológico de Boas Práticas da Investigação Defensiva orienta a atividade de tratamento de dados pessoais realizada com fundamento no direito à tutela judicial efetiva, à ampla defesa e ao direito ao uso de todos os meios de prova para a defesa dos direitos individuais, elencando as hipóteses em que pode ocorrer o tratamento, além de equiparar o tratamento de dados pessoais à ideia de fontes fechadas. Já o art. 37, além de indicar a possibilidade de tratamento e conceituar dados provenientes de fontes abertas, também indica a necessidade de observância dos princípios relativos ao tratamento de dados pessoais a essa espécie de fonte, tudo de forma a assegurar a governança das informações.

O tema é instigante. A tese apontou muitas questões que devem ser debatidas nos próximos anos em face da nova realidade digital, no âmbito do processo penal. Não se espera

que tenham sido apresentadas respostas definitivas ao problema, mas o simples fato de trazer este tipo de discussão para o âmbito do processo penal, por si só, parece ser uma relevante contribuição.

REFERÊNCIAS

AB2L – ASSOCIAÇÃO BRASILEIRA DE LAWTECHS & LEGALTECHS. **Radar maio** 2022. Disponível em: https://ab2l.org.br/wp-content/uploads/2022/06/RADAR-MAIO-2022.pptx-7.png. Acesso em: 3 jul. 2022.

ABOUT DARPA. **DARPA**. Disponível em: https://www.darpa.mil/about-us/about-darpa. Acesso em: 22 fev. 2022.

AGAMBEN, Giorgio. A propósito de Tiqqun. *In*: TIQQUN. **Contribuição para a guerra em curso**. São Paulo: N-1 edições, 2019.

AGÊNCIA CÂMARA DE NOTÍCIAS. **Projeto altera Lei de Proteção de Dados para resguardar segurança pública e defesa nacional**. Disponível em: https://www.camara.leg.br/noticias/893704-projeto-altera-lei-de-protecao-de-dados-para-resguardar-seguranca-publica-e-defesa-nacional/. Acesso em: 27 ago. 2022.

AKHGAR, Babak. OSINT as an integral part of the National Security Apparatus. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation: from strategy to implementation**. Genebra: Springer, 2016.

ALEXY, Robert. **Teoría de los derechos fundamentales**. Madrid: Centro de Estúdios Políticos e Constitucionales, 2008.

ALIPRANDI, Carlo; DE LUCA, Antonio E.; DI PIETRO, Giulia; RAFFAELLI, Matteo; GAZZÉ, Davide; LA POLLA, Mariantonietta; MARCHETTI, Andrea; TESCONI, Maurizio. CAPER: Crawling and analysing Facebook for intelligence purposes. **IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)**, Beijing, China, p. 665-669, outubro 2014. DOI: 10.1109/ASONAM.2014.6921656. Disponível em: https://ieeexplore.ieee.org/document/6921656. Acesso em: 26 fev. 2022.

ANDRADE, Fabiana de Oliveira. **A Escola nacional de Informações**: a formação dos agentes para a inteligência durante o regime militar. 2014. 138 f. Dissertação (Mestrado) – Universidade Estadual Paulista Júlio de Mesquita Filho, Faculdade de Ciências Humanas e Sociais, 2014. Disponível em: http://hdl.handle.net/11449/121960. Acesso em: 8 abr. 2022.

ANTONIALLI, Dennys; CRUZ, Francisco Brito. **Privacidade e internet**: desafios para a democracia brasileira. Rio de Janeiro: Centro Edelstein de Pesquisas Sociais; São Paulo: Fundação Fernando Henrique Cardoso, 2017.

ARGENTINA. Governo da Província de Buenos Aires. **Anexo nº IF-2021-06806836-GDBA-DPFCEMSGP**. La Plata, Buenos Aires. 22 de março de 2021. Disponível em: https://www.mseg.gba.gov.ar/areas/boletin_informativo/14IF-2021-06806836-GDEBA-DPFCEMSGP.pdf. Acesso em: 26 fev. 2022.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 1/2010 on the concepts of "controller" and "processor"**. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Acesso em: 7 ago. 2022.

AZEVEDO, Rodrigo Ghiringhelli de. Elementos para a Modernização das Polícias no Brasil. **Revista Brasileira de Segurança Pública**, São Paulo, v. 10, p. 8-20, mar. 2016.

BACON, Francis. **O progresso do conhecimento.** Tradução, apresentação e notas Raul Fiker. São Paulo: Editora Unesp, 2007.

BARRETO, Alexandre Gonçalves; WENDT; Emerson. **Inteligência e Investigação Criminal em Fontes Abertas**. Rio de Janeiro: Brasport, 2020.

BAUMAN, Zygmunt. **Modernidade Liquida**. Rio de Janeiro: Editora Zahar, 2001.

BAVA, Silvio Caccia. **A guerra das ideias**: a disputa das narrativas. Disponível em: https://diplomatique.org.br/a-guerra-das-ideias-a-disputa-das-narrativas/. Acesso em: 21.abr. 2022.

BAZZEL, Michael. **Open Source Intelligence Techniques**: resources for searching and analyzing online information. 6th ed. [*S. l.*: *s. n.*], 2016.

BECK, Ulrich. **A metamorfose do mundo**: novos conceitos para uma nova realidade. Rio de Janeiro: Zahar, 2018.

BELL¿NGCAT. Disponível em: https://www.bellingcat.com/. Acesso em: 14 abr. 2022.

BINDER, Alberto; CAPE, Ed; NAMORADZE. **Defesa Penal Efectiva em America Latina**: Argentina, Brasil, Colômbia, Guatemala, México, Peru. [*S. l.*]: ADC, Cerjusc, Conectas, DeJusticia, ICCPG, IDDD, IJPP, Inecip, 2015.

BLANTON, Anderson. **Until the Stones Cry Out**: materialities of faith and technologies of the holy ghost in southern appalachia. 2011. 294 f. Tese (Doutorado) – Curso de Philosophy, School Of Arts And Sciences, Columbia University, Columbia, 2011. Disponível em: https://academiccommons.columbia.edu/doi/10.7916/D87W6QR0/download. Acesso em: 15 jun. 2020.

BOEING, Daniel Henrique Arruda; ROSA, Alexandre Morais da. **Ensinando um Robô a Julgar: pragmáticas, discricionariedades, heurísticas e vieses no uso de aprendizado de máquina no judiciário**. 1ª Ed. Florianópolis: Emais Academia. 2020.

BRASIL. Câmara dos Deputados. **Anteprojeto de lei da Comissão de Juristas sobre o Tratamento de Dados Pessoais para fins de Segurança Pública e persecução penal**. Brasília: Câmara dos Deputados, 2020.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1515/2020**, de 7 de junho de 2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274. Acesso em: 20 jun. 2022.

BRASIL. Departamento de Polícia Federal. **Manual de Doutrina de Inteligência Policial – Volume I**. Brasília, 2011

BRASIL. **Lei nº 13.432, de 11 de abril de 2017**. Dispõe sobre o exercício da profissão de detetive particular. Brasília, DF: Presidência da República – Secretaria-Geral – Subchefia para Assuntos Jurídicos, 11 de abril de 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13432.htm. Acesso em: 12 abr. 2022.

