DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

DOUTRINA E PRÁTICA EM DEBATE < VOL.3 >

FRANCISCO BRITO CRUZ (ED.) / NATHALIE FRAGOSO (ED.) / AGATHA ROSA / ALCIDES PERON / ANDRÉ NICOLITT / ANTÔNIO MAGALHÃES GOMES FILHO / ANTONIO SANTORO / CLARICE TAVARES / CLEOPAS ISAÍAS SANTOS / DIEGO COLETTI OLIVA / EMANUEL QUEIROZ RANGEL / EVANILDA GODOI / FERNANDA DOMINGOS / FLÁVIA MITRI / GERALDO PRADO / JACQUELINE DE SOUZA ABREU / KATERINA HADJIMATHEOU / MARCOS CÉSAR ALVAREZ / MARGARET HU / NORMA SUELI BONACCORSO / SAMYR BÉLICHE VALE

INTERNETLAB
pesquisa em direito e tecnologia

SÃO PAULO, 2020

InternetLab é uma organização sem fins lucrativos dedicada à produção de pesquisa acadêmica aplicada com impacto em políticas públicas de tecnologia e Internet no Brasil.

Citação sugerida
BRITO CRUZ, Francisco; FRAGOSO, Nathalie (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. III. São Paulo. InternetLab, 2020.

Avenida Ipiranga 344 cj 11B | 01046-010 | São Paulo | SP | Brasil
ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA
www.internetlab.org.br

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Direitos fundamentais e processo penal na era digital / Francisco Brito Cruz, Nathalie Fragoso [editores] -- 1. ed. -- São Paulo: InternetLab, 2020. -- (Doutrina e prática em debate; 3)

Vários autores.
Bibliografia.
ISBN 978-65-88385-06-7

1. Direito processual penal **2.** Direitos fundamentais **3.** Processo penal **4.** Tecnologia e direito **5.** Tecnologias da informação e comunicação **I.** Cruz, Francisco. **II.** Fragoso, Nathalie. **III.** Série.

20-42487 **CDU-343.1:004**

Índices para catálogo sistemático:
1. Direito e tecnologia : Direito processual penal **343.1:004**
Maria Alice Ferreira - Bibliotecária - CRB-8/7964

AUTORES /

< AGATHA ROSA >

Mestre em Ciências pelo Instituto Oswaldo Cruz/Fiocruz (2017). Bacharel em Ciências Biológicas (modalidade genética) pela Universidade Federal do Rio de Janeiro – UFRJ (2014). Graduanda do 9º período em Direito pela Universidade Federal Fluminense – UFF.

< ALCIDES PERON >

Graduado em Relações Internacionais (2006), em Ciências Econômicas (2007) pela Facamp. Mestre (2011) e doutor (2016) em Política Científica e Tecnológica pela Universidade Estadual de Campinas (UNICAMP). Pesquisador visitante do Departamento de Estudos Sociais da Ciência e da Tecnologia da Lancaster University (Inglaterra). Foi professor do curso de Relações Internacionais da Facamp (2007-2014). Fundou e coordenou o Observatório de Fenômenos Transnacionais das Américas (OFTA). Foi também professor na Graduação e no MBA em Relações Internacionais da Universidade Anhembi Morumbi. Atualmente é pesquisador do Grupo de Análise de Políticas e Inovação DPCT-UNICAMP (GAPI), onde desenvolve pesquisas ligadas à ciência, tecnologia e sociedade na América Latina; e pesquisador de Pós Doutorado FAPESP no Departamento de Sociologia da Universidade de São Paulo, debatendo os novos instrumentos de vigilância, policiamento e governo da cidade de São Paulo. É autor do Livro "American Way of War: Guerra Cirúrgica e o emprego de Drones Armados em Conflitos Internacionais".

< ANDRÉ NICOLITT >

Doutor em Direito pela Universidade Católica Portuguesa - Lisboa (2011). Mestre em Direito pela Universidade do Estado do Rio de Janeiro – UERJ (2003). Professor do PPGD – Faculdade Guanambi – BA. Professor Adjunto da Faculdade de Direito da Universidade Federal Fluminense – UFF. Juiz de Direito do TJRJ.

< ANTÔNIO MAGALHÃES GOMES FILHO >

Possui graduação (1970), mestrado (1982), doutorado (1989), Livre Docência (1995) e Titularidade pela Faculdade de Direito da Universidade de São Paulo. Foi Diretor da Faculdade de Direito da USP (2010 a 02/2014).

< ANTONIO SANTORO >

Professor Titular de Direito Processual Penal do IBMEC/RJ. Professor Adjunto de Direito Processual Penal e Prática Penal da Faculdade Nacional de Direito da Universidade Federal do Rio de Janeiro - FND/UFRJ. Professor do Programa de Pós-Graduação em Direito da FND/UFRJ. Professor Adjunto do Programa de Pós-Graduação em Direito (Mestrado) da Universidade Católica de Petrópolis - UCP. Coordenador do Grupo de Pesquisa "O Sistema Penal sob Olhar Crítico" UFRJ/UCP Pós-Doutorando em Democracia e Direitos Humanos pela Universidade de Coimbra - Portugal. Pós-Doutor em Direito Penal e Garantias Constitucionais pela Universidad Nacional de La Matan-

za - Argentina. Doutor e Mestre em Filosofia pela UFRJ. Mestre em Direito Penal Internacional pela Universidad de Granada - Espanha. Especialista em Direito Penal Econômico pela Universidade de Coimbra - Portugal. Especialista em Direito da Economia pela Fundação Getúlio Vargas. Graduado em Direito pela UERJ. Licenciando em História pela UNIRIO. Membro da Associação Internacional de Direito Penal. Membro do Instituto Brasileiro de Ciências Criminais. Membro do Instituto Brasileiro de Direito Processual Penal. Membro da Sociedade Internacional de Criminologia. Membro da Sociedade Americana de Criminologia. Membro do Instituto de Direito Comparado Luso-brasileiro. Membro do Conselho Nacional de Pesquisa e Pós-Graduação em Direito. Advogado criminalista.

< CLARICE TAVARES >

Bacharela em Ciências Sociais pela Universidade de São Paulo (2019) e graduanda em Direito pela Pontifícia Universidade Católica –PUC. Estagiária de pesquisa no InternetLab.

< CLEOPAS ISAÍAS SANTOS >

Doutorando em Direito Constitucional pelo IDP. Mestre em Ciências Criminais pela PUCRS. Prof. Efetivo de Processo Penal da Universidade Estadual do Maranhão – UEMA. Delegado de Polícia.

< DIEGO COLETTI OLIVA >

Professor colaborador de Sociologia do Departamento de Educação (DEED) da Universidade Estadual de Ponta Grossa (UEPG). Mestre e doutor em Sociologia pela Universidade Fe-

deral do Paraná (UFPR). Pesquisador do Centro de Estudos sobre Segurança Pública e Direitos Humanos da UFPR (CESPDH), atuando nas linhas de pesquisa "Controle Social, Vigilância e Direitos Humanos" e "Prisão, Punição e Justiça Criminal".

< EMANUEL QUEIROZ RANGEL >

Coordenador do Núcleo de Defesa Criminal da Defensoria Pública do Estado do Rio de Janeiro.

< EVANILDA GODOI >

Professora Adjunta do Departamento de Direito da Universidade Federal de Viçosa. Doutora e Pós-Doutora em Direito pela UFMG. Mestre em Derechos Fundamentales y Libertades Públicas pela Universidad de Castilla-La Mancha/Espanha (diploma revalidado pela UFRJ). Foi professora convidada na Faculdade de Direito da UFMG, professora de Direito Constitucional e Teoria do Direito na Universidade do Estado de Minas Gerais - UEMG. Foi assessora-chefe da Assessoria Técnico-Legislativa da Secretaria de Estado de Casa Civil do Estado de Minas Gerais; assessora de gabinete da mesma Secretaria; membra do Comitê Executivo do Núcleo Mineiro de Internacionalização do Ensino Superior da Secretaria de Estado de Ciência Tecnologia e Ensino Superior de MG; Foi advogada nas áreas de Direito Constitucional, Administrativo e do Trabalho. Atualmente é Coordenadora do Laboratório de Práticas Jurídicas da UFV, presidenta da Comissão de Estágio do Departamento de Direito da UFV, membra da Comissão de Pesquisa e da Comissão de Extensão do Departamento de Direito da UFV.

< FERNANDA DOMINGOS >

Especialista em direitos difusos e coletivos pela Escola Superior do Ministério Público de São Paulo (ESMPSP) e em direitos humanos e trabalho pela Escola Superior do Ministério Público da União (ESMPU). Graduada em Direito pela Universidade de São Paulo - USP. Fez curso de Curta Duração em Direito Digital Aplicado pela Escola de Direito de São Paulo da Fundação Getúlio Vargas- (GVLaw). Coordenadora do Grupo de Combate aos Crimes Cibernéticos da Procuradoria da República em São Paulo. Coordenadora Adjunta do Grupo de Apoio sobre Criminalidade Cibernética da 2ª Câmara de Coordenação e Revisão da Procuradoria-Geral da República (PGR). Capacitadora no Curso de Iniciação e Vitaliciamento e do Curso de Investigação em Crimes Cibernéticos da Escola Superior do Ministério Público da União (ESMPU). Representante do MPF no Projeto Internet&Jurisdiction. Procuradora da República desde 1998.

< FLÁVIA MITRI >

Formada em Direito pela PUC-Rio e mestra pela New York University School of Law. Trabalhou no Jurídico Internacional da TV Globo, tem passagem pela Organização Mundial de Propriedade Intelectual e passou mais de 10 anos na Intel, até ir para Uber, onde assumiu a Diretoria de Privacidade para América Latina em 2017. Na Uber, Flávia coordena todos os temas relacionados à proteção de dados pessoais na região, que atualmente representa o maior mercado global da empresa.

< GERALDO PRADO >

Professor Associado da Universidade Federal do Rio de Janeiro (UFRJ). Bacharel em Direito pela Universidade do Estado

do Rio de Janeiro (1983 - UERJ), mestre e doutor em Direito pela Universidade Gama Filho (1998 e 2003 - UGF). Realizou estudos de pós-doutoramento em História das Ideias e Cultura Jurídicas na Universidade de Coimbra (2010). Consultor externo da Agência de Acreditação de Ensino Superior de Portugal. Membro do Centro de Investigação em Direito Penal e Ciências Criminais da Universidade de Lisboa (CIDPCC). Integrante do RATIO LEGIS - Centro de Investigação e Desenvolvimento em Ciências Jurídicas, da Universidade Autónoma de Lisboa, com pesquisa na Linha Mercado, Regulação e Fiscalidade: o papel das Instituições Superiores de Controlo Financeiro na promoção de uma boa governança. Professor visitante na Universidade Autónoma de Lisboa. Colaborador permanente da Revista Portuguesa de Ciência Criminal (RPCC). Autor de livros e artigos publicados no Brasil e no exterior, integrou Comissão instituída pelo Ministério da Justiça para Reforma do Livro de Recursos e Ações de Impugnação no âmbito do Código de Processo Penal. Magistrado de carreira, aposentou-se no Tribunal de Justiça do Rio de Janeiro no cargo de Desembargador (2012). É Consultor Jurídico.

< JACQUELINE DE SOUZA ABREU >

Doutoranda em Direito na Faculdade de Direito da Universidade de São Paulo e advogada no Barroso Fontelles, Barcellos, Mendonça & Associados. Mestra em direito pela University of California, Berkeley (EUA), com foco em direito e tecnologia, e pela Ludwig-Maximilians-Universität München (Alemanha), com foco em direitos fundamentais. Graduada em direito pela Universidade de São Paulo. Foi pesquisadora-júnior na FGV DIREITO SP e assistente de pesquisa visitante do Berkman Klein Center for Internet and Society da Harvard University. Participou do Summer Doctoral Programme do Oxford Internet Institu-

te e coordenou a área "Privacidade e Vigilância" no InternetLab, centro independente de pesquisa em direito e tecnologia.

< KATERINA HADJIMATHEOU >

Pesquisadora Sênior do Departamento de Sociologia da Universidade de Essex, no Reino Unido. Ela trabalhou em vários projetos de investigação sobre segurança financiados pela União Europeia, centrados na ética das tecnologias de segurança e vigilância, incluindo DETECTER e SURVEILLE. Atualmente, Katerina está envolvida no projeto "Direitos Humanos, Big Data e Tecnologia", financiado pelo Economic and Social Research Council (ESRC), focando-se especificamente em temas ligados policiamento e vigilância. A sua publicação mais recente (2018, European Journal of Criminology) é "UK anti-slavery policy at the border: Humanitarian opportunism and the challenge of victim consent to assistance". Presidente do Comitê de Ética da Polícia de Gloucestershire. Faz parte do Grupo de Referência Independente da Agência Nacional de Crimes do Reino Unido e é membro do Independent Digital Ethics Policing Panel.

< MARCOS CÉSAR ALVAREZ >

Professor Livre Docente no Departamento de Sociologia da USP. Graduado em Ciências Sociais (1984), Mestrado (1989) e Doutorado (1996) em Sociologia, todos obtidos na Universidade de São Paulo, e pós doutorado na École des Hautes Études en Sciences Sociales, Paris (2008-2009). Orientador no Departamento de Sociologia e no programa de pós-graduação em Sociologia da FFLCH-USP (mestrado doutorado e pós-doutorado), tendo lecionado na Universidade Estadual de Londrina/UEL, Paraná (1987-1991) e na Universidade Estadual Paulista /UNESP, Campus de Marília (1991-2004). Foi assistente de pesquisa no

CEBRAP (1985-1986), consultor de pesquisa no Instituto Brasileiro de Ciências Criminais (2009-2010) e pesquisador sênior no Núcleo de Estudos da Violência da USP desde 2004 até o presente. Pesquisador principal do Programa de Inovação Tecnológica/CEPID, Centro de Pesquisa, Inovação e Difusão do NEV-USP (em execução desde 2013) e foi pesquisador principal do projeto FAPESP "A gestão do conflito na produção da cidade contemporânea: o caso paulista" (2014-2018), coordenado pela professora Vera Telles (USP). Faz parte do corpo editorial da revista Plural (USP), da Revista Brasileira de Sociologia (SBS) e atua como parecerista da Tempo Social (USP), Dilemas (UFRJ), Delito y Sociedad (UNL), DADOS (IESP), Revista Sociologia e Política (UFPR), Revista de Estudios Brasileños (USAL), EchoGeó (Paris 1), entre outros periódicos. Diretor de Publicações da ANPOCS e editor da Revista Brasileira de Ciências Sociais entre 2013 e 2015. Foi Vice-chefe do Departamento de Sociologia (2014-2016) e Coordenador do Programa de Pós-Graduação em Sociologia da USP (2015-2018). Membro da diretoria da Associação Nacional de Direitos Humanos, Ensino e Pesquisa (ANDHEP) e coordenador do Núcleo de Estudos da Violência a partir de 2020.

< MARGARET HU >

Professora Associada da Washington and Lee University School of Law (EUA). Atuou como conselheira sênior de política para a Iniciativa da Casa Branca para Americanos Asiáticos e Ilhas do Pacífico, e consultora de política especial no Gabinete do Conselho Especial para Práticas Trabalhistas Desleais Relacionadas a Imigração (OSC), Divisão de Direitos Civis, Departamento de Justiça dos Estados Unidos, em Washington, DC. Recebeu seu B.A. em Línguas e Culturas da Ásia Oriental na Universidade do Kansas e seu J.D. na Duke Law School.

< NATHALIE FRAGOSO >

Doutora em Direito pela Faculdade de Direito Universidade de São Paulo e graduada em Direito pela mesma instituição. Possui o Zertifikat in den Grundzügen des deutschen Rechts e o LLM (Master of Laws) pela Ludwig-Maximilians-Universität München. Coordenadora da Clínica de Direitos Humanos Luiz Gama entre os anos de 2013-2014. Atualmente, é coordenadora da área de Privacidade e Vigilância do InternetLab.

< NORMA SUELI BONACCORSO >

Graduada em Ciências Biológicas e em Direito, mestra e doutora em Direito Penal pela Universidade de São Paulo. Exerceu o cargo de Perita Criminal de 1987 a 2015. Trabalhou 10 anos no Laboratório de Toxicologia do Instituto Médico Legal e por 13 anos no Laboratório de DNA do Instituto de Criminalística. De abril de 2013 a janeiro de 2015, exerceu a função de Superintendente da Polícia Técnico-Científica de São Paulo. Professora Colaboradora de Medicina Legal de Criminalística na da Faculdade de Direito da USP e Professora Titular das mesmas disciplinas na FAAP e em cursos da pós-graduação em Ciências Forenses das Faculdades Oswaldo Cruz.

< SAMYR BÉLICHE VALE >

Doutorado em Ciência da Computação (Informatique) pela Université d'Angers - França. Mestrado em Engenharia de Eletricidade com área de concentração em Ciência da Computação pela Universidade Federal do Maranhão. Graduação em Ciência da Computação pela Universidade Federal do Maranhão e em Direito pelo Centro Universitário Dom Bosco – UNDB. Professor do PPG em Ciências da Computação da UFMA.

SUMÁRIO /

APRESENTAÇÃO DOS EDITORES /

O avanço da tecnologia digital hoje disponível, a vultosa quantidade de informação coletada, compartilhada e processada atualmente impactam as dinâmicas criminais e a forma como as agências penais operam em resposta. São mais de 4 bilhões de usuários de internet no mundo, o acesso e a capacidade de processamento de computadores e smartphones cresce, os órgãos de investigação incorporam novas técnicas - às vezes, controversas em sua precisão e segurança - amparadas em tecnologia e ciência de dados, nas suas atividades de prevenção e repressão. Nesse contexto, emergem e se renovam questões sobre a proteção da intimidade e do sigilo, novos meios de obtenção de prova e sua admissibilidade e valor para fins de instrução processual.

Para avançar o debate a respeito das garantias do devido processo penal e da tutela de direitos fundamentais diante das novas tecnologias, o InternetLab, centro independente de pesquisa em direito e tecnologia, com apoio institucional da Faculdade de Direito da Universidade de São Paulo (FDUSP), organiza, anualmente, o congresso "Direitos Fundamentais e Processo Penal na Era Digital".

A terceira edição do congresso, que aconteceu nos dias 21 e 23 de agosto de 2019, tratou especificamente da utilização de tecnologias de vigilância em massa e da crescente coleta e emprego de dados biométricos e genéticos na justiça criminal e em políticas de segurança pública e do consequente desafio de atualização de garantias penais constitucionais. As palestras e intervenções dos participantes foram registradas e estão disponíveis para acesso online.

Esta obra reúne artigos e contribuições que, além de aprofundarem parte das discussões iniciadas durante o congresso, pretendem arejar a reflexão e prática em processo penal, e evitar a frequente dessincronia entre a tecnologias e as leis, entre academia e justiça criminal, entre problemas da era digital e suas respostas.

Boa leitura,
FRANCISCO BRITO CRUZ
NATHALIE FRAGOSO
São Paulo, agosto de 2020

01.

VIGILÂNCIA, CONFIANÇA E A PRESUNÇÃO DE INOCÊNCIA[1]

Título original:
Surveillance, Trust and the Presumption of Innocence[2]

Katerina Hadjimatheou

It is of paramount importance that law enforcement agencies should take full advantage of the available techniques of modern technology and forensic science. Such real evidence has the inestimable value of cogency and objectivity. It is in large measure not affected by the subjective defects of other testimony. It enables the guilty to be detected and the innocent to be rapidly eliminated from enquiries.
Lord Steyn [2004] UKHL 39

As palavras de Lord Steyn chamam nossa atenção para algo raramente reconhecido: o uso de provas reunidas por tecnologias de vigilância pode nos proteger contra suspeitas e condenações injustas. Se e na medida em que for correta sua afirmação, ela deveria nos levar a rever nossas avaliações sobre os custos e benefícios da vigilância. Em particular, deveria nos levar a reconhecer que, além de aumentar a segurança, a vigilância pode ser usada de forma a proteger importantes liberdades civis - neste caso, a liberdade contra a criminalização indevida.

A garantia contra a criminalização indevida tem sido tradicionalmente protegida através do princípio legal da presunção de inocência. Este artigo se baseia em trabalhos empíricos recentes sobre as causas e a prevenção de condenações equivocadas, para mostrar como também podem ser prevenidas pelo uso de provas colhidas por tecnologias de vigilância. As implicações desta declaração para avaliações generalistas do impacto da vigilância sobre a presunção de inocência são consideradas à luz das recentes tentativas dos estudiosos da vigilância de demonstrar os efeitos corrosivos do seu uso sobre esse princípio.

O artigo prossegue da seguinte forma. Em primeiro lugar, os debates atuais em torno do entendimento correto acerca da presunção de inocência são delineados. Em seguida, são apresentadas razões para defender que se considere a presunção de inocência como um princípio que protege os cidadãos contra a criminalização indevida pelo Estado. Esta consideração é defendida em relação a alternativas, em particular aquelas que fundamentam a presunção em um direito dos cidadãos a serem confiados. A alegação de que a vigilância mina a presunção de inocência é então avaliada. As críticas à vigilância que se baseiam em afirmações de que ela necessariamente trata as pessoas como presumivelmente não confiáveis ou criminosas são rejeitadas. Argumenta-se que a vigilância pode ser feita de formas que não minem a presunção de inocência, e que a vigilância em massa é geralmente praticada de formas que minam menos a presunção de inocência do que a vigilância dirigida.

O trabalho baseia-se, então, nos resultados de trabalhos empíricos recentes sobre as causas de acusações e condenações indevidas para ilustrar que os dados de vigilância podem e devem ser utilizados para proteger a presunção de inocência, fornecendo provas para absolver os suspeitos ou acusados de crimes. A seção final do trabalho considera as implicações do que tem sido argumentado para o nosso entendimento sobre o impacto das práticas de vigilância sobre a presunção de inocência. Argumenta-se que, apesar dos impactos aparentemente contraditórios da vigilância sobre a presunção de inocência, as medidas destinadas a reduzir o risco daquela não precisam inibir esta. Pelo contrário, uma redução no uso da vigilância que prejudique a presunção de inocência é compatível com um aumento no uso da vigilância que a proteja.

A PRESUNÇÃO DE INOCÊNCIA EM DEBATES SOBRE VIGILÂNCIA

A privacidade tem sido tradicionalmente o principal interesse ou valor considerado ameaçado pelas práticas de vigilância (Warren e Brandeis, 1890; Westin, 1967; Jarvis-Thomson, 1975). Nos últimos anos, a igualdade e as normas antidiscriminação também se tornaram um foco de preocupação acadêmica (Lyon, 2002; Bou-Habib, 2008; Ryberg, 2011). Hoje, uma nova vertente de crítica foca-se na presunção de inocência, apresentando-a como a última de nossas liberdades a se tornar uma vítima das práticas de vigilância (Minaj e Bonnici 2014; Galetta e de Hert 2012; Pavone e Pereira 2008).

Práticas específicas de vigilância que têm sido criticadas como minando ou restringindo a presunção de inocência incluem o monitoramento em massa das comunicações eletrônicas representadas pelo programa PRISM da Agência Nacional de Segurança dos EUA (EU Parliament, 2013)[3]; a retenção de dados de telecomunicações conforme prescrito pela Diretiva de Retenção de Dados da UE[4] (Minaj e Bonnici 2014); o uso de câmeras de reconhecimento de placas ANPR e câmeras de vigilância em vias públicas (Haggerty e Ericson, 1997, p. 42; Monahan, 2010, p. 99; Galetta, 2013, p. 280); e o uso, por empresas de telecomunicações, de técnicas de inspeção profunda de pacotes (*deep packet inspection* ou DPI) para detectar compartilhamento ilegal de arquivos (Fuchs, 2012, p. 50; Privacy International, 2009).

Os estudiosos identificam uma série de formas pelas quais a presunção de inocência é aparentemente minada por essas práticas. Alguns apontam para os efeitos estigmatizantes sobre aqueles vigiados como criminosos ou potencialmente criminosos (Campbell, 2010). Outros apontam a implicação da desconfiança depositada sobre indivíduos inocentes (Nance, 1994; Duff, 2013). Outros ainda identificam e se opõem à cria-

ção de um 'ethos' ou 'cultura' da suspeita (Kimmelman, 2000; Minaj e Bonnici, 2014) ou a uma 'erosão' da confiança que forma a base das relações sociais em uma sociedade liberal (Lyon, 1994). Todas essas críticas compartilham uma interpretação expansiva da presunção de inocência. Todos argumentam que a presunção de inocência não deve ser entendida meramente em termos jurídicos restritos, como um aspecto particular do direito dos réus a um julgamento justo. Ao contrário, argumentam que também deve ser entendida como um direito moral geral, parte do qual é protegido através de um direito legal.

Essas reconceitualizações da presunção de inocência têm sido criticadas por teóricos do direito que se preocupam com as consequências não intencionais de interpretações expansivas. Uma grande preocupação é que o poder normativo da presunção de inocência, como princípio jurídico, será minado pelas tentativas de estender sua aplicação para além daqueles que correm o risco da grave injustiça da condenação errônea, abarcando os que correm o risco, por exemplo, da intrusão bastante banal de estarem sujeitos à vigilância por câmeras de segurança. Não é difícil ver como isso pode ocorrer. Atualmente, a presunção de inocência goza do status legal de direito fundamental e, portanto, é tratada como resistente às pressões de aumentos moderados de utilidade (por exemplo, no número de culpados condenados) em que as restrições propostas a ela podem resultar. Mas aumentos moderados em segurança podem ser pensados de forma bastante razoável para justificar medidas que correm o risco de resultar em medidas de suspeita como o aumento da vigilância por câmeras de segurança ou a inclusão em bases de dados policiais. Associar a proteção de pessoas inocentes contra condenações injustas com a proteção de pessoas inocentes contra suspeição ou desconfianças corre o risco de corroer os compromissos com a primeira à luz da rela-

tiva trivialidade do último. Por outro lado, a afirmação de que a vigilância mina a presunção de inocência pode muito bem incentivar, entre aqueles não versados nos detalhes do debate, a visão equivocada de que ela realmente resulta em maior número de erros de justiça, levando as pessoas a se oporem a ela com uma força mais forte do que a merecida.

Os teóricos que são movidos por estas preocupações tendem a favorecer a limitação do escopo da presunção de inocência às regras processuais, nomeadamente a regra de que o ônus da prova deve ser suportado pelo Estado. Esta presunção limitada de inocência não é diluída, mantendo assim a sua força moral e jurídica e continuando a beneficiar do estatuto de direito fundamental, que só pode ser restringido em circunstâncias excepcionais. De acordo com aqueles que são a favor desta abordagem, as pessoas preocupadas com a estigmatização ou a desconfiança devem limitar-se a falar de estigmatização e desconfiança, e devem ser combatidas quaisquer tentativas suas de se aproveitarem da força retórica considerável da presunção de inocência devem ser resistidas.

Alguns dos que favorecem leituras expansivas da presunção de inocência tentaram responder a estas preocupações alegando que não existe uma presunção única, mas sim uma série de presunções, cada uma das quais protege as pessoas de diferentes aspectos da coerção injusta do Estado em nome da justiça penal (Duff, 2013). Esta medida reformula o princípio da presunção de inocência como um princípio geral, que inclui a proteção contra as condenações injustas ao lado da proteção contra as desconfianças ou suspeitas injustas. O êxito desta iniciativa é questionável, embora o seu espírito conciliador e inclusivo seja bem-vindo. Isto se deve, em parte, ao fato de mais se desviar do que abordar o problema do estatuto normativo da presunção: enquanto antes éramos confrontados com a dificuldade de chegar a acordo sobre a importância da

"presunção", agora somos confrontados com a dificuldade de decidir o quão importante é cada presunção e como se relacionam entre si.

Infelizmente, a proliferação de presunções de inocência não foi acompanhada pelo tipo de análise normativa que estabelece a importância dos interesses ou valores protegidos por cada presunção e a gravidade dos danos morais aparentes ou dos erros que lhes são causados pelas técnicas de vigilância. Consequentemente, a abordagem das presunções múltiplas convida à paralisia normativa se, após a devida análise, verificar-se que as práticas de vigilância minam uma presunção de inocência e, ao mesmo tempo, protegem ou promovem outra.

As dificuldades enfrentadas pela abordagem das presunções múltiplas poderiam ser parcialmente evitadas se eliminássemos completamente a linguagem das presunções de inocência e nos concentrássemos antes na descrição dos encargos específicos que queremos salientar. Pode argumentar-se que estes encargos - de estigmatização, de ingerência na privacidade - são o que torna a vigilância problemática, e não o fato de serem chamados por um determinado nome. No entanto, esta interpretação também não é inteiramente satisfatória, pois nega a uniformidade entre esta classe específica de encargos impostos pela vigilância, uma uniformidade que muitos identificam intuitivamente com infracções ou diminuição da presunção de inocência e que ressoa inegavelmente tanto dentro como fora dos círculos acadêmicos. Em que poderia consistir esta uniformização?

Um recente entendimento de filosofia do direito conceitualiza a presunção de inocência como a proteção contra a criminalização indevida (Tadros, 2007; Tomlin, 2013). Esta abordagem restringe o âmbito da presunção à justiça penal, em vez de (como veremos com as interpretações baseadas na confiança) vê-la como um princípio básico de morali-

dade interpessoal que também se aplica às relações entre o Estado e o cidadão. No entanto, alarga também o âmbito da presunção de inocência para além dos limites do julgamento, de modo a aplicar-se a todas as práticas estatais criminalizadoras, incluindo potencialmente a vigilância. Esta abordagem tem uma série de vantagens que a tornam uma opção atrativa. Por exemplo, parece captar e expressar bem as principais preocupações das pessoas sobre o impacto das práticas de vigilância contemporâneas na presunção de inocência: as pessoas invocam a presunção de inocência não só porque a vigilância implica frequentemente prestar atenção aos indivíduos de uma forma que interfere, digamos, na privacidade, mas que o faz em nome de uma criminalidade implícita de algum tipo. É esta percepção de criminalização daqueles que são atingidos que une as objeções contemporâneas às práticas de vigilância e as torna conceitualmente contínuas com as objeções contra condenações injustas. Além disso, aceitar a interpretação da criminalização indevida permite-nos ir além dos debates sobre se aqueles que se opõem à vigilância podem ou não legitimamente invocar a presunção de inocência em apoio da sua causa: podem, se puderem demonstrar que as práticas de vigilância criminalizam as pessoas de forma indevida.

Este artigo defenderá a interpretação da presunção de inocência baseada na criminalização indevida. Mas antes de poder fazê-lo, deve primeiro defender essa interpretação contra a sua mais proeminente alternativa atual, ou seja, a interpretação baseada na confiança. No que se segue, aponto o que considero ser um problema sério com essa interpretação e sugiro que a rejeitemos. Muitas das críticas atuais às práticas de vigilância que apelam para a presunção de inocência falam de seu inevitável impacto negativo sobre a confiança. Minha rejeição à interpretação baseada na confiança também envolverá a

rejeição de algumas dessas críticas. Aplico então o raciocínio usado para rejeitar essas críticas de práticas de vigilância à questão de saber se as práticas de vigilância minam a presunção de inocência ao criminalizar indevidamente as pessoas.

A PRESUNÇÃO DA INOCÊNCIA COMO UM DIREITO A SER CONFIADO

Tal como acima referido, alguns teóricos do direito, nomeadamente Nance (1994) e Duff (2013), tentaram reformular a presunção de inocência como um direito moral de ser tratado como digno de confiança (para os proponentes mais recentes deste ponto de vista, ver Stewart, 2014; DeAngelis, 2014). Especificamente, o direito de ser tratado como digno de confiança foi justificado como corolário do "princípio da civilidade" ou do "princípio da confiança cívica", ou de ambos. Nance argumenta que o princípio da civilidade impõe a todas as pessoas o dever de se tratarem umas às outras como se tivessem agido e agissem de acordo com as suas obrigações sociais importantes, incluindo o respeito ao direito penal (Nance, 1994), mas não se limitando a este. Não tratar as pessoas de forma coerente com o princípio da presunção de civilidade equivale a não lhes conceder "a dignidade associada ao estatuto de membro da comunidade que é regido pelas normas cuja violação está em questão" (Nance, 1994, p. 653).

Com base no trabalho de Nance, Antony Duff propõe fundamentar a presunção de inocência no princípio da confiança cívica. Este princípio é muito semelhante ao princípio da civilidade, mas inclui o dever de tratar as pessoas como se estas fossem continuar a agir de acordo com as suas obrigações importantes. Isto faz com que o princípio da confiança cívica se oriente para o futuro, ao contrário do princípio da civilidade, que é puramente retrospectivo. De acordo com Duff, não conceder às pessoas uma confiança cívica adequada é não as

tratar "como agentes que podem reconhecer e orientar as suas ações por razões adequadas para agir" (Duff, p. 10). Em outras palavras, o fracasso em presumir que as pessoas são inocentes de comportamentos ou intenções que violem as normas é incompatível com o respeito por elas como agentes morais: como pessoas que podem reconhecer e ser guiadas por razões morais para não fazer certas coisas, como envolver-se em ações que causem danos a outros, das quais os crimes são paradigmáticos.

A afirmação de que a falta de confiança nas pessoas equivale a desconfiar ativamente delas (DeAngelis, 2014) é uma característica persistente das interpretações do direito a ser confiado. As críticas à vigilância envolvem frequentemente esta alegação, afirmando que o fato de a vigilância interferir na ausência de suspeita individualizada significa que ela subverte a presunção de inocência ao presumir que todos são culpados (entendido como não digno de confiança) até que as provas que revela provem o contrário. Assim, por exemplo, Norris argumentou, no seu testemunho na consulta da Câmara dos Lordes do Reino Unido sobre a vigilância, que a vigilância em massa "promove a opinião... de que ninguém é digno de confiança". Se estamos sempre coletando dados sobre as pessoas com base no fato de poderem fazer algo de errado, isso está promovendo a opinião de que, como cidadãos, não podemos ser confiados (Norris in House of Lords, 2009, p. 27[107]; ver também Monahan, 2010, p. 99; Norris e Armstrong, 1999, p.24). A vigilância em massa ou indiscriminada, como a utilização de câmeras de segurança em vias públicas, é também considerada uma sombra de desconfiança ou suspeita sobre as populações (Minaj e Bonnici, 2014, p. 421).