BRASIL. Ministério Público Federal. 2ª Câmara de Coordenação e Revisão Criminal. Edital 2CCR nº 7, de 6 de março de 2018. [Seleção de Participantes do Curso]. Brasília: 2ª Câmara de Coordenação e Revisão Criminal, 6 de março de 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/comunicados-da-2a-ccr-1/2018/comunicado_17_edital_curso_oea_brasilia.pdf. Acesso em: 23 abr. 2022.

BRASIL. Ministério Público Federal. **Membros e servidores participam de curso da OEA sobre pesquisa em dados abertos**. 2 de abril [20--]. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/noticias/noticias-1-1/membros-e-servidores-participam-de-curso-da-oea-sobre-pesquisa-em-dados-abertos. Acesso em: 23 abr. 2022.

BRASIL. Portal Brasileiro de Dados Abertos. **O que são dados abertos?** Disponível em: https://dados.gov.br/pagina/dados-abertos. Acesso em: 8 abr. 2022.

BRASIL. Superior Tribunal de Justiça. **HC nº 149.250-SP**. Relator: Ministro Adilson Vieira Macabu (Desembargador Convocado do TJ/RJ), 07 de junho de 2011. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200901925658&dt_publicacao=05/09/2011. Acesso em: 22 dez. 2022.

BRASIL. Supremo Tribunal Federal. **RE 593.727 -MG**. Relator: Min. Gilmar Mendes, 03 de outubro de 2017. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2641697. Acesso em: 20 abr. 2022.

BRASIL. Supremo Tribunal Federal. **ADI 6.387 MC-Ref/DF**. Relator: Min. Rosa Weber, 17 de novembro de 2020. Disponível em: https://bit.ly/2X3Gg3B. Acesso em: 31 agosto de 2022. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15345022689 &ext=.pdf. Acesso em: 20 abr. 2022.

BRASIL. Supremo Tribunal Federal. **Inq. 4.831-DF**. Relator: Min. Celso de Mello, 05 de dezembro de 2020. Acesso em: 31 agosto de 2022. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15345201506&ext=.pdf. Acesso em: 20 abr. 2022.

BRASIL. Tribunal de Justiça do Estado do Rio Grande do Sul. **Apelação Criminal nº 5123185-30.2020.8.21.0001/RS**, 1ª Câmara Criminal. Relator Desembargador Manuel José Martinez Lucas.

BRASIL. Tribunal de Justiça do Estado do Rio Grande do Sul. **AgRg em MS n.º 70056759152**, Órgão Especial. Relator Desembargador Gaspar Marques Batista.

BRASIL. Tribunal de Justiça do Estado do Rio Grande do Sul. **AgRg no RMS nº 62.562**, Órgão Especial. Relator Desembargador Manuel Jose Martinez Lucas.

CAMARGO, Rodrigo Oliveira de; BULHÕES, Gabriel. Defesa Penal Efetiva no Brasil: desafios da atuação defensiva na investigação preliminar em meio ao sistema acusatório. *In*: GONZÁLEZ, Leonel; BALLESTREROS, Paula. **Desafiando a Inquisição**: ideias e propostas para a reforma processual no Brasil. Santiago: Ceja-JSCA, 2019.

CAMARGO, Rodrigo Oliveira de; WEBBER, Lair. A dogmática e a política criminal do combate à corrupção e à criminalidade econômica nos últimos 80 anos: retrospectiva e perspectiva. *In*: REALE JR., Miguel Reale; MOURA, Maria Thereza de Assis. **Coleção 80 anos do Código Penal**. [*S. l.*]: Thompsons Reuters-Revista dos Tribunais. 2021. v. III.

CAMARGO, Rodrigo Oliveira de; MONTANARO, Domingo. A Cadeia de Custódia de Evidências Digitais: mais um desafio da intersecção entre Direito e Tecnologia. *In*: ARAÚJO, Guilherme Silva. CARDOSO, Luis Eduardo Dias. PRADO, Rodolfo Macedo. **Advocacia Criminal: temas atuais.** Florianópolis: Tirant Lo Blanch, 2022.

CAMARGO, Rodrigo Oliveira de. Ilicitude da Devassa: Tratamento de Dados Pessoais de Jurados em Face dos Princípios da Convenção de Budapeste e do Anteprojeto da LGPS-Penal no Brasil. **Boletim do IBCCRIM**, São Paulo, ano 30, n. 159, p. 10-12, out/2022

CANI, Luiz Eduardo; NUNES, João Alcantara**.** Diante de Argos: Notas sobre a ilicitude das informações produzidas em atividade de inteligência. **Boletim do IBCCRIM**, São Paulo, ano 30, n. 157, 11-12, ago/2022.

CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da constituição**. 9. ed., 7. reimpressão. Coimbra: Almedina, [20--].

CARNEIRO, Ramon Mariano. "Li e aceito": violações a direitos fundamentais nos termos de uso das plataformas digitais. **Revista Internet & Sociedade**, São Paulo: Internetlab, n. 1, v. 1, p. 200-229, fevereiro de 2020.

CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003.

CERTIFIED in Open Source Intelligence (C|OSINT). **Niccs** – National Initiative for Cybersecurity Careers and Studies. Disponível em: https://niccs.cisa.gov/training/search/mcafee-institute/certified-open-source-intelligence-cosint. Acesso em: 20 abr. 2022.

CHASE, Oscar G. **Direito Cultura e Ritual**: Sistemas de resolução de conflitos da cultura comparada. São Paulo: Marcial Pons, 2014.

CNIL – Comission Nationale de l'informatique e des Libertés. **Dados Pessoais:** definição. Disponível em: https://www.cnil.fr/en/personal-data-definition. Acesso em: 11 abr. 2022.

COELHO, Adelino de Matos. O "Duplo Uso" – Uma Questão De Terminologia. **Revista Militar**, n. 2629-2630, p. 131-146, fevereiro/março de 2021. Disponível em: https://www.revistamilitar.pt/artigo/1537. Acesso em: 27 ago. 2022.

COLOMER, Juan-Luis Gómez. Estado democrático y modelo policial: Una propuesta de diseño de cara a lograr una investigación eficaz del crimen. *In*: AMBOS, Kai; COLOMER, Juan-Luis Gómez; VOGLER, Righard. **La Policía en los Estados de Derecho Latinoamericanos**: un proyecto internacional de investigación. Chile: Ediciones Jurídicas Gustavo Ibáñez G. LTDA, 2003.

COLOMER, Juan-Luis Gómez. **El proceso penal adversarial**: una crítica constructiva sobre el llamado sistema acusatorio. Editorial Ubijus: México-DF, 2012.

COMISSÃO DE INVESTIGAÇÃO DEFENSIVA E NOVAS TECNOLOGIAS DA ABRACRIM. **Código Deontológico de Boas Práticas da Investigação Defensiva**. Florianópolis: Emais Editora, 2022.

COMISSÃO EUROPEIA. Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime. EU research Results. Disponível em: https://cordis.europa.eu/project/id/261712. Acesso em: 11 ago. 2022.

COMISSÃO EUROPEIA PARA A EFICÁCIA DA JUSTIÇA. **Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e seu ambiente adoptada pela CEPEJ na sua 31.ª reunião plenária**. Estrasburgo, 3 e 4 de dezembro de 2018. Disponível em: https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0. Acesso em: 5 abr. 2022.

COMMUNITY RESEARCH AND DEVELOPMENT INFORMATION SERVICE (CORDIS). **Early pursuit against organized crime using environmental scanning, the Law and IntelligenCE systems**. Disponível em: https://cordis.europa.eu/project/id/312651/reporting. Acesso em: 26 fev. 2022.

COMO funciona a Pesquisa Google (para iniciantes). **Google**. Disponível em: https://developers.google.com/search/docs/beginner/how-search-works#:~:text=they're%20wrong.-,Indexing,tries%20to%20understand%20the%20page. Acesso em: 26 out. 2021.

CORDERO, Franco. **Procedimiento Penal**. Tomo I. Santa Fé de Bogotá: Editorial Themis, 2013.

COUNCIL OF EUROPE. Convenio sobre la ciberdelincuencia. **Serie de Tratados Europeos**, Budapeste, n. 185, 23.XI.2001. Disponível em: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf. Acesso em: 5 abr. 2022.

COUTINHO, Jacinto Nelson de Miranda. Sistema acusatório: cada parte no lugar constitucionalmente demarcado. *In* **Revista de Informação Legislativa**. Brasília. a. 46 n. 183 julho./set. 2009.

COUTURE, Eduardo Juan. **Os Mandamentos do Advogado**. Tradução de Ovídio A. Baptista e Carlos Otávio Athayde. Porto Alegre: Fabris. 1979.

CRAVEIRO, Gisele da Silva; MACHADO, Jorge A. S.; SOLETTO; Juliana Strumiello. Um balanço da demanda de dados abertos no Brasil. **Revista Internet & Sociedade**, v. 1, n. 2, p. 273-276, dez 2020. Disponível em: https://revista.internetlab.org.br/um-balanco-da-demanda-de-dados-abertos-no-brasil/. Acesso em: 3 jan. 2022.

DAMASKA, Mirjan. **Las Caras de La Justicia y el Poder del Estado**: análisis comparado del proceso legal. Santiago: Editora Juridica de Chile, 2000.

DAMASKA, Mirjan. **El derecho probatorio a la deriva**. Madri: Marcial Pons, 2015.

DANIELE, Marcelo. Obtenção de provas digitais por servidores: uma preocupante mudança de paradigma na cooperação internacional. **Revista Brasileira de Direito Processual Penal**, *[S. l.]*, v. 5, n. 3, p. 1277–1296, 2019. DOI: 10.22197/rbdpp.v5i3.288. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/288. Acesso em: 27 abr. 2022.

DELGADO MARTÍN, Joaquín. **Investigación tecnológica y prueba digital en todas las jurisdicciones**. Madrid: España, 2018.

DELGADO MARTÍN, Joaquín. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020.

DEVENPORT, Thomas H; HARRIS, Jeanne G. **Competing on Analytics**: the new science of winning. [*S. l.*]: Harvard Business School Publishing Corporation, 2006. *E-book*.

DIAS, Gabriel Bulhões Nóbrega. **Manual prático de investigação defensiva**: um novo paradigma na advocacia criminal brasileira. Florianópolis: Emais, 2019.

DIAZ MANILLA, Luis Felipe. **Open Source Intelligence en la CPI**: hacia un nuevo paradigma de investigación más allá de la cooperación internacional. Colômbia*:* Uniandes, 2018.

DIETER, Maurício Stegemann. **Política Criminal Atuarial**: a criminologia do fim da História. 2012. (Doutorado – Direito do Estado) – Programa de Pós-Graduação da Faculdade de Direito da Universidade Federal do Paraná, Curitiba: UFPR. 2012. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/28416/R%20-%20T%20-%20MAURICIO%20STEGEMANN%20DIETER.pdf?sequence=1. Acesso em: 30 dez. 2022.

DIZ, Fernando Martín. Justicia Predictiva: inteligencia artificial y algoritmos aplicados al proceso judicial en materia probatoria. *In*: DE MATA, Frederico Bueno. **El Impacto de las Nuevas Tecnologías Disruptivas en el Derecho Procesal**. [*S. l.*]: Thomson Reuters Aranzadi, 2022.

DURKHEIM; Émile. **Da Divisão do Trabalho Social**. São Paulo: Abril Cultural, 1979.

DURKHEIM; Émile. **O suicídio**: estudo de sociologia. São Paulo: Martins Fontes, 2000.

DWORKIN, Ronald. **Levando os direitos a sério**. São Paulo: Editora WMF Martins Fontes, 2010.

EARLY Pursuit Against Organized Crime Using EnvirOnmental Scanning, the Law and IntelligenCE Systems (ePoolice). **Unicri**. Disponível em: http://www.unicri.eu/topics/organized_crime_corruption/epoolice/. Acesso em: 11 ago. 2022.

ESPANHA. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. **Agência Estatal Boletín Oficial del Estado**: Espanha, seção I – Disposiciones generales, n. 294, p. 119788-119857, 6 de dezembro de 2018. Disponível em: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673. Acesso em: 11 abr. 2022.

ESTADOS UNIDOS DA AMÉRICA. Constitution of the United States – Sixth Amendment. **Constitution Annotated – Analysis and Interpretation of the U.S. Constitution**. Disponível em: https://constitution.congress.gov/constitution/amendment-6/#:~:text=In%20all% 20criminal%20 prosecutions%2C%20the,of%20the%20accusation%3B%20to%20be. Acesso em: 20 fev. 2022

ESTADOS UNIDOS DA AMÉRICA. Departament of Defense. **Instruction Number 3115.12**. Disponível em: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/311512p.pdf?ver= 2019-03-06-093811-687. Acesso em: 22 abr. 2022.

ESTADOS UNIDOS DA AMÉRICA. United States Government Publishing Office (GPO) – GovInfo. **Content Details –** Preparing for the 21st Century: An Appraisal of U.S. Intelligence. Disponível em: https://www.govinfo.gov/app/details/GPO-INTELLIGENCE/. Acesso em: 17 abr. 2022.

EUR-Lex – Acess to European Union Law. **Document 32016R0679**. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE). 04/05/2016**.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 21 jun. 2019.

FENOLL, Jordi Nieva. **Inteligencia Artificial y Proceso Judicial**. Madrid: Marcial Pons, 2018.

FERRAJOLI, Luigi. **Direito e Razão**: teoria do garantismo penal. 3. ed. São Paulo: Revista dos Tribunais, 2002.

FIDALGO, Sónia. A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo. *In*: RODRIGUES. Anabela Miranda (coord.). **A Inteligência Artificial no Direito Penal**. Coimbra: Edições Almedina, 2020.

FIGUEIREDO DIAS, Jorge de; BRANDÃO, Nuno. **Sujeitos Processuais Penais**: o Arguido e o Defensor. Coimbra: [*s. n.*], 2020.