Mas a afirmação de que a falta de confiança ativa equivale a uma desconfiança ativa é uma falácia. Assume, erroneamente, que a confiança e a desconfiança são as duas únicas atitudes relacionadas à confiança que se é possível adotar.

Na verdade, ambas existem em extremos opostos de um espectro de atitudes. Como salienta Ullmann-Margalit no seu artigo de 2002 sobre esta questão, nas nossas relações com outras pessoas, exigimos normalmente motivos para confiar ou desconfiar das pessoas, geralmente sob a forma de provas retiradas do nosso conhecimento do seu caráter ou da sua conduta passada. Quando essas provas não existem ou são insuficientes, é razoável e justo adotar uma atitude que se situe em algum lugar entre a confiança e a desconfiança, e agir de forma que reflita essa atitude. Com efeito, não seria razoável exigir que os indivíduos se tratassem uns aos outros como se fossem de confiança, na ausência de provas que demonstrem a sua fiabilidade. Seria igualmente pouco razoável exigir que a polícia tratasse todos os indivíduos para os quais não existem provas individuais incriminatórias de delitos como se existissem provas da sua inocência no que diz respeito ao direito penal. Mas afirmar um direito de confiança, como fazem Duff e Nance, implica que é precisamente isso que a moralidade exige.

A visão nuançada de confiança elaborada por Ullmann-Margalit é apoiada pelo trabalho do psicólogo social Toshio Yamagishi, cujo estudo seminal distingue a desconfiança — ou seja, a suposição de que alguém não pode ser confiado — da vigilância — ou seja, a busca prudente de garantias na ausência de uma base prévia a partir da qual se possa confiar (Yamagishi, 2011, p. 28). O trabalho de Yamagishi reflete melhor as nossas práticas psicológicas e sociais do que as afirmações de uma dicotomia grosseira entre confiança e desconfiança. Pode ajudar-nos a distinguir entre as práticas de vigilância que comunicam desconfiança e as que devem ser interpretadas como vigilância. Vejamos de que forma.

A interpretação de Yamagishi sobre confiança, desconfiança e vigilância pode nos ajudar a fornecer uma justificati-

va para as práticas de vigilância que envolvem exigir que as pessoas comprovem suas credenciais antes de acessarem certos bens ou áreas. Um exemplo são as práticas de segurança aeroportuária. Seria errado afirmar que as pessoas são obrigadas a passar por verificações de segurança nos aeroportos porque há uma suposição de que todos que viajam de avião são suspeitos ou não confiáveis. Ao contrário, tais medidas fornecem as garantias necessárias para que as pessoas concordem em se envolver em uma atividade coletiva potencialmente altamente perigosa. Observações semelhantes podem ser feitas sobre a vigilância que serve para proteger pessoas vulneráveis de danos. Como tenho argumentado em outros lugares, os indivíduos que desejam trabalhar com crianças não são obrigados a se submeter à verificação do registro criminal com o fundamento de que seu desejo de trabalhar com crianças os torna suspeitos (Hadjimatheou, 2014). Ao contrário, tais verificações demonstram um reconhecimento de que as crianças são vulneráveis e merecem proteção especial.

Como isto sugere, uma crença na falta de confiança não é necessariamente a única ou mesmo a explicação mais racional para este tipo de prática de vigilância em massa. A utilização de cartões de identificação, câmeras de vigilância, leitura de placas de veículos, práticas de retenção de dados etc. são compatíveis com a convicção de que a grande maioria das pessoas são cidadãos bem intencionados, cumpridores da lei, que não interessam às autoridades de justiça penal. Embora seja verdade que eles se baseiam necessariamente no pressuposto de que alguém irá cometer algum crime, isso reflete apenas os fatos. Assumir o contrário seria não só irracional, mas também um desrespeito pelos Estados do dever de proteger os indivíduos contra o crime. Por esta razão, parece errado afirmar que tais práticas, meramente pelo fato de envolve-

/ É COLHIDA UMA GRANDE QUANTIDADE DE INFORMAÇÃO SOBRE NÓS, MAS POR UMA VARIEDADE DE AGENTES E POR DIVERSAS RAZÕES /

/ DAR AOS RÉUS ACESSO AUTOMÁTICO A TODOS OS DADOS RETIDOS CONTRIBUIRIA PARA QUE SE PROTEJAM CONTRA CONDENAÇÕES INJUSTAS /

rem algum monitoramento da população, tratam todos como presumivelmente não confiáveis.

Para estender um pouco a argumentação, imaginemos o que seria uma política que presumisse que todas as pessoas são culpadas de transgressões criminosas. Certamente se assemelharia muito a políticas postas em prática para controlar reclusos numa prisão. Na verdade, uma presunção de culpa apoiaria uma política de observar literalmente as pessoas a toda a hora e, portanto, pareceria semelhante ao infame panóptico de Bentham ou ao Grande Irmão de Orwell, ambos concebidos para controlar aqueles que já provaram ser culpados e, por conseguinte, presumivelmente não confiáveis. A maioria das utilizações atuais das democracias liberais da vigilância por parte dos agentes de segurança do Estado está longe de ser tão abrangente, intrusiva ou comunicativa de desconfiança como algo do tipo. É, de fato, recolhida uma grande quantidade de informação sobre nós, mas por uma variedade de agentes distintos e por diversas razões; não existe uma consciência única, individual ou coletiva, que esteja consciente de todos os nossos movimentos. É certo que as forças policiais manifestam frequentemente o desejo de aumentar o acesso às fontes de informação. Mas o debate em curso sobre esta questão nos parlamentos liberais e as recentes disputas com as empresas tecnológicas ilustram que não é de modo algum inevitável que venham a obtê-las (The Guardian, 14 de Março de 2016). O fato de a maioria dos crimes não só ficarem por resolver e impunes, como nunca serem levados ao conhecimento das agências de justiça criminal, ilustra ainda mais o quão longe da polícia do pensamento de Orwell, que tudo enxerga, ainda estamos (UK Office for National Statistics, 2013, p. 1/2).

Façamos um balanço por um momento do que foi discutido e do que aprendemos sobre a presunção de inocência e o efeito da vigilância sobre esta. Na seção anterior, propunha-se que a

interpretação da presunção de inocência baseada na criminalização indevida apresentasse uma base sólida para a compreensão contemporânea do princípio. Nesta seção, foram apresentados argumentos que sugerem que a principal interpretação que a ela se opõe, a que baseia a presunção de inocência na confiança, é conceitualmente inconsistente. A partir de agora, o documento partirá do pressuposto de que estes argumentos estão corretos e de que a interpretação da presunção de inocência com base na criminalização indevida deve ser adotada.

Esta seção também argumentou que, ao contrário do que afirmam os críticos da vigilância que apelam a essa interpretação, as práticas de vigilância em massa não tratam necessariamente as pessoas como presumivelmente não dignas de confiança. Na seção seguinte, estendo estes últimos argumentos à questão de saber se as práticas de vigilância minam a presunção de inocência ao criminalizarem injustamente as pessoas.

VIGILÂNCIA E CRIMINALIZAÇÃO INDEVIDA

A criminalização indevida foi definida acima como o ato de tratar alguém como se tivesse uma propensão particular para a criminalidade ou como se já estivesse envolvido em atividade criminosa, sem motivos adequados para tal. A criminalização indevida encontra sua pior versão quando resulta na condenação de inocentes, algo que o direito de ser presumido inocente se destina a prevenir (Stumer, 2010), e sua versão mais amena quando resulta em pequenas interferências com a privacidade. Se algo se qualifica ou não como criminalização indevida dependerá tanto de como realmente tratamos os criminosos, quanto do que conta como base adequada para tratar alguém como criminoso. Em relação a esta última questão, podemos dizer que os fundamentos adequados consistem em evidências suficientemente confiáveis e que indicam a criminalidade de forma suficientemente forte para justificar

a medida preventiva ou punitiva específica proposta. Assim, nas jurisdições anglo-americanas, a "suspeita razoável" pode ser o limiar epistêmico para a prisão, enquanto que "sem dúvida razoável" é o da condenação. A questão de saber se as práticas de vigilância criminalizam erroneamente as pessoas será respondida em referência a essas noções. Finalmente, para responder plenamente à questão, precisamos nos perguntar se as práticas de vigilância resultam necessariamente em criminalização indevida ou se elas podem, em princípio, ser usadas sem que nisso se resulte.

Muitas das afirmações que acabamos de fazer em relação às implicações para a confiabilidade impostas pelas práticas de vigilância em massa ou indiscriminada aplicam-se às suas implicações para a criminalização indevida. É difícil, por razões conceituais, demonstrar que as práticas de vigilância em massa criminalizam as pessoas de forma ilícita. A criminalidade é desviante ou transgressiva por definição e (pelo menos nas democracias liberais) a crença de que todos são criminosos implicaria que o direito penal não conseguiu acompanhar as normas da sociedade e deveria ser reformado. Mesmo em sociedades autoritárias e não liberais que praticam formas altamente intrusivas de vigilância em massa destinadas a dissuadir e detectar dissidentes, parece mais correto descrever tais práticas como se implicassem que as pessoas são inimigas do Estado, e não criminosas. Há algo de errado com essas práticas, mas é discutível que se trate de criminalização indevida. Em todo o caso, parece razoável concluir que a vigilância em massa não necessariamente criminalizará indevidamente as pessoas e que, portanto, não é, em princípio, incompatível com a presunção de inocência.

As coisas tornam-se mais complicadas quando consideramos as práticas de vigilância que identificam determinados grupos ou indivíduos para efeitos de monitoramento ou trata-

mento diferenciado semelhante. Qualquer medida que distinga as pessoas com base em uma suspeita de propensão para a criminalidade potencial ou real é, em certa medida, criminalizadora. Por exemplo, a definição de perfis raciais e étnicos pela polícia tem sido objeto de fortes objeções, com base no fato de criminalizar não só os indivíduos a quem sujeita a interferência policial, mas também grupos raciais ou étnicos inteiros (Lever, 2007; Hadjimatheou, 2012). Em alguns casos, a criminalização ocorre mesmo que a medida seja justificada, considerando-se a situação como um todo. Por exemplo, os funcionários do controle de fronteiras podem responder com vigilância às informações sobre uma rede de tráfico de pessoas operada por indivíduos de uma determinada origem étnica que viajam entre locais específicos. A vigilância pode ser criminalizadora de pessoas com essa origem étnica, mesmo que as vítimas que a política se destina a proteger partilhem essa origem, mas a criminalização não seria ilícita se as provas fossem suficientemente confiáveis. Podemos concluir desta discussão que a vigilância que visa grupos ou indivíduos não é intrinsecamente criminalizadora, mas pode ser e, na verdade, é utilizada tanto de formas que criminalizam injustamente como de formas que não criminalizam.

Não é necessário, para efeitos do presente artigo, tentar determinar que tipos de vigilância são mais suscetíveis de criminalizar indevidamente e, por conseguinte, o que se pode dizer legitimamente para minar a presunção de inocência. O objetivo do presente artigo é tentar compreender o impacto sobre a presunção de inocência das práticas de vigilância em geral e à luz da possibilidade de estas poderem ser e serem utilizadas de forma a proteger as pessoas de acusações e condenações injustas. A primeira parte desse projeto está agora concluída: as práticas de vigilância podem e devem, mas não precisam, ser utilizadas de forma a minar a presunção de inocência, tratando as pessoas indevidamente como criminosas. Podemos

agora passar à segunda parte do projeto, que se preocupa em desenvolver uma melhor compreensão de como as práticas de vigilância podem evitar acusações e condenações erradas.

REDUÇÃO DE CONDENAÇÕES ERRADAS: O PAPEL DAS PROVAS RECOLHIDAS ATRAVÉS DA VIGILÂNCIA

Esta seção propõe a seguinte tese, não intuitiva e sem dúvida controversa: as práticas de vigilância podem e, em certa medida, já protegem, pessoas inocentes de serem erroneamente acusadas e condenadas por crimes, promovendo assim a presunção de inocência. Fazem-no principalmente fornecendo uma fonte de dados que pode ser utilizada como prova para afastar os suspeitos das investigações, poupando-os assim do ônus significativo de serem acusados ou condenados por crimes que não cometeram. Isto é atingido de três maneiras: primeiro, corrigindo a visão em túnel nas investigações policiais; segundo, reduzindo a taxa de falsas confissões; e terceiro, aumentando as provas ilibatórias disponíveis para a defesa. O recente trabalho empírico dos EUA e do Reino Unido sobre as causas das acusações e condenações erradas é aproveitado para desenvolver estas alegações.

Cientistas sociais estão testando e fundamentando teorias sobre as causas de acusações e convicções errôneas que sejam convincentes e possam influenciar a direção e o foco deste debate sobre o impacto da vigilância na presunção de inocência. Uma dessas perspectivas é que, ao contrário do que alguns teóricos do direito supõem (Naughton, 2007), as condenações erradas não são causadas de forma significativa pela flexibilização das regras sobre as provas, como a admissão de rumores ou provas de mau caráter (*bad character evidence*) (Gould et al., 2013). São, antes, o resultado de um ou mais dos seguintes fatores: identificação incorreta por testemunhas oculares, fal-

sas confissões, má defesa e/ou acusação e, muito menos significativo, erro na interpretação da prova forense (Ibid). Todos os fatores são causas simultâneas e provocados pela presença de uma "visão em túnel" pela polícia: ou seja, as heurísticas e falácias lógicas comuns que levam a polícia a "concentrar-se num suspeito, selecionar e filtrar as provas que irão "construir um caso" de condenação, ignorando ou suprimindo as provas que apontam para o afastamento da culpa" (Martin, 2002, p. 847-848). Como resultado desta e de outras investigações, a visão em túnel é agora amplamente reconhecida como um fator essencial para uma condenação errada.

A visão em túnel tende a manifestar-se cedo numa investigação criminal. Por conseguinte, não é surpreendente que as pesquisas sugiram também que as causas de acusações e condenações errôneas residam em erros que são mais eficazmente corrigidos por medidas tomadas nas fases relativamente iniciais de um caso. Já que as pesquisas sugerem que esses erros se enraízam e se amplificam em cada fase do processo de justiça penal, o recurso a procedimentos judiciais relativamente tardios para os corrigir não é a estratégia mais eficaz. As intervenções corretivas devem ser efetuadas muito mais cedo e, de preferência, antes de os suspeitos serem oficialmente acusados de infrações penais (Gould et al., 2013, p. 85).[5]

Como poderão as práticas de vigilância, tais como câmeras de vigilância, leitura de placas de veículos e as bases de dados de DNA, desempenhar um papel na redução de acusações e condenações errôneas? Há pelo menos três formas. Em primeiro lugar, as provas recolhidas através da vigilância têm potencial para corrigir ou obstruir o desenvolvimento da visão em túnel na polícia e, assim, contrariar o que a investigação sugere ser o fator mais significativo nas condenações erradas. A forma mais óbvia de o fazer é incorporar o recolhimento de provas geradas pela vigilância em medidas

destinadas a combater a visão em túnel. Por exemplo, em países como o Canadá e os Países Baixos, as recentes tentativas de reformar as práticas de investigação policial de forma a fazer um contraponto à visão em túnel incluem a nomeação de "contrários" ou advogados do diabo (Salet e Terpstra, 2013). Trata-se de agentes individuais que atuam de forma independente, frequentemente trazidos de uma autoridade externa, cujo papel consiste em desafiar as decisões de investigação com vista a evitar o desenvolvimento de preconceitos ou pressupostos que possam influenciar a direção de uma investigação. Não é ainda claro o êxito destas iniciativas, mas as expectativas são altas (Ibid). Os contrários podem e devem apontar aos agentes de investigação os casos em que os dados recolhidos pelas tecnologias de vigilância podem fornecer elementos de prova suscetíveis de eximir os suspeitos e que devam, por consequência, ser recolhidos.

Ora, pode-se argumentar que a tecnologia é um instrumento e que, por mais confiável que seja, não contribuirá para melhorar a justiça penal, a menos que seja utilizada corretamente. O exemplo dos contrários que acabamos de apresentar corrobora esta afirmação: é a nomeação do contrário que fará a verdadeira diferença, não a disponibilidade de dados de vigilância. Enquanto a abordagem de uma unidade policial à investigação criminal estiver orientada para a confirmação de uma hipótese e não para a descoberta da verdade, a tecnologia será utilizada ao serviço desse objetivo e o problema da visão em túnel persistirá. A menos que e até que se consiga mudar de mentalidade, pode-se argumentar, falar do potencial das tecnologias é, em grande medida, irrelevante.

Embora este argumento tenha algum mérito, é um pouco rápido demais. Se usadas como uma questão de rotina, certas tecnologias podem corrigir a visão em túnel e, assim, reduzir o risco de convicção indevida. O exemplo mais óbvio é a utili-

zação de DNA, impressões digitais e outras técnicas forenses. O êxito dos testes de DNA, em particular na correção de erros judiciários, é inegável. Quando as provas de DNA estão disponíveis e são confiáveis, podem proporcionar a tão necessária objetividade para cortar a visão em túnel e proteger os suspeitos inocentes de se tornarem réus ou mesmo criminosos condenados. Poderão algumas das vantagens das provas de DNA ser igualmente partilhadas pelas provas recolhidas através da vigilância? Há razões para pensar que sim.

Vamos considerar as câmeras de segurança. A coleta rotineira (mas não o exame) de imagens coletadas por câmeras em torno de uma cena de crime poderia ajudar a combater a visão em túnel, fornecendo evidências ilibatórias. Embora o Reino Unido seja famoso por ser um dos países mais filmados do mundo, a maioria das filmagens de câmeras de segurança é apagada dentro de 3 semanas após terem sido gravadas. Mesmo assumindo que a polícia investigadora decida que quer acessar as filmagens, elas podem ter sido apagadas antes de que se chegue a essa decisão. Na prática, a polícia no Reino Unido frequentemente falhará em acessar as filmagens de uma cena de crime a menos que precise de mais provas para recomendar a acusação da pessoa que acredita ter cometido o crime.[6] Suspeitos em casos criminais estão cada vez mais solicitando acesso a essas filmagens, que eles alegam que serão exculpatórias, e descobrindo que elas foram apagadas.[7] A retenção das filmagens e sua análise, pelo menos nos casos em que prometem revelar provas materiais da inocência ou culpa de um suspeito, é uma das formas pelas quais as provas obtidas a partir de tecnologias de vigilância poderiam ser utilizadas para reduzir os riscos de condenações injustas.

Estes pontos ganharão força no futuro à medida que as técnicas de reconhecimento facial se tornarem cada vez mais confiáveis. No Reino Unido, o uso de super-reconhecedo-

res, ou seja, indivíduos que são excepcionalmente bons em identificar indivíduos, mesmo com imagens e fotografias de câmeras de segurança de qualidade bastante ruim, está aumentando nos últimos anos, tanto na fase de pré-julgamento quanto na fase de julgamento de um caso criminal. Os super-reconhecedores são muito mais eficazes na identificação de indivíduos a partir de imagens e filmagens coletadas de vigilância do que qualquer tecnologia atual de reconhecimento facial no mercado.[8] No momento em que escrevemos, esforços estão sendo feitos para desenvolver a certificação para tais indivíduos, o que estabeleceria suas credenciais como especialistas forenses em tribunal. O uso de super-reconhecimento em conjunto com imagens de câmeras de segurança também poderia reduzir a dependência dos procedimentos de reconhecimento e outras oportunidades para identificação por testemunhas. A falta de confiabilidade da identificação por testemunhas é notória, mas as evidências mostram a polícia e os procuradores ainda dependem dela e que, portanto, continua sendo um fator persistente de condenação errônea (Gould et al., 2013, p. 95).

À luz desses desenvolvimentos, a exigência de reunir imagens de câmeras de segurança das cenas de crime pode (e deve) adquirir um status legal no futuro. Enquanto a polícia é obrigada a revelar provas ilibatórias já em sua posse, na maioria das jurisdições ela não é obrigada a reuni-las em primeiro lugar. A regulamentação britânica vai mais longe do que a maioria dos países ao exigir por lei que os investigadores policiais busquem todas as "linhas razoáveis de investigação". Conforme o conhecimento público das fontes de prova disponíveis cresce, é possível que a polícia se encontre como alvo de uma ação legal se, por exemplo, os condenados por crimes alegarem a existência de provas potencialmente ilibatórias de câmeras de segurança que a polícia poderia ter, mas

não conseguiu recuperar. Como MacFarlane (2008) observa, este caminho para a contestação legal não é muito útil aos réus hoje em dia, porque muito depende do que é "razoável" e porque depende de uma contestação *a posteriori* pelo réu, em vez de apresentar salvaguardas aplicáveis desde o início. No entanto, na medida em que as técnicas digitais de coleta e análise de provas se tornam mais fáceis e baratas, as percepções legais do que é razoável podem mudar para incorporar a coleta rotineira de provas coletadas a partir da vigilância.

Segundo, a coleta e retenção rotineira de dados de vigilância relevantes para um crime — como imagens de câmeras de segurança, dados da leitura de placas de veículos e metadados de comunicações — pode reduzir a taxa de confissões falsas, assegurando aos acusados que sua inocência pode ser revelada. Nos EUA, um em cada quatro casos de exoneração por meio de provas de DNA revelou condenação indevida com base em uma falsa confissão.[9] No Reino Unido, trabalhos psicológicos recentes mostram que entre 10 e 20% dos criminosos reincidentes relatam ter feito falsas confissões (Gudjonsson, 2011, p. 41). Uma das principais causas é a pressão ou manipulação por parte dos interrogadores policiais, e um fator agravante é a percepção entre os suspeitos de que seu caso resultará inevitavelmente em um veredito de culpa. Se tais suspeitos soubessem que sua equipe de defesa teria acesso a todos os dados disponíveis em suas comunicações, bem como à vigilância em ruas abertas, como câmeras de segurança, dados da leitura de placas de veículos, eles poderiam muito bem ter maior confiança sobre suas chances de serem considerados inocentes e decidir não se declararem culpados.

Em terceiro lugar, a disponibilização de provas de vigilância para as equipes jurídicas dos acusados pode ajudá-los a defender com mais sucesso seus clientes, abordando

assim outro fator importante nas condenações injustas. Escrevendo em relação ao Reino Unido, Naughton descreve como o sistema atual coloca toda a responsabilidade e, na verdade, o direito de reunir provas nos ombros da polícia e da acusação e, portanto:

> ...torna passivos os suspeitos do crime, o que simultaneamente justifica recursos mínimos para a defesa, enquanto o "ônus" pressiona e direciona a maior parte dos recursos da polícia e da acusação para que se desfaçam da presunção de inocência e construam casos a partir apenas de provas incriminatórias que possam levar a uma condenação, tornando as vítimas inocentes vulneráveis a condenações errôneas (Naughton, 2011, p. 41, tradução livre).

Naughton propõe a disponibilização de técnicas de coleta de provas para as equipes de defesa, bem como para a polícia e a acusação (Ibid). Dar aos réus acesso automático a todos os dados que registraram suas próprias atividades e que já foram retidos contribuiria de alguma forma para capacitar os réus a se protegerem contra condenações injustas.

Antes de continuarmos a considerar as implicações normativas das alegações apresentadas nesta seção sobre o impacto potencial das provas de vigilância sobre a taxa de acusações e condenações injustas, é importante reconhecer que elas são especulativas. No momento em que escrevemos, ainda não foi publicado nenhum estudo empírico examinando o papel atual e potencial das provas reunidas pela vigilância na exclusão de suspeitos de investigações criminais ou mesmo na sua absolvição em julgamentos. Isto deve ser contrastado com a considerável quantidade de trabalho realizado que tenta avaliar o impacto das técnicas e poderes de vigilância na prevenção, detecção e repressão do crime.[10] A disparidade é

explicada pelo fato de que a legitimação democrática de tais técnicas e poderes se justifica pela referência ao seu papel como meio de aumentar a segurança contra o crime e não como um meio de promover a presunção de inocência.

Um resultado disso é que é difícil avaliar até que ponto os dados já coletados para fins de prevenção e detecção de crimes poderiam ser utilizados de forma a evitar tipos bastante graves de criminalização indevida. Para os propósitos deste trabalho, porém, é suficiente ter demonstrado que os dados de vigilância têm um potencial significativo para serem colocados a tal uso e que, em certa medida, isso já está ocorrendo. Vale notar também que a acusação e a condenação errôneas são muito mais prejudiciais aos indivíduos do que muitos dos tipos mais comuns de interferências impostas pela vigilância, como, por exemplo, ser erroneamente apontado para uma busca em um aeroporto. Quais são as implicações desta conclusão para nossa avaliação do impacto das práticas de vigilância sobre a presunção de inocência, dado o que já foi discutido sobre seu potencial de miná-la ao criminalizar injustamente algumas pessoas?

AS IMPLICAÇÕES NORMATIVAS DO IMPACTO DA VIGILÂNCIA SOBRE A PRESUNÇÃO DE INOCÊNCIA

Se o que tem sido argumentado até agora está correto, as práticas de vigilância têm o potencial tanto de minar a presunção de inocência, criminalizando indevidamente alguns através da imposição de suspeitas, quanto de promovê-la, protegendo outros de serem erroneamente acusados ou condenados. Como estas conclusões devem determinar nosso entendimento do impacto das práticas de vigilância em geral sobre a presunção de inocência? É possível dizer que a vigilância protege a presunção de inocência em geral, pois a criminalização que

ela tem o potencial de prevenir (ou seja, a condenação errônea) é mais grave do que a que ela inflige (ou seja, a suspeita equivocada)? Ou devemos dizer que a vigilância tanto prejudica como protege a presunção de inocência?[11]

Nenhuma das duas soluções está sem suas dificuldades. Por um lado, o fato de que a criminalização de inocentes em geral possa ser reduzida por práticas de vigilância não significa que tenhamos razão em não reconhecer a criminalização indevida sofrida por alguns. No entanto, pelo menos essa abordagem agregadora nos dá uma base para fazer alguma avaliação do impacto ponderado dessas medidas sobre a presunção de inocência, uma avaliação que pode alimentar as decisões sobre a justificativa geral de tais práticas. Por outro lado, a segunda opção, que não agrega suspeita equivocada e convicção errônea, parece descrever com mais precisão o impacto da vigilância sobre a presunção de inocência. No entanto, pelo menos à primeira vista, parece menos útil do que a primeira, pois não produz nenhuma avaliação geral clara que possa informar considerações políticas mais amplas.

Apesar destas considerações, há pelo menos uma razão convincente para preferirmos a segunda opção, não agregadora, acima da primeira. A opção agregadora é o tipo de abordagem utilitária agregadora bruta para determinar a interferência na presunção de inocência, que pesaria a injusta suspeita infligida pela vigilância contra a acusação e a condenação errônea evitadas. Esse raciocínio utilitário também levaria em conta o fato de que a acusação e a condenação errôneas envolvem danos a interesses mais vitais para o bem-estar das pessoas do que aqueles afetados pela suspeita errônea, e concluiria, portanto, que a prevenção da primeira pesa mais do que a prevenção da segunda.

Esta abordagem não seria aceita pelos teóricos de uma persuasão deontológica como base válida para a avaliação, pois

pressupõe que as injustiças para uns podem ser justificadas por referência aos benefícios obtidos por outros. A oposição a tais compensações (*trade-offs*) não poderia ser mais formidável. Dois dos mais importantes filósofos políticos do século XX, Rawls e Nozick, argumentaram que as compensações entre indivíduos são incompatíveis com o respeito às pessoas, pois não reconhecem o que ficou conhecido como a "separatividade das pessoas". Nas palavras de Nozick: "Usar uma pessoa [em benefício de outra] não respeita suficientemente e leva em conta o fato de que ela é uma pessoa separada, que a sua é a única vida que ela tem. Ela não recebe um bem em excesso do seu sacrifício" (Nozick, 1974, p. 33). Nem todos concordam que essa objeção é fatal, mas é grave o suficiente para sugerir que uma alternativa à abordagem utilitária deva ser explorada.

Uma alternativa possível é sugerida considerando uma outra objeção à posição utilitária agregada: essa objeção que ficou conhecida como a "doutrina dos atos e omissões". A doutrina dos atos e omissões afirma que é pior infligir dano do que deixar de intervir para evitá-lo. Embora o apoio a essa doutrina esteja minguando na filosofia moral, ela ainda figura regularmente nos argumentos morais, pelo menos em parte porque há um claro sentido em que ela se conjuga com intuições morais de senso comum.[12] Os proponentes filosóficos dessa posição afirmam que o dever do Estado de se abster de prejudicar inocentes deve ter prioridade sobre seu dever de prevenir danos infligidos a inocentes por outros (Kagan, 1992). Aplicada à questão em pauta, sugere que a suspeita indevida causada pela vigilância é um dano contra inocentes e deve, portanto, ser evitada, mesmo que as práticas que a causam também impeçam condenações errôneas. Em outras palavras, a doutrina dos atos e omissões cede um argumento claro para que os Estados se abstenham da vigilância, quando e na medida em que implique na criminalização indevida de indivíduos

inocentes em qualquer de suas formas. Se este argumento for aceito, parece que poderíamos ter fundamentos suficientes não só para rejeitar a abordagem utilitária agregadora para avaliar o impacto da vigilância sobre a presunção de inocência, mas também para resolver o aparente dilema colocado pela abordagem não agregadora: se estamos proibidos de infligir qualquer tipo de criminalização indevida, então estamos proibidos de realizar muitas dessas práticas de vigilância que também poderiam ajudar a evitar condenações errôneas.

Entretanto, há fortes razões para rejeitar esta linha de argumentação, razões que poderiam ser aceitas mesmo por aqueles cujas intuições insistem em alguma distinção entre atos e omissões. Consideremos dois desses motivos. Em primeiro lugar, a doutrina dos atos e omissões pode ser interpretada de forma mais flexível do que foi apresentada acima. Não é preciso, portanto, que se entenda que infligir dano é sempre pior do que deixar de intervir para evitá-lo, princípio que parece implausível. Se a utilização de provas recolhidas pela vigilância pode prevenir uma grande quantidade de danos criminosos, infligindo aos inocentes um aumento muito pequeno do número de pessoas tratadas como criminosamente suspeitas, pode ser conciliável com alguma versão mais moderada da distinção entre atos e omissões.

Segundo, e mais importante, em relação às práticas de vigilância, a objeção à abordagem agregadora oferecida pela referência à doutrina dos atos e omissões pressupõe um conflito na prática entre o imperativo de abster-se de criminalizar injustamente e o dever de evitar condenações errôneas. Na verdade, não existe tal conflito. A tendência das práticas de vigilância em infligir suspeitas errôneas a alguns inocentes pode ser reduzida sem, ao mesmo tempo, reduzir o potencial dessas práticas para serem utilizadas de forma a proteger os indivíduos de acusações e condenações errôneas. Isto porque, como foi argumenta-

do anteriormente, a vigilância não precisa (embora tenha sido na prática) ser usada de forma a minar a presunção de inocência, impondo suspeitas às pessoas e, assim, criminalizando-as erroneamente. Os ajustes que precisariam ser feitos para evitar tal criminalização indevida não prejudicam de forma alguma a disponibilidade do tipo de dados que poderiam ser utilizados para exculpar ou, de outra forma, afastar da suspeita aqueles já sujeitos à investigação policial. Em outras palavras, é possível praticar a vigilância de forma a reduzir o número de indivíduos erroneamente criminalizados no limite inferior do espectro de suspeitas, ao mesmo tempo em que se aumenta a proteção para aqueles em risco de criminalização muito mais grave.

Por isso, a segunda opção não agregadora apresentada acima, ou seja, buscar reconhecer tanto as formas como a vigilância prejudica, quanto as formas como ela protege a presunção de inocência, não precisa levar à paralisia normativa. Ao contrário, combinada com as afirmações feitas acima sobre o impacto real e potencial das práticas de vigilância sobre a suspeita indevida e a convicção errônea, ela produz uma mensagem clara de que devemos adaptar o uso estatal da vigilância para que a primeira seja reduzida e a segunda reforçada.

Muitas vezes as críticas à vigilância consistem em listas das várias formas pelas quais ela mina os nossos valores mais preciosos e fundamentais. Raramente são feitas tentativas sistemáticas de refletir sobre os benefícios potenciais para tais valores, especialmente aqueles que não são de segurança. Este trabalho tem tentado ir um pouco no sentido de corrigir isso e refletir sobre as implicações normativas de sua análise, de forma a apoiar recomendações claras de ação.

NOTAS

1. Uma versão deste artigo foi publicada pela primeira vez na revista Philosophy & Technology, volume 30, pp. 39-54 (2017).

2. Tradução de Enrico Roberto.

3. Em 2013, o Parlamento da União Europeia anunciou o lançamento de um inquérito sobre a compatibilidade do PRISM, declarando que "o inquérito da Comissão das Liberdades Cívicas irá avaliar o impacto das alegadas atividades de vigilância no direito dos cidadãos da UE à privacidade e à proteção de dados, à liberdade de expressão, à presunção de inocência e ao direito a um recurso efetivo" (Parlamento da UE citado no investigador, 9 de Julho de 2013).

4. Os resultados desta pesquisa complementam trabalhos recentes normativa - e empiricamente informados sobre as injustiças sistêmicas no sistema de justiça criminal, o que tem sido eficaz em destacar o impacto das práticas de vigilância policial preventiva pela polícia sobre os resultados do sistema de justiça criminal. Um excelente exemplo é o trabalho de Bernard Harcourt prevendo o impacto da perfilização racial praticada pela polícia nas ruas sobre as taxas relativas de criminalidade de diferentes grupos étnicos, bem como a taxa geral de criminalidade (Harcourt, 2006). Esta linha de pesquisa não é diretamente relevante para a questão da criminalização indevida, mas chama a atenção para o fato de que as escolhas investigativas sobre quem identificar e quem excluir da suspeita, mesmo numa fase muito preliminar da prevenção do crime, podem ter efeitos previsíveis e moralmente significativos sobre os resultados dos julgamentos criminais.

5. Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Diretiva 2002/58/CE.

6. Entrevista particular com policial do Serviço de Polícia Metropolitana de Londres.

7. Entrevista com Simon McKay,advogada da defesa britânica.

8. Cf. Potts, L. (2015). The Police Super Recognisers Putting Names to Faces' Lauren Potts, BBC News. https://bbc.in/32kuCUV.

9. Cf. Innocence Project dos EUA para explicação das causas da falsa confissão: https://bit.ly/3fpWpXr.

10. Por exemplo, muitos estudos têm sido realizados em todo o mundo sobre a eficácia das câmeras de segurança como medida de prevenção e detecção de crimes (Germain et al., 2013).

11. A escolha entre estas duas opções não é uma escolha entre duas implicações normativas, mas uma escolha entre duas maneiras de conceituar o impacto.

REFERÊNCIAS

Bou-Habib, R. (2008). Security, profiling and equality. *Ethical Theory and Moral Practice*, 11 (2).

Campbell L. (2010). A rights-based analysis of DNA retention: "non-conviction" databases and the liberal state. Criminal *Law Review*.

DeAngelis, P. (2014). Racial profiling and the presumption of innocence. *Netherlands Journal of Legal Philosophy*, 2014 (1).

Duff, A. (2013). Who must presume whom to be innocent of what? *Netherlands Journal of Legal Philosophy*, 42 (3).

Fuchs, C. (2012). Implications of deep packet inspection (DPI) internet surveillance for society. https://bit.ly/3gs8R9S.

Galetta, A. (2013). The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies? *In European Journal of Law and Technology*.

Galetta A, De Hert, P. (2012). *Effects of surveillance on the rule of law, and on the presumption of innocence.* IRISS Deliverable 1.1: surveillance, fighting crime and violence. https://bit.ly/2C80NPp.

Germain et al. (2013). A prosperous "business": the success of CCTV through the eyes of international literature. *Surveillance and Society,* 11 (1/2).

Gould et al. (2013). *Predicting erroneous convictions: a social science approach to miscarriages of justice*. USA Department of Justice Report. https://bit.ly/2BZ4uEl.

Gudjonsson, G. (2011). *Suspect interviews and false confessions*. Current Directions in Psychological Science, 20(1), 33–37.

Hadjimatheou, K. (2012). *Moral Risks of Profiling in Counter-Terrorism*, research paper for the EU-funded FP7 Security project DETECTER (Detection Technologies, Terrorism, Ethics and Human Rights). https://bit.ly/2ATBl7h.

Hadjimatheou, K. (2014). The relative moral risks of targeted and untargeted surveillance. *Ethical Theory and Moral Practice*, 17, 187–207.

Haggerty; Ericson. (1997). *Policing the Risk Society.* Clarendon Studies in Criminology, Oxford: Clarendon

Harcourt, B. (2006). *Against prediction: profiling, policing, and punishing in an actuarial age*. Chicago: University of Chicago Press.

House of Lords Constitution Committee, (2009). 'Surveillance: Citizens and the State'. 2nd Report of Session 2008-09, 2.

Inquirer. (2013). European Parliament votes for PRISM snooping investigation. At https://bit.ly/32bMFfO.

Jarvis-Thomson, J. (1975). The right to privacy. *Philosophy and Public Affairs*, 4 (4), 295–314.

Kagan, S. (1992). *The limits of morality*. Oxford: Clarendon.

Kimmelman, G. (2000). The promise and perils of criminal DNA databanking. *Nature*, 18(7).

Lever, A. (2007). What's wrong with racial profiling? Another look at the problem. *Criminal Justice Ethics*, 26(1) 20–28.

Lyon, D. (1994). *The electronic eye: the rise of surveillance society*. University of Minnesota Press.

Lyon, D. (2002). ***Surveillance as social sorting.*** Privacy, risk, and automated discrimination.

MacFarlane, B. (2008). *Wrongful convictions: the effect of tunnel vision and predisposing circumstances in the criminal justice system*, prepared for the Inquiry into Pediatric Forensic Pathology in Ontario, The Honourable Stephen T. Goudge, Commissioner. https://bit.ly/393Wxd7.

Martin, D. (2002). Lessons about justice from the laboratory of wrongful convictions: tunnel vision, the construction of guilt, and informer evidence. *70 UMKC L Rev*., 847.

Minaj, J., & Bonnici, J. (2014). Unwitting subjects of surveillance and the presumption of innocence. *Computer Security and Law Review*, 30(4).

Monahan, T. (2010). Surveillance as governance: social inequality and the pursuit of democratic surveillance. In Haggerty, K.; Samatas, M. (eds.). *Surveillance and democracy*. Routledge.

Nance, DA. (1994). Civility and the burden of proof. *Harvard Journal of Law and Public Policy*, 17.

Naughton, M. (2007). *Rethinking miscarriages of justice: beyond the tip of the iceberg*. Basingstoke: Palgrave Macmillan.

Naughton, M. (2011). How the presumption of innocence renders the innocent vulnerable to wrongful conviction. *Irish Journal of Legal Studies*, 2 (1).

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society.*

Nozick, R. (1974). *Anarchy, State, Utopia***.** New York: Basic Books.

Pavone, V., & Pereira, M. (2008). *The privacy vs. security dilemma in a risk society: insights from the PRISE project on the public perception of new security technologies in Spain*. https://bit.ly/2WjbtPk.

Privacy International, PI warns that new ISP interception plans will be illegal. November 26, 2009.

Ryberg, J. (2011). Racial profiling and criminal justice. *Journal of Ethics*, 15 (1)

Salet, R., & Terpstra, J. B. (2013). Critical review in criminal investigation: evaluation of a measure to prevent tunnel vision. *Policing*, 8 (1), 43–50.

Stewart, G. (2014). The right to be presumed innocent. *Criminal Law and Philosophy***,** 8 (2).

Stumer, A. (2010). *The presumption of innocence*. Oxford.

Tadros, V. (2007). Rethinking the presumption of innocence. *Criminal Law and Philosophy,* 1 (2), 193–213

Teson (2005). Liberal security. *In Human rights in the age of terror.* Cambridge: Cambridge University Press.

The Guardian (2016, março). *Facebook, Google and WhatsApp plan to increase encryption of user data*. https://bit.ly/303zv1G.

Tomlin. (2013). The golden thread? Criminalisation and the presumption of innocence. *Journal of Political Philosophy*.

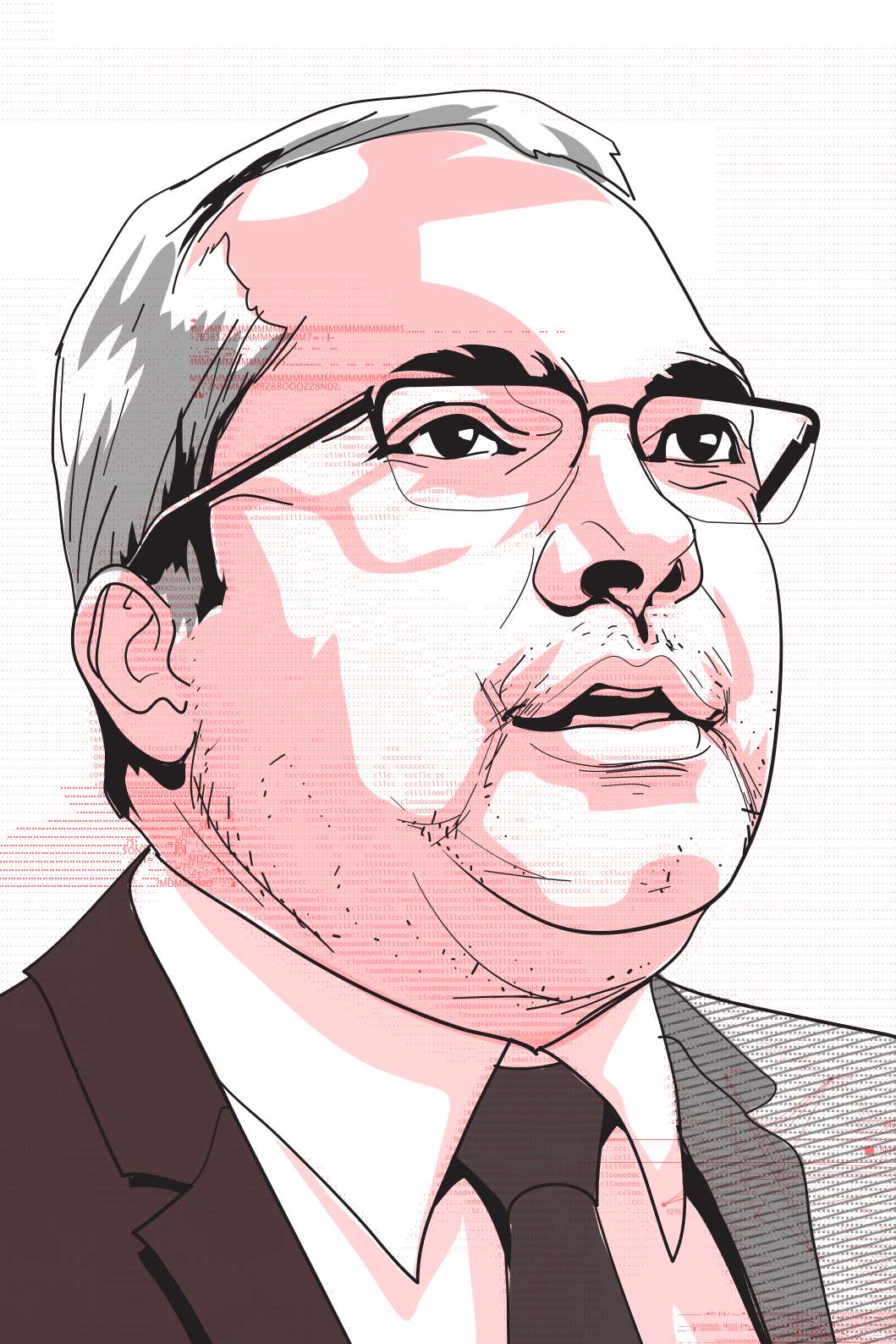
UK Office for National Statistics (2013). *Crime in England and Wales***,** statistical bulletin. https://bit.ly/32l03y2.

Ullmann-Margalit, E. (2002). *Trust out of distrust.* Journal of Philosophy, 99 (10) 532–548.

Warren and Brandeis (1890). *The right to privacy*. Harvard Law Review, 4 (5)

Westin, A. (1967). *Privacy and freedom*. New York: Athenaeum.

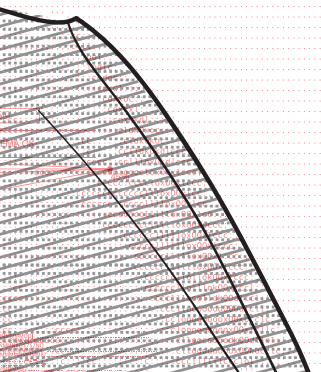
Yamagishi, T. (2011). *Trust: the evolutionary game of mind and society***.** Springer.



02.

TUTELA CONTRA A GEOLOCALIZAÇÃO CONTÍNUA

Geraldo Prado



I.

Inicialmente, gostaria de agradecer ao InternetLab, na pessoa do Dennys Antonialli, pelo gentil convite para participar do III Congresso Internacional "Direitos Fundamentais e Processo Penal na Era Digital". Na ocasião, apresentei comunicação, no dia 22 de agosto de 2019, no painel intitulado "Dados de Deslocamento e Geolocalização: a investigação em tempo real", junto com o professor da Universidade Estadual do Maranhão Cleopas Isaías Santos e a diretora jurídica de privacidade para Uber na América Latina Flavia Mitri. O texto que ora apresento equivale, em sua maior parte, à minha fala no mencionado painel.

Optarei por abordar, em um primeiro momento, os temas da decisão judicial e da técnica de decisão judicial. Assim o faço por entender que o assunto (dados de deslocamento e geolocalização) impõe ao jurista brasileiro o desafio de entender como lidar com situações que afetam direitos fundamentais numa perspectiva de jurisdicionalização dos questionamentos, isto é, como estabelecer regras que confiram segurança a respeito da melhor interpretação e aplicação dos direitos fundamentais. A escolha justifica-se também porque vivemos hoje em um ambiente de profunda instabilidade e insegurança jurídica. Em um momento como este, creio que o Direito é desafiado a oferecer respostas e recolocar as coisas nos seus devidos lugares.

II.

Discorda-se da ideia enunciada por Pontes de Miranda, logo na abertura dos seus comentários ao código do processo civil, de que a função da jurisdição é a pacificação social, porque, da maneira como ele a imaginava, sua noção de pacificação estava associada a uma concepção de sociedade homogênea, e somos, por felicidade nossa, uma sociedade plural que

deve reconhecer as diferenças. No entanto, sem dúvida, a jurisdição cumpre uma função política e social de primeira ordem consistente na institucionalização dos conflitos. No lugar de guerrearmos, contamos com um espaço, um território em que os conflitos e as controvérsias são inseridos e devem ser resolvidos.

Com efeito, caberá ao Poder Judiciário e em especial ao Supremo Tribunal Federal cumprir essa função de maior relevância, devendo interpretar "as regras do jogo" para os casos concretos, no sentido de dizer como resolvem-se e processam-se estes casos, mas também nos dizer claramente qual o sentido e o âmbito normativo de determinados direitos e deveres, especialmente naquelas situações que implicam constrição de direitos fundamentais.

Os Tribunais Superiores e o principal órgão de autogoverno do Poder Judiciário no Brasil, o Conselho Nacional de Justiça, têm manifestado constante preocupação com a expansão e a vulgarização das medidas de invasão de privacidade e intimidade das pessoas, por meio dos chamados métodos ocultos de investigação.[1] A matéria suscitou a instalação da CPI das escutas telefônicas, no âmbito do Congresso Nacional, com a apresentação de relatório que entre outras providências sugeriu que cada decisão judicial expressamente indicasse no caso das interceptações telefônicas a linha telefônica a ser monitorada. Perseguia-se assim o objetivo de prover o processo penal brasileiro de um, ainda que rudimentar, "regime de execução de medidas" capaz de evitar abusos ou identificar interesses escusos, ocultados por um pronunciamento judicial legítimo.

Não se trata de um cuidado exclusivo da realidade brasileira. Ao contrário, as técnicas de investigação que recorrem a modernas tecnologias de comunicação e informação estão dotadas de extraordinário potencial de invasão da vida pri-

vada e de violação de direitos fundamentais, de modo que terminam por se transformar em sedutores instrumentos de investigação criminal.

As pesquisas policiais são incrementadas pelo emprego destes métodos ocultos de investigação autorizados judicialmente: a interceptação de dados, a interceptação telefônica, as escutas domiciliares, as escutas ambientais, a infiltração de agentes. Hoje, há um modelo de infiltração de agentes que é digital, há monitoramento contínuo das pessoas pelo processamento via equipamentos que trabalham com inteligência artificial de dados de localização. Esse conjunto de práticas converte-se em um modelo de atuação preliminar, um esquema peculiar de atuação na investigação criminal.

Modernamente, compartilha-se o entendimento de que a restrição do exercício de determinados direitos deve estar orientada ao fim de assegurar a proteção de bens jurídicos alheios ou da coletividade. Esse entendimento decorre de uma estrutura pensada na modernidade europeia ocidental com lastro na noção do contrato social. Tal restrição, porém, não pode, a partir de um princípio de justiça material, nos levar à condição de sujeição em virtude da qual sejamos dirigidos a produzir informações que, enviesadas, funcionam como base fática para a atribuição de responsabilidade que pode não ser sequer verdadeira.

Em nosso país, sob a vigência da Constituição de 1988 consolidaram-se as condições para nossa adesão aos tratados internacionais de direitos humanos e, de fato, em 1992, o Brasil aderiu à Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica) e ao Pacto de Direitos Civis e Políticos, estatutos jurídicos que regulam a proteção contra a autoincriminação compulsória.[2]

À vista do senso comum, a tutela contra a autoincriminação compulsória costuma ser reconhecida no direito de não

nos submetemos ao bafômetro, não sermos obrigados a fornecer material gráfico para comparação grafotécnica etc.[3]

Releva notar apesar disso que a tutela contra a autoincriminação compulsória possui escopo muito mais amplo do que o que tradicionalmente lhe é reconhecido e que se revela importante nos casos de interceptação das comunicações telefônicas, por exemplo, na interceptação das comunicações de dados, uma vez que a pessoa alvo da medida não tem, obviamente, ciência de que está sendo interceptada. No limite, a pessoa que tem suas conversas, seus diálogos, suas comunicações interceptadas, está produzindo provas contra ela própria. Portanto, toda interceptação de ligação telefônica ou de interceptação de produção de dados tende a ser em tese contrária à ideia da tutela contra a autoincriminação compulsória.

Embora essa interceptação seja permitida, a Constituição estabelecerá o espaço de tensão. A Constituição dirá: aqui limitaremos a tutela contra a autoincriminação compulsória em benefício de um interesse público que se justifique e seja mais importante. A Constituição operará nesta frequência. Por que a Constituição? Porque é a Constituição e, por via dela os tratados internacionais de direitos humanos, que estabelece o âmbito de proteção contra a autoincriminação compulsória. A Constituição da República define uma regra e somente a própria Constituição estará legitimada a estabelecer qualquer exceção.

Francisco Muñoz Conde sustenta que esses métodos ocultos debilitam progressivamente o princípio do nemo tenetur, que trata da noção da tutela contra a autoincriminação compulsória. Fato é que, se é necessária essa debilitação, ela tem que partir de uma exceção constitucionalmente autorizada e vai levar em consideração outros fatores.

No direito português o jurista Manuel Valente também adverte que:

> A eufórica e deslumbrante necessidade de apetrechamento dos operadores judiciários de meios de obtenção de prova sem que primeiramente se avalie os resultados objetivados com os meios já existentes – muitas das vezes esquecidos na prateleira dos livros empoeirados – é uma praxis a que nos habituamos. Ou, concretizando melhor, a desmedida e facilitada autorização das escutas telefónicas – de necessidade duvidosa -, sem que primeiramente se avaliem os meios menos delatores dos direitos e liberdades pessoais, converteu um meio de obtenção de prova de ultima ratio – de exceção – em prima ratio – em vulgar.[4]

Winfried Hassemer igualmente alertará, em seu ensaio denominado "Verdad y búsqueda de la verdad en el proceso penal: La medida de la Constitución", acerca dos riscos inerentes à proliferação de atos de ingerência na intimidade como metodologia corrente das investigações criminais na Alemanha.[5]

As práticas penais do gênero tendem a violar o âmbito essencial de configuração da vida privada e a legalidade penal não se desenvolve na mesma velocidade para estipular critérios e definir mecanismos que protejam este âmbito essencial contra as intrusões repudiadas constitucionalmente.

Por essa razão observa-se a tendência a um maior protagonismo judicial na definição dos limites normativos relativos à execução das medidas de investigação dessa natureza. O Judiciário antecipa-se ao legislador quer por conta da atuação dos tribunais constitucionais, que proclamam a proteção do âmbito essencial da vida privada como critério de aferição da constitucionalidade dos métodos invasivos, quer em concreto, por força da fiscalização que em cada caso os juízes exercem sobre a execução das providências.

Na Alemanha, em relação à lei sobre os meios de vigilância das comunicações, submetida a critérios de adequação extraídos do acórdão do Tribunal Constitucional Federal alemão, de 03 de março de 2004,[6] na linha preconizada pelo Tribunal Europeu de Direitos Humanos (TEDH), Claus Roxin informa que o Supremo Tribunal alemão proferiu decisão em 10 de agosto de 2005, por meio da qual, ao declarar a ilicitude probatória de determinada aplicação de métodos ocultos, por violação do mencionado âmbito essencial, contribuiu para estipular o critério de "prognóstico negativo do âmbito essencial" a orientar a jurisprudência quanto ao sentido que deve ser configurado quando da interpretação/aplicação da medida investigatória de intervenção.

Reitere-se que o fato de o tribunal alemão ter decidido excluir da ponderação de interesses da persecução penal o "âmbito essencial de configuração da vida privada", ao exercitar o controle de constitucionalidade sobre a lei de 28 de março de 1998, que alterou o § 100, c, I, nº 3, do CPP alemão, apenas revela a abrangência e profundidade de uma das espécies de intervenção oculta para identificação de meios de prova[7] e o contágio que deriva do emprego de recursos de investigação que capturam o que há de mais íntimo das pessoas.[8]

A adoção de um prognóstico negativo de âmbito essencial de afetação da vida privada configura critério que à luz do direito brasileiro também tem plena aplicação pois, à semelhança do sistema constitucional alemão, o brasileiro reconhece a primazia dos direitos fundamentais e o caráter excepcional da adoção de técnicas de índole probatória que penetram na intimidade e vida privada.[9]

Por essa razão observa-se a tendência a um maior protagonismo judicial na definição dos limites normativos relativos à execução das medidas de investigação dessa natureza. O Judiciário antecipa-se ao legislador quer por conta da atuação

dos tribunais constitucionais, que proclamam a proteção do âmbito essencial da vida privada como critério de aferição da constitucionalidade dos métodos invasivos, quer em concreto, por força da fiscalização que em cada caso os juízes exercem sobre a execução das providências.

A busca por um critério jurídico de análise de investigação e de decisão de tudo aquilo que diz respeito à restrição aos nossos direitos fundamentais, incluindo aqui a questão da geolocalização contínua, configura o desafio que se apresenta ao Poder Judiciário brasileiro.

III.

De acordo com Eloy Velasco Núñez, a geolocalização continua consiste em método de tecnovigilância que opera por meio da análise dos rastros e dados das várias espécies de comunicações e transmissões de dados por meio digital, recorrendo as chamadas *non trespassory surveillance techniques*.[10]

Como método potencialmente *invasor*, que processa os rastros e dados das várias espécies provenientes do meio digital, a "geolocalização" viabiliza uma forma de vigilância extrema do indivíduo em uma sociedade que massivamente faz uso da rede mundial de computadores.[11]

O caráter de domínio sobre a vida digital da pessoa alvo da vigilância é de tal ordem que, salienta Velasco Núñez, o que antes parecia inimaginável em termos de sociedade policial, as máquinas hoje tornaram algo muito real.[12]

Uma tecnovigilância dessa grandeza sem dúvida afeta a vida privada e por este ângulo, de defesa da privacidade e, no extremo, da intimidade, que as possibilidades práticas de emprego dos métodos de geolocalização contínua começaram a esbarrar na resistência dos tribunais.

Com efeito, o mencionado Tribunal Constitucional Federal da Alemanha, a respeito das comunicações, já havia decidido que:

> Uma 'vigilância total' temporal e espacial será inadmissível porque é alta a probabilidade de que as conversas pessoais sejam interceptadas. A dignidade humana também é violada se a vigilância se estende por um longo período temporal e é tão extensa que quase todos os movimentos e expressões da vida da pessoa afetada são registradas e podem atingir o fundamento da sua personalidade.[13]

Migrando o mesmo raciocínio para a questão do acompanhamento em tempo integral do indivíduo, processando seus passos, mas conhecendo da mesma maneira o conteúdo das suas ações, é que o Tribunal Europeu de Direitos Humanos reconheceu que a "geolocalização contínua de veículos por meio das balizas de GPS afeta a vida privada.[14]"

Também por essa perspectiva vale recorrer às informações de Velasco Núñez:

> Así, la reciente jurisprudencia de referencia internacional, por diferentes vías, ha reconocido que la geolocalización continua – de un coche, a través de balizas, a la larga, con sistema GPS – afecta a la vida privada: STEDH de 2 de septiembre de 2010, caso Uzún vs. Alemania – a través del art. 8 del Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales, de 4 de noviembre de 1950 (en adelante, CEDH) –, y más recientemente, algo similar ha hecho la sentencia del caso Estados Unidos vs. Jones 10 US 1259 (de) 2011 – a través de la cuarta enmienda a su Constitución.[15]

É prudente advertir que se a simetria com a "vida analógica" nos oferece as ferramentas teóricas para compreender

que a privacidade e a intimidade são afetadas por uma investigação criminal que possa recorrer a este tipo de dispositivo, o passo mais importante a ser dado – e é inevitável que o seja – está em reconhecer que nos encontramos em mundo novo digital, que configurando as variadas dimensões da nossa vida e tornando onipresente a esfera digital, reclama que sejam reconhecidos direitos fundamentais da mesma natureza.

Com razão Velasco Núñez leciona que não é mais possível analisar a privacidade sob uma ótica aderente a um território específico. A mobilidade das tecnologias que por força da convergência potencializam o cruzamento e processamento em tempo real de uma quantidade incalculável de informações, na forma de dados, reclama novas noções de domicílio e identidade.[16]

O domicílio digital e a identidade digital configuram um contínuo à semelhança de uma sombra de dados que vai deixando seus rastros – invisíveis a olho nu, mas plenamente detectáveis pelo emprego da Inteligência Artificial (IA) – que, se beneficiam o titular que encarna a identidade e está ao abrigo deste domicílio, terminam por ser mais facilmente devassáveis e atingíveis que o domicílio territorial e a identidade tradicional.

Neste contexto, assume especial relevo o papel que desempenha o Poder Judiciário convocado a decidir sobre quando, de que forma, para que fins e por quanto tempo o Estado por seus agentes poderá exercer válida e legitimamente a tecnovigilância, em especial aquela prevista no art. 13-B do Código de Processo Penal.

A autorização judicial de que trata o citado artigo deve estar sujeita a um modelo de fundamentação diferenciada em que se destaca a necessidade de enunciação de um prognóstico negativo do âmbito essencial de configuração da vida privada, como um trajeto, um percurso absolutamente incontornável de qualquer decisão judicial.

/ A
“GEOLOCALIZAÇÃO”
VIABILIZA UMA
FORMA DE
VIGILÂNCIA
EXTREMA
DO INDIVÍDUO
EM UMA SOCIEDADE
QUE FAZ USO DA
REDE MUNDIAL DE
COMPUTADORES /

Como critério de decisão a respeito da aplicação da técnica de geolocalização, será importante ver consolidada pela jurisprudência dos tribunais superiores a exigência de que a decisão do caso concreto afirme o prognóstico negativo do âmbito essencial de configuração da vida privada ao deferir, em caráter excepcional, a transmissão das informações em tempo real sobre a localização de pessoas.

A necessidade de se trabalhar com um critério judicial de prognóstico negativo do âmbito essencial exige que se reconheça fundamentadamente: aqui não há problema, foi realizado o prognóstico a partir do qual se concluiu que a restrição aplicada não afetará o âmbito essencial de determinado direito fundamental.

Consequência jurídica inevitável é a admissão de que a hipótese está sujeita à reserva de jurisdição. Se o deferimento da medida interfere em direitos fundamentais, não se pode conferir acesso direto da autoridade policial e do Ministério Público. Este é o sentido da previsão dos novos artigos 13-A e 13-B do CPP.[17] A experiência alemã por excluir da ponderação de interesses da persecução penal o "âmbito essencial de configuração da vida privada", ao exercitar o controle de constitucionalidade sobre a lei de 28 de março de 1998, que alterou o § 100, c, I, nº 3, do CPP alemão, apenas revela a abrangência e profundidade de uma das espécies de intervenção oculta para identificação de meios de prova e o contágio que deriva do emprego de recursos de investigação que capturam o que há de mais íntimo das pessoas.

David Silva Ramalho, jurista português, postula a especificidade da matéria a reclamar reflexão cuidadosa que, todavia, parte do reconhecimento da existência de direitos fundamentais na esfera digital.

Salienta Ramalho em contexto pouco diverso, mas no qual o princípio é reconhecido:

O reconhecimento da existência de um novo direito fundamental à confidencialidade e integridade dos sistemas informáticos que fundou a declaração de inconstitucionalidade por parte do Tribunal não foi, porém, completamente inovador.

Desde logo porque cerca de dois anos antes da sua prolação, NICOLA GONZÁLEZ-CUELLAR SERRANO, num escrito com passagens muito semelhantes às do acórdão do BVerfG, reconhecera já a insuficiência do quadro jus-fundamental vigente para tutelar adequadamente o *ambiente digital*, pelo que cunhou, ainda que de forma pouco aprofundada, o direito à não intromissão no ambiente digital ('*derecho a la no intromisión en el entorno digital*'), emergente do direito fundamental à liberdade informática consagrado no artigo 18.º, nº 4, da Lei Fundamental espanhola, a conjugar, quando e se necessário, com a tutela conferida pelos direitos fundamentais à privacidade, à inviolabilidade do domicílio e ao segredo das comunicações. A tutela emergente do direito à não intromissão no *ambiente digital* não se afere, contudo, por referência directa a um ou mais sistemas informáticos, mas sim ao ambiente digital do indivíduo, definido como '*la información en forma electrónica, magnética o luminosa que, voluntaria o involuntariamente, de forma consciente o inconsciente, genera con su actividad, no importa donde se encuentren los archivos informáticos que la contengan o los canales de comunicación a través de los cuales discurra*'. O Autor refere, inclusivamente, que é irrelevante o local onde se encontra fisicamente o suporte com os bytes armazenados, uma vez que é frequente os mesmos encontrarem-se em diferentes países ou continentes. A tutela procurada deve conceber o ambiente digital como uma realidade, por natureza, deslocalizada e globalizada.[18]

Há, portanto, identidade digital, domicílio digital, o direito a não ser localizado permanentemente, o direito ao anonimato. Todos esses conceitos fazem parte de uma nova forma de compreensão da autodeterminação informativa de todos nós.

Estes direitos formam um conjunto e, sobre esse conjunto, os tribunais, juízes nos casos concretos e Supremo Tribunal Federal no controle de constitucionalidade, têm que definir qual é o âmbito essencial e têm que levar a cabo juízo negativo, concreto e fundamentado de afetação deste âmbito, sob pena de autorizarem intromissão inconstitucional e juridicamente inválida no patrimônio de direitos fundamentais da pessoa visada.

A decisão deve considerar, expressamente, o prognóstico de juízo negativo de afetação do direito essencial. Se a decisão não realiza esse juízo, não se pode presumir não ter sido afetado o direito essencial. Não há na hipótese presunção de legalidade.

Dispomos, pois, desse conjunto de tutelas que tem por alicerce o direito fundamental à autodeterminação informativa e que, alcançando a garantia contra a geolocalização contínua, protege as pessoas contra poderes extraordinariamente danosos.

Danosos às pessoas, lesivos à sociedade e corrosivos à liberdade.

Em linha gerais, é isso.

NOTAS

1. Ao julgar o Mandado de Segurança impetrado em face do Ministro de Estado de Justiça (SUPERIOR TRIBUNAL DE JUSTIÇA. Mandado de Segurança nº.STJ. MS 18.800/DF. Primeira Seção. Ministra Relatora Min. Rel. Eliana Calmon. Impetrante: Herika Teixeira Moreira. Autoridade Coatora: Ministro de Estado da Justiça. Data do julgamento:j. 11 de setembroset. de 2013) o STJ reconheceu a ilicitude da prática da chamada "barriga de aluguel". Trata-se de técnica por meio da qual o investigador acrescenta, indevidamente, ao rol das linhas telefônicas cuja interceptação pretende, número de telefone estranho à investigação. A frequência do emprego da providência ilícita levou o deputado Nelson Pellegrino (PT – BA) a sugerir no âmbito da CPI das Escutas Telefônicas criação de preceito dispositivo que relacionasse a decisão judicial a cada linha a ser mo-

nitorada. REVISTA CONSULTOR JURÍDICO. Policial é demitida por incluir telefone em grampo. (2013, outubro). Revista Consultor Jurídico, 1º de outubro de 2013. Disponível em. http://www.conjur.com.br/2013-out-01/policial-demitida-incluir-telefone-interesse-particular-grampo. Consultado em 07 de outubro de 2013. https://bit.ly/32dbKXN.

2. Convenção Americana sobre Direitos Humanos. Artigo 8. Garantias judiciais. 1. Toda pessoa tem direito a ser ouvida, com as devidas garantias e dentro de um prazo razoável, por um juiz ou tribunal competente, independente e imparcial, estabelecido anteriormente por lei, na apuração de qualquer acusação penal formulada contra ela, ou para que se determinem seus direitos ou obrigações de natureza civil, trabalhista, fiscal ou de qualquer outra natureza. 2. Toda pessoa acusada de delito tem direito a que se presuma sua inocência enquanto não se comprove legalmente sua culpa. Durante o processo, toda pessoa tem direito, em plena igualdade, às seguintes garantias mínimas: [...] g. direito de não ser obrigado a depor contra si mesma, nem a declarar-se culpada; Pacto Internacional Sobre Direitos Civis e Políticos. Artigo 14. 1. Todas as pessoas são iguais perante os tribunais e as cortes de justiça. Toda pessoa terá o direito de ser ouvida publicamente e com devidas garantias por um tribunal competente, independente e imparcial, estabelecido por lei, na apuração de qualquer acusação de caráter penal formulada contra ela ou na determinação de seus direitos e obrigações de caráter civil. [...] 3. Toda pessoa acusada de um delito terá direito, em plena igualmente, a, pelo menos, as seguintes garantias: [...] g) De não ser obrigada a depor contra si mesma, nem a confessar-se culpada.