FISCALÍA GENERAL DEL ESTADO. Secretaría Técnica. **7.3 Formacíon Continuada**. p. 74-84. Disponível em: https://www.fiscal.es/memorias/memoria2021/FISCALIA_SITE/capitulo _ I/cap_I_7_3.html. Acesso em: 23 abr. 2022.

FOUCAULT, Michel. **Em defesa da sociedade**. São Paulo: Martins Fontes, 1999.

FOUCAULT, Michel. **A verdade e as formas jurídicas**. 3. ed. Rio de Janeiro: Nau Editora, 2002.

FRANÇA JÚNIOR, Francisco de Assis; LEITÃO SANTOS, Bruno Cavalcanti; NASCIMENTO, Felipe Costa Laurindo. do. (2020). Aspectos críticos da expansão das possibilidades de recursos tecnológicos na investigação criminal: a inteligência artificial no âmbito do sistema de controle e de punição. **Revista Brasileira De Direito Processual Penal**, v. 6, n. 1, p. 211–246, 2020. DOI: https://doi.org/10.22197/rbdpp.v6i1.334.

GALBRAITH, J. Kenneth. **Anatomia do Poder**. 2. ed. São Paulo: Pioneira, 1986.

GARAPON, Antonie; PAPAPOULOS, Ioannis. **Julgar nos Estados Unidos e na França**: cultura jurídica francesa e *Common law* em uma perspectiva comparada. Rio de Janeiro: Lumen Juris Editora, 2008.

GARLAND, David. **La Cultura del Control**: crimen y orden social en la sociedad contemporánea. Barcelona: Gedisa, 2005.

GIACOMOLLI. Nereu José. **A Fase Preliminar do Processo Penal**: crises, misérias e novas metodologias investigatórias. Rio de Janeiro: Lumen Juris Editora, 2011.

GIBSON, Helen. Acquisition and Preparation of data for OSINT Investigations. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016.

GLOECKNER, Ricardo Jacobsen. **Autoritarismo e Processo Penal**: uma genealogia das ideias autoritárias do processo penal brasileiro. Florianópolis: Tirant lo Blanch, 2018.

GOLDSCHMIDT, James. **Princípios generales del processo: problemas juridicos y políticos del proceso penal.** Vol. II. Buenos Aires: E.J.E.A., [20--].

GOVLAB. Disponível em: https://datacollaboratives.org/introduction.html#section7/7d. Acesso em: 8 abr. 2022.

GREENWALD, Glenn. **Sem lugar para se esconder**: Edward Snowden, a NSA e a espionagem do governo americano. TraduçãoFernanda Abreu. Rio de Janeiro: Sextante, 2014.

GUARIENTO, Daniel Bitencourt; MAFFEIS, Ricardo. **Qual o Papel dos advogados enquanto agentes de tratamento de dados: controladores ou operadores?** Disponível em: http://www.yalelawjournal.org/forum/open-source-evidence-on-trial. Acesso em: 7 ago. 2022.

HAN, Byung-Chul. **Psicopolítica**. O neoliberalismo e as novas técnicas de poder. Tradução Maurício Liesen. Belo Horizonte: Âyiné, 2018.

HAN, Byung-Chul. **No enxame**: perspectivas do digital. Trad. Lucas Machado. Petrópolis: Vozes, 2018.

HARARI, Yuval Noah. **21 Lições para o século 21**. São Paulo: Companhia das Letras, 2018.

HIATT, Keith. **Open Source Evidence on Trial**. 125 Yale LJF 323 (2016), Disponível em: http://www.yalelawjournal.org/forum/open-source-evidence-on-trial. Acesso em 23 abr. 2022.

HIGGINS, Eliot. These are the Cluster Munitions Documented by Ukrainian Civilians. **Bell¿ngcat**. Disponível em: https://www.bellingcat.com/news/rest-of-world/2022/03/11/these-are-the-cluster-munitions-documented-by-ukrainian-civilians/. Acesso em: 14 abr. 2022.

HOSPITALS Bombed and Apartments Destroyed: Mapping Incidents of Civilian Harm in Ukraine. **Bell¿ngcat**. Disponível em: https://www.bellingcat.com/news/2022/03/17/hospitals-bombed-and-apartments-destroyed-mapping-incidents-of-civilian-harm-in-ukraine/. Acesso em: 14 abr. 2022.

HUIJBOOM, Noor; VAN DEN BROECK. Tijs. **Open data**: An international comparison of strategies. 2011. Disponível em: https://www.researchgate.net/publication/285735704_Open_data_An_international_comparison_of_strategies. Acesso em: 20 abr. 2022.

HUREL, Louise Marie; FRANCISCO, Pedro Augusto P; TELES, Daisy. **Pegasus, a ponta do iceberg da fragilidade no controle de inteligência**. Disponível em: https://www.fundacaoastrojildo.org.br/pegasus-a-ponta-do-iceberg-da-fragilidade-no-controle-de-inteligencia/. Acesso em: 29 dez. 2021.

HUXLEY, Aldous. **Admirável Mundo Novo**. 21. São Paulo: Editora Globo, 2001.

IBPTECH. **E-Discovery**. Disponível em: https://ediscovery.com.br/. Acesso em: 20 abr. 2022.

INTELIGÊNCIA Cibernética em Fontes Abertas (Curso). **Daryus**. Disponivel em: https://www.daryus.com.br/curso/inteligencia-cibernetica-em-fontes-abertas-osint. Acesso em: 23 abr. 2022

INVASION of Ukraine: Tracking use of Cluster Munitions in Civilian Areas. **Bell¿ngcat**. Disponível em: https://www.bellingcat.com/news/2022/02/27/ukraine-conflict-tracking-use-of-cluster-munitions-in-civilian-areas/. Acesso em: 14 abr. 2022.

JAKOBS, Günther; MELIÁ, Manuel Cancio. **Direito penal do inimigo: noções e críticas**. Tradução André Luís Callegari e Nereu José Giacomolli. Porto Alegre: Livraria do Advogado, 2005.

JANELA da Alma. Direção/Roteiro: JARDIM, João; CARVALHO, Walter. Rio de Janeiro: Copacabana Filmes e Produções, 2001. *Online* (73 min). Disponível em: https://www.youtube.com/watch?v=_I9l7upG0DI. Acesso em: 28 jun. 2022.

KERCHOVE. **A Pele da Cultura**: investigando a nova realidade electrônica. São Paulo: Annablume, 2009.

KRAMER, Rodrigo. Incompreensão do conceito de inteligência na segurança pública. *In*: **Revista Brasileira de Inteligência**. Brasília: Abin, n. 10, dezembro 2015, pg. 73-82. Disponível em: https://rbi.enap.gov.br/index.php/RBI/article/view/128/103, acesso em 26. dez. 2022.

LACAN, Jacques. Introdução do grande outro. *In*: **O Seminário – Livro 2**: o eu na teoria de Freud e na técnica da psicanálise. Rio de Janeiro: Jorge Zahar, 1985. cap. XIX.