3. A propósito: QUEIJO, M. E. (2012). *O direito de não produzir prova contra si mesmo*: o princípio nemo tenetur se detegere e suas decorrências no processo penal. 2ª edição. São Paulo: Saraiva., pp. 93-94, 96, 99, 239-242, 307-313. FERNANDES, A. S. (2012). *Processo penal constitucional*. 7ª edição. São Paulo: *Revista dos Tribunais*., pp. 264-265. GIACOMOLLI, N. J. (2014). O devido processo penal: abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica. São Paulo: Atlas., p. 193. MALAQUIAS, R. A. D. Princípio nemo tenetur se detegere no Estado Democrático de Direito. Revista dos Tribunais, vol. 941., p. 13. & GOMES, L. F. (2014) Capítulo VI: A) As garantias mínimas do devido processo criminal nos sistemas jurídicos brasileiro e interamericano: estudo introdutório. In: GOMES, L. F.; PIOVESAN, F. (coord.) (2000). *O sistema interamericano de proteção dos direitos humanos e o direito brasileiro*. São Paulo: Editora Revista dos Tribunais., p. 221.

4. VALENTE, M. M. G. (2008). *Escutas telefónicas*: da excepcionalidade à vulgaridade. 2ª edição. Coimbra: Almedina., p. 17.

5. HASSEMER, W. (2009). Verdad y búsqueda de la verdad en el proceso penal: La medida de la Constitución. México: Ubijus Editorial., p. 18.

6. ROXIN, C. (2008). La prohibición de autoincriminación y de las escuchas domiciliarias. Buenos Aires: Hammurabi., p. 86, 89, 106-107. Também: ROGALL, K. A, nova regulamentação da vigilância das telecomunicações na Alemanha. In: MENDESMendes, P. de S. & DIAS.; Dias, A. S.; & PALMA, M. F. (orgs.) (2010). 2º Congresso de Investigação Criminal. Coimbra: Almedina., p. 118. Os fundamentos são equivalentes às razões da edição da Lei nº 12.850/2013.

7. BverfGE 109, p. 279-391, referido por Claus Roxin em ROXIN, C. (2008). La prohibición de autoincriminación y de las escuchas domiciliarias. Buenos Aires: Hammurabi., p. 86. Também: ROGALL, K. A nova regulamentação da vigilância das telecomunicações na Alemanha. In: MENDES, P. de S.; & DIAS, A. S.; & PALMA, M. F. (orgs.) (2010). 2º Congresso de Investigação Criminal. Coimbra: Almedina., p. 118. Os fundamentos são equivalentes às razões da edição da Lei nº 12.850/2013.

8. § 100d, do Código de Processo Penal Alemão – Núcleo essencial da vida privada; pessoas autorizadas a se recusar a depor (1) Se houver elementos fáticos que permitam concluir que uma medida referida nos §§ 100a a 100c sozinha fornecerá conhecimento sobre o núcleo essencial da vida privada, a medida não será admissível. (2) As descobertas sobre o núcleo essencial da vida privada, adquiridas com base em uma das medidas referidas nos §§ 100a a 100c, não podem ser usadas. Os registros dessas descobertas devem ser excluídas imediatamente. O fato de essas informações terem sido obtidas e excluídas deve ser documentado. (3) Sempre que possível, relativamente às medidas mencionadas no § 100b, deve-se empregar meios técnicos para garantir que os dados referentes ao núcleo essencial da vida privada não sejam capturados. As constatações feitas, a partir das medidas mencionadas no § 100b, que dizem respeito ao núcleo essencial da vida privada, devem ser excluídas imediatamente ou submetidas pelo Ministério Público ao tribunal, que decidirá quanto à sua usabilidade e exclusão. A decisão do tribunal sobre a usabilidade dos dados será vinculativa em relação ao demais procedimentos. (4) As medidas previstas no § 100c podem ser ordenadas apenas se, com base em elementos fáticos, for possível concluir que declarações relativas ao núcleo essencial da vida privada não serão alcançadas pelo registro. O monitoramento e a gravação devem ser interrompidos imediatamente se houver indicação de que, durante o monitoramento, surgiram declarações sobre o núcleo essencial da vida privada. Nos casos em que uma medida tenha sido interrompida, ela poderá ser recomeçada, sujeita às condições da Sentença 1. Em caso de dúvida, o Ministério Público deve solicitar imediatamente uma decisão do tribunal quanto à interrupção ou continuação da medida; o § 100e, Ap. (5), aplica-se, no que couber. O Ministério Público também deve solicitar imediatamente ao tribunal uma decisão, se for possível que o uso das informações já obtidas seja proibido, nos termos do Aparato (2). O Aparato (3), Sentença 3, aplica-se, no que couber. (5) Nos casos mencionados no § 53, as medidas previstas nos §§ 100b e 100c são inadmissíveis; se, durante ou após a implementação da medida, se tornar evidente que existe uma

situação descrita no § 53, o Aparato (2) deve ser aplicado, no que couber. Nos casos descritos nos §§ 52 e 53a, as informações adquiridas por meio das medidas mencionadas nos §§ 100b e 100c podem ser usadas apenas se, levando em consideração a importância da relação de confiança subjacente, o uso não for desproporcional ao interesse em estabelecer os fatos ou determinar a paradeiro de um acusado. Aplica-se o § 160a, Ap. (4), no que couber. Tradução livre. No original: **Strafprozeßordnung (StPO) § 100d Kernbereich privater Lebensgestaltung; Zeugnisverweigerungsberechtigte** (1) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach den §§ 100a bis 100c allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig. (2) Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den §§ 100a bis 100c erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. (3) Bei Maßnahmen nach § 100b ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach § 100b erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der Staatsanwaltschaft dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend. (4) Maßnahmen nach § 100c dürfen nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Das Abhören und Aufzeichnen ist unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Ist eine Maßnahme unterbrochen worden, so darf sie unter den in Satz 1 genannten Voraussetzungen fortgeführt werden. Im Zweifel hat die Staatsanwaltschaft über die Unterbrechung oder Fortführung der Maßnahme unverzüglich eine Entscheidung des Gerichts herbeizuführen; § 100e Absatz 5 gilt entsprechend. Auch soweit für bereits erlangte Erkenntnisse ein Verwertungsverbot nach Absatz 2 in Betracht kommt, hat die Staatsanwaltschaft unverzüglich eine Entscheidung des Gerichts herbeizuführen. Absatz 3 Satz 3 gilt entsprechend. (5) In den Fällen des § 53 sind Maßnahmen nach den §§ 100b und 100c unzulässig; ergibt sich während oder nach Durchführung der Maßnahme, dass ein Fall des § 53 vorliegt, gilt Absatz 2 entsprechend. In den Fällen der §§ 52 und 53a dürfen aus Maßnahmen nach den §§ 100b und 100c gewonnene Erkenntnisse nur verwertet werden, wenn dies unter Berücksichtigung der Bedeutung des zugrunde liegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes eines Beschuldigten steht. § 160a Absatz 4 gilt entsprechend. (ALEMANHA. Strafprozeßordnung. Disponível em: https://www.gesetze-im-internet.de/stpo/index.html#BJNR006290950BJNE016803311. Consulta-

do em 22 de junho de 2020).https://bit.ly/2WfNHDU). Tradução livre. No original: Strafprozeßordnung (StPO) § 100d Kernbereich privater Lebensgestaltung; Zeugnisverweigerungsberechtigte (1) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach den §§ 100a bis 100c allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig. (2) Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den §§ 100a bis 100c erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. (3) Bei Maßnahmen nach § 100b ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach § 100b erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der Staatsanwaltschaft dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend. (4) Maßnahmen nach § 100c dürfen nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Das Abhören und Aufzeichnen ist unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Ist eine Maßnahme unterbrochen worden, so darf sie unter den in Satz 1 genannten Voraussetzungen fortgeführt werden. Im Zweifel hat die Staatsanwaltschaft über die Unterbrechung oder Fortführung der Maßnahme unverzüglich eine Entscheidung des Gerichts herbeizuführen; § 100e Absatz 5 gilt entsprechend. Auch soweit für bereits erlangte Erkenntnisse ein Verwertungsverbot nach Absatz 2 in Betracht kommt, hat die Staatsanwaltschaft unverzüglich eine Entscheidung des Gerichts herbeizuführen. Absatz 3 Satz 3 gilt entsprechend. (5) In den Fällen des § 53 sind Maßnahmen nach den §§ 100b und 100c unzulässig; ergibt sich während oder nach Durchführung der Maßnahme, dass ein Fall des § 53 vorliegt, gilt Absatz 2 entsprechend. In den Fällen der §§ 52 und 53a dürfen aus Maßnahmen nach den §§ 100b und 100c gewonnene Erkenntnisse nur verwertet werden, wenn dies unter Berücksichtigung der Bedeutung des zugrunde liegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes eines Beschuldigten steht. § 160a Absatz 4 gilt entsprechend. (ALEMANHA. Strafprozeßordnung. Disponível em: https://www.gesetze-im-internet.de/stpo/index.html#BJNR006290950BJNE016803311. Consultado em 22 de junho de 2020).https://bit.ly/2WfNHDU).

9. Art. 5º, CF. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos

termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [...] LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos.

10. VELASCO NÚÑEZ, E. (2016). Límites a las investigaciones y a la prueba en el proceso penal. In: *Delitos tecnológicos*: definición, investigación y prueba en el proceso penal. Madrid: Editorial Jurídica Sepín,., p. 17.

11. INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE) (2018). Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal: 2017. Rio de Janeiro. Informativo, 12 p., e Notas Técnicas, 93 p. Catálogo disponível em: https://biblioteca.ibge.gov.br/index.php/biblioteca-catalogo?view=detalhes&id=2101631. Informativo disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Notas técnicas disponíveis em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101621_notas_tecnicas.pdf. Consultado em: 23 de junho de 2020; INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). Catálogo disponível em: https://bit.ly/2CxKkAS. Informativo disponível em: https://bit.ly/30cVLqa. Notas técnicas disponíveis em: https://bit.ly/2ZncKXt; Instituto Brasileiro de Geografia e Estatística (IBGE). Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal 2018. Rio de Janeiro, 2020. Informativo, 12 p., e Notas Técnicas, 115 p Catálogo disponível em: https://biblioteca.ibge.gov.br/index.php/biblioteca-catalogo?view=detalhes&id=2101705. Informativo disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101705_informativo.pdf. Notas técnicas disponíveis em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101674_notas_tecnicas.pdf. Consultado em: 23 de junho de 2020. Catálogo disponível em: https://bit.ly/2AYEtEw. Informativo disponível em: https://bit.ly/3gVTEh8. Notas técnicas disponíveis em: https://bit.ly/3fsKA2N.

12. VELASCO NÚÑEZ, E. (2016). Límites a las investigaciones y a la prueba en el proceso penal. In: Delitos tecnológicos: definición, investigación y prueba en el proceso penal. Madrid: Editorial Jurídica Sepín., p. 22.

13. Tradução livre. No original: "Eine zeitliche und räumliche "Rundumüberwachung" wird regelmäßig schon deshalb unzulässig sein, weil die Wahrscheinlichkeit groß ist, dass dabei höchstpersönliche Gespräche abgehört werden. Die Menschenwürde wird auch verletzt, wenn eine Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können." ALEMANHA. Bundesver-

fassungsgerricht. Band 109, 279-323. Julgamento em 03 de março de 2004. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2004/03/rs20040303_1bvr237898.html. Consultado em 18 de junho de 2020.pp. 279-323. Julgamento em 03 de março de 2004. https://bit.ly/3fwQL6c

14. VELASCO NÚÑEZ, E. (2016). Límites a las investigaciones y a la prueba en el proceso penal. In: *Delitos tecnológicos*: definición, investigación y prueba en el proceso penal. Madrid: Editorial Jurídica Sepín., p. 25.

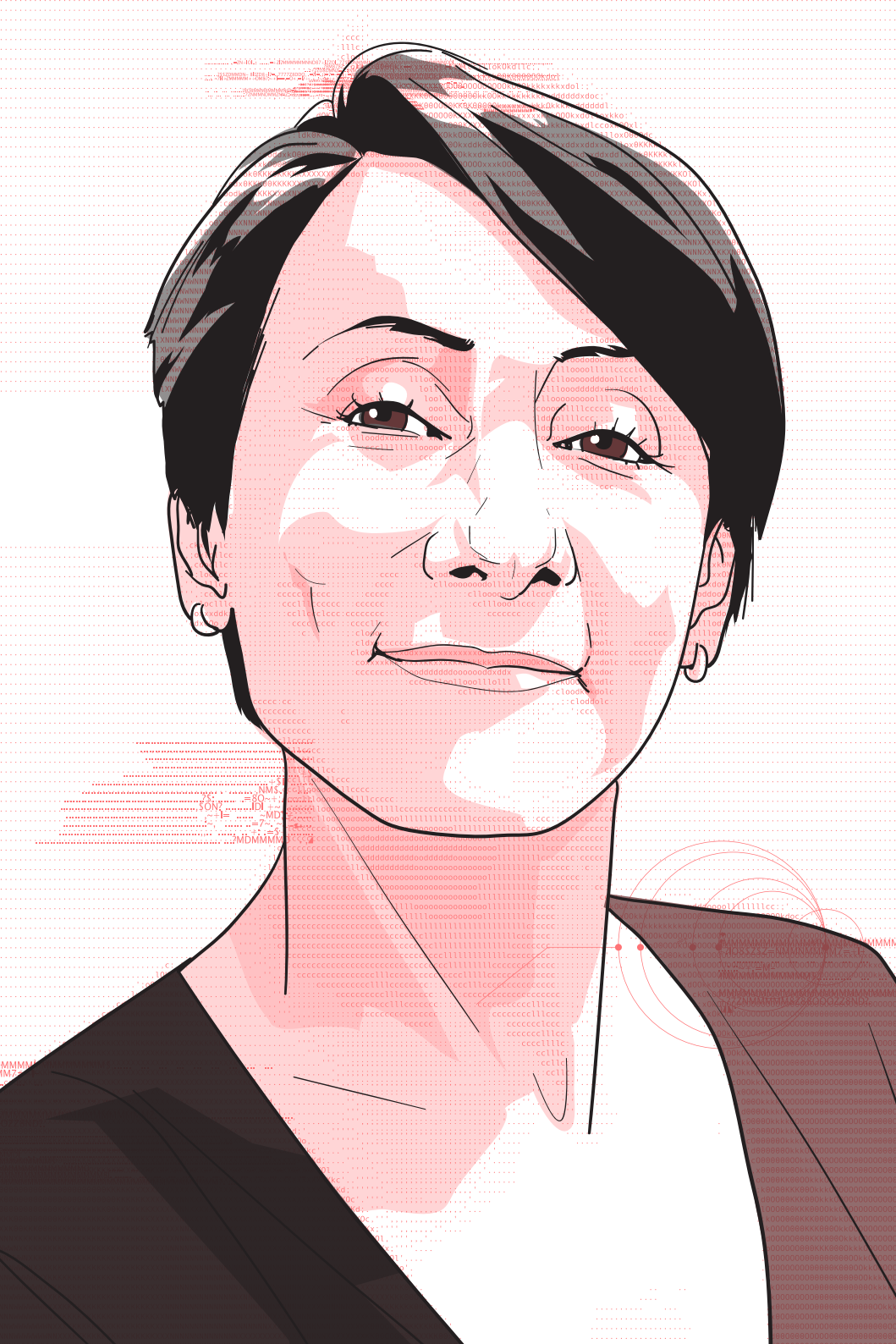
15. VELASCO NÚÑEZ, E. (2016). Límites a las investigaciones y a la prueba en el proceso penal. In: *Delitos tecnológicos*: definición, investigación y prueba en el proceso penal. Madrid: Editorial Jurídica Sepín., p. 25.

16. VELASCO NÚÑEZ, E. (2016)). Límites a las investigaciones y a la prueba en el proceso penal. In: *Delitos tecnológicos*: definición, investigación y prueba en el proceso penal. Madrid: Editorial Jurídica Sepín., p. 27.

17. Art. 13-A, CPP. Nos crimes previstos nos arts. 148, 149 e 149-A, no § 3º do art. 158 e no art. 159 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), e no art. 239 da Lei no 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos. (Incluído pela Lei nº 13.344, de 2016) (Vigência) Parágrafo único. A requisição, que será atendida no prazo de 24 (vinte e quatro) horas, conterá: (Incluído pela Lei nº 13.344, de 2016) (Vigência) I - o nome da autoridade requisitante; (Incluído pela Lei nº 13.344, de 2016) (Vigência) II - o número do inquérito policial; e (Incluído pela Lei nº 13.344, de 2016) (Vigência) III - a identificação da unidade de polícia judiciária responsável pela investigação. (Incluído pela Lei nº 13.344, de 2016) (Vigência). Art. 13-B, CPP. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso. (Incluído pela Lei nº 13.344, de 2016) (Vigência) § 1o Para os efeitos deste artigo, sinal significa posicionamento da estação de cobertura, setorização e intensidade de radiofrequência. (Incluído pela Lei nº 13.344, de 2016) (Vigência) § 2o Na hipótese de que trata o caput, o sinal: (Incluído pela Lei nº 13.344, de 2016) (Vigência) I - não permitirá acesso ao conteúdo da comunicação de qualquer natureza, que dependerá de autorização judicial, conforme disposto em lei; (Incluído pela Lei nº 13.344, de 2016) (Vigência) II - deverá ser fornecido pela prestadora de telefonia móvel celular por período não superior a 30 (trinta) dias, renovável por uma única vez,

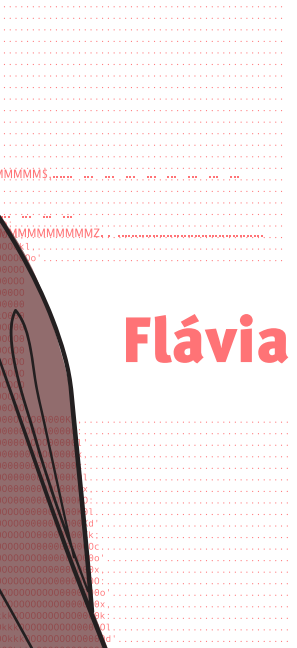
por igual período; (Incluído pela Lei nº 13.344, de 2016) (Vigência) III - para períodos superiores àquele de que trata o inciso II, será necessária a apresentação de ordem judicial. (Incluído pela Lei nº 13.344, de 2016) (Vigência) § 3º Na hipótese prevista neste artigo, o inquérito policial deverá ser instaurado no prazo máximo de 72 (setenta e duas) horas, contado do registro da respectiva ocorrência policial. (Incluído pela Lei nº 13.344, de 2016) (Vigência) § 4o Não havendo manifestação judicial no prazo de 12 (doze) horas, a autoridade competente requisitará às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, com imediata comunicação ao juiz. (Incluído pela Lei nº 13.344, de 2016) (Vigência).

18. RAMALHO, David Silva.Ramalho, D. (2017). *Métodos ocultos de investigação criminal em ambiente digital*. Coimbra: Edições Almedina, 2017. p. 249-250.



03.

DADOS DE DESLOCAMENTO E GEOLOCALIZAÇÃO: A INVESTIGAÇÃO EM TEMPO REAL



Flávia Mitri

Não sou uma advogada criminalista, só para acertar bem as expectativas! Quem aqui usa Uber? Espero que vocês, depois da conversa de hoje, passem a olhar aplicativo com carinho, porque eu quero contar para vocês o que acontece nos bastidores da operação do ponto de vista prático, no que se refere à entrega de dados, tanto para investigações policiais ou processos criminais e também do ponto de vista regulatório.

A Uber é regulada por autoridades municipais do Brasil na sua operação. Especificamente na cidade de São Paulo, existe uma regulação que nos pede um dado de latitude e longitude para o início e fim de cada viagem. A minha opinião, minha opinião pessoal e institucional de empresa, é que, a depender de quão detalhada for essa latitude e longitude, é possível saber exatamente o metro quadrado em que a pessoa entrou e saiu do carro. Eu não vejo utilidade alguma, para fins de políticas públicas, que o órgão regulador saiba o ponto de partida e de chegada de cada uma das viagens.

A Uber é uma empresa muito solitária nesse debate, porque os nossos concorrentes não têm a mesma preocupação com a exposição do comportamento de ida e vinda de seus usuários. E a gente briga muito por isso. Especificamente em São Paulo, o pedido original era de cinco dígitos de latitude e longitude, o que permitiria saber onde, em que número da rua, você entrou no carro e onde você desceu. Imagine uma pessoa que faz viagens diárias do ponto A ao ponto B, da sua casa a alguma entidade religiosa, a uma sede sindical, a uma clínica de saúde... Isso começa a revelar vários elementos da vida daquele indivíduo, que mesmo quando entregues anonimizados ao regulador podem ser facilmente analisados. Chega-se, assim, a um perfil comportamental que é muito delicado para nós, como integrantes da população.

Estou levantando isso, porque eu acho que a questão de geolocalização para o regulador ainda é confusa para que

eles entendam que esse dado é também um dado pessoal. A nossa briga é para que eles entendam que dado pessoal não é só o nome, CPF, endereço. Um dado que obviamente identifica uma pessoa, para mim, o dado de geolocalização entregue de forma massiva e recorrente é muito mais delicado do que eu entregar o nome, CPF, endereço.

Falemos agora da questão de requerimentos criminais. Diferente de muitas empresas de tecnologia, a Uber sempre adotou uma postura de cooperar com investigações criminais, porque nós temos todo interesse de ter a plataforma mais segura para os nossos usuários, sejam eles passageiros, motoristas, entregadores, ou as pessoas que pedem a sua comida através da nossa plataforma de delivery. Então, a Uber nunca se opôs a fazer entrega de dados, apesar de esses dados nunca terem sido exigidos no Brasil e nunca terem sido controlados pela entidade brasileira. Então, nunca recorremos ao argumento de que é necessário pedir um dado para a minha entidade controladora que fica baseada fora do Brasil. O que acontece especificamente com requisições policiais e criminais? Por ser uma empresa de tecnologia e um aplicativo de internet, nós somos regulados pelo Marco Civil e seu decreto regulamentador. Isso significa que a empresa é engessada para entrega de determinados dados dependendo da localização. Para ofícios policiais, o que o Marco Civil determina é que a gente só faz a entrega de dados cadastrais. Dado cadastral é definido por lei como o nome, a filiação, o que não permitiria, em tese, que uma autoridade policial conseguisse localizar aquele indivíduo.

A Uber adotou um entendimento mais flexível para entregar dados cadastrais, que são aqueles que as pessoas nos entregam no momento do seu cadastro na plataforma, considerando a necessidade de manutenção da plataforma mais segura. Então, para o motorista, entregamos os dados que ele

nos oferece no cadastro e, para o usuário, são basicamente nome, login, e-mail e celular. Quando existe uma autoridade policial que pede mais que dados cadastrais, há uma dificuldade frustrante de entender que a nossa recusa em fornecer esses dados não vem de uma vontade de desobedecer a ordem ou da falta de vontade de colaborar com a investigação, mas do Marco Civil e também da minha política de privacidade.

Frequentemente, temos que levar essa discussão para o Judiciário. No Judiciário, enfrentamos um outro problema: juízes que também não conseguem entender o Marco Civil e os limites que coloca. O que o Marco Civil também determina é que uma ordem judicial pedindo a entrega de dados é inválida em uma série de casos, como a ordem judicial com um pedido genérico. A Uber recebe centenas de ordens judiciais para a entrega de dados com mais ou menos a seguinte descrição: "Eu quero saber os dados cadastrais de todos os motoristas que dirigem um carro branco na cidade de Natal". Primeiro, não é possível fazer essa triagem na minha base, porque vão aparecer milhares de dados. Segundo, o que a polícia ou o Judiciário vão fazer com milhões ou milhares de dados do motorista só porque ele dirige um carro branco?

Se a ordem não é fundamentada, não indica natureza da investigação, ela é genérica. Nosso embate com o Judiciário é porque muitos juízes olham aquilo e falam: "mas a minha ordem não é genérica, eu estou pedindo o carro branco". Mas ela ainda é genérica, pela quantidade de dados envolvidos. Esse é um debate muito solitário, porque é muito difícil o processo de educação no que, efetivamente, pode ser entregue e o motivo pelo qual a empresa recusa a entrega. O motivo pelo qual a Uber se recusa fazer entrega nessas situações nunca é falta de vontade de cooperar, quero deixar isso muito claro, porque muitas vezes somos retratados na imprensa como uma empresa que desobedece, uma empresa disruptiva.

/ O DADO DE GEOLOCALIZAÇÃO ENTREGUE DE FORMA MASSIVA E RECORRENTE É MUITO MAIS DELICADO DO QUE O NOME, CPF, ENDEREÇO /

A Uber é altamente cooperativa para investigações policiais e criminais, sobretudo quando ela se refere a incidentes que ocorrem dentro da plataforma. Nós somos os maiores interessados em garantir que a plataforma seja segura, mas nós também somos os maiores interessados em proteger a privacidade das pessoas que usam a nossa plataforma.

Uma outra coisa acontece com o Uber. Existe um mito de que em algum momento todas as pessoas já pediram uma viagem, existe uma crença de que todo mundo está na nossa plataforma, então se o fulano, que cometeu um delito absolutamente dissociado da Uber, não é achado, a gente recebe uma ordem com um pedido de localização. Existe uma expectativa de que em algum momento esse fulano vai entrar em um carro que esteja na nossa plataforma. São ordens impossíveis de serem cumpridas, flagrantemente ilegais e que nos colocam numa posição muito complicada de ter que educar o Judiciário, educar a força policial, porque a gente não pode ceder a uma ordem que ou é ilegal ou se refere a um dado que eu simplesmente não tenho.

Um outro tipo de cenário que a gente enfrenta de maneira crescente no Brasil é a questão de monitoramento em tempo real, através de pedidos de policiais ou ordens judiciais criminais. A pessoa está sendo investigada por seja lá qual for o crime e aí a gente recebe uma ordem, usando por analogia a lei de interceptação telefônica, pedindo que a gente faça o monitoramento em tempo real daquela pessoa com a expectativa de que, no momento que a pessoa entrar em um carro, alguém da Uber de plantão ligue e comunique: "alô, delegado ou alô, juiz, fulano está indo do ponto A ao ponto B".

Tecnicamente não tem como isso ser implementado, ter uma equipe de plantão monitorando os nossos usuários ou nossos motoristas. Eu sei que, para quem está de fora, às vezes a impressão é que: "por que eles não simplesmente fa-

zem isso? deve ser muito fácil, porque não tem controle de todos os seus carros e onde estão todos os seus usuários?". Isso exigiria um plantão, em tempo permanente, para o reporte a uma autoridade sobre o local aonde os nossos usuários e nossos motoristas estão indo. Nós nos recusamos a fazer isso em todas as instâncias. Um pedido de monitoramento em tempo real, quando ele vem através de um ofício policial apenas, ele é muito fácil de ser derrubado, porque o Marco Civil não dá base à autoridade policial fazer esse tipo de requisição, sem uma ordem judicial que a suporte. Então, quando ele vem sem ordem judicial, o meu nível de preocupação é bem pequeno, porque é muito fácil de ser derrubado. Quando vem com ordem judicial, a preocupação é um pouco maior, porque o juiz precisa entender a nossa limitação técnica e entender que nós não somos uma empresa de telecom.

Então, o que a gente oferece [nesses casos] é o seguinte: primeiro tentamos entender qual é o crime que está sendo investigado, porque nós não nos sentimos à vontade de ficar fazendo esse tipo de "monitoramento" sem ter ideia do que está acontecendo. Se se trata de pessoa acusada de tráfico ou homicídio, eu também tenho interesse em não a ter na minha plataforma. Então, tomamos uma medida, porque quando somos informados de um crime cometido por uma determinada pessoa, temos a prerrogativa de removê-la da plataforma pelo compromisso que temos com todos vocês de que a plataforma será o mais segura que nós podemos oferecer.

Conhecendo a natureza do crime, e sendo um crime para o qual faça sentido que haja aquele monitoramento, há dois cenários: muitas vezes temos uma ordem de sigilo, o que nos impede de tomar qualquer ação com relação àquele usuário, porque tem uma investigação em curso. Se bloquearmos a pessoa, ela poderia descobrir a investigação e sumir mais uma vez. Se não há essa obrigação de sigilo, fazemos o "mo-

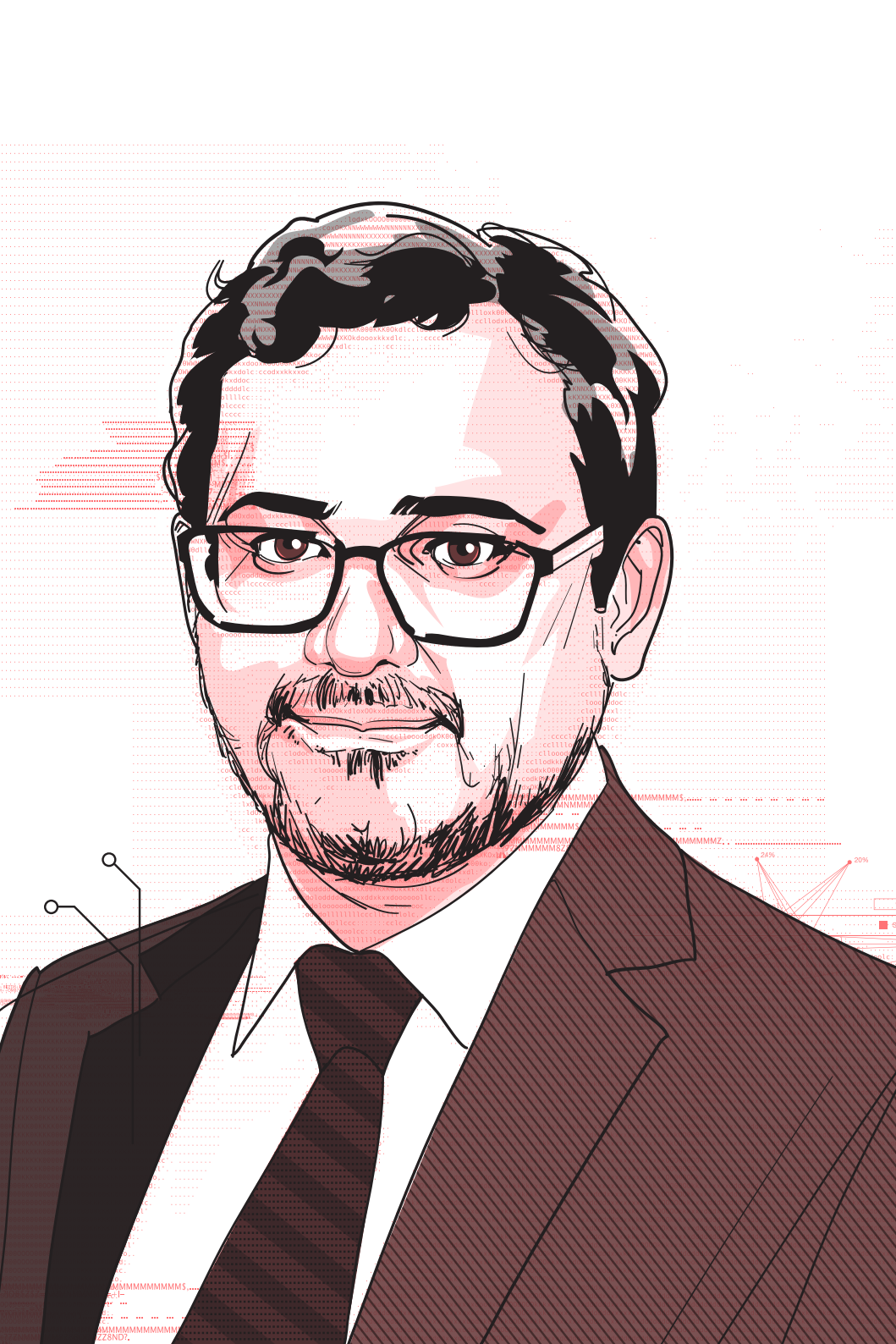
nitoramento", que funciona da seguinte forma: durante o período de 15 dias, que é o mesmo da lei de interceptação, a gente reporta para a autoridade requisitante a cada três dias todas as viagens que aquela pessoa realizou, com itinerário.

O único cenário em que a Uber entrega itinerário de viagem é quando tem uma ordem judicial que fundamente o pedido. Esse é um outro ponto que nós temos muito atrito com a polícia, porque eles às vezes não entendem que, em função do Marco Civil, eu não posso entregar uma rota de viagem sem ordem judicial. O Marco Civil é super limitante para empresas de tecnologia, quanto ao que elas podem entregar, em termos de dados pessoais sem uma ordem judicial. E a gente tem um departamento que faz, especificamente, educação externa para órgãos requisitantes de dados, porque é compreensível. Afinal, não são todas as empresas que são sujeitas ao Marco Civil; são poucas, mas precisam cumprir a lei. E para cumprir a lei, eu não posso atender a um ofício policial que me peça algo além de dados cadastrais sem uma ordem judicial.

Eu queria trazer essa explicação para vocês, porque eu acho que esse é um trabalho de muito pouca visibilidade da Uber. E, eu, como usuária, quando entrei na empresa, fiquei muito confortável de ver a precaução no tratamento dos dados da sua base e na entrega dos dados quando essa requisição chega.

Eu espero que essa fala breve tenha dado a vocês um pouco de conforto e nos ajude a criar um debate, como sociedade civil, sobre o perigo dessas requisições de dados de deslocamento, sejam requisições regulatórias, sejam requisições ligadas a uma investigação criminal. Eu não acho que as pessoas têm a noção real da quantidade de informação que você pode traçar acerca de determinado indivíduo a partir de dados de geolocalização. Imaginem isso com as operações variadas, a operação de bicicleta e scooter que temos fora do país e, felizmente, está chegando em breve a São Paulo: nas cidades

em que operamos alguns dos reguladores pediam identificação nominal de cada um desses usuários e rotas de viagem. A Uber nesses casos prefere nem entrar na cidade, não lançar aquela operação, porque entendemos que é mais precioso garantir privacidade na nossa base do que o crescimento ou ganho econômico. 



04.

INVESTIGAÇÃO EM TEMPO REAL: A LEI Nº 13.344/2016 E AS NOVAS TÉCNICAS DE GEOLOCALIZAÇÃO DE VÍTIMAS E SUSPEITOS DE CRIMES DE TRÁFICO DE PESSOAS.

Cleopas Isaías Santos

Samyr Béliche Vale

INTRODUÇÃO

Entre as mudanças trazidas pela Lei nº 13.344/2016, a de maior ressonância na investigação policial, seja pelo ineditismo, seja pelas dúvidas sobre sua constitucionalidade ou eficácia, segundo reputamos, é a prevista no novo art. 13-B do CPP.[1]

De acordo com este dispositivo, quando necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o delegado de polícia poderá requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso. Esta é uma medida inédita no nosso sistema processual, tanto no que tange à sua natureza quanto no que diz com sua sistemática. E em razão disso, será certamente a mais questionada em relação à sua adequação constitucional.

Essas empresas, conforme dispõe o art.13-B, *caput*, devem disponibilizar os meios técnicos adequados – como sinais, informações e outros – que permitam a localização de vítimas e suspeitos dos crimes referidos, mais especificadamente, a localização dos dispositivos móveis dos envolvidos no delito em curso. O legislador define sinal como o posicionamento da estação de cobertura, setorização ou intensidade de rádio frequência (art.13-B, § 1º).

A mencionada lei de 2016 proporciona ao delegado de polícia – através dos meios técnicos mencionados – maior autonomia para desempenhar suas atividades com eficácia e celeridade durante o procedimento investigatório, no intuito de identificar a localização dos usuários de dispositivos móveis durante um crime em curso.

Embora as outras mudanças trazidas pela Lei nº 13.344/2016 sejam relevantes e dignas de análise em apartado, nesta oca-

são, nosso interesse cognitivo será voltado à análise da eficácia e das limitações dos meios técnicos legais que podem ser utilizados como instrumento de localização de vítimas e suspeitos. O objetivo deste artigo, portanto, é responder o seguinte problema: os meios técnicos disponíveis e normalmente utilizáveis são eficazes para a localização de vítimas e suspeitos de crime de tráfico de pessoas? Para tanto, parte-se da hipótese de que os meios técnicos normalmente utilizados nesse processo não são eficazes.

Desse modo, far-se-á uma análise da eficácia da localização utilizando os sinais de radiofrequência, bem como das outras tecnologias disponíveis para a localização dos dispositivos, encontradas na literatura científica sobre o tema e já utilizadas pela polícia investigativa estrangeira. Será também objeto deste trabalho a identificação da legalidade dessas demais técnicas na legislação brasileira e sua conformação constitucional.

Antes, porém, é importante que analisemos a natureza jurídica dessa novel medida de investigação.

1. NATUREZA JURÍDICA E OUTROS ASPECTOS DA MEDIDA PREVISTA NO ART. 13-B DO CÓDIGO DE PROCESSO PENAL

Entendemos que a nova ferramenta investigativa, prevista no art. 13-B do Código de Processo Penal, possui natureza jurídica de medida cautelar probatória ou de meio de obtenção de prova, que visa a localização de investigados e vítimas de crimes relacionados ao tráfico de pessoas. Mostra-se, portanto, como uma medida eficaz tanto para a cessação do estado flagrancial, com a consequente prisão dos autores e asseguramento dos elementos de prova porventura encontrados e essenciais ao desenvolvimento de uma regular investigação dos crimes praticados, quanto para a salvaguarda da vítima. A redação do mencionado dispositivo não possui a melhor

técnica legislativa, pois, ao mesmo tempo em que diz que o delegado de polícia poderá requisitar às empresas de telefonia ou telemática que disponibilizem os referidos meios técnicos, condiciona tal requisição à autorização judicial. Ou seja, aparentemente, de requisição não se trata, pois quem requisita, ordena. Parece, de início, tratar-se de representação, como ocorre normalmente com a iniciativa da autoridade policial em provocar o judiciário pela decretação das demais medidas cautelares. Essa aparente contradição e atécnica legislativa já enseja divergências doutrinárias.

Guilherme Nucci considera esse aspecto "um ponto bizarro da nova Lei, pois, se é o delegado ou membro do Ministério Público que requisita (exige o cumprimento por força de lei), tal medida independe de outra autoridade, no caso a judicial, autorizar. No entanto, cuidando-se de invasão da intimidade/privacidade, pois gera a localização da vítima ou dos suspeitos (hipóteses diversas de simples registro cadastral), depende-se de autorização judicial. Assim sendo, quem, na verdade, *requisita* o meio técnico adequado para a localização de vítima/suspeito é a autoridade judiciária."[2]

Outro não é o entendimento de Renato Brasileiro, para quem o art. 13-B é inconstitucional, uma vez que o acesso, pelo delegado de polícia, à localização de vítimas e suspeitos de crimes de tráfico de pessoas afeta a própria privacidade e a intimidade, as quais somente poderão ser restringidas mediante autorização judicial.[3] Também consideram inconstitucional o citado dispositivo, por dispensar a ordem judicial, Rogério Sanches e Ronaldo Batista, para os quais "ou bem se entende que a ordem judicial é necessária e pouco importa o tempo que o juiz demorará para proferir a decisão, ou bem se entende que a diligência em estudo prescinde do filtro judicial e, por consequência, não será o atraso de 12 horas que impedirá sua efetivação."[4]

Não obstante o respeitável posicionamento dos autores citados, entendemos que a medida é constitucional, que se trata mesmo de requisição e, como tal, não se submete à reserva de jurisdição. E assim pensamos pelas seguintes razões.

A uma, porque os sinais, informações e outros meios técnicos que possibilitem localizar vítimas e investigados não são protegidos por sigilo. Estamos de acordo com a doutrina acima referida, no sentido de que os dados e outros meios que possibilitem a localização de suspeitos e vítimas, nos crimes relacionados ao tráfico de pessoas, encontram-se no âmbito de incidência do direito à privacidade e/ou intimidade.[5] Contudo, "a intimidade que está protegida constitucionalmente é o uso legítimo do direito à intimidade,"[6] não podendo, pois, ser anteparo para a prática de crimes. O que se tem, de maneira ampla, tal qual prevista no texto constitucional, é o que, no direito norte-americano, se convencionou chamar de "expectativa razoável de privacidade" (*reasonable expectation of privacy*).[7] Além disso, "perceba que a cláusula de respeito à intimidade e à privacidade, prevista no inc. X, não está submetida expressamente ao princípio da reserva de jurisdição, ou seja, não pressupõe uma ordem judicial para ser restringida."[8]

A duas, essa medida só pode ser requisitada quando algum dos crimes acima elencados estiver em curso. E todos são crimes permanentes, ensejadores, portanto, de medidas restritivas de direitos fundamentais importantes, como a inviolabilidade do domicílio e até mesmo a liberdade de locomoção, já que estariam em situação flagrancial. Veja-se que a casa é, por excelência, o espaço de proteção da privacidade e intimidade, razão pela qual o constituinte a considera inviolável, inviolabilidade essa que só poderá ser afastada nas hipóteses de situação flagrancial de crime, de prestação de socorro ou, durante o dia, para cumprir ordem judicial. Desse modo, inegavelmente, "a Constituição afasta a intimidade e a

inviolabilidade do domicílio de quem está em flagrante delito, autorizando qualquer pessoa do povo a ingressar no domicílio e efetuar a prisão em flagrante."[9]

A três, esta medida não permitirá o acesso ao conteúdo da comunicação de qualquer natureza. Caso se deseje ter acesso também ao conteúdo, será necessário autorização judicial, conforme disposto na Lei nº 9.296/1996 e previsto no § 2º, inc. I, do art. 13-B do CPP. A *contrario sensu*, o acesso apenas à localização de vítimas e investigados não depende de autorização judicial.

A quatro, nas hipóteses autorizadoras da requisição desses dados de localização, por serem todos de crimes permanentes e por estarem em curso, portanto, em situação flagrancial, a requisição do delegado de polícia seria lícita, pois acobertada pelo manto de uma causa excludente de antijuridicidade:[10] ou estrito cumprimento de um dever legal, ou legítima defesa de terceiro, ou ainda, em estado de necessidade de terceiro, já que, nos crimes relacionados ao tráfico de pessoas, existirá sempre uma vítima em situação de ameaça, restrição forçada de sua liberdade e até mesmo sob risco de morte.

A cinco, pela leitura conjunta dos incs. II e III do § 2º do mencionado art. 13-B, a autorização judicial só seria necessária para o fornecimento das informações requisitadas por período superior a 60 (sessenta) dias. Ou seja, até este prazo, ela seria dispensável.

Por todas essas razões é que entendemos que o fornecimento dos meios técnicos para se localizar vítimas e investigados nos crimes de tráfico de pessoas não depende de autorização judicial.

O que, segundo o dispositivo, depende de autorização judicial, embora também sem qualquer lógica ou parâmetro na nossa sistemática processual, é a própria requisição da autoridade policial. Ou seja, o Delegado de Polícia precisará de

/ O FORNECIMENTO DOS MEIOS TÉCNICOS PARA LOCALIZAR VÍTIMAS E INVESTIGADOS NOS CRIMES DE TRÁFICO DE PESSOAS NÃO DEPENDE DE AUTORIZAÇÃO JUDICIAL /

/ O QUE DEPENDE DE AUTORIZAÇÃO JUDICIAL, EMBORA TAMBÉM SEM QUALQUER LÓGICA, É A PRÓPRIA REQUISIÇÃO DA AUTORIDADE POLICIAL /

autorização judicial para requisitar os dados de localização. Entretanto, se autorizado, ele próprio irá fazer a requisição. E mais! Apenas como regra, pois, se não houver manifestação judicial no prazo de 12 (doze) horas, a autoridade competente requisitará às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, comunicando imediatamente ao juiz, conforme previsto no § 4º do art. 13-B, o que ratifica que essa medida não está submetida à reserva de jurisdição.

Aury Lopes Jr. adota um posicionamento intermediário, entendendo que esse meio investigatório exige, como regra, autorização judicial, "[...] mas, se não houver manifestação do juízo no prazo de 12 horas, a autoridade requisitante (polícia ou MP) poderá fazê-lo diretamente à empresa prestadora de serviço de telecomunicações e/ou telemática."[11]

Sabe-se que a doutrina é uníssona no sentido de afirmar que a jurisdicionalidade (judicialidade ou reserva de jurisdição) é princípio reitor das medidas cautelares. Ou, de outro modo, que as medidas cautelares no processo penal somente poderiam ser decretadas por ordem judicial[12]. Apesar disso, e estranhamente, a doutrina também não diverge quanto à possibilidade de a autoridade policial (e até mesmo o Ministério Público, em alguns casos), determinar a prática de diversas medidas de caráter cautelar, a exemplo da própria prisão em flagrante (não se desconhece a discussão acerca de sua natureza subcautelar[13] ou pré-cautelar[14]); da requisição de dados cadastrais de suspeitos e vítimas de crimes; fiança; da identificação criminal do indiciado; da apreensão,[15] seja quando decorrente de busca pessoal, seja em outras hipóteses em que o delegado de polícia não dependerá de autorização judicial para apreender o que interessar à investigação.

Desse modo, apesar de a maioria das medidas cautelares penais encontrarem-se acobertadas pela reserva de jurisdição, nenhum problema, técnico ou de legitimidade, haverá na atribuição, pelo legislador ordinário, a outras autoridades, como delegados de polícia, membros do Ministério Público ou parlamentares (quando membros de CPI's), de poder para determinar ou decretar medidas cautelares penais.

Vejamos agora os aspectos técnicos dessa nova medida cautelar, essenciais para alcançarmos o objetivo principal deste trabalho.

2. REDES MÓVEIS

Notícia veiculada pela Revista Exame em 22 de abril 2016 informou que o brasileiro utiliza mais o aparelho celular do que o computador pessoal para acessar a Internet. O ano de 2015 encerrou-se com 191,8 milhões de acessos 3G e 4G. O Brasil, em 2014, já era o sexto maior mercado da venda de *smartphones*. Revelou ainda que a grande maioria dos seus usuários não sai de casa sem o dispositivo.[16]

Um *smartphone* é um tipo de dispositivo móvel que se constitui em um equipamento telefônico que inclui recursos computacionais, interfaces de redes, sistema operacional e que é capaz de executar aplicações. As redes celulares foram estendidas para dar suporte, além da comunicação vocal, ao acesso à rede mundial de computadores, capacitando o telefone celular com recursos de acesso e troca de dados e serviços. A comunicação entre esses dispositivos se dá através do uso de diferentes tecnologias que constituem uma grande infraestrutura denominada de redes móveis.

A Estação Rádio Base (ERB) é um importante mecanismo dessa infraestrutura, sendo responsável pela transmissão e recebimento de voz e dados de um dispositivo que está ligado a ela. Cada estação base recebe e envia informações ao

dispositivo móvel e se conecta a outras redes (à Internet, inclusive). Uma ERB fornece, ao mesmo tempo, serviços para vários dispositivos móveis.

Ao se conectar a uma ERB, o dispositivo recebe todos os serviços de rede disponíveis pela empresa prestadora de serviços. Isso inclui a criação de um enlace (*link*) direto entre o dispositivo e a ERB, bem como a distribuição de endereços lógicos de identificação (endereço IP - *Internet Protocol*).[17]

As ERB's compreendem antenas que emitem sinais de radiofrequência -.dispostas em torres de transmissão - e que fornecem sinais que abrangem uma área geográfica (de cobertura) denominada célula -, normalmente representados sobre um formato de hexágono. Células adjacentes possuem faixas de frequência diferentes, evitando interferência entre os serviços fornecidos por diferentes antenas, conforme ilustrado pela Figura 1.

Segundo Kurose e Ross,[19] a área de cobertura de uma célula depende de vários fatores, tais como: potência de transmissão da antena e do dispositivo móvel do usuário; tipo, altura e posicionamento da antena, faixa de frequência utilizada, obstáculos (como prédios), dentre outros. As antenas transmitem sinais de rádio de maneira unidirecional ou omnidirecional (em várias direções), dependendo do seu tipo.

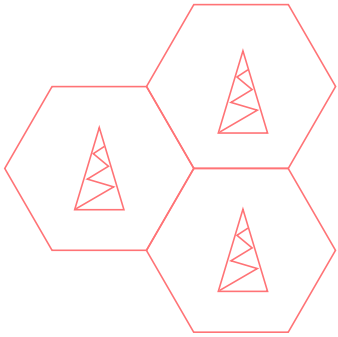


FIGURA 1: ANTENAS DE TRANSMISSÃO E CÉLULAS[18]

O número de telefone do dispositivo móvel não identifica a localização física do mesmo, como acontece com as linhas fixas. São os dígitos iniciais que permitem a identificação da rede de origem da linha telefônica. A rede nativa do telefone mantém um Registro Nativo de Localização (*Home Location Register* - HLR).

Em caso de *roaming*, os centros de comutação móveis (*Mobile Switching Center* - MSC) demandam ao HLR que localize o dispositivo móvel. Neste caso, o dispositivo móvel recebe um número efêmero,[20] o qual é fornecido pelo HLR de maneira temporária, através de um serviço semelhante ao de distribuição de um endereço IP. O MSC nativo, em sequência, estabelece a conexão com o MSC visitado e, por sua vez, com a ERB que está atendendo o usuário móvel naquele momento.

Quando o usuário móvel – utilizando os serviços de telefonia – está em trânsito e ultrapassa os limites de determinada célula, é necessário que se faça uma transferência (denominada de handoff) entre ERBs. Outros fatores que demandam o handoff são: degradação do sinal da ERB que fornece o serviço, sobrecarga das células mediante grande número de conexões, entre outros.

3. EFICÁCIA DOS MEIOS TÉCNICOS LEGAIS PARA A COLETA DE DADOS E INFORMAÇÕES POR MEIO DE DISPOSITIVOS MÓVEIS

Como já anunciado, a Lei nº. 13.344/2016 ampliou significativamente o poder requisitório do delegado de polícia, especialmente com o novel e especial meio de investigação de acesso aos meios técnicos adequados à localização de vítimas e suspeitos de tráfico de pessoas.

Com efeito, como assevera Aury Lopes Jr.[21], por meio da redação do art. 13-B, pode-se depreender ser possível a obtenção da localização do suspeito (ou vítima) através do posicio-

namento da estação de cobertura, setorização e intensidade de radiofrequência. Essas informações são fornecidas pela Estação Rádio Base (ERB), acionada quando da realização ou recebimento das chamadas do telefone celular da vítima (ou dos suspeitos), relacionados aos crimes de tráfico de pessoas.

O mesmo autor afirma ainda, com acerto, que os dados de localização, fornecidos pela empresa de telecomunicações, indicam apenas uma localização aproximada do dispositivo móvel e que estas informações não podem ser confundidas com seu conteúdo, ao qual somente se terá acesso mediante autorização judicial, nos termos da Lei n.º 9.296/96.[22]

É precisamente a eficácia da localização do dispositivo móvel, através da técnica de medição da intensidade do sinal, que norteia a presente investigação e sobre a qual passamos a analisar.

A Associação Nacional de Advogados de Defesa Criminal dos EUA utiliza duas das técnicas existentes para a localização de um dispositivo móvel celular, quais sejam: a Informação da Localização pelo Local da Célula (CSLI) e o Sistema de Posicionamento Global (GPS). Ademais, um dispositivo móvel pode ser localizado pela técnica do Sistema de Posicionamento Baseado em Wi-Fi.

Pela técnica do CSLI, a posição do dispositivo móvel é localizada mediante a intensidade do sinal de transmissão entre o aparelho e a Estação Rádio Base (ERB). Essa é a técnica autorizada, como regra, pela Lei nº. 13.344/2016. Passemos à sua análise.

Como a ERB fornece serviço a uma área de cobertura com até quilômetros de distância, através de sinal de radiofrequência – normalmente, transmitidos em diversas direções –, a identificação da ERB que está fornecendo serviço a um dispositivo não permitirá sua localização precisa. Através deste recurso, ter-se-á apenas a área de cobertura em que o usuário móvel se encontra. Uma possível análise, à distância, da in-

tensidade do sinal de recepção do aparelho fornecerá estimativas quanto à sua proximidade da torre de transmissão.

Esta técnica, por si só, mostra-se ineficaz para a localização de um indivíduo, não contribuindo, assim, com a investigação policial que estiver em curso.

3.1. TRIANGULAÇÃO E TRILATERAÇÃO

A literatura científica sobre o tema da localização por meio da intensidade do sinal apresenta dois métodos que permitem uma maior acurácia na identificação do posicionamento do dispositivo móvel, a saber: a triangulação e a trilateração.

Sem olvidar do propósito deste artigo, que se concentra na análise da eficácia, apresentaremos esses métodos, sem aprofundamentos quanto aos cálculos matemáticos ou algoritmos que os envolvem.

A triangulação, segundo Roxin *et al.*,[24] permite a estimação da direção de chegada do sinal do dispositivo móvel pela intersecção da identificação de seu sinal por três torres (ERB) adjacentes.

Na trilateração - um avanço da triangulação -, segundo o mesmo autor, é calculada a distância entre a ERB e o dispositivo móvel, por meio da análise da força do sinal recebido pelo aparelho (*Received Signal Strength* – RSS). Esta análise é realizada através de um algoritmo matemático que envolve como parâmetro o raio de alcance do sinal, também calculado pela intersecção entre três torres. A figura 2 ilustra este princípio.

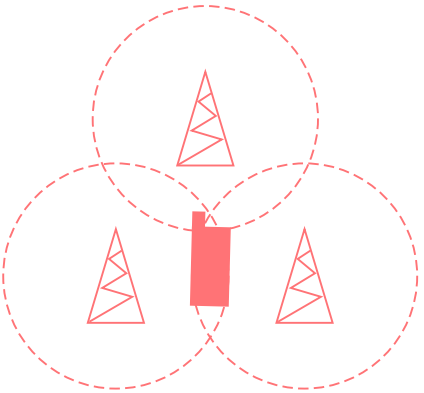


FIGURA 2: INTERSECÇÃO DO RAIO DE COBERTURA DE TRÊS TORRES[25]

As técnicas mencionadas para localização do dispositivo por meio da análise da intensidade do sinal, e que se interpreta como estando entre as permitidas pelo texto legal, quando menciona o referido termo, explicando o seu significado (§ 1º do art. 13-B), são, a saber: "posicionamento da estação de cobertura, setorização e intensidade de radiofrequência."

As técnicas baseadas em RSS não apresentam acurácia nem precisão na localização do dispositivo, fornecendo informação de posicionamento do dispositivo móvel com margem de erro de até centenas de metros. A imprecisão aumenta em área rural ou de baixa densidade populacional, pois, pelo maior espaçamento entre as células (ou seja, entre as ERBs), a triangulação/trilateração se torna menos eficaz.

Outros algoritmos matemáticos podem ser utilizados em técnicas de mapeamento - frutos de pesquisas científicas sobre o problema da geolocalização - para aumentar a precisão do cálculo do posicionamento mediante a análise do sinal (permitida pela lei em análise). Nada obstante, necessitam de um conjunto complexo de parâmetros, como: altura precisa

da torre, posição da antena na torre, ângulo de inclinação da antena, real intensidade do sinal no instante da análise, tempo de chegada do sinal, análise dos obstáculos que as ondas de radiofrequência atravessam, entre outros. O esquema da Figura 3 ilustra alguns parâmetros utilizados nessa análise.

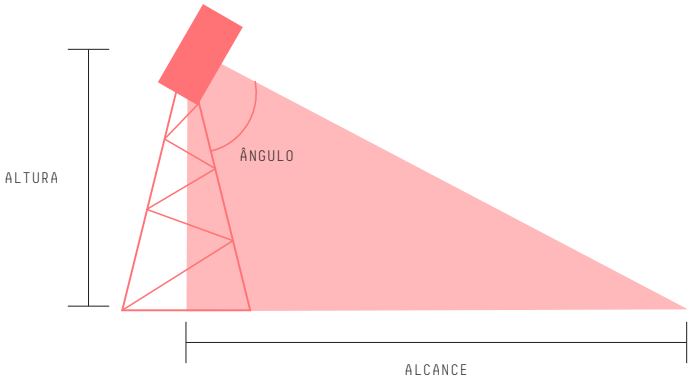


FIGURA 3: ALGUNS PARÂMETROS UTILIZADOS PARA AUMENTAR A ACURÁCIA NA LOCALIZAÇÃO[26]

Mesmo que seja possível a inferência de tais fatores, e que a prestadora de serviços de telecomunicações possua recursos humanos e materiais para calculá-los, a localização pela análise do sinal continuará sendo uma tarefa demorada e imprecisa. Yassin e Rachid[27] também corroboram esse entendimento ao relatarem os problemas da acurácia das técnicas de CSLI em virtude da interferência e variedade de direções das ondas de radiofrequência.

3.2. OUTRAS TÉCNICAS DE LOCALIZAÇÃO

Técnica mais moderna de geolocalização, e que fornece precisão muito maior - com margem de erro de centímetros - na identificação do posicionamento do dispositivo móvel celular, é o GPS (*Global Position System*). Para Roxin *et al.*,[28] o GPS

é considerado o dispositivo de localização outdoor de maior precisão, e é um recurso presente na grande maioria dos dispositivos móveis disponíveis no mercado. Nada obstante, os dados de localização não são fornecidos pela Estação Rádio Base (ERB), mas por satélites.

Os satélites que orbitam em torno da Terra fornecem a posição do dispositivo móvel do usuário através de sinais de *broadcasting* contínuos, informando o posicionamento e a direção em caso de deslocamento. A distância entre o satélite e o receptor é calculada pelo tempo preciso que o sinal leva até chegar ao seu destino.[29] Aqui a técnica utilizada também é a trilateração, porém, livre das interferências que acometem a localização CSLI.

Yassin e Rachid[30] também apresentam gráfico comparativo sobre a acurácia da localização por meio das técnicas mencionadas, que mostram o GPS com acurácia muito superior à identificação do celular por intensidade do sinal de rádio.

A *Mobile Marketing Association* (MMA)[31] publicou documento que trata da acurácia de dados de localização de dispositivos móveis. No referido artigo, esclareceu que a acurácia (exatidão) se relaciona com a localização real do dispositivo no momento da medição; e precisão refere-se à proximidade de duas ou mais medições entre si. A Figura 4 elucida estes termos técnicos.

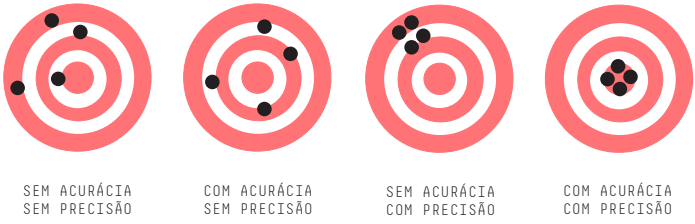


FIGURA 4: ACURÁCIA E PRECISÃO NA LOCALIZAÇÃO DE DISPOSITIVOS MÓVEIS [ADAPTADO DE *MOBILE MARKETING ASSOCIATION*]

A MMA também esclarece que o GPS possui maior acurácia e precisão; e que a triangulação celular possui acurácia, mas constitui-se em técnica imprecisa – sendo mais adaptada para localização por vizinhança.

Ademais, as vantagens da localização por GPS em relação ao CSLI, os sistemas operacionais dos dispositivos móveis (*e.g.* IOS e *Android*) fornecem, nativamente, serviços de localização por meio de aplicativos computacionais. Outros inúmeros *softwares* também são encontrados para localizar o dispositivo móvel em casos de perda ou furto. Outros sensores, também disponíveis em diversos smartphones, permitem, por meio desses aplicativos que rodam no sistema operacional do dispositivo, incrementar a acurácia com dados de altitude e velocidade de deslocamento. Informações como endereço IP do dispositivo também são úteis no processo de localização.

A localização através da tecnologia GPS pode se enquadrar em "outros" meios técnicos dos quais faz referência o citado art. 13-B, do CPP, não se tratando, portanto, de prova atípica, aplicável por analogia ou interpretação extensiva.[32] Em verdade, estamos diante de uma interpretação analógica, o que está de acordo com o princípio da legalidade. Entretanto, alguns detalhes técnicos são necessários para a utilização deste recurso – mais rápido e preciso de localização –, de acordo com as situações que se esmiúçam a seguir:

I) *Dispositivo possui pacote de dados habilitado e a antena GPS está habilitada*: constitui-se no cenário ideal e mais simples para captura da informação desejada, *i.e.*, a identificação remota dos dados de localização é imediata. Inclusive com possibilidade de acesso, não só ao posicionamento atual, como ao histórico de navegação do GPS. Há, ademais, aplicativos nativos de alguns sis-

temas operacionais de *smartphones* e *tablets* que permitem tal localização automática, como um serviço de auxílio de localização em caso de perdas.

II) *Dispositivo possui pacote de dados habilitado e a antena GPS está desabilitada:* a prestadora de serviços deve usar recurso tecnológico necessário para habilitação remota da antena GPS, para então capturar as informações de localização.

III) *Dispositivo não possui pacote de dados habilitado e a antena GPS está habilitada*: a provedora de serviços deve habilitar remotamente um pacote de dados para aquela linha telefônica, a fim de que se possa capturar as informações de localização, haja vista que os dados de localização são transmitidos por pacote de dados e não por cálculo de intensidade do sinal de radiofrequência.

IV) *Dispositivo não possui pacote de dados habilitado e antena GPS está desabilitada*: a prestadora de serviços deve habilitar remotamente tanto o pacote de dados quanto a antena GPS.

Faz-se necessário esclarecer que, em todos os casos supracitados, a habilitação/utilização de um pacote de dados gerará um ônus financeiro cuja responsabilidade deve ser questionada, se pertencente ao Estado, à provedora de serviços de telefonia, à vítima ou ao suspeito. Para o caso da simples captura da localização atual do dispositivo, não há que se falar em ônus substancial; nada obstante, o mesmo não acontece com um monitoramento da navegação do dispositivo durante um intervalo considerável de tempo, ou seja, a análise da movimentação do aparelho.

Ademais, conforme mencionado nos itens (ii) e (iv), a habilitação remota da antena GPS requer – em caso de não haver aplicativos gerenciadores de localização pré-instalados e configurados no dispositivo – o acesso remoto ao aparelho para instalação de aplicativos/serviços que venham habilitar o dispositivo de localização por GPS.

A análise da intensidade do sinal de radiofrequência, diferentemente da captura de dados de geolocalização por GPS, é transparente ao usuário[33], haja vista não necessitar de nenhuma informação de dados fornecida pelo seu dispositivo móvel.

Outra técnica de localização, discutida por Akabari *et al.*,[34] trata do uso da trilateração para localização de dispositivos via rede Wi-fi. Nesta técnica, semelhante à trilateração anteriormente discutida, a localização é realizada pela intensidade do sinal dos dispositivos móveis que estão conectados a uma determinada rede Wi-fi (com acesso à Internet), como as disponíveis em aeroportos, *shoppings*, empresas, restaurantes, dentre outros. A acurácia desta técnica – apesar de utilizar a intensidade do sinal da antena Wi-fi – é bem maior, haja vista que não se trata de grandes áreas geográficas (como as redes de telefonia móvel celular), mas pequenas áreas (normalmente, uma infraestrutura *indoor*) de abrangência de um sinal Wi-fi.

Nada obstante, a problemática legal é semelhante à discutida na localização por GPS, qual seja, é necessário que o dispositivo móvel possua um pacote de dados habilitado, bem como sua antena Wi-fi deve estar habilitada e que o usuário esteja conectado à Internet através da rede sem fio do estabelecimento. Algumas redes Wi-fi, anteriormente acessadas pelo dispositivo, podem ter conexão automática quando o mesmo se encontrar em sua área de alcance. Isto pode facilitar a localização de uma vítima, nestas situações.

Ademais, a localização através desta técnica necessita de algumas informações adicionais, a saber: a identificação do usuário e do endereço IP (*Internet Protocol*) que está utilizando para acessar a Internet (naquele dado momento). O endereço IP permitirá a identificação da infraestrutura Wi-fi (localização do estabelecimento) a qual o dispositivo móvel está conectado.

A partir desta informação, a trilateração para a localização indoor, segundo Akabari *et al.*,[35] pode ser realizada por diferentes algoritmos computacionais, com acurácia de até 1,5 metros em ambientes internos.

Outra técnica é a identificação do endereço IP, a qual mostra-se de grande importância para a localização, sobretudo quando o dispositivo móvel se encontra conectado a uma rede Wi-fi. Tal tipo de conexão já se tornou bastante frequente e é instrumento de grande acurácia para localização em locais fechados (*indoor*), como em residências, *shoppings*, aeroportos, universidades ou outros estabelecimentos que fornecem o acesso (gratuito ou não) a essas redes. Por meio do endereço IP fornecido ao dispositivo móvel pelos pontos de acesso Wi-fi pode-se determinar a sua localização enquanto fizer uso dos serviços dessa rede.

Tal mecanismo permite que outros dispositivos, da vítima ou dos suspeitos, possam ser localizados – mesmo os que não acessam as redes móveis 3G ou 4G –, o que inclui *tablets* ou *laptops*.

Técnicas e serviços mais modernos, já disponíveis e em pleno uso, permitem a combinação de dados de triangulação celular, triangulação Wi-fi (realizada pela intersecção de três pontos de acesso Wi-fi) e posicionamento GPS, proporcionando grande acurácia na localização.

4. LEGALIDADE E CONFORMAÇÃO CONSTITUCIONAL DOS "OUTROS" MEIOS TÉCNICOS DISPONÍVEIS PARA A LOCALIZAÇÃO DE DISPOSITIVOS MÓVEIS

Para se obter a informação de localização do dispositivo móvel, através das técnicas supracitadas, que perpassam a simples análise da intensidade do sinal de radiofrequência, faz-se necessário o acesso a recursos e serviços inovadores que, como dito acima, encontram-se entre os "outros" meios previstos no art. 13-B do CPP. Apesar disso, não faltarão vozes questionando sua legalidade e conformação constitucional.

Antes de tudo, é necessário que o dispositivo móvel tenha ativado o sensor GPS e habilitado um pacote de dados, uma vez que as informações de localização, por essas técnicas, são transmitidas via tráfego de pacote de dados e não por cálculo de intensidade de sinal de antenas.

Com o GPS e o pacote de dados habilitados, poder-se-á identificar, em tempo real, a localização do dispositivo via posição do GPS ou – se autenticado em alguma rede Wi-fi pública ou privada – pela identificação do local do dispositivo que lhe forneceu o endereço IP. Pode-se, inclusive, combinar as diferentes técnicas de localização, como apresentado.

Caso o dispositivo não tenha habilitado os serviços referidos, a operadora de serviços de telecomunicações pode fazê-lo remotamente, como explicado acima. Existem aplicações de *software* disponíveis no mercado que também permitem a habilitação remota do sensor GPS.

As rotas percorridas pelo dispositivo móvel também são armazenadas no histórico de tais aplicações, as quais permitem uma análise do percurso que o aparelho fez durante determinado tempo. Nada obstante, a habilitação do pacote de dados pode gerar ônus financeiro para o usuário do dispositivo móvel e, em casos normais, precisa de sua autorização.