LA FUENTE; Elvira Tejada de. Introducción: Ciberseguridad y Ciberdelincuencia: respuestas desde el Estado de Derecho. La Armonización Legislativa Transnacional, en particular: las medidas de investigación criminal en la Convención de Budapest. *In*: ZARAGOZA TEJADA, Javier Ignácio. **Investigación Tecnológica y Derechos Fundamentales**: comentarios a las modificaciones introducidas por la Ley 13/2015. Navarra: Editorial Aranzadi, 2017.

LEE, Kai-Fu. **Inteligência artificial:** como os robôs estão mudando o mundo, a forma como amamos, nos comunicamos e vivemos. Rio de Janeiro: Globo Livros, 2019.

LEITE, Sara Souza. O Emprego das Fontes abertas no Âmbito da Atividade de Inteligência Policial. **Revista Brasileira de Ciências Policiais**, Brasília, v. 5, n. 1, p. 11-45, jan/jun 2014.

LOPES JÚNIOR. Aury. **Direito Processual Penal**. 16. ed. Saraiva: São Paulo, 2019.

MACHADO, Bruno Amaral. O inquérito policial e a divisão do trabalho jurídico-penal no Brasil: discursos e práticas. **Revista Brasileira de Segurança Pública**, São Paulo, v. 9, n. 1, p. 12-33, fev./mar. 2015.

MACHADO, Leonardo Marcondes. **Introdução Crítica à Investigação Preliminar**. Belo Horizonte: Editora d' Plácido, 2018.

MANDARINI, Marcos. **Segurança Corporativa Estratégica: fundamentos**. Barueri: Manole, 2005.

MANZINI, Vincenzo. **Trattato de Procedura Penle e di Ordenamento Giudiziario.** Torini: Fratelli Bocca Editori, 1920. v. I.

MARTÍN, Joaquín Delgado. **Judicial-Tech, el proceso digital y la transformación de la justicia**: obtención, tratamiento y protección de datos en la justicia. Madrid: Wolters Kluwer, 2020.

MARTINS JÚNIOR, Ayrton Figueiredo. **Atividade de Inteligência**: uma proposta de controle judicial. 2015. 152 f. Dissertação (Mestrado) – Curso de Programa de Pós-Graduação em Ciências Criminais, Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2015.

MARTINS, Rafael Moro; SANTI, Alexandre de; GREENWALD, Glenn. **"Não é muito tempo sem Operação**?": chats privados revelam colaboração proibida de Sérgio Moro com Deltan Dallagnol na Lava-Jato. 2019. Disponível em: https://theintercept.com/2019/06/09/ chat-moro-deltan-telegram-lava-jato/. Acesso em: 20 abr. 2022.

MARZELL, Laurence. OSINT as a parto f the Strategic National Security Landscape. *In:* AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016.

MATEUS COELHO. Nuno. **A Nova Ordem Digital. A trama adensa-se e descobrem-se as verdades...** Disponível em: https://cnnportugal.iol.pt/guerra/ucrania/nuno-mateus-coelho-a-nova-ordem-digital-a-trama-adensa-se-e-descobrem-se-as-verdades/20260426/621a26960cf21a10a421b8b3. Acesso em: 19 mar. 2022.

MATHIAS, Suzeley Kalil; ANDRADE, Fabiana de Oliveira. O Serviço de Informações e a cultura do segredo. **Dossiê: Relações Civis Militares e Segurança Nacional**, Varia História, Belo Horizonte, v. 28, n. 547, p.537-554, jul/dez 2012. Disponível em: https://repositorio.unesp.br/bitstream/handle/11449/8818/S0104-87752012000200004.pdf?sequence=1&isAllowed=y. Acesso em: 27 ago. 2022.

MAYER-SCHONBERG, Viktor; RAMGE, Thomas. **Reinventing Capitalism in the Age of Big Data**. New York: Basic Books, 2018.

MELO, Felipe Pereira de Melo. **A utilização dos serviços de inteligência no Inquérito Policial**. Curitiba: Íthala, 2017.

MENDES, Carlos Hélder Carvalho Furtado; MELO, Marcos Eugenio Vieira; MENDES, Tiago Bunning. A lei 13.245/2016 e a efetivação das prerrogativas do advogado na investigação criminal: garantia constitucional ao direito de defesa na fase preliminar. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 159, n. 0, p. 261-296, set. 2019.

MERCADO, Stephen C. **Sailing the Sea of OSINT in the Information Age**. Disponivel em: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-48-no-3/sailing-the-sea-of-osint-in-the-information-age/. Acesso em: 20 abr. 2022.

MINISTERIO PÚBLICO DE LA PROVINCIA DE BUENOS AIRES. **Informe de Gestión 2020**. Disponível em: https://www.mpba.gob.ar/files/content/Informe%20de%20Gestion%202020.pdf. Acesso em: 23 abr. 2022.

MINISTÉRIO PÚBLICO DE PERNAMBUCO. **Curso de Inteligência e Investigação em Fontes Abertas – OSINT**. [2021]. Disponível em: https://www.mppe.mp.br/mppe/institucional/escola-superior/ultimas-noticias-escola-superior/15370-curso-de-inteligencia-e-investigacao-em-fontes-abertas-osint. Acesso em: 23 abr. 2022.

MINISTÉRIO PÚBLICO DE SERGIPE. **Membros e servidores do MPSE participam de workshop presencial sobre investigação digital em fontes abertas**. Aracaju, Sergipe. Disponível em: https://www.mpse.mp.br/index.php/2021/11/16/membros-e-servidores-do-mpse-participam-de-workshop-presencial-sobre-investigacao-digital-em-fontes-abertas/. Acesso em: 23 abr. 2022.

MINISTÉRIO PÚBLICO DO ESTADO DO AMAPÁ. Edital de licitação. Pregão nº 046/2020. Processo nº 20.06.0000.0003919/2020-65/MPAP. [OBJETO: Cessão anual de direito de uso sobre programas de computador para coleta de dados em fontes abertas, de acordo com as especificações e exigências dispostas no Termo de Referência]. **Procuradoria-Geral de Justiça.** Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/noticias/noticias-1-1/membros-e-servidores-participam-de-curso-da-oea-sobre-pesquisa-em-dados-abertos. Acesso em: 23 abr. 2022.

MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS. **Segurança e Inteligência**. Disponível em: https://gestaoestrategica.mpmg.mp.br/areas_tematicas/seguranca_inteligência.html. Acesso em: 15 ago. 2022.

MONTESQUIEU, Charles de Secondat. **O espírito das leis**. São Paulo: Martins Fontes, 1996.

MORAIS, Flaviane de Magalhães Barros Bolzan de; MARQUES, Leonardo Augusto Marinho; SARKIS, Jamilla Monteiro. Dados Pessoais no Processo Penal: Tutela da Personalidade e da Inocência Diante da Tecnologia. **Revista Brasileira de Ciências Criminais**, São Paulo, ano 30, v. 190, p. 117-156, maio/jun. 2022. DOI: https://doi.org/10.54415/rbccrim.v190i190.120.