Na investigação policial, a utilização desses recursos se constitui em técnicas mais precisas e rápidas para a localização da vítima e/ou suspeito. Ademais, não há necessidade de conhecimento técnico aprofundado para habilitar tais serviços e obter essas informações. Reitera-se, existem ferramentas disponíveis pelo próprio fabricante do dispositivo que permitem sua localização remota. Nada obstante, normalmente a ativação de tais recursos necessita da autorização do proprietário da linha habilitada no dispositivo.

A informação da posição – por meio do GPS – embora não se configure como "sinal", sem dúvida está autorizada legalmente, vez que se mostra como "outro" meio técnico adequado à localização de vítimas ou suspeitos, podendo, portanto, ser requisitado pelo delegado de polícia, nos termos do art. 13-B, *caput*, do CPP.

O que não está previsto em lei e cuja constitucionalidade mostra-se questionável é a obrigação de as empresas prestadoras de serviços telefônicos e/ou telemáticos habilitarem um pacote de dados sem autorização do cliente (vítima ou suspeito de tráfico de pessoas), quando esses não o tiverem, claro. A quem caberia o ônus financeiro dessa medida? À vítima ou ao suspeito de tráfico de pessoas? À operadora telefônica e/ou telemática? Ao Estado?

No direito comparado, a NACDL[36] apresenta uma variedade de regimes legais utilizados nos EUA, para permitir o acesso à informação de localização do dispositivo móvel. Tais permissões englobam o acesso a essa informação via CSLI e via GPS. Segundo esse documento, para fatos específicos e articuláveis que mostram que as informações solicitadas são materiais e relevantes para a investigação criminal em andamento, permite-se liberação ao histórico de localização, e, mais raramente, informações prospectivas de localização.

Ponderando-se a importância dos bens jurídicos em questão, especialmente a vida e a liberdade da vítima de tráfico de pessoas, de um lado, e o patrimônio (da vítima ou do suspeito), de outro, entendemos que é razoável a habilitação automática, pelas empresas de serviços telefônicos e/ou telemáticos, do pacote de dados necessários para a localização de vítimas e suspeitos de crime de tráfico de pessoas através das técnicas mais precisas e eficazes, a exemplo do GPS.

Sobre o ônus de arcar com os custos financeiros de tais medidas, entendemos que deve ser do Estado, detentor do monopólio da investigação criminal. Nada obsta, porém, que haja um acordo de parceria entre o Estado e as empresas prestadoras de serviços telefônicos e/ou telemáticos para que caiba a estas, e não ao Estado, arcar com os custos dessas operações. Esse ônus só não pode recair às vítimas ou aos suspeitos, pelo menos não na atual arquitetura constitucional e legal.

CONSIDERAÇÕES FINAIS

O presente trabalho buscou analisar se os meios técnicos disponíveis e normalmente utilizáveis são eficazes para a localização de vítimas e suspeitos de crime de tráfico de pessoas. Para tanto, apresentou uma perspectiva técnica e tecnológica de alguns dos principais recursos disponíveis para a localização de dispositivos móveis que – em inúmeras situações – podem auxiliar na localização da vítima ou dos suspeitos de um delito.

Ademais, foi apresentada uma análise da eficácia dos meios técnicos disponíveis, notadamente, a Localização pelo Local da Célula (CSLI) que se dá por técnicas de triangulação e trilateração, envolvendo a aplicação de cálculos matemáticos. Tais artifícios são necessários para que se aumente a acurácia e precisão na localização, pois a intensidade do sinal de recepção do aparelho permite apenas uma localização aproximada.

Mesmo que a provedora de serviços de telecomunicações possua recursos para aplicação de tais técnicas, estas ainda são consideradas – pela literatura –, meios imprecisos de localização. Apesar disso, a análise da intensidade do sinal de radiofrequência, bem como seu posicionamento na área de cobertura da rede celular é a regra entre os recursos técnicos previstos pelo art. 13-B do CPP, incluído da Lei nº 13.344/2016.

Existem outras técnicas de localização relatadas na literatura como meios mais precisos para a localização, *e.g.*, o *Global Position System*, que permite a localização do dispositivo através da captura da informação de sua localização pelo sinal GPS. Constitui-se em método com maior acurácia e precisão, sobretudo para a localização em áreas externas.

O GPS até se enquadra nos "outros" meios técnicos dos quais faz referência o citado art. 13-B do CPP, atendendo, pois, ao princípio da legalidade probatória, reconhecível a partir da assim chamada interpretação analógica. Entretanto, para a utilização desse recurso, faz-se necessária a ativação da antena GPS do dispositivo móvel, bem como a utilização da rede de dados, o que geraria custos financeiros.

Quanto à habilitação de dados da vítima, ou apenas a utilização do seu pacote, caso já o possua, parece razoável se sustentar que o ônus de arcar com esses custos estaria dentro do que poderíamos chamar de consentimento presumido, já que, nas circunstâncias do caso, ela não poderia expressar seu aceite, mas que, igualmente pela configuração do caso concreto, seria justificável, por ser necessário, adequado e proporcional à cessação de um estado flagrancial. Veja-se que a restrição ao direito fundamental de propriedade, mais especificamente, do *patrimônio* da vítima, mostra-se justificada diante da salvaguarda dos demais direitos fundamentais cuja afetação ou restrição, pelos autores de crimes, estaria em risco ou já configurada.

O problema maior revela-se quando a necessidade for de habilitação de dados dos suspeitos. De quem será o ônus de sua ativação? Deles mesmos, ainda que sem autorização? Das empresas prestadoras desses serviços? Ou do Estado?

Entendemos deva ser, como regra, do Estado, detentor do monopólio da investigação criminal e do próprio poder punitivo. Nada obsta, porém, que haja um acordo de parceria entre o Estado e as empresas prestadoras de serviços telefônicos e/ou telemáticos, para que estas, e não o Estado, arquem com os custos dessas operações. Esse ônus só não pode recair aos suspeitos, ao menos não na atual arquitetura constitucional e legal.

Por fim, concluímos que os sinais, informações e outros meios técnicos que possibilitem localizar vítimas e investigados não se encontram protegidos por sigilo. E, embora restrinja os direitos fundamentais à privacidade e/ou intimidade dos envolvidos (vítimas e suspeitos), sua restrição não depende de prévia autorização judicial. Mesmo para aqueles que defendem que a restrição à privacidade e/ou intimidade está reservada à autorização judicial, ainda assim esta seria afastada, já que em todas as hipóteses autorizadoras da medida analisada configuram situação flagrancial permanente, ensejadoras de medidas investigativas análogas às excludentes de ilicitude.

NOTAS

1. Art. 13-B. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso. § 1o Para os efeitos deste artigo, sinal significa posicionamento da estação de cobertura, setorização e intensidade de radiofrequência. § 2o Na hipótese de que trata o *caput*, o sinal: I - não permitirá acesso ao conteúdo da comunicação de qualquer natureza, que dependerá de autorização judicial, conforme disposto em lei; II - deverá ser fornecido pela prestadora de telefonia móvel celular por período não superior a 30 (trinta) dias, renovável

por uma única vez, por igual período; III - para períodos superiores àquele de que trata o inciso II, será necessária a apresentação de ordem judicial. § 3o Na hipótese prevista neste artigo, o inquérito policial deverá ser instaurado no prazo máximo de 72 (setenta e duas) horas, contado do registro da respectiva ocorrência policial. § 4o Não havendo manifestação judicial no prazo de 12 (doze) horas, a autoridade competente requisitará às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, com imediata comunicação ao juiz.

2. Nucci, G. de S. (2017). *Código de processo penal comentado*. Forense, p. 109.

3. Lima, R. B. de. (2017). *Código de processo penal comentado*. Juspodivm, p. 104.

4. Cunha, R. S.; Pinto, R. B. (2016). *Tráfico de pessoas*: lei 13.344/2016 comentada por artigos. Juspodivm, p. 125.

5. Apesar de usarmos as expressões *intimidade* e *privacidade* sem estabelecermos suas distinções, não as desconhecemos. Mas, por não ser o foco do presente trabalho, remetemos o leitor à análise distintiva feita por Sampaio, J. A. L. (1998). *Direito à intimidade e à vida privada*. Belo Del Rey, p. 208.

6. Bedê Júnior, A. (2015). *A retórica do direito fundamental à privacidade*: a validade da prova obtida mediante filmagens nos ambientes público e privado. Juspodivm, p. 75.

7. Ramón Augustina, J. (2013). *Sobre la utilización oculta de GPS en investigaciónes criminales y detención de fraudes laborales*: análisis jurisprudencial comparado en relación con el derecho a la intimidad. La ley penal: revista de derecho penal, procesal penal y penitenciario, Madrid, v. 10(102), pp. 21-29, mai./jun. 2013, p. 22.

8. Marmelstein, G. (2011). *Curso de direitos fundamentais*. Atlas, p. 147 (grifos no original). Apesar disso, o STF tem se manifestado, em diversas ocasiões, no sentido de exigir decisão judicial para restringir o acesso a alguns dados, como o financeiro e o fiscal, que restringem os direitos à intimidade e a privacidade do cidadão.

9. Bedê Júnior, A., op. cit., p. 75.

10. Em sentido semelhante, entendendo que as medidas investigativas com reserve de jurisdição poderão ser realizadas sem autorização judicial nas hipóteses análogas às excludentes de ilicitude; e, de forma específica, sobre o uso do GPS, cf. Soares, G. T. (2016). *Investigação criminal e inovações técnicas e tecnológicas*. D'Plácido, pp. 304-306.

11. Lopes Jr., A. (2017). *Direito processual penal*. Saraiva, p. 149.

12. Por todos, cf. Armenta Deu, T. (2013). *Lecciones de derecho procesal penal*. Marcial Pons, p. 173; Pujadas Tortosa, V. (2008). *Teoría general de medidas cautelares penales*: peligrosidad del imputado y protección del proceso. Marcial Pons, p. 156; Lopes Jr., A. (2013). *Prisões cautelares*. Saraiva, p. 32; Mendonça, A. B. (2011). *Prisão e outras medidas cautelares pessoais*. Método, p. 59; Giacomolli, N. J. (2013). *Prisão, liberdade e as cautelares alternativas ao cárcere*. Marcial Pons, p. 13; e Nicolitt, A. (2015). *Processo penal cautelar*: prisão e demais medidas cautelares. RT, 50.

13. Cordero, F. (2012). *Procedura penale*. Giuffrè, p. 488.

14. Lopes Jr., A. (2013). *Prisões cautelares*. Saraiva, p. 50.

15. Pintombo, C. B. (2005). *Da busca e da apreensão no processo penal*. RT, pp. 109-117, analisa, com percuciência, a natureza jurídica da busca e da apreensão.

16. https://bit.ly/3idRUR3.

17. Kurose, J.; Ross, K. (2011). *Redes de computadores e a internet*: uma abordagem top-down. Pearson Education do Brasil, p. 379.

18. Adaptado de Kurose, J.; Ross, K. (2011). *Redes de computadores e a internet:* \ uma abordagem top-down. Pearson Education do Brasil, p. 403.

19. Kurose, J.; Ross, K., *op. cit.*, p. 381.

20. Kurose, J.; Ross, K. *op. cit.*, p. 417.

21. Lopes Jr., A. *op. cit.*, p. 148.

22. Lopes Jr., A. *op. cit.*, p. 149.

23. National Association Of Criminal Defense Lawyers (NACDL). (2016). *Cell Phone Location Tracking*, p. 1. https://bit.ly/3hjPoce

24. Roxin, A.; Gaber, J.; Wack, M.; Nait Sidi Moh, A. (2007). Wireless Geolocation Techniques: a survey. *Globecom Workshops*, IEEE.

25. Adaptado de Roxin, A.; Gaber, J.; Wack, M.; Nait Sidi Moh, A. (2007). Wireless Geolocation Techniques: a survey. *Globecom Workshops*, IEEE.

26. Adaptado de Roxin, A.; Gaber, J.; Wack, M.; Nait Sidi Moh, A. (2007). Wireless Geolocation Techniques: a survey. *Globecom Workshops*, IEEE.

27. Yassin, M.; Rachid, E. (2015). A Survey of Positioning Techniques and Location Based Services in Wireless Networks. In IEEE *2015 Int. Conf. Signal Processing, Informatics, Communication and Energy Systems*, Feb 2015, Kozhikode, India.

28. Roxin, A.; Gaber, J.; Wack, M.; Nait Sidi Moh, A. (2007). Wireless Geolocation Techniques: a survey. *Globecom Workshops*, IEEE.

29. Yassin, M.; Rachid, E., *op. cit.*

30. Yassin, M.; Rachid, E., *op. cit.*

31. Mobile Marketing Association. (out. 2015). *Demystifying Location Data Accuracy*: The new frontier and biggest mobile opportunity, p. 7. https://bit.ly/2XSoY6w

32. Para Soares, G. T., (op. cit., p. 299), inovações investigativas baseadas na analogia e na interpretação analógica são toleráveis.

33. Akabari, V.; Dhedhi, D.; Rabadiya, V.; Doiphode, S. (2016). A Survey on Android based Indoor Wi-Fi Positioning System using Tri-Lateration. In *International Journal of Computer Applications – IJCA. Proceedings on National Conference on Role of Engineers in National Building*. NCRENB 2016, p. 25. https://bit.ly/2N36RrD

34. Akabari, V.; Dhedhi, D.; Rabadiya, V.; Doiphode, S., op. cit., p. 26.

35. Akabari, V.; Dhedhi, D.; Rabadiya, V.; Doiphode, S., op. cit., p. 27.

36. National Association of Criminal Defense Lawyers (NACDL). (2016). *Cell Phone Location Tracking*, p. 1. https://bit.ly/3hjPoce

REFERÊNCIAS BIBLIOGRÁFICAS

Armenta Deu, T. (2015). *Lecciones de derecho procesal penal*. Marcial Pons.

Bedê Júnior, A. (2015). *A retórica do direito fundamental à privacidade:* a validade da prova obtida mediante filmagens nos ambientes público e privado. Juspodivm.

Cordero, F. (2012). *Procedura penale*. Giuffrè.

Cunha, R. S.; & Pinto, R. B. (2016). *Tráfico de pessoas: lei 13.344/2016 comentada por artigos*. Juspodivm.

Giacomolli, N. J. (2013). *Prisão, liberdade e as cautelares alternativas ao cárcere*. Marcial Pons.

Akabari, V.; Dhedhi, D.; Rabadiya, V.; & Doiphode, S. (2016). A Survey on Android based Indoor Wi-Fi Positioning System using Tri-Lateration. *In International Journal of Computer Applications – IJCA. Proceedings on National Conference on Role of Engineers in National Building*. NCRENB, p. 25. https://bit.ly/2N36RrD.

Kurose, J.; & Ross, K. (2011). *Redes de Computadores e a Internet: uma abordagem top-down* (5ª ed). Pearson Education do Brasil.

Lopes Jr., A. (2013). *Prisões cautelares*. Saraiva.

Lopes Jr., A. (2017). *Direito processual penal*. Saraiva.

Lima, R. B. de. (2017). *Código de processo penal comentado*. Juspodivm.

Marmelstein, G. (2011). *Curso de direitos fundamentais*. Atlas.

Mendonça, A. B. (2011). *Prisão e outras medidas cautelares pessoais*. Método.

Mobile Marketing Association. (out. 2015). *Demystifying Location Data Accuracy: the new frontier and biggest mobile opportunity*. https://bit.ly/2XSoY6w.

National Association of Criminal Defense Lawyers (NACDL). (2016). *Cell Phone Location Tracking*. https://bit.ly/3hjPoce.

Nucci, G. de S. (2017). *Código de processo penal comentado*. Forense.

Nicolitt, A. (2015). *Processo penal cautelar: prisão e demais medidas cautelares*. RT.

Pintombo, C. B. (2005). *Da busca e da apreensão no processo penal*. RT.

Pujadas Tortosa, V. (2008). *Teoría general de medidas cautelares penales:* peligrosidad del imputado y protección del proceso. Marcial Pons.

Ramón Augustina, J. (2013). *Sobre la utilización oculta de GPS en investigaciones criminales y detención de fraudes laborales:* análisis jurisprudencial comparado en relación con el derecho a la intimidad. La ley penal: revista de derecho penal, procesal penal y penitenciario, v. 10(102), pp. 21-29.

Roxin, A.; Gaber, J.; Wack, M.; & Nait Sidi Moh, A. (2007). *Wireless Geolocation Techniques: a survey*. Globecom Workshops, IEEE.

Sampaio, J. A. L. (1998). *Direito à intimidade e à vida privada*. Del Rey.

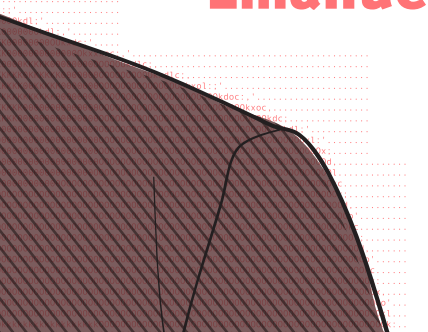
Soares, G. T. (2016). *Investigação criminal e inovações técnicas e tecnológicas*. D'Plácido.

Yassin, M.; Rachid, E. (2015). A Survey of Positioning Techniques and Location Based Services in Wireless Networks. In *IEEE 2015 Int. Conf. Signal Processing, Informatics, Communication and Energy Systems*, Feb 2015, Kozhikode, India.

05.

CÂMERAS DE SEGURANÇA E RECONHECIMENTO FACIAL — COMO AS IMAGENS SÃO UTILIZADAS COMO PROVA NO PROCESSO PENAL — NOTÍCIAS DO RIO DE JANEIRO

Emanuel Queiroz Rangel



As tecnologias de controle através da obtenção de imagens adquiriram, em especial nas duas últimas décadas, proporção praticamente universal: os espaços privados sequer mais utilizam a frase de advertência "sorria, você está sendo filmado", ante a ampla difusão das câmeras de vigilância, ao passo que o Poder Público apresenta como revolucionária a utilização da tecnologia do controle de imagens de espaços públicos para coibir a prática de crimes, agregando, recentemente, programas de reconhecimento facial.

Pode-se afirmar que já há uma naturalização, especialmente no ambiente privado, do controle por câmeras de vigilância, valendo citar que é atitude comum das crianças adentrarem ao elevador e acenarem para "o porteiro" utilizando-se dessa tecnologia.

Restringindo-se à utilização das câmeras de vigilância nos espaços privados, é comum a utilização dessas imagens como prova para fins da lavratura de autos de prisão em flagrante e, posteriormente, como prova judicial, especialmente em crimes contra o patrimônio.

No Estado do Rio de Janeiro, o atual cotidiano dos Defensores Públicos aponta para a utilização das imagens obtidas por câmeras de vigilância, em especial em furtos praticados em supermercados, gerando o debate, quando a *res furtivae* é recuperada em sua integralidade, da aplicação do art. 17 do Código Penal, que trata da figura jurídica do *crime impossível*, afastando o delito patrimonial. Oportuno registrar, embora não concordemos com a conclusão, que o Superior Tribunal de Justiça, quando do julgamento do REsp 1385621/MG, chancelou o tema repetitivo 924, o qual preceitua que "*a existência de sistema de segurança ou vigilância eletrônica não torna impossível, por si só, o crime de furto cometido no interior de estabelecimento comercial*".

Afora as questões patrimoniais, os Defensores Públicos nos reportam poucos casos nos quais há utilização de imagens de circuitos internos de vigilância como prova nos processos criminais fluminenses.

A sufragar a higidez dessa prova, normalmente se apresenta laudo pericial do Instituto de Criminalística oficial atestando que as imagens são autênticas, não contendo intervenção estranha de terceiros.

Não se pode ignorar, no entanto, que imagens de segurança também já auxiliaram a atividade defensiva dos colegas com a finalidade de demonstrar que os fatos trazidos ao conhecimento do Poder Judiciário através de depoimentos policiais não guardam relação com o que de fato ocorreu, acarretando, com muita luta, na absolvição de acusados.

Caso marcante ocorreu recentemente, ganhando certo destaque na mídia, envolvendo o jovem L. S. F., o qual foi preso em flagrante acusado de tráfico e associação para o tráfico de drogas, com utilização de arma de fogo. Segundo a polícia civil, que realizou a abordagem de L. S. F., ele estaria comercializando drogas próximo à estação do metrô de Maria da Graça, subúrbio carioca, estando sobre uma motocicleta, ao lado de seu comparsa, que também dirigia uma motocicleta. Os policiais descreveram que, quando da abordagem, ocorrida num sinal de trânsito, L.S.F. teria tentado utilizar a arma de fogo que possuía, o que fez com quem os policiais disparassem um tiro de fuzil em suas pernas, conseguindo detê-lo, ao passo que o seu comparsa teria fugido. Com L.S.F. teria sido encontrada uma mochila com quilos de *maconha*. Preso em flagrante, medicado, o pai de L.S.F. conseguiu contato com ele ainda na delegacia de polícia, ocasião na qual o jovem lhe disse ser inocente, afirmando ter sido abordado em outro

local, sozinho, sem nada portar, arma ou droga. A partir de tal informação, o sofrido pai se dirigiu a diversos estabelecimentos comerciais que possuíam câmeras de segurança solicitando o compartilhamento das imagens para provar a inocência de seu filho, somente obtendo êxito de um comerciante, dono de um bar, justamente no local da abordagem, segundo a versão de L.S.F., conflitante com a dos policiais. Uma vez obtida as imagens, constatou-se que o jovem foi abordado sozinho, quando estava parado na calçada com sua motocicleta, aparentemente aguardando a chegada de terceira pessoa (L.S.F. dizia que aguardava sua namorada), não possuindo qualquer mochila em suas costas, tendo sido determinado que o mesmo levantasse sua camisa, em ação típica policial para analisar se o suspeito está armado. Como o automóvel era descaracterizado, L.S.F. ficou com medo da abordagem e correu, ocasião na qual os policiais saíram da viatura e o detiveram, sem não antes efetuar um disparo de fuzil que, por certo, atingiu de raspão uma das pernas do estudante. Mesmo com a juntada das imagens aos autos do processo, inexistindo qualquer impugnação do órgão público de acusação sobre sua autenticidade, L.S.F. foi condenado em primeira instância, sequer a sentença se referindo das imagens. Somente em segundo grau de jurisdição L.S.F. foi absolvido da imputação, por maioria de votos, tendo um dos julgadores apontado em suas conclusões que as imagens, mesmo demonstrando que os fatos não se deram como narrados pelos policiais civis, não têm força probante frente ao *harmônico depoimento dos agentes públicos, os quais gozam de presunção de veracidade* (Processo n.º 0233294-95.2016.8.19.0001).

Percebe-se que a defesa somente teve acesso às imagens das câmeras de vigilância em razão da solidariedade do comerciante para com o pai do cidadão aprisionado. Normalmente, as imagens obtidas só se prestam a alimentar a persecução penal.

No início do ano de 2019, o Estado do Rio de Janeiro adquiriu *software* de reconhecimento facial com a finalidade de identificar foragidos e veículos objeto de crimes patrimoniais. Sequer se fala na utilização desse mecanismo como instrumento de investigação, mesmo porque seria de todo incoerente alegar a aquisição de tal tecnologia para tanto, já que a coleta diuturna de imagens prescinde da existência de uma suspeita a amparar ação estatal repressiva por parte das forças de segurança: todos estamos sob vigilância.

Interessante observar que, segundo noticia o jornal O Globo de 01/03/2019, as câmeras com reconhecimento facial, num total de 28 (vinte e oito), estavam localizadas num único bairro da *Cidade Maravilhosa*, qual seja, Copacabana, durante o projeto piloto. O Governador Wilson Witzel alardeou que 140 (cento e quarenta) câmeras com reconhecimento facial serão espalhadas pela capital fluminense, informando que estariam em mais dois locais: ao redor do Aeroporto Santos Dumont e do Estádio do Maracanã.

Note-se que o confronto entre os locais escolhidos para instalação de tecnologia não guarda qualquer relação com os dados de *georeferência* dos eventos criminosos do Rio de Janeiro. Nenhum dos locais escolhido para monitoramento com reconhecimento facial está entre os mais violentos da cidade.

Nesse passo, bom relembrar que a utilização do instrumento de reconhecimento facial pela polícia fluminense já proporcionou atuação ilegal por parte do Estado, com o a detenção de condução da Sra. Sandra Maria de Alencar em 09/07/2019, fato que se deu na movimentada Avenida Nossa Senhora de Copacabana, no bairro de mesmo nome, na Zona Sul carioca. Detida enquanto trabalhava com uma placa de propaganda "compro joias", foi levada à Delegacia de Polícia, posto que reconhecida como foragida da justiça. Acontece que a imagem em que se baseou a ação policial era de outra

pessoa, a qual já estava presa, inclusive. Sandra Maria Alencar relatou o constrangimento pelo qual foi submetida, bem como o temor decorrente da ação em reportagem do jornal *O Dia* de 21/07/2019.

Digno de nota que a Sra. Sandra é NEGRA, o que potencializa discussões sobre o viés segregacionista do sistema de reconhecimento facial. O *The Guardian*, em 08/04/2016, noticiou estudo da *Georgetown Law School* no qual a base de dados utilizada é desproporcionalmente afro-americana, sendo que o *software* seria especialmente ruim para reconhecer rostos negros. Consta da notícia que programas das empresas HP, Microsoft e Google têm dificuldades em reconhecer rostos negros, tendo o Google Photos identificado dois negros como gorilas. Aliás, Maria Laura Canineu, diretora da Human Rights Watch no Brasil, publicou artigo na Veja em 05 de junho de 2019 no qual afirma que "*o uso do reconhecimento facial levanta sérias dúvidas sobre sua confiabilidade e potencial para discriminação. Estudos independentes indicam que esses sistemas podem ampliar preconceitos raciais, étnicos e de gênero existentes. No Brasil, pode afetar desproporcionalmente homens jovens, negros, com baixa escolaridade, que já estão sobrerepresentados no sistema de justiça criminal*".

Salta aos olhos que a tecnologia de reconhecimento facial utilizada pelo Estado do Rio de Janeiro seria, segundo os periódicos, da empresa chinesa *Huawei*, não se tendo conhecimento da aquisição formal da tecnologia empregada, muito menos do desenvolvimento da mesma. Não se sabe, ainda, qual a extensão do acesso que os técnicos da empresa têm aos bancos de dados das polícias e do sistema penitenciário fluminense, muito menos se há compartilhamento de informações entre os mesmos.

Vale lembrar que a citada empresa chinesa é acusada pelo governo estadunidense de espionagem industrial e fraude

/ SEJAM AS IMAGENS OBTIDAS POR INSTRUMENTOS DE VIGILÂNCIA PARTICULAR OU PÚBLICA, DIFICILMENTE A DEFESA TEM ACESSO PARA SUAS TESES /

bancária, estando proibida de operar e instalar sua tecnologia em diversos países sob a alegação de questões de segurança nacional. Guerra tecnológica ou não, fato é que a experiência chinesa de monitoramento dos 13 (treze) milhões de mulçumanos residentes na região de Xinjiang, retratada em relatório publicado em 02 de maio de 2019 pela *Human Rights Watch*, aponta para um estado policial de proporções inimagináveis, "*com a polícia coletando ilegalmente informações sobre comportamento totalmente legal das pessoas e usando com elas*", afirmou a pesquisadora Maya Wang, tudo através de um aplicativo IJOP (Plataforma Integrada de Operações Conjuntas). No caso de Xinjiang, a empresa que desenvolveu o aplicativo é a CEIEC, controlada pelo Estado.

A tecnologia chinesa já vem sendo utilizada no Equador, no Zimbábue, Uzbequistão, Paquistão, Quênia, Emirados Árabes Unidos e Alemanha, segundo o *The New York Times* de 24/04/2019, que concentra a reportagem na experiência equatoriana, iniciada em 2011. Segundo o jornal, as informações coletadas pelo sistema de monitoramento foram repassadas para a agência de inteligência governamental, acarretando perseguição de opositores do governo. Interessante o método de aquisição do sistema de vigilância: acordo sem licitação pública, financiado por empréstimos chineses, tendo em troca o petróleo equatoriano. Por fim, revela a matéria que a instalação do sistema de segurança em nada diminuiu a criminalidade no país.

Não podemos esquecer que os Deputados Federais e Senadores da bancada do PSL no Congresso Nacional viajaram à China para conhecer o sistema de vigilância, sendo que o custo do deslocamento, segundo a Folha de São Paulo de 16/01/2019, teria sido pago pelo governo chinês.

Relevante pontuar que a utilização indevida de informações criminais da população é recorrente nos atendimentos realizados pela Defensoria Pública do Rio de Janeiro. Atuava

em Duque de Caxias, cidade da região metropolitana do Rio de Janeiro, quando existia emprego no país – entre os anos de 2007 a 2011 – sendo comum atender pessoas que foram aprovadas em processos seletivos da Refinaria Duque de Caxias, da Petrobras, e não alcançavam o contrato de trabalho por ordens da equipe de segurança da empresa, formada por policiais em hora de folga. Invariavelmente, essas pessoas tinham anotações criminais relativas a infrações penais de pequeno potencial ofensivo com a punibilidade extinta – na maioria dos casos em razão de medidas despenalizadoras – informações que não são acessíveis numa consulta pública junto ao Instituto de Identificação Criminal, disponíveis, no entanto, nos bancos de dados da polícia civil.

Voltando ao *Big Brother* fluminense, como dito no início, ao revés das imagens obtidas por câmeras de vigilância privadas, as imagens coletadas pelos órgãos públicos fluminenses com seus sistemas de reconhecimento facial não foram utilizadas, até o momento, como prova em processos penais; ao menos as Defensoras e Defensores Públicos não têm notícia alguma de casos nesse sentido.

Certo é que, sejam as imagens obtidas por instrumentos de vigilância particular ou pelas câmeras públicas, dificilmente a defesa pública consegue obter acesso a essas evidências para construção de suas teses.

Tem-se, ainda, que não há na estrutura orgânica das defensorias públicas brasileiras departamento científico apto a amparar tecnicamente os órgãos da instituição na análise das imagens apresentadas como provas nos processos em curso, ampliando, ainda mais, a relação desigual entre Estado-acusação e exercício do direito de defesa, aprofundando a desigualdade no ferramental da construção do contraditório.

Oportuno registrar, no entanto, que consta do projeto de plano plurianual apresentado pela Defensoria Pública do Es-

tado do Rio de Janeiro ao Poder Executivo, para consolidação e posterior remessa ao Poder Legislativo, a criação de departamento científico a amparar uma melhor qualidade da defesa.

Em síntese, podemos afirmar, a partir das informações obtidas junto às Defensoras e aos Defensores Públicos que oficiam em processos criminais no Estado do Rio de Janeiro, que:

< 01 > As imagens que fazem parte do cotidiano dos processos criminais são, fundamentalmente, oriundas de câmeras de vigilância privadas, vinculadas a feitos que tratam de delitos patrimoniais, em especial, furto de estabelecimento comercial;

< 02 > Não se tem notícia da utilização de tecnologias de reconhecimento facial em investigações criminais que tenham desaguado no Poder Judiciário fluminense em processos que a Defensoria Pública atue;

O acesso às imagens coletadas pelos serviços de vigilância, públicos ou privados, são de difícil acesso para a defesa;

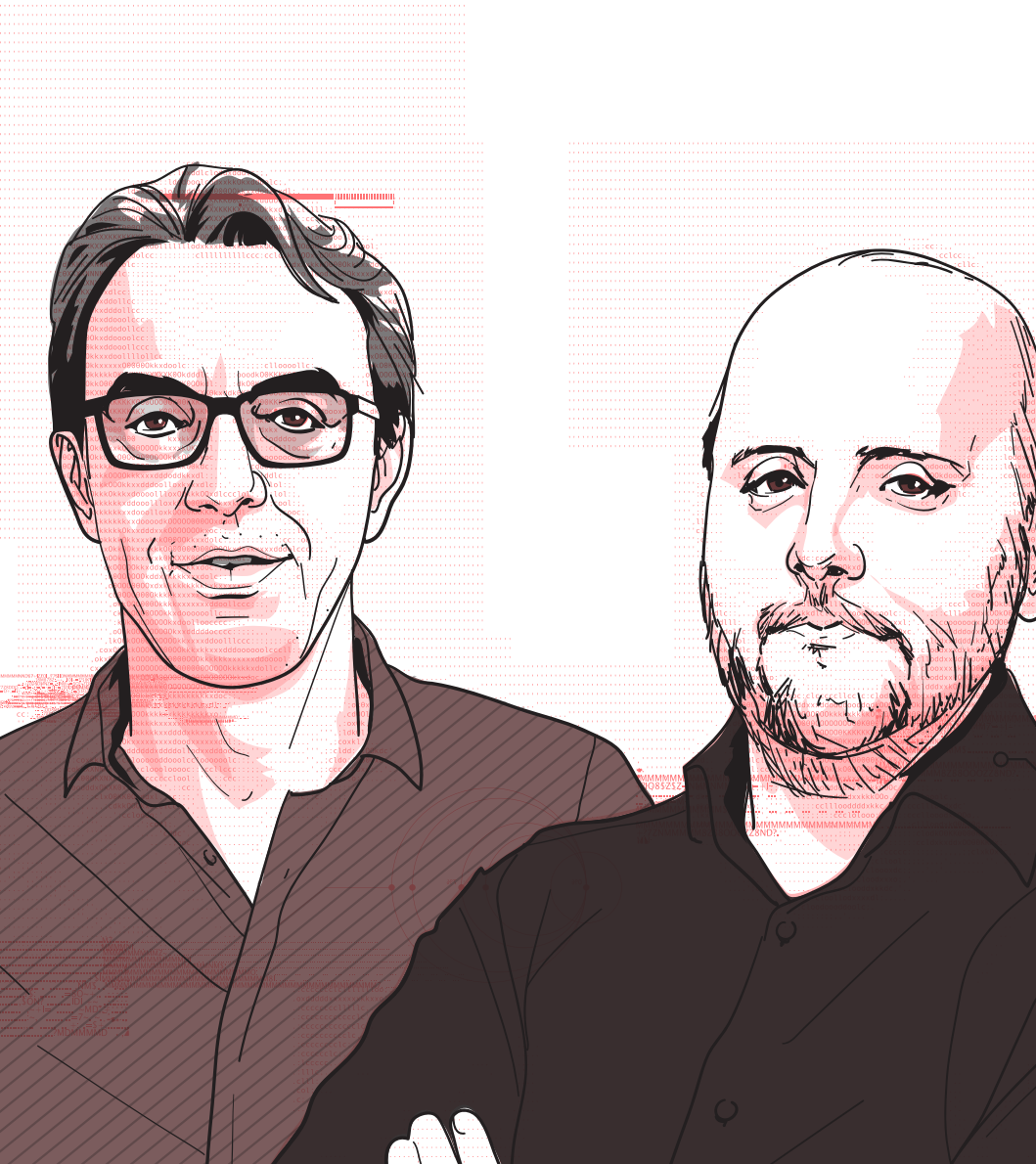
< 03 > Há carência de apoio técnico qualificado à defesa exercida pelas Defensorias Públicas para análise de imagens que se prestam à prova criminal;

< 04 > Existe uma utilização por parte das empresas de vigilância privada, invariavelmente composta por profissionais que atuam na segurança pública, de dados sigilosos de forma afrontosa à legislação.