MOROZOV, Evgeny. Big Tech**. A ascensão de dados e a morte da política**. [*S. l.*]: Ub Edition, 2018.

NAVARRO; Susana Navas. Da assistência à substituição dos advogados – a repercussão da Proposta europeia de Regulamento sobre a Inteligência Artificial no Legal Tech. *In*: ABREU, Joana Covelo de; COELHO, Larissa; CABRAL, Tiago Sérgio. **O Contencioso da União Europeia e a cobrança transfronteiriça de créditos**: compreendendo as soluções digitais à luz do paradigma da Justiça electrónica europeia (e-Justice). Braga: UNIO EU Law Journal, 2021. v. III.

NICOLITT, André. Prova ilícita, hackeamento, incompetência e suspeição: as subversões de Ferrajoli. **Revista Brasileira de Ciências Criminais**, São Paulo, ano 29, v. 184, p. 141-159, outubro de 2021.

NUNES, João Alcântara. **Diagnóstico de Inteligência de Fontes Abertas para fins de persecução penal no contexto da sociedade do controle**. 2021. (Monografia – Trabalho de Conclusão de Curso) – PUCRS, Porto Alegre, 2021.

OBAR, Jonathan A.; OELDORF-HIRSH, Anne. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. **Information, Communication & Society**, p. 1-20, 2018.

O´NEIL; Cathy. **Algoritmos de Destruição em Massa**: como o big data aumenta a desigualdade e ameaça a democracia. Santo André: Editora Rua do Sabão, 2020.

OPEN GOVERNMENT PARTNERSHIP. **Europe Regional Meeting** – october, 11-12, 2022. Disponível em: https://www.opengovpartnership.org/. Acesso em: 11 abr. 2022.

OPEN KNOWLEDGE BRASIL. Disponível em: https://ok.org.br/sobre/. Acesso em: 21 dez. 2021.

OPEN KNOWLEDGE FOUNDATION. Disponível em: https://okfn.org/. Acesso em: 8 abr. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. **Estatuto de Roma de la Corte Penal Internacional**. Disponível em: https://www.ohchr.org/es/instruments-mechanisms/instruments/rome-statute-international-criminal-court. Acesso em: 15 ago. 2022.

ORLANDI, Renzo. Investigações preparatórias nos procedimentos de criminalidade organizada: uma reedição da inquisitio generalis? Tradução Ricardo Jacobsen Gloeckner e

Luiz Eduardo Cani. *In*: TERRA, Luiza Borges (org.). **Lições Contemporâneas do Direito Penal e do Processo Penal**. São Paulo: Tirant lo Blanch, 2021.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

OSINT hub. Disponível em: https://osinthub.org/#about. Acesso em: 26 out. 2021.

PASTOR-GALINDO, Javier; NESPOLI, Pantaleone; GÓMEZ MÁRMOL, Félix; MARTÍNEZ PÉREZ, Gregório. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. **IEEE Access**, v. 8, p. 10282-10304, 9 jan. 2020. DOI: 10.1109/ACCESS.2020.2965257. Disponível em: https://ieeexplore.ieee.org/abstract/document/8954668. Acesso em: 24 fev. 2022.

PAYÁ-SANTOS, Claudio; JUÁREZ, José María Luque. El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. **Revista Científica General José María Córdova**. Bogotá, v. 19, n. 36, p. 1121-1136, outubro-dezembro 2021.

PENIDO, Ana; STÉDILE, Miguel Enrique. **Ninguém regula a América**: guerras híbridas e intervenções estadunidenses na América Latina. São Paulo: Fundação Rosa Luxemburgo; Expressão Popular, 2021.

PÉREZ ESTRADA, Miren Josune. La inteligencia artificial como prueba científica en el proceso penal español. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 7, n. 2, maio-ago. 2021.

PITCH, Tamar. **La sociedad de la prevención.** Buenos Aires: Ad Hoc, 2009.

POSSAMAI, Ana Júlia; SOUZA, Vitoria Gonzatti de. Transparência e Dados Abertos Governamentais: Possibilidades e Desafios a partir da Lei de Acesso à Informação. **Administração Pública e Gestão Social**, v. 12, n. 2, 2020. Disponível em: https://periodicos.ufv.br/apgs/article/view/5872/5460. Acesso em: 27 ago. 2022.

POZZEBON, Fabrício Dreyer de Ávila; CAMARGO, Rodrigo Oliveira de. A relevância do Juiz das Garantias para investigação defensiva na fase preliminar. **Boletim do IBCCRIM**. São Paulo, ano 28, n. 334, p. 21-23, set/2020.

PRADO, Geraldo. **Sistema Acusatório: a conformidade constitucional das Leis Processuais Penais**. 3 ed. Rio de Janeiro: Lumen Juris, 2005

PRADO, Geraldo. Proteção de dados, prova digital e devido processo legal. **VI Seminário Internacional "Proteção de dados pessoais na segurança pública e investigação criminal"**. Câmara dos Deputados do Congresso Nacional Brasileiro: Brasília, jul-2020. Disponível em: https://www.youtube.com/watch?v=J4m5yiQnLbI&feature=youtu.be. Acesso em: 20 abr. 2022.

PROPOSTA de corte de 58% no orçamento do DataSUS compromete direito à saúde, à informação e à proteção de dados, alerta Fórum. **Fórum de Direito de Acesso a Informações Públicas.** Disponível em: https://informacaopublica.org.br/. Acesso em: 21 dez. 2021.

PROVINCIA DE SANTA FE (Argentina). **Poder Judicial – Ministerio Público de la Acusacíon**. Disponível em: https://mpa.santafe.gov.ar/news/view/se_realizar_en_rosario_el_curso_nuevas_tecnolog_ as_digitales_ para_la_investigaci_n_de_delitos. Acesso em: 23 abr. 2022.

RIO DE JANEIRO (Estado). Defensoria Pública do Estado do Rio de Janeiro. **Defensoria do Rio terá novo Núcleo de Investigação Defensiva**. Rio de Janeiro: Defensoria Pública do Estado do Rio de Janeiro, 24 de agosto de 2022. Disponível em: https://www.defensoria.rj.def.br/noticia/detalhes/20445-Defensoria-do-Rio-tera-novo-nucleo-de-Investigacao-defensiva. Acesso em: 20 abr. 2022.

RIO GRANDE DO SUL. Ministério Público do Estado do Rio Grande do Sul. **Provimento nº 20/2010**. Dispõe sobre a reestruturação, a redefinição das atribuições e o funcionamento do Núcleo de Inteligência e a criação, as atribuições e o funcionamento do Laboratório de Tecnologia Contra a Lavagem de Dinheiro do Ministério Público do Estado do Rio Grande do Sul. Porto Alegre: Procuradoria-Geral de Justiça, 21 de maio de 2010. Disponível em: https://www.mprs.mp.br/legislacao/provimentos/5172/. Acesso em: 15 ago. 2022.

RIO GRANDE DO SUL. Ministério Público do Estado do Rio Grande do Sul. **Provimento nº 68/2020 – PGJ – Revogado pelo Provimento nº 17/2022 – PGJ**. Disponível em: https://www.mprs.mp.br/legislacao/provimentos/14204/. Acesso em: 15 ago.2022.