Derradeiramente, não custa lembrar que o trajeto entre a Casa das Pretas, na Lapa, e o local do assassinato da vereadora Marielle Franco e do seu motorista Anderson Gomes, ocorrido em 14/03/2018 no Catumbi, na cidade do Rio de Janeiro, era monitorado por 11 (onze) câmeras da prefeitura da cidade, sendo que, justamente naquele fatídico dia, como noticiou *O*

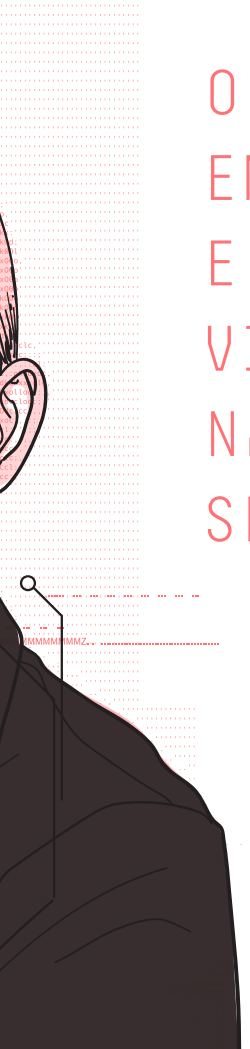
Globo de 22/03/2018, cinco delas estavam desligadas, não sabendo o ente municipal justificar o porquê da falha.

Ao que parece, as imagens de segurança só se prestam para desvendar crimes patrimoniais, nos quais os detidos geralmente têm o perfil da população prisional brasileira, qual seja, negros ou pardos, periféricos. Quando se prestam para desvendar crimes nos quais negros ou pardos, periféricos são vitimados, as câmeras de segurança se encontram, casualmente, desligadas.



06.

O SISTEMA DETECTA EM SÃO PAULO E O PAPEL DO VIGILANTISMO NAS PRÁTICAS DE SEGURANÇA DA CIDADE



Alcides Peron[1]

Marcos César Alvarez[2]

INTRODUÇÃO

Em 2014, o governo do estado de São Paulo anunciou uma parceria com a Microsoft e o Departamento de Polícia de Nova York para importar um sistema de vigilância e monitoramento nomeado como Detecta. O aparato original, chamado *Domain Awareness System* (DAS), é caracterizado como uma tecnologia para rastrear e traçar perfis de conduta criminosa e suspeita com base em câmeras inteligentes integradas a bancos de dados criminais e de imagens. Esse sistema foi desenvolvido em Nova York, anos após os ataques de 11 de setembro de 2001, como forma de mitigar a possibilidade de ameaças terroristas e aumentar a capacidade da polícia em antecipar e reagir a práticas criminosas. A peculiaridade dessa tecnologia é a capacidade de construir modelos estatísticos a partir de mineração de dados públicos e seu cruzamento com plataformas de dados criminais e dados de várias ordens, classificando grupos de indivíduos e apontando para padrões de crimes futuros. Além disso, o sistema incorpora algoritmos de análise de imagem (analíticos), com capacidade de "ler" imagens da câmera e emitir alertas se alguma ação programada for detectada.

Esse saber "estatístico-preditivo", que fundamenta a classificação de risco em relação ao crime, é apresentado como uma resposta urgente ao terrorismo doméstico nos EUA, que exige esforços preventivos da polícia para impedir sua ocorrência (New York Policy Department, 2009). Além disso, essa mesma tecnologia, invocada como medida excepcional no combate ao suposto terrorismo, acaba tendo uma dupla funcionalidade, empregada no combate a atividades criminais, desvios e infrações de cidadãos comuns, tornando-os alvos de suspeita (Graham, 2016).

Assim, com base na analítica do poder de Michel Foucault, especificamente sua ideia de dispositivos e de governamentalidade, bem como apoiado nos Estudos Críticos de Segurança,

este capítulo tem como objetivo entender como a instauração de um novo regime de visibilidade, por meio do sistema Detecta, ao espalhar câmeras "inteligentes" privadas por toda a cidade, introduz um tipo de “cultura de controle” que reordena as práticas de segurança de São Paulo. Embora o Detecta não incorpore totalmente os sistemas "preditivos", como o desenvolvimento de bancos de dados e todas as funções de analítica de vídeo, o texto indicará como essa adoção parcial pode sustentar uma série de práticas discriminatórias e segregacionais em São Paulo. Isso aconteceria quando a profusão de uma cultura de controle sobre o aparato de segurança pública exigisse um estado permanente de medo e de desconfiança e a incorporação de uma retórica econômica nas práticas policiais.

Esta reflexão está, assim, dividida em três partes e uma seção de conclusão. Primeiro, são debatidos o desenvolvimento do DAS e sua relação com a cultura emergente de controle e governamentalidade. Em segundo lugar, aborda-se o processo de adaptação do Detecta ao Brasil, ao explorar os discursos e práticas que levam à formação e estabilização do dispositivo de segurança. Por fim, descreve-se a formação dos perímetros de segurança, e como eles se tornam territórios onde uma forma particular de violência assistida por tecnologia (Haggerty & Ericsson, 1999) é dominante, reforçando as práticas segregacionais na cidade.

SEGURANÇA COMO “CONTROLE”: DO DAS AO DETECTA

Ao longo do século XX, diversas abordagens foram desenvolvidas no campo da assim chamada Criminologia Crítica, principalmente nos anos 1970, as quais Long (2016) entende como unidas no entorno da noção de que classe e desigualdades são um fator determinante para a ocorrência do crime. No entanto, em meados dos anos 1980 e início de 1990, a abor-

dagem denominada “ambiental” ganha destaque e influencia diversas abordagens policiais no período – principalmente nos EUA. Os trabalhos de Paul e Patricia Brantingham (1991) envolviam a noção, por exemplo, de que espaço geográfico, vítima, criminoso e lei interagiam de forma a estimular e produzir o crime, sendo portanto este o foco dessa abordagem (os motivos que levaram a sua ocorrência, os atores, as circunstâncias). Não o criminoso ou sua recuperação, mas a prevenção da situação e do crime.

De acordo com Wortley e Mazerolle (2008) o crime seria influenciado por várias condições ambientais, fatores situacionais facilitados pelas oportunidades, e os aspectos criminais do ambiente – basicamente a tendência e característica criminal de certas localidades. Seguindo essa linha argumentativa, popularizam-se as teorias das atividades rotineiras elaboradas por Felson (2002), e as teorias dos padrões criminais, trabalhada novamente por de Paul e Patricia Brantingham (1991) cuja interação entre vítimas (ou alvo), criminosos (ou violadores), ambiente e oportunidades irão organizar as percepções acerca da ocorrência de crimes. Nessas teorias, a ação sobre o ambiente, a arquitetura etc., seriam os principais fundamentos da ação policial, de forma a inibir as oportunidades para o crime, de forma preventiva.

Aproximando-se de forma crítica dessa perspectiva, no início dos anos 2000, David Garland aponta para mudanças no modelo de policiamento nos Estados Unidos que teriam ocorrido desde meados dos anos 1980, afastando-se das estratégias reativas de enfrentamento do crime, ao mesmo tempo em que uma tecnologia “liberal avançada” do governo se desenvolvia. Ele indica como uma série de agências, práticas, discursos e políticas redirecionará seus esforços para produzir formas de policiamento direcionadas e baseadas na comunidade, com o objetivo de "salvaguardar a ordem" e policiar a

"qualidade de vida". Segundo o mesmo autor, "o policiamento se tornou mais inteligente" ao abordar a comunidade e enfatizar a prevenção, concentrando-se nas circunstâncias locais para a resolução de crimes (Garland, 2008, pp. 367-368).

Essencialmente, o que Garland diagnostica, ao se debruçar sobre essas teorias ambientais, é a emergência de uma nova cultura de controle policial, na qual "as tecnologias da informação e as novas técnicas gerenciais se combinaram para produzir maior controle de recursos e condutas mais direcionadas e pontuais" (Garland, 2008, p. 368). Além disso, a adoção de premissas cognitivas ligadas a uma racionalidade econômica neoliberal seria a marca dessa nova cultura policial, na qual "os custos do crime são agora rotineiramente calculados, assim como os custos de prevenção, policiamento, repressão e punição; os números produzidos ajudam a nortear escolhas políticas e prioridades operacionais "(Garland, 2008, p. 396).

Essa nova cultura do controle tem um forte paralelo com a noção de governamentalidade explorada por Foucault na década de 1970, a partir da qual considera-se que a dinâmica da ação estatal seria substancialmente alterada, figurando como uma técnica de governo cujo alvo seria a população e que instrumentalizaria o conhecimento econômico como meio de produzir e conduzir um comportamento adequado. Pressuporia uma administração permanente do medo, uma vez que a produção e a reprodução constantes de ameaças à “liberdade” seriam meios de expandir os instrumentos disponíveis para combater e gerenciar essas mesmas ameaças. Essa noção evoluiria da articulação entre um “Poder Pastoral”, ancorado na ideia de salvação do "rebanho" como justificativa para a condução das condutas, e o surgimento da arte liberal de governar, que conceberia o governo como uma técnica reativa às demandas de um corpo social com aparen-

te racionalidade econômico-utilitária (Foucault 2008, p. 298). Nesse contexto, as tecnologias governamentais (ou tecnologias de segurança) operariam de maneira a sistematizar, regular e estabilizar as relações sociais e de poder, evitando a dissolução das liberdades individuais ou a imposição de um poder e dominação soberanos (cf. Lemke, 2017, p. 27). Assim, "as tecnologias governamentais reúnem conhecimento científico, dispositivos técnicos, hipóteses antropológicas e formas arquitetônicas de formas estratégicas para estabelecer relações de conduta" (Opitz, 2011, p. 22).

Daí a proximidade dessas discussões de Foucault com a ideia de Garland de cultura de controle, uma espécie de "criminologia da vida cotidiana" na qual os processos e arranjos sociais em que as pessoas estão imersas precisariam ser integrados para produzir menos incentivos ao crime. Como Garland aponta: "(...) a criminologia da vida cotidiana aborda a ordem social como um problema de integração de sistemas. Eles não são mais as pessoas que precisam ser integradas, mas os processos e arranjos sociais em que vivem" (Garland, 2008, p. 388).

Diante disso, pode-se considerar o desenvolvimento do DAS pela *Microsoft* e pelo Departamento de Polícia de Nova York em 2009 como parte da cultura do controle caracterizada por Garland. Tal desenvolvimento integra informações de diversos bancos de dados a sistemas de câmeras com leitura analítica de imagens e dispositivos policiais periféricos, permitindo maior eficiência de atividades de serviço e expedição, construção de estatísticas e mapas de calor de práticas criminosas e ações policiais proativas. O DAS, nesse sentido, é uma ferramenta de contraterrorismo, orientada para interromper a preparação e ataques terroristas, mas também utilizada para conter manifestações e crimes menores (New York Policy Department, 2009, p. 2).

Assim, o DAS foi responsável por organizar a segurança pública como instrumento de governo da segurança, por um lado, introduzindo um sistema amplo e permanente de vigilância e desconfiança, por outro, trazendo à esfera da segurança pública empresas e tecnologias privadas, não apenas como fornecedores, mas como atores com grande capacidade de atuação no sistema. Esse papel privado ativo sobre segurança é intenso em Nova York desde os ataques terroristas de 2001 e aumentou nos últimos dez anos, como pode-se ver pelo papel da consultoria McKinsey atuando junto ao Departamento de Polícia de Nova York, ajudando-o a "moldar seu futuro" (Amoore, 2013).

Nesse sentido, a cultura de controle pode ser vista como estando inscrita no DAS. A ideia de uma dinâmica de policiamento com ampla e permanente visibilidade parece se inscrever no DAS através das linhas de código que compõem seus algoritmos, e do modo como a infraestrutura do sistema é disposta. Essa perspectiva se aproxima dos debates levados a cabo por Bruno Latour a respeito das redes sociotécnicas e daquilo que define enquanto mediação técnica. Em sua "Teoria Ator Rede" (TAR), o autor entende que quaisquer interpretações sobre a sociedade só serão completas ao se considerar a possibilidade de agência de elementos não-humanos (como tecnologias, elementos arquitetônicos, dentre outros arranjos sociotécnicos). A sociedade seria, portanto, composta de redes de interações que se transformam e se recompõem a cada novo contato e interação, na qual intermediários (que carregam uma mensagem) e diversos mediadores (tradutores e ressignificadores de mensagens) interagem em uma rede na qual a agência é um fenômeno distribuído entre humanos e não humanos (Latour, 2015, pp. 65-67). Nesse processo de "reagregação do social", Latour entende a tecnologia como a "sociedade tornada durável", um conjunto de relacionamen-

tos, programas de ações, inscritos em artefatos técnicos, trazendo estabilidade para as relações sociais, bem como compondo novas formas de agir (Latour, 1991). Nesse caminho argumentativo, o autor realiza um debate acerca da noção de "mediação técnica" desses instrumentos. Assim, dois sentidos de mediação são importantes aqui: a ideia de tradução e de composição. Em seu estudo, Latour descreve a noção de tradução como "deslocamento, derivação, invenção, mediação, a criação de um elo que não existia antes e que, em certa medida, modifica dois elementos ou agentes" (Latour, 1994, p. 32). Em suma, a relação entre agentes humanos e não humanos desloca um curso de ação anterior, criando "desvios", novos cursos e programas de ação. A ideia de composição, por sua vez, implica que uma série de objetivos, etapas, ações e intenções tornadas possíveis através de um *assemblage* entre homem e tecnologia, produz troca de competências entre ambos agentes, levando à constituição de novos objetivos e novas funções nesse híbrido (Latour, 1994, p. 35). Em outras palavras, as interações entre actantes de diversas ordens produzem um híbrido, que pode ser um deslocamento ou uma nova possibilidade de ação, e compreender esse hibridismo, esses novos cursos, o modo como esse deslocamento ocorre, é um dos programas de estudo de Latour.

Para ele, a interação entre humanos e não humanos alteraria dinâmicas de ação, produzindo desvios, e a sua composição final seria um híbrido sociotécnico: "Um curso regular de ação é suspenso, um desvio é iniciado através de vários tipos de actantes, e o retorno é um novo híbrido que carrega ações passadas no presente, e permite suas múltiplas maneiras de desaparecer enquanto se faz presente" (Latour, 1994, p. 40). Assim, ao entender que a tecnologia seria a cristalização dos valores, políticas, interesses em aparatos duráveis, per-

petuando-os no corpo social, Latour (1991; 1994) abre outro campo de discussão que interessa aqui, acerca da invisibilização da sociedade nas tecnologias. Ele define essa invisibilização como um processo de encaixotamento (*blackboxing*), no qual a produção conjunta entre artefatos e humanos se torna opaca, desaparece e se torna desapercebida pela sociedade (Latour, 1994, p. 36). Cada parte e componente desse encaixotamento possui história, conflitos, embates que se perdem – como as estruturas arquitetônicas e outras conjunções entendidas como "não ditos" (implícitos) que Foucault, por sua vez, propõe em seu entendimento sobre os dispositivos (Agambem, 2014, p. 24) – cuja recuperação permite uma compreensão mais ampla dos mecanismos sociais em operação.

Assim, pensar os instrumentos de vigilância, monitoramento e classificação de risco em termos de governamentalidade da segurança pública (que evolui, como foi visto, das teorias criminológicas ambientais e situacionais, organizando-se como uma cultura do controle) implica em entender não apenas como esses instrumentos se adaptam e são utilizados pelas autoridades, mas igualmente como eles produzem efeitos sociais, mas em primeiro lugar, como o seu desenvolvimento "invisibiliza" (*Blackboxing*) interesses, valores, programas de ação que irão se reproduzir *a posteriori*; em seguida, como a interação entre essas novas tecnologias, em um novo contexto, e com os usuários deslocarão programas de ação e comporão novos híbridos. Isso é esclarecido pelo argumento de um executivo da Microsoft entrevistado: "(...) [o DAS] tem um preço, do qual é o código-fonte que foi construído com base em muitas boas práticas, e a tradução desse conhecimento é adicionada à realidade desse novo cliente. Esse é o conceito chamado solução, onde o contexto do Detecta está inserido" (Entrevista 2, 2018).

Na visão desse executivo, o código fonte do sistema DAS é constituído a partir das consideradas boas práticas de policiamento e vigilância, e torna-se um produto (*commodity*) customizado aos objetivos do cliente. Assim, essas tecnologias traduzem e compõem a rotina da atividade policial em uma prática mais intensiva em dados, trazendo à tona a "consciência situacional" como um conceito operacional, útil e, fundamentalmente, comercializável. Não apenas vemos o lançamento de um novo modelo de segurança expresso na noção de vigilância permanente e suspeita, governando as condutas das pessoas para produzir estabilidade e ordem, mas vemos que ele está inscrito em um instrumento mercantilizado através da agência ativa de empresas transnacionais privadas.

Tanto o DAS quanto a Detecta são, desse modo, o resultado de uma iniciativa público-privada de construir e consolidar internacionalmente um padrão para "boas" práticas de policiamento e vigilância, replicando a dinâmica de prevenção e criminologia ambiental através desse intercâmbio tecnológico.

RUMO A UM NOVO DISPOSITIVO DE SEGURANÇA? O PÚBLICO E O PRIVADO NA ADOÇÃO DO DETECTA

Em 2013, a Secretaria de Segurança Pública (SSP) criou uma comissão para investigar novas soluções tecnológicas para fins de segurança desenvolvidas em todo o mundo. Em maio, essa comissão visitou várias cidades nos EUA e na Europa, analisando tecnologias de vigilância, soluções de comunicação e procedimentos adotados pelos departamentos de polícia de Londres, Nova York e Amsterdã. Seu relatório concluiu que os sistemas híbridos de vigilância tecnológica, ambos voltados para o combate ao terrorismo e ao crime, seriam a vanguarda das soluções desenvolvidas nas cidades visitadas, e que a adoção de modelos semelhantes ao DAS

/ O OLHAR
DO AGENTE DE
SEGURANÇA OU DO
CIDADÃO VIGILANTE
COMPLETA O
APARELHO DE
VIGILÂNCIA COM
SUA "INTUIÇÃO"
OU "EXPERIÊNCIA"/

/ O DETECTA PERMITE A COMBINAÇÃO DAS PRÁTICAS DISCRIMINATÓRIAS COSTUMEIRAS COM UM REGIME DE VISIBILIDADE ESTENDIDO E DISTRIBUÍDO /

de Nova York seria decisiva para São Paulo (Assessoria Especial para Assuntos Internacionais, 2013).

Sob o argumento de redução de custos e dificuldades administrativas nas instituições policiais, além de aparentemente produzir efeitos mais visíveis na redução do crime, o Detecta foi adotado pela SSP, supostamente incorporando tanto as funcionalidades da análise de imagens, quanto a produção de mapas de calor em áreas de ocorrência de crimes. Segundo a Secretaria de Segurança Pública (2015), a intenção era expandir o leque de perfis de suspeitos, além de atividades relacionadas ao tráfego, cruzando informações de bancos de dados de outras instituições (Governo do Estado de São Paulo, 2015).

No entanto, desde a sua adoção, apenas algumas informações sobre a operação do sistema Detecta foram reveladas. Além disso, no ano de 2016, foi elaborado um relatório pelo Tribunal de Contas do Estado de São Paulo que afirma que o sistema não funciona adequadamente, suas funções de policiamento preditivo seriam inexistentes e sua capacidade de integração de dados seria frágil (Tribunal de Contas do Estado de São Paulo, 2016). O Tribunal apontou que os sistemas analíticos não estavam integrados ao Detecta, alguns computadores não funcionavam corretamente, não havia pessoas suficientes trabalhando no processamento de dados, muitos departamentos policiais não tinham acesso ao sistema e, principalmente, o sistema de câmeras não estava devidamente espalhado pela cidade.

O argumento mobilizado pelas autoridades desde então é que a falta de recursos e a insuficiente capacidade para lidar com esse sistema forçaram a reorganização do Detecta como um extenso *assemblage* público-privado, no qual o setor privado teria um importante papel na dispersão de câmeras e administração de informações. No entanto, o mesmo relatório mencionado acima mostra que a comissão estava ciente

desde o início que o setor privado desempenharia um papel vital na execução do sistema.

Assim, o Detecta passou a representar um sistema abrangente para espalhar câmeras e integrar dados, produzindo estatísticas e mapas de calor, auxiliando as forças policiais na subsequente resolução de crimes. Ele atualmente integra um sistema de câmeras públicas, do Radar, do sistema municipal de câmeras e imagens, do City Câmeras e de sistemas de câmeras privadas dos residentes de certos bairros. Em conversas com empresários da área, e com autoridades do estado e município, verifica-se que a expansão do sistema de câmeras é comandada pelo setor privado – uma vez que são empresas e associações de condomínio e de moradores que voluntariamente buscam a adesão; quando não, são estimulados através de programas de policiamento comunitário – o qual assume um papel de destaque nesse relacionamento com a dimensão pública do Detecta. No entanto, isso não significa necessariamente que o Detecta seja falho, pelo contrário, configura um relacionamento em que a simbiose público-privada é determinante no processo de governança de segurança.

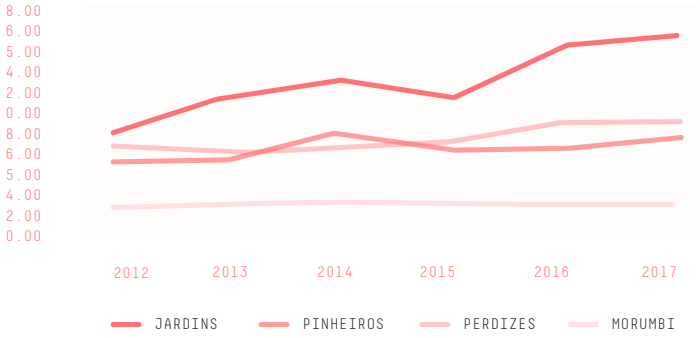
Nesse espírito, entende-se aqui que é insuficiente analisar apenas o Detecta, ignorando o conjunto de agentes em seu entorno. Seus relacionamentos com o Detecta são decisivos para compreender os efeitos desse sistema sobre São Paulo, sejam eles projetos em empresas municipais, nacionais e transnacionais, como Microsoft, Genetec, Techvoz, Seg D'Boa, dentre outras, seus operadores (Polícia Civil, Polícia, Militar, Secretaria de Segurança Pública) ou usuários, como associações e instituições (associações de moradores, universidades ou espaços públicos). A relação entre esses atores parece estruturar uma poderosa e simbiótica rede na qual as linhas de segurança pública e privada, negócios e direitos, e até agenciamentos de humanos e não humanos são obscurecidos, o

que exige não uma abordagem sobre a essência dessas partes, mas sobre o conjunto de relacionamentos e estratégias produzidos por este conjunto.

A organização da segurança pública de São Paulo parece funcionar como um dispositivo (Castro, 2016, p. 194) composto por instituições policiais, empresas privadas, agentes públicos e privados, tecnologias de vigilância, perímetros de segurança, cidadãos, políticas, todos organizados de forma a dar vazão a uma espécie de estratégia. A estrutura que organiza o aparato de segurança em São Paulo ainda permanece em vários aspectos semelhante à de sua criação durante o período ditatorial, marcada por uma forte hierarquia e divisão de atividades entre as forças policiais. Ao passo que a Polícia Militar é orientada a proteger a sociedade civil por meio de patrulhas, atuando também sobre flagrantes, as atividades de investigação são deixadas para a Polícia Civil. Como salienta Costa e Lima (2014), não existe um conceito adequado de segurança pública desenvolvido na ordem jurídica brasileira, e todos os assuntos relacionados a ela vêm da década de 1930 ou foram complementados na década de 1960 durante o período ditatorial. Entendendo a segurança pública como um campo heterogêneo e de características e dinâmicas bastante particulares, os autores descrevem o modo como ele é influenciado pelos militares. Sob essa influência, a polícia adotou práticas repressivas para lidar com a criminalidade, em detrimento de formas de prevenção e controle, como também apontam Sinhoreto, Schlittler e Silvestre (2016).

Nesse sentido, o Detecta não afeta necessariamente a estrutura desse sistema, nem altera diretamente os parâmetros e características desse aparato, cujo conjunto de relações "tradicionais" é descrito por Alvarez, Salla e Souza (2004) como elitista, excludente e geralmente violento contra segmentos sociais marginalizados. Antes, a urgência que o sistema parece

GRÁFICO 1: CRIMES COMETIDOS EM BAIRROS "NOBRES" EM SÃO PAULO, COMO % DOS RESIDENTES (1972-1995)



FONTE: SECRETARIA DE SEGURANÇA PÚBLICA DE SÃO PAULO (2018)

responder é a instauração e sequência de estratégias preventivas que, em sua essência, garantam a manutenção de práticas repressivas e segregacionais. Em outras palavras, o Detecta não insere a polícia e o policiamento em uma dinâmica necessariamente moderna, na qual as práticas atuariais, preventivas e de classificação de risco inibiriam a ação violenta da polícia, mas pelo contrário, ele parece dar margem para novas formas de produção de violência e insegurança. Isso pode ser observado a partir dos dados publicados pela Secretaria de Segurança do Estado de São Paulo (2018). Desde a adoção do sistema Detecta (2014), houve apenas uma ligeira queda nas taxas de assalto na cidade (de 209.536 assaltos para 186.078, em 2017), em homicídios culposos (de 587 para 423 em 2017). No entanto, houve um grande aumento no tráfico de drogas (de 6.521 para 9.173 em 2017) e um grande salto na ocorrência de violência policial, não apenas na cidade, mas em todo o estado (que salta de 369 ocorrências em 2013 para 939 em 2017).

O Gráfico 1 vai além e mostra que os crimes cometidos em bairros de classe média alta ou alta de São Paulo - espaços

que adotaram o Detecta ou iniciaram sua adoção - como assaltos comuns, homicídios, tráfico de drogas, aumentaram ligeiramente desde a introdução do Detecta em São Paulo. Ao mesmo tempo, as estatísticas da Secretaria dos últimos dez anos mostram que os mesmos crimes, principalmente homicídios e estupros, ainda afetam substancialmente bairros pobres de São Paulo, como Jardim Herculano, Capão Redondo e São Mateus, o que corrobora com os argumentos de Paula Miraglia (2011) de que a violência ainda se distribui geograficamente de maneira desigual na cidade.

O Detecta parece espalhar um modelo comum de vigilância, produzido em conjunto por instituições privadas (transnacionais) e públicas, reorganizando a segurança pública como um aparato público-privado, o que, como veremos, irá reforçar características tendenciosas e segregacionais na cidade.

No entanto, a maioria dos discursos recentemente difundidos sobre a eficácia desse sistema de vigilância não estava relacionada exclusivamente às altas taxas de criminalidade na cidade, mas à sua capacidade de lidar com problemas que supostamente surgiriam do que James Holston (2013) define como "cidadania insurgente". Essa, muitas vezes manifestada na intensa circulação de pessoas e de grupos de diversas origens e condições sociais em espaços anteriormente exclusivos, como praças no centro da cidade, *shopping centers*, aeroportos e bairros nobres. Em vista disso, o Detecta garante às autoridades de segurança governar e modular os fluxos circulantes da cidade, atuando potencialmente em problemas como: a instabilidade política e os riscos políticos que supostamente surgiriam das manifestações populares; a aglomeração de pessoas e os riscos de ataques terroristas durante grandes eventos que seriam baseados na cidade; o confronto com o que o governo chama de processos de degradação social, como no caso da região da Luz, denominada popularmente como "cracolândia",

onde há um crescente conflito entre interesses imobiliários e a permanência de moradores de rua e drogados na região da Luz.

O diagnóstico que sustenta a implementação do Detecta parece responder à intensa circulação e mobilização que supostamente resultariam em crimes em alguns espaços, como pontua a criminologia ambiental (Clarke, 1980; Felson, 2002). Portanto, a capacidade de governar pessoas em espaços públicos, interrompendo sua circulação, produzindo espaços estéticos favoráveis à produção de segurança, parece ser a realização estratégica que orienta esse dispositivo.

No entanto, para a estabilização e expansão interna desse dispositivo, a violência diária precisa ser constantemente abordada e evocada, e o estado de desconfiança deve ser mantido permanentemente. Essa perspectiva sobre o dispositivo coincide com a ideia de securitização de questões sociais exploradas por Didier Bigo (1995), na qual o aumento da capacidade de governar a segurança depende da produção de insegurança na própria sociedade. Estritamente, também a governamentalidade em Foucault, como explorada por Lemke (2017) e Optiz (2011), pressupõe um governo (através) do medo, ou seja, a produção e reprodução constantes de ameaças à liberdade como forma de expandir as tecnologias disponíveis combater e "gerenciar" essas ameaças.

Nesse dispositivo de segurança no qual o Detecta está inserido, um *assemblage* público-privado, opera um discurso de medo sobre determinadas formas de circulação na cidade – como será apresentado em seguida, na discussão dos eventos de segurança eletrônica – , ao mesmo tempo em que é reorganizada a distribuição de aparatos de segurança na cidade, introduzindo perímetros de intensa vigilância e controle. Esse discurso é pronunciado inúmeras vezes em congressos, por autoridades, empresários e gerentes, a fim de garantir o fluxo circulatório de pessoas na cidade, entendendo que qualquer

forma de circulação não registrada, qualquer forma de circulação desviante de pessoas em determinados bairros pode ser considerada uma ameaça e gatilho para a intensificação de ilegalidades e desordens. Como resposta, este dispositivo estimula, por um lado, a dispersão e integração de câmeras público-privadas que ajudariam a reduzir os custos da gestão da segurança pública por meio de um monitoramento automático e constante da cidade, por outro, estimula que os cidadãos desenvolvam e mantenham um exercício ativo de vigilantismo.

Com relação aos gestores estaduais e municipais, e aos agentes de segurança que operam o Detecta, existe a percepção de que esse sistema seria útil para reduzir o tempo de serviço e as operações de despacho de oficiais e veículos a partir da aquisição de uma "maior consciência situacional". Mais do que isso, a automação do sistema permitiria a rápida identificação de veículos a partir da leitura analítica de placas, facilitando as abordagens pela Polícia Militar e a investigação e identificação de suspeitos pela Polícia Civil.

Assim, a ideia de integrar sistemas de segurança que antes eram "ineficientes" se torna a chave para garantir que a segurança seja governada com eficiência. Projetos como o *Citiwise* da Genetec e o Segurança Pública e Segurança Nacional da Microsoft, presentes em alguns distritos de São Paulo, sustentam que o governo da segurança só seria possível se distribuído entre agentes de segurança e residentes, uma vez que este é responsável pela vigilância e zeladoria de seus territórios. Conforme afirmam Amicelle, Aradau e Jeandezbos (2015, p. 46), os dispositivos de segurança realizam a segurança a partir da reconfiguração dos espaços sociais, redefinindo fronteiras e redistribuindo significados nas redes de relacionamentos.

Entre os eventos de segurança pública de 2018 e 2019 que buscaram apresentar os sistemas que compõem o Detecta, quatro deles se destacaram: a *International Security Confe-*

rence & Exposition (ISC); a Feira de Segurança de Defesa da América Latina (Segurança da LAAD); o "*DroneShow*"; e, finalmente, o Simpósio de Segurança do Condomínio, organizado pelo deputado estadual "Coronel Camilo" em 2018. Esses eventos ocorrem anualmente e são organizados por empresários, nacionais e internacionais, geralmente mediados pela Associação Brasileira das Empresas de Sistemas Eletrônicos de Segurança (ABESE). Frequentada por empresários, membros de associações condominiais, membros do poder público e profissionais de segurança, essas feiras dispõem de estandes nos quais empresas divulgam seus produtos, apresentam informações em seminários, além de mesas redondas em que são debatidos temas relativos à segurança. Frequentemente, ministros e secretários de segurança, além de militares, apresentam falas e perspectivas relativas à segurança pública e internacional. Nesses espaços, as "redes de especialistas", principalmente empresários de segurança e segurança eletrônica, empresas de defesa e agentes de segurança, são responsáveis pela manutenção de um "*continuum* semântico" em relação à maneira como a segurança é gerenciada (conectando segurança pública e segurança internacional), operando discursos de medo e explorando possíveis soluções. Com base na abordagem de Bigo (2008), esses eventos demonstram como a segurança se torna uma atividade gerenciada por "especialistas", organizados em cadeias globais de defesa e segurança que:

> Clamam, pela "autoridade das estatísticas" ter a habilidade de ranquear e priorizar ameaças, e determinar o que constitui exatamente a segurança. (...) Segurança é, assim, reduzida conceitualmente a tecnologias de vigilancia, extração de informações, ações coercitivas contra vulnerabilidades sociais e estatais, em geral, uma forma de sobrevivência ampla contra ameaças de

> diferentes setores, mas também, segurança é algo desconectado do humano, das garantias legais e sociais, e das proteções individuais (Bigo, 2008, p. 12).[3]

Assim, o foco desses discursos e diagnósticos nunca é direcionado para a compreensão das ameaças (criminalidade) com relativa profundidade, mas aponta continuadamente para a certeza de que os ganhos de eficiência nas operações policiais e um regime de ampla visibilidade se traduzirão na redução do desconforto. No evento ISC Brasil 2018, era comum encontrar revistas especializadas estimulando o medo, produzindo o *continuum* semântico de segurança (como se ameaças terroristas estivessem relacionadas a crimes e outras ofensas no Brasil) e sustentando agendas conservadoras para lidar com os problemas de segurança. Algumas das manchetes dispostas nessas revistas destacavam: "Infra-estrutura: como um colapso estrutural pode afetar o planejamento de segurança corporativa e pessoal"; "Terrorismo doméstico e segurança privada"; "O sutil terrorismo brasileiro"; (Almeida, 2015a; Nunes, 2015; Almeida, 2015b). Em geral, as manchetes procuravam fundir pânico moral, discursos de medo, "tabus" e sugerir noções de empreendedorismo na segurança pública e soluções "tecnofílicas" para lidar com isso.