ROBLES, Victor M. (*executive insight – chief*). Open Source Intelligence & Analytics Team, rmy G-2 for Intelligence. **Digital Government Institute**. Disponível em: https://digitalgovernment.com/tags/defense-open-source-council/. Acesso em: 20 fev. 2022.

ROCCO, Arturo. **Sul concetto del diritto subietivo di punire**. Opere Giuridiche. Scrtitti giuridici vari. Roma: Società Editrice Del Foro Italiano, 1933. v. III.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRIGUES. Anabela Miranda. Inteligência artificial e Direito Penal – a justiça preditiva entre a Americanização e a Europeização. *In*: RODRIGUES. Anabela Miranda (coord.). **A Inteligência Artificial no Direito Penal**. Coimbra: Edições Almedina, 2020.

ROSA, Alexandre Morais da. **Guia do Processo Penal Estratégico**: de acordo com a teoria dos jogos e MCDA-A. Florianópolis: Emais, 2021.

ROSA, Alexandre Morais da; SILVA, Viviani Ghizoni; MELO E SILVA, Philipe Benoni. ***Fishing Expedition* e Encontro Fortuito na Busca e Apreensão**. Florianópolis: EMais, 2019.

ROSA, Alexandre Morais; CANI, Luis Eduardo. Gravações com Câmeras Individuais em Policiais Geram Outros Problemas. *In*: CUNHA, Rogério Sanchez. **Atualidades do Direito**: obra em homenagem ao professor Luis Flávio Gomes. Salvador: Editora JusPodivm, 2020.

ROSA, Alexandre Morais da; CAMARGO, Rodrigo Oliveira de. O desafio de qualificar a prática da investigação defensiva. **Revista Consultor Jurídico**, 23 de setembro de 2022.

Disponível em: https://www.conjur.com.br/2022-set-23/limite-penal-desafio-qualificar-pratica-investigacao-defensiva. Acesso em: 23 set. 2022.

RÚSSIA-Ucrânia: O que é uma guerra híbrida? **JN**. 15 fevereiro 2022. Disponível em: https://www.jn.pt/mundo/russia-ucrania-o-que-e-uma-guerra-hibrida-14592565.html. Acesso em: 20 abr. 2022.

SAMPAIO, André Rocha. Polícia para quê (quem), ou o ataque do coiote fracote ao poder disciplinar do soberano. *In*: **Biopolíticas**: estudos sobre Política, Governamentalidade e Violência. Curitiba: IEA academia, 2015.

SAMPAIO, André Rocha. **Profanando o dispositivo Inquérito Policial e seu Ritual de Produção de Verdades. Revista Brasileira de Ciências Criminais**, São Paulo, ano 25, v. 134, p. 351-383, 2017.

SANDLER, Ronald L. **Ethics and Emerging Technologies**. London: Palgrave Macmillan, 2014.

SANS487: Open-Source Intelligence (OSINT) Gattering and Analisys. **SANS**. Disponível em: https://www.sans.org/cyber-security-courses/open-source-intelligence-gathering/. Acesso em: 24 abr. 2022.

SCHAUER, Florian; STöRGER, Jan. The Evolution of Open Source Intelligence (OSINT). **Journal of U.S. Intelligence Studies**, v. 19, n. 3, p. 53-56, 2013. Disponível em: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-48-no-3/sailing-the-sea-of-osint-in-the-information-age/. Acesso em: 20 abr. 2022.

SEISDEDOS, Carlos. Curso de Técnicas y Herramientas Avanzadas en Ciberinvestigación OSINT. **Lisa News**. Disponível em: https://www.lisanews.org/formacion/curso-tecnicas-herramientas-avanzadas-ciberinvestigacion-osint/. Acesso em: 23 abr. 2022.

SILVA, Franklyn Roger Alves da. **Investigação Direta pela Defesa**. 2. ed. Salvador: Editora Juspodivm, 2020.

SILVEIRA, Felipe Lazzari; CAMARGO, Rodrigo Oliveira de. O Legado Tecnicista do Pacote Anticrime. **Revista Brasileira de Ciências Criminais**, São Paulo, n. 168. ano 28. p. 19-36. São Paulo: Ed. RT, junho 2020.

SMITH, Russel Jack. **The Unknow CIA: My Three Decades With the Agency.** Pergamon-Brassey's, 1989.

SOUSA, Elaine Parros Machado de. **Emulação de um Gerenciador de Dados Orientado a Objetos através de uma Interface de Programação de Aplicativos sobre um Gerenciador Relacional**. 2020. Dissertação (Mestrado em Ciências de Computação e Matemática Computacional) – Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo – ICMS-USP São Carlos, 2020. Disponível em: https://www.teses.usp.br/teses/disponiveis/55/55134/tde-01072003-163859/publico/Sousa_ Mestrado.pdf. Acesso em: 27 ago. 2022.

STANIFORTH, Andrew. Police Use of Open Source Intelligence: the longer arm of law. *In*: AKHGAR, Babak. SASKIA BAYERL, P; SAMPSON, Fraser. **Open Source Intelligence Investigation**: from strategy to implementation. Genebra: Springer, 2016.

STRICK, Benjamin. Follow the Russia-Ukraine Monitor Map. **Bell¿ngcat**. Disponível em: https://www.bellingcat.com/news/2022/02/27/follow-the-russia-ukraine-monitor-map/. Acesso em: 14 abr. 2022.

SUSSKIND, Richard E. **Tomorrow's lawyers**: An introduction to your future. USA: Oxford University Press, 2017.

SUTHERLAND, Edwin. White-collar criminality, *in* **American Sociological Review**, v. 5, n. 1, 1940, p. 01-12.

THE people's panopticon: Open-source intelligence comes of age. **The Economist – edição semanal**, [*S. l.*], agosto 2021. Disponível em: https://www.economist.com/weeklyedition/ 2021-08-07. Acesso em: 11 abr. 2022.

THE WMD COMMISSION REPORT. **Final Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction**. Disponível em: https://irp.fas.org/offdocs/wmdcomm.html. Acesso em: 25 abr. 2022.

THOMPSON, Augusto. **Quem são os criminosos? O crime e o criminoso:** Entes políticos. 2. ed. Rio de Janeiro: Lumen Juris, 2007.

THOMSON Reuters World-Check Uncover Risk. Take Action. **Thomson Reuters** – the answer companhy. Disponível em: https://www.sifma.org/wp-content/uploads/2019/01/Refinitiv-WC_brochure.pdf. Acesso em: 13 abr. 2022.

TILT, Rodrigo Trindade de. **Tá com medo?** App da Uber terá função de gravar toda conversa no carro. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/ 11/06/uber-introduz-gravacao-de-audio-para-tornar-corridas-mais-seguras.htm?cmpid= copiaecola. Acesso em: 23 abr. 2020.

TOR Project. Disponível em: www.torproject.org. Acesso em: 13 abr. 2022.

TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy. **SSRN**. 2016. Disponível em: https://ssrn.com/abstract=2757465 ou em http://dx.doi.org/ 10.2139/ssrn.2757465. Acesso em: 27 jun. 2022.

UM dia isto tudo poderá ser seu. **Twitter**. Disponível em: https://dev.twitter.com/cards/ markup. Acesso em: 20 abr. 2022.

UNIÃO EUROPEIA. Consejo de la Unión Europea. REGLAMENTO (CE) nº 428/2009 DEL CONSEJO de 5 de mayo de 2009, por el que se establece un régimen comunitario de control de las exportaciones, la transferencia, el corretaje y el tránsito de productos de doble uso. **Diario Oficial de la Unión Europeia**, p. 134-268, 29.5.2009. Disponível em: https://www.boe.es/doue/2009/134/L00001-00269.pdf. Acesso em: 20 ago. 2022.

UNIÃO EUROPEIA. Council of Europe. **Strengthening the rule of law and anti-corruption mechanisms**. Disponível em: https://pjp-eu.coe.int/en/web/pgg2/anti-corruption/-

/asset_publisher/6W7G8ke6G0qc/content/ open-source-intelligence-osint-training-in-azerbaijan?_101_INSTANCE_6W7G8ke6G0qc_viewMode=view/. Acesso em: 23 abr. 2022.

UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial da União Europeia**: p. L 119/89-L 119/131, 4.5.2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri= CELEX:32016L0680. Acesso em: 11 abr. 2022.

VALENTE, Manuel Monteiro Guedes. **Os Desafios do Processo Penal do Estado Democrático de Direito**: A Sociedade Internético-Personocêntrica. 2014. Disponível em: http://www.ibadpp.com.br/1773/. Acesso em: 17 jun. 2019.

VALENTE, Manuel Monteiro Guedes. O reforço dos Princípios Constitucionais na obtenção da prova no mundo digital. **RDJP**, Brasília, ano 2, n. 3, p. 11-25, jan/jun 2018.

VALIDADE Jurídica. **Verifact**. Disponível em: https://www.verifact.com.br/validade juridica/. Acesso em: 25 jun. 2022

VERONESE, Jorvel Eduardo Albring. Lei de Acesso à Informação e os Reflexos sobre a Produção de Inteligência na Polícia Federal. **Revista Brasileira de Inteligência**, v. 8, p. 49-59, 1.09.2013. Disponível em: https://rbi.enap.gov.br/index.php/RBI/article/view/105. Acesso em: 8 abr. 2022.

VERWALTUNGSGERICHTSHOF Mannheim: Kriminalpolizeiliche personenbezogene Akten nur zu präventiv-polizeilichem Zweck. **Neue Juristische Wochenschrift**, v. 47, 18 de maio de 1987. p. 3022.

VERWALTUNGSGERICHT Frankfur: Ermächtigungsgrundlage zur Aufbewahrung erkennungsdienstlicher Unterlagen. **Neue Juristische Wochenschrift**, v. 36, 18 de fevereiro de 1987.

VIEIRA, Luis Guilherme; ROSA, Alexandre Morais da. Veto a uso das agências de inteligência e nulidade das investigações (parte 1). **Revista Consultor Jurídico**. 7 de dezembro de 2022. Disponível em https://www.conjur.com.br/2022-dez-07/vieirae-rosa-veto-uso-agencias-inteligencia-parte, acesso em 15.12.2022.

VIEIRA, Luis Guilherme; ROSA, Alexandre Morais da. Veto a uso das agências de inteligência e nulidade das investigações (parte 2). **Revista Consultor Jurídico**. 7 de dezembro de 2022. Disponível em https://www.conjur.com.br/2022-dez-08/vieirae-rosa-veto-uso-agencias-inteligencia-parte, acesso em 15.12.2022.

VIEIRA, Luis Guilherme; ROSA, Alexandre Morais da. Veto a uso das agências de inteligência e nulidade das investigações (parte 3). **Revista Consultor Jurídico**. 7 de dezembro de 2022. Disponível em https://www.conjur.com.br/2022-dez-09/vieirae-rosa-veto-uso-agencias-inteligencia-parte, acesso em 15.12.2022.

WEBER, Max. **Ciência e política: duas vocações**. 18. ed. São Paulo: Cultrix, 2011.

WHO we are. **Experian**. Disponível em: https://www.experianplc.com/. Acesso em: 13 abr. 2022.

WILLIANS. Heather J; BLUM, Ilana. **Defining second generation Open Source Intelligence (OSINT) for the Defense Enterprise**. National Defense Research Institute. Santa Mônica: RAND Corporation, 2018.

ZAFFARONI, Raúl Eugenio; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro**: parte geral. 5. ed. São Paulo: Revista dos Tribunais, 2004.

ZUBOFF. Shoshana. **A era do capitalismo da vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.

GLOSSÁRIO

Adequação: pertinência e relevância do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento.

Agentes de tratamento: o controlador e o operador.

Análise de impacto regulatório: documentação para instruir o processo legislativo acerca da autorização para a utilização de tecnologias de vigilância e o tratamento de dados pessoais por autoridades competentes que implique elevado risco aos direitos, às liberdades e às garantias dos titulares dos dados.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Atividade de persecução penal: toda e qualquer atividade exercida para investigação, apuração, persecução e repressão de infrações penais e execução de penas, realizada por autoridades competentes, inclusive aquelas de inteligência policial, institucional e financeira para a finalidade de persecução penal.

Atividade de segurança pública: toda e qualquer atividade exercida para a preservação da ordem pública e para prevenção e detecção de infrações penais, inclusive aquelas de inteligência institucional, policial e financeira, realizada por autoridades competentes para a finalidade de segurança pública.

Autoridade competente: autoridade pública, órgão ou entidade do Poder Público responsável pela prevenção, detecção, investigação ou repressão de atos infracionais e infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, ou qualquer outro órgão, ou entidade que, nos termos da lei, exerça autoridade ou execute políticas públicas para os referidos efeitos, total ou parcialmente.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador: autoridade competente responsável pelas decisões referentes ao tratamento de

dados pessoais.

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou dado biométrico, quando vinculado à pessoa natural.

Dado pessoal sigiloso: dado pessoal protegido por sigilo constitucional ou legal.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e o Conselho Nacional de Justiça (CNJ).

Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Licitude: embasamento do tratamento de dados pessoais em hipótese legal.

Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Proporcionalidade: compatibilidade do tratamento com os objetivos pretendidos, de acordo

com o contexto do tratamento.

Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Registros criminais: informações sobre investigações, indiciamentos, medidas cautelares, processos, condenações ou execução da pena.

Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Segurança da informação: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Tecnologia de monitoramento: equipamento, programa de computador ou sistema informático que possa ser usado ou implementado para tratamento de dados pessoais captados ou analisados, entre outros, em vídeo, imagem ou áudio.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organização internacional.

Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, uso compartilhado, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Uso compartilhado de dados: divulgação por transmissão, comunicação, transferência,

difusão ou qualquer forma de disponibilização, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas 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.

ANEXO I – CÓDIGO DEONTOLÓGICO DE BOAS PRÁTICAS DA INVESTIGAÇÃO DEFENSIVA