Em uma versão menor, um evento de segurança de condomínios que acompanhamos como convidados reuniu em uma sala agentes de segurança, representantes dos Conselhos de Segurança Comunitária (Consegs), empresários e políticos manobrando a mesma lógica de vigilância de segurança, mas enfatizando a participação da comunidade na divisão de custos e responsabilidades pela administração da segurança. Durante a palestra de um comandante da Polícia Militar sobre a série de crimes que ocorrem em torno desse condomínio comercial, foi solicitado que a plateia (residentes, curadores,

presidentes de associações e comerciantes) refletisse sobre a importância de adquirir equipamentos de vigilância e segurança, além de incentivá-los a participar do programa Vizinhança Solidária.[4] Este é um projeto que organiza o vigilantismo civil em bairros da capital – inspirado pelas práticas de "*neighborhood watch*" no Reino Unido e EUA – e ajuda a criar um ambiente de engajamento em segurança entre os moradores, bem como abre espaço para introduzir sistemas de vigilância eletrônica, e apresenta recomendações de segurança que variam de "não seja indiferente ao que acontece ao seu redor"; "Seja amigável [com os funcionários], mas discreto"; "Verifique os sinais de perigo no seu bairro"; "atenção a disfarces comuns", "seja um bom observador" e, principalmente: "instale câmeras de segurança", porque "Esse controle visual é fundamental, pois uma imagem pode ser decisiva para prevenir, reprimir ou investigar um crime" (Camilo, 2018).

É justamente nesse contexto, da organização sociotécnica das comunidades nos distritos de classe média e alta, que um novo conjunto de empresas de sistemas de alarmes e de câmeras de segurança começa a se estabelecer. Em geral, essas empresas passam a mediar a relação entre associações de moradores, empresas de tecnologia, estado e município, orientando a aquisição, fornecimento, instalação de câmeras e sistemas de comunicação entre os moradores, em alguns casos até treinando os residentes para identificar problemas. Uma das maiores empresas nesse campo entende sua atividade como um verdadeiro "projeto social", pois dá a sensação de empoderamento entre os moradores para lidar com problemas relacionados à segurança pública.

A introdução do Detecta modifica uma série de relacionamentos, comprometendo e capacitando os setores privados e associações de moradores para auxiliar no "combate ao crime", ativando-os como um segmento do dispositivo de segu-

rança. Mas como cidadãos capacitados, agentes de segurança e sistemas baseados em algoritmos se combinam em uma *assemblage* que intensifica o processo de segregação na cidade?

OS NOVOS PERÍMETROS DE SEGURANÇA, E VELHOS PADRÕES DE SEGREGAÇÃO

A automação não está em nenhum lugar 'completa', nem em São Paulo, nem em Nova York; ela sempre depende de algum tipo de agência humana para o gerenciamento das imagens produzidas e monitoramento das câmeras. Em São Paulo, esses sistemas são fortemente dependentes de agentes de segurança pública e privada nos processos de monitoramento e produção de informações para as estratégias do governo. Esse processo de vigilância é auxiliado pelo uso de aplicativos de comunicação (ou particulares, ou o próprio *Whatsapp*) disponibilizados aos moradores em perímetros de segurança, que não são apenas direcionados ao monitoramento, mas também à identificação de áreas perigosas, sugestão de melhores caminhos para o transito dos usuários em certas localidades, além de disponibilizar um canal exclusivo para a comunicação entre usuários, agentes de segurança privados ou com a polícia.

Diante disso, o olhar subjetivo do agente de segurança ou do cidadão vigilante completa o aparelho de vigilância com sua "intuição" ou "experiência". Por meio desse processo, um sistema de vigilância extremamente sofisticado atende à tradição de preconceito e discriminação que marca a atividade policial do estado, conforme explorado por Alvarez, Salla e Souza (2004) e Caldeira (2016). O Detecta, portanto, ativa o olhar humano (dos residentes em perímetros, de agentes de segurança privados, em geral, de não profissionais de segurança), seus tradicionalismos e preconceitos como partes de um aparato de visuali-

zação amplificado e sofisticado, capaz de modular e restringir padrões indesejados de circulação em determinados espaços.

O Detecta, assim, permite a combinação das práticas discriminatórias costumeiras com um regime de visibilidade estendido e distribuído, controlando e modulando as circulações em ambientes específicos da cidade. Isso é permitido dada a dinâmica de expansão do sistema de câmeras, amplamente dependente da iniciativa privada, a qual tende a se concentrar nos bairros de classe média alta de São Paulo, nos centros de negócios e em alguns espaços públicos de alta circulação pública, formando o que chamamos "perímetros de segurança". Esses territórios são formados através da agência de empresas de monitoramento eletrônico nacionais e transnacionais, que convocam reuniões com associações de moradores, comerciantes e agentes de segurança, onde oferecem soluções eletrônicas como sistemas eficazes para lidar com as ameaças e sua difusão. Eles fornecem serviços de instalação de câmeras, aplicativos móveis para acesso a imagens e comunicação entre residentes (às vezes os treinando), e conferindo acesso exclusivo à polícia.

Nesses perímetros, o medo do crime e da circulação de pessoas indesejadas é constantemente amplificado por empresas eletrônicas, policiais e pela comunicação desordenada em aplicativos de bate-papo. Esse processo, juntamente com o empoderamento dos moradores ou trabalhadores para visualizar, identificar e "agir" sobre determinadas "ameaças", ajuda a produzir alguns efeitos adversos. Como Lucas Melgaço (2010, p. 105) aponta, muitas vezes o sentimento de insegurança mobilizado em certos espaços é desproporcional a riscos reais e isso forma uma "psicoesfera do medo" na qual ideias, crenças e paixões são frequentemente mobilizadas para produzir sensações e temores entre os habitantes. Segundo o autor: “A psicoesfera aparece como pré-condição e justificativa

para a instalação de uma tecnosfera de segurança. Ela diz respeito a todas as formas de materialidade técnica em torno do ideal de segurança e inclui processos de securitização".

Alimentada pela disponibilidade de recursos privados de vigilância para a expansão do dispositivo, essa psicosfera potencializa tensões relacionadas à circulação de "indesejados" nesses perímetros. Conforme já mencionado na cartilha "Vizinhança Solidária", nota-se que a circulação de pessoas, bem como a multiplicidade de relações adversas que supostamente levariam ao crime, são objetos a serem securitizados e mantidos em vigilância permanente.

Em geral, as empresas de segurança eletrônica atuarão de forma a mediar a relação entre associações de moradores, estado e município, por um lado, orientando a aquisição, fornecimento, instalação de câmeras e sistemas de comunicação entre os moradores, em alguns casos até treinando o residentes para identificar problemas, por outro lado, garantindo que as imagens dessas câmeras possam ser acessadas e usadas pelo estado e pelo município - vendendo também dados analíticos adquiridos ao estado. Como já afirmado, uma das maiores empresas nesse campo entende sua atividade como um "projeto social", pois fornece o sentimento de empoderamento entre os moradores para lidar com problemas relacionados à segurança pública. Em uma entrevista com um executivo desta empresa, a ideia de empoderamento social, aproximação entre os moradores e o dispositivo é esclarecida:

> E o viés social é o que norteia [a empresa]. Claro que qualquer projeto social tem um fomentador, alguém que o mantenha. E quem o mantém são os moradores, que pagam uma taxa mensal para a sua instalação, e para ter acesso a essas imagens, e em contrapartida, ceder a internet, as imagens e a energia dele, para que as câmeras

> possam ficar no ar permanente, e sem nenhum tipo de contaminação política. Pois nosso maior problema, desde o início, foi não ter nenhum tipo de ingerência política, pode mudar o político, mas não a política social. Então a responsabilidade de não usar o poste da prefeitura, pois nós usamos o poste do morador afixado na calçada. Enfim, usamos tudo da comunidade, e ela entende que ela é um agente ativo agora, e o que é melhor, ela cede a câmera dela e ganha todas as outras, então a diferença é que ela sai do eu e vai para o nós, com um ganho multiplicador (Entrevista 01, 2018).

A exposição do executivo enfatiza muito não apenas a ideia de associativismo, e solidarismo que adviria da instalação desses sistemas de monitoramento inteligentes ligados ao Detecta e City Cameras, mas fundamentalmente uma ideia de despolitização do sistema, que se torna permanente e pertencente aos residentes, bem como sua independência em relação aos poderes políticos – cuja escassez de recursos poderia comprometer as dinâmicas de policiamento. Mais adiante, o executivo explica melhor a relação entre a propagação do Vizinhança Solidária e seu modelo de negócio que amplia as câmeras disponíveis ao sistema Detecta:

> O Projeto da PM me despertou, pois eles querem se relacionar pelo Whatsapp, mas eles não podem fazer com que eles [os residentes/clientes] tenham custo ou gasto, mas eu posso como empresa, apresentar para eles uma ferramenta que seja de baixo custo e que melhore essa relação. Assim, a câmera que não é um primeiro momento do Vizinhança Solidária, se tornou um atrativo para que as pessoas venham para o Vizinhança Solidária para ter a câmera do outro. É a curiosidade, é a natureza

> humana, só que isso faz com que ele possa participar de forma tranquila, de relacionar com seus vizinhos. Como você faz com que os vizinhos se conhecerem, acaba a desinteligência, a falta de inteligência. E quando tem mais inteligência na relação, aparece o respeito, diminui o tráfico e diminui o crime (Entrevista 01, 2018).

Haveria portanto uma simbiose de interesses entre a promoção de um programa de policiamento comunitário, interessado em alterar as condutas e práticas de uma determinada localidade, em favor de um maior vigilantismo e um estado de permanente desconfiança – tal qual descrito por Garland (2008) ao explorar a nova cultura de controle, como forma para sua expansão – e os interesses das empresas privadas em expandir os serviços prestados.

Como David Lyon (2018) aponta em sua discussão sobre a nova cultura de vigilância que organiza o capitalismo contemporâneo e a dinâmica social e urbana, o indivíduo se torna um nó extremamente relevante na rede, pois produz deliberadamente informações que revelam uma série de dados considerados preciosos para empresas de análise de dados. Da mesma forma, o residente desses perímetros se torna um componente fundamental desse dispositivo de segurança, não apenas como amplificador de receptores do discurso do medo que o faz crescer, mas como produtor-consumidor desse sistema de vigilância, uma espécie de *hub* que produz informações através da disposição e compartilhamento dos *links* de suas câmeras, e consome permanentemente as informações produzidas por elas e pelas de seus vizinhos. Seu olhar destreinado, condicionado pelas perspectivas de suspeita permanente dos grupos comunitários do *WhatsApp* e pelas palestras de consultores particulares, parece estimular práticas discriminatórias contra "indesejáveis" nesses perímetros.

Em um perímetro no Alto de Pinheiros, a empresa Aster opera um sistema chamado "Suspicious Cam". Este sistema de câmeras possui um analítico de imagens (um algoritmo de análise de imagens a partir de critérios pré-estabelecidos) que acusa a invasão de um determinado espaço, emitindo um alerta de evento para agentes privados. Esse analítico específico é conhecido no mercado como "Loitering", cuja tradução direta para o português seria "vadiagem", termo que no Brasil se refere a uma lei de 1941 considerada um instrumento elitista para a sujeição das classes trabalhadoras, comumente conhecida como "Lei da Vadiagem" – que criminaliza a ociosidade do indivíduo que circula nos espaços públicos. Durante o período ditatorial, essa lei foi responsável pela maioria das prisões em flagrante delito nas áreas metropolitanas (Villela, 2014). Não é de surpreender que essa analítica pareça reencenar essa prática de subjugação na forma de uma sequência de "códigos-fonte" que comporão o algoritmo, justificando suspeitas preventivas sobre as pessoas que circulam nesses perímetros de segurança, atendendo às demandas dos moradores estimulados pela psicosfera do medo.

O algoritmo é um produto da ação humana, resultado de uma série de interações, disputas entre valores, interesses e programação que, como toda tecnologia, são cristalizadas (feitas permanentes) e encaixotadas (*black-boxed*) em artefatos Latour (1991; 1994). Dependendo dos arranjos entre os participantes, que variam de cientistas de dados, empresas, agentes de segurança, residentes, sistemas de câmeras, algoritmos e os dados anteriores que "treinam o algoritmo", uma configuração específica da análise é desenvolvida e acaba incorporando formas enviasadas de identificação e visualização das imagens pelos sistemas de processamento Scannel (2016) e Benjamin (2019). Nesse sentido, essas análises fixam um certo padrão de conduta considerado normal pelos par-

ticipantes que a desenvolveram, e qualquer coisa que não se encaixe nisso pode estar suscetível a alertas suspeitos. Os analíticos agem de forma a dificultar as possibilidades de movimentos aleatórios de seus sujeitos (circular ou não em calçadas, permanecer por muito tempo parado em certo lugar, vestir-se de forma específica, etc.), forçando um padrão único de comportamento considerado normal; a rigor, ele institui uma forma de previsão que elimina outros cursos de ação possíveis. A incerteza e a aleatoriedade dos indivíduos são traduzidas pelas análises como certas e claras rupturas da normalidade, autorizando e legitimando ações discricionárias sob o manto preventivo-proativo.

Um caso em que essas *assemblages* entre visões tendenciosas e o sistemas de monitoramento do Detecta é o de uma universidade em São Paulo investigada. Esse espaço é um perímetro de segurança formado durante a expansão do Detecta no início de 2018, composto por uma multiplicidade de aplicativos e câmeras distribuídos pelo campus e plataformas de mediação digital. O território passa a ser controlado eletronicamente a partir de uma central de monitoramento. Com todos os seus acessos assistidos por câmeras que podem incorporar análises, a universidade fornece aos alunos e servidores um aplicativo móvel que inclui um "botão de pânico" que pode emitir alertas no caso de um incidente. O alerta emitido é relatado em um mapa da plataforma do Google em uma tela e as câmeras de perímetro são acionadas. Em geral, a rotina é o monitoramento das câmeras por agentes que, como dizem, têm a "experiência" para identificar desvios e comportamentos suspeitos.

Por algumas vezes, no entanto, as câmeras dessa central pareciam apontar para as mesmas pessoas, jovens negros ou pardos que "divergiam" do estereótipo tradicional de estudante. Os casos demonstrados também envolveram assaltos cometidos por pessoas com as mesmas características, fazen-

do aparecer um padrão recorrente. Em uma situação atípica durante a visita, o oficial de segurança identificou um comportamento suspeito: um jovem pula nas grades de uma das faculdades e depois é surpreendido pelos agentes de segurança. Após a verificação, concluiu-se que o jovem trabalhava com serviços gerais naquele colégio e encontrou nesse "desvio" a melhor maneira de chegar ao local de trabalho, como sempre fazia.

Esse “falso positivo” expõe o fato de que as câmeras, dispostas em locais estratégicos do campus (e em geral dos demais perímetros de segurança), além de fornecer suporte para investigações, costumam apontar para um tipo de circulação indesejada, alinhada com um padrão estético das periferias, reforçando uma legitimação por um regime de visualização em seus registros. Por outro lado, o interessante é que esse regime de visibilidade expõe comportamentos, desvios e práticas que não necessariamente constituem crimes, mas também não se enquadram nos padrões aceitáveis dessa cultura de controle, o que os torna passíveis de identificação e modulação por agentes privados em nome da segurança.

Por um lado, percepções particulares de moradores e trabalhadores dos perímetros de segurança parecem interagir com as câmeras com algoritmos analíticos, tornando durável uma dinâmica de suspeição permanente governada por algoritmos e agentes privados. Por outro lado, nos perímetros em que esse analítico não estaria disponível, o estado de suspeita é perpetuado pela *assemblage* entre olhares e percepções enviesadas e os novos sistemas de câmeras. Nesses casos, a discriminação parece ser mediada por algoritmos que performam alertas preventivos, enquanto a dinâmica de segregação se dá a partir da ação de grupos privados, que atuam sobre a circulação de pessoas em determinadas áreas, interrompendo-a sempre que necessário.

CONSIDERAÇÕES FINAIS

Esta reflexão explorou como o processo de inscrição de conceitos policiais (ligados a uma Criminologia ambiental, traduzida por Garland como cultura de controle) em um sistema de vigilância e monitoramento permitiu diferentes resultados, quando adaptadas ao contexto brasileiro. Além disso, foi explorado como as novas tecnologias da informação condicionam a segurança como uma espécie de exercício da governamentalidade, produzindo medos, estabelecendo padrões de normalidade e desvio e agindo sobre formas de circulação. As *assemblages* sociotécnicas e público-privadas que compõem o Detecta dão vazão aos interesses e práticas dos diversos agentes que o compõem (residentes de bairros nobres, comerciantes e empresários) e permitem o estabelecimento de uma forma plural de gerenciamento da segurança nesses espaços.

Em geral, a governamentalidade parece paulatinamente informar as práticas policiais, combinando-se com práticas originalmente disciplinares (isolamento territorial, uso do e encarceramento). Como Feldman (2004, p. 334) irá colocar em sua análise sobre segurança pública na cidade pós terrorismo, a "(...) disciplina busca produzir ordem, enquanto a segurança quer guiar a desordem", e consequentemente as práticas de policiamento tornam-se proativas em termos de uma vigilância geográfica, ocupação e estrangulamento de certas comunidades, em paralelo à prisão de transgressores individuais. Esse governo é distribuído entre agentes de segurança pública e privada, residentes e trabalhadores em perímetros de segurança e, nos casos em que a análise de imagens está presente, esse governo é distribuído entre algoritmos e aparelhos sociotécnicos, também dotados de capacidade de agência para estipular comportamentos "normais" e desvios generalizados (Rouvroy & Berns, 2018). De modo mais detalhado, esse partilhamento do governo da segurança nos perímetros se organiza a partir

de uma hierarquia estabelecida por policiais incumbidos para uma determinada área – pelo programa Vigilância Solidária – os quais irão elencar tutores para ruas, criar grupos de Whatsapp para a integração de moradores e tutores, partilhamento de imagens de câmeras, circulação de percepções de suspeitos (a partir das imagens de câmeras de vigilância integradas ao City Cameras ou Detecta), dicas de segurança, além de circulação de reclamações e demandas gerais. Pode ser entendido como um governo coletivo, posto que uma racionalidade preventiva, uma percepção comum de temores parece se constituir ali, estimulando um auto governo entre os moradores.

A menção ao sistema Detecta como um instrumento que "reformula" o aparato de segurança pública não implica em dizer necessariamente que este produziu uma mudança perturbadora na organização das atividades policiais e criminais. Na verdade, a suspeita é que, com toda a nova tecnologia criada pela Detecta, buscando reordenar o policiamento como uma atividade baseada em dados, e com o objetivo de reduzir custos, o único resultado observável parece ser a introdução de um novo protagonismo das empresas nacionais e transnacionais e de civis na modulação do policiamento e vigilância.

A formação de perímetros de segurança não é algo inédito na cidade, como Teresa Caldeira (2016) explorou em seus escritos sobre enclaves fortificados (condomínios) formados entre 1980 e 1990. Naquele período, esses enclaves murados eram diretamente orientados a bloquear a circulação de pessoas, com uma presença fortemente armada de agentes privados, promovendo uma espécie de insularidade da "vida externa".

Os perímetros de segurança contemporâneos, em contraste com os enclaves analisados por Caldeira (2016), não necessariamente bloqueiam ou evitam a circulação de pessoas, mas permitem uma circulação modulada, ao passo que exigem uma atitude vigilante e de zeladoria dos moradores que,

como um executivo de um sistema de monitoramento privado aponta, extrapola questões de segurança, governando várias ações: se as crianças vão à escola, se o descarte do lixo é feito corretamente, etc. (uma espécie de governo da vida cotidiana). A aparência de segurança e controle, a exposição de placas, câmeras e os avisos são entendidos como uma ferramenta fundamental para modular a circulação de pessoas nesses espaços, difundindo a mensagem de uma comunidade empoderada, permanentemente vigilante contra condutas dissonantes.

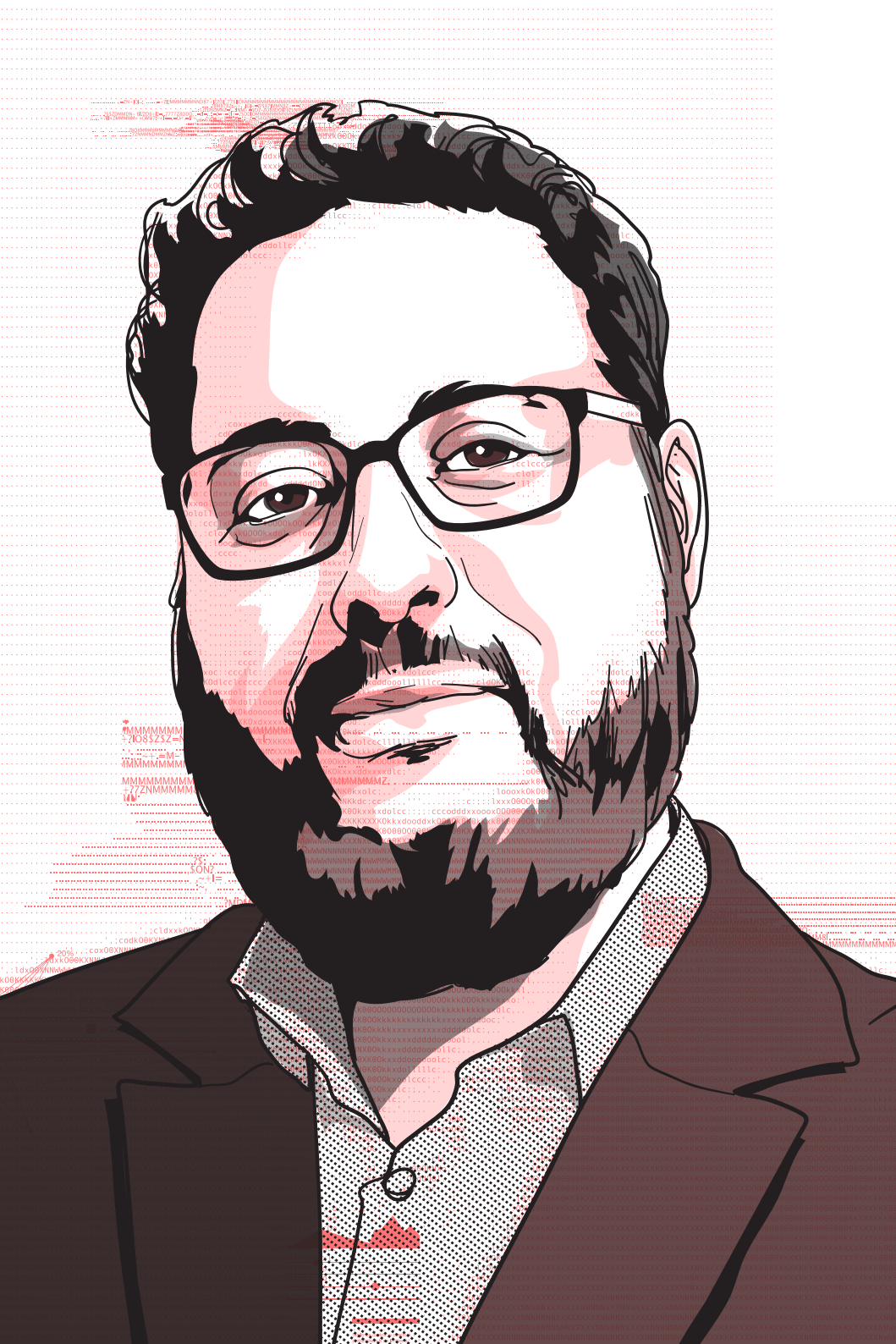
A introdução do sistema Detecta em São Paulo parece articular interesses privados, clientelistas e elitistas no dispositivo de segurança. O vigilantismo e a formação de perímetros de segurança parecem ser respostas exageradas do Detecta em bairros e espaços com taxas de criminalidade relativamente baixas. Em contrapartida, capacita certos grupos sociais e empresas privadas a governarem a segurança pública, tornando-a ainda mais porosa e permeável a interesses particulares.

NOTAS

1. Departamento de Sociologia, Universidade de São Paulo; Pós-doutorando FAPESP; dudperon@gmail.com;

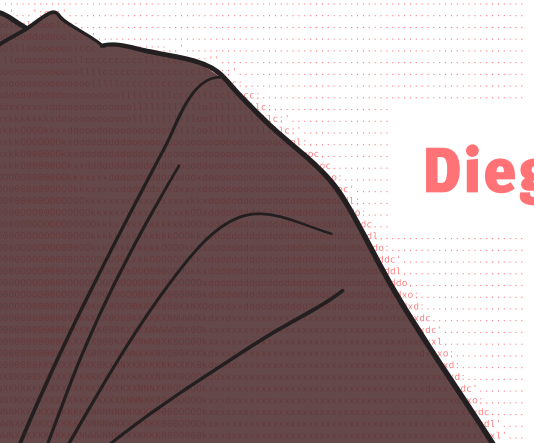
2. Departamento de Sociologia, Universidade de São Paulo; Professor Livre-Docente; mcalvarez@usp.br; pesquisador da FAPESP e do CNPq; coordenador do Núcleo de Estudos da Violência da USP.

3. Tradução nossa, do original "(...) claim, by the "authority of statistics," to have the ability to rank and prioritize threats, and determine what constitutes security exactly. (...) Security is thus conceptually reduced to surveillance technologies, information extraction, coercive actions against social and state vulnerabilities, in general a form of general survival against threats from different sectors, but also, security is disconnected from human, legal and social guarantees and individual protections. (Bigo, 2008, p. 12).



07.

DAS CÂMERAS DE SEGURANÇA AO RECONHECIMENTO FACIAL: OS LIMITES DA TECNOLOGIA COMO RESPOSTA À CULTURA DO MEDO



Diego Coletti Oliva

Nas últimas décadas vivemos um contexto de crescente insegurança em relação à violência e à criminalidade e assim a cultura do medo torna-se parte da vida social e política contemporânea, legitimando discursos e práticas que trazem diversas transformações nas relações sociais contemporâneas, especialmente no que diz respeito aos espaços públicos, ao uso de certas técnicas e processos de securização urbana e à estruturação de determinados padrões de controle e segregação.

A presença cada vez mais intensa de aparatos tecnológicos é evidente, desde as câmeras de segurança e *softwares* de reconhecimento facial, que são o tema deste painel, mas também reconhecimento de placas de veículos, de sons de disparo de armas de fogo, e mesmo o uso de *drones*.

O estudo dos impactos e das transformações trazidas pela presença das câmeras de vigilância em espaços públicos, bem como as justificativas que legitimam esta prática e os recursos investidos em sua instalação e manutenção, tem ganhado cada vez mais espaço e atenção no debate acadêmico, especialmente em países como Inglaterra, Canadá e Alemanha, que hoje abrigam importantes centros de estudo sobre o tema.[1]

O uso e implantação dessas tecnologias tem sido a resposta padrão da segurança pública e privada, e os sistemas de videovigilância ganham destaque nesse cenário, aparecendo como uma espécie de solução definitiva para a criminalidade, trazendo consigo uma diminuição da percepção de risco e insegurança para a população.

E esse padrão se repete, de grandes centros urbanos como Londres, onde um cidadão qualquer tende a ser capturado por cerca de trezentas câmeras de vigilância andando pelo centro da cidade, ou em cidades como Lucas do Rio Verde, no Mato Grosso, que alcançou 100% de sua área urbana monitorada com a instalação de 12 câmeras de videomonitoramento.

Não nego os potenciais benefícios que os sistemas de videovigilância podem trazer tanto para a segurança pública quanto para o sistema de justiça de forma mais ampla. Meu foco aqui nesta breve apresentação será sobre os usos práticos de um desses sistemas, dentro de um contexto que pude analisar empiricamente durante minha pesquisa e que traz à tona algumas questões que considero centrais para se pensar as implicações sociotécnicas da vigilância.

Minha pesquisa foi realizada em Curitiba, famosa por ser considerada uma cidade modelo quando se trata de planejamento urbano e uma pioneira no Brasil na implantação de um sistema de videomonitoramento de espaços públicos. Esse sistema foi inaugurado em 2001, com 14 câmeras instaladas no centro da cidade. Em 2008 esse número sobe para 36, em 2013 eram 116, em 2014 eram 175 e hoje esse número já ultrapassa 500 câmeras em várias regiões da cidade.

A gestão direta do sistema é feita pela Guarda Municipal em cooperação com a Polícia Militar, Secretarias Municipais de Trânsito e Urbanismo e a participação ocasional da Polícia Civil, Polícia Federal e Abin. Por uma questão de logística e infraestrutura, o monitoramento dessas câmeras é feito a partir de vários centros de controle operacional responsáveis por um conjunto de câmeras de uma área monitorada específica.

Aqui surge uma questão interessante sobre o caso curitibano: apesar do discurso oficial e midiático de enfrentamento da criminalidade, combate à violência e até redução de homicídios, quando mapeei a distribuição das câmeras, pude notar que a maioria delas são instaladas em áreas valorizadas, espaços destinados ao consumo, parques e áreas turísticas e as chamadas "Ruas da Cidadania", que são uma espécie de galeria de serviços públicos localizadas em pontos estratégicos da cidade. Poucas são as câmeras instaladas em regiões consideradas perigosas ou com altos índices de criminalidade, salvo exceções.

Assim, a instalação de sistemas de videomonitoramento urbano é associada a um processo de revitalização dos centros das cidades e de revalorização do espaço público enquanto espaço de consumo, agindo no sentido de manutenção de uma certa ordem socioespacial já estabelecida, garantindo a permanência das desigualdades.

VIGILÂNCIA E DESAPARECIMENTO

Diversas técnicas de securização urbana têm sido postas em prática ao redor do mundo, muitas vezes, como no caso de Curitiba, aliando-se a estratégias de planejamento e de gestão urbana, visando revalorizar e ressignificar o espaço público. Apesar de provocarem diferentes transformações e efeitos diversos, todas elas reforçam a segregação e desencorajam encontros entre as diferenças. No limite, todas elas criam fronteiras policiadas e, consequentemente, promovem a intolerância, a suspeita e o medo.

> No contexto de crescente medo do crime e de preocupação com a decadência social, os moradores não mostram tolerância em relação às pessoas de diferentes grupos sociais, nem interesse em encontrar soluções comuns para seus problemas urbanos. Em vez disso eles adotam técnicas cada vez mais sofisticadas de distanciamento e divisão social. Assim, os enclaves fortificados – prédios de apartamentos, condomínios fechados, conjuntos de escritórios ou shopping centers – constituem o cerne de uma nova maneira de organizar a segregação, a discriminação social e a reestruturação econômica [...] diferentes classes sociais vivem mais próximas umas das outras em algumas áreas, mas são mantidas separadas por barreiras físicas e sistemas de identificação e controle. (CALDEIRA, 2000, p. 255).

É aqui que se encaixam as câmeras de videomonitoramento urbano, legitimadas pelo discurso do medo e da busca constante por segurança, mas profundamente ligadas a ideias como a de permanência e de mobilidade, de visibilidade e de desaparecimento. Não o desaparecimento de todos, nem tão pouco o desaparecimento apenas do crime e da violência, mas a invisibilização também daqueles que não podem contribuir com a propaganda da cidade modelo, moderna e limpa, nem como consumidores nesses espaços de consumo, nem sequer como cidadãos.

Nesse contexto, a análise foucaultiana do panóptico de Jeremy Bentham parece não dar conta do sistema de videomonitoramento e, em certa medida, o foco nos mecanismos disciplinares e na vigilância sobre o indivíduo perde um pouco de sentido. Não posso negar que a armadilha da visibilidade interiorizada pelo próprio vigiado continua presente modelando gestos e comportamentos, assim como a invisibilidade do vigia e a inverificabilidade de sua ação também continuam garantidas. O que falta nessa equação, contudo, é a correção dos desvios, seja através de uma rotina rigorosa e repetitiva, seja através de sanções normalizadoras típicas das disciplinas. O *vigiar* está presente, mas não se conecta tão diretamente como antes ao *punir*. Quando a vigilância é exercida através das câmeras, com o observador deslocado do lugar onde estão os observados, o indivíduo que desvia da normalidade não é mais alvo de punição exemplar, mas antes da recusa ao acesso, da exclusão e da segregação.

Nesses novos ambientes monitorados urbanos o objeto do poder e do saber do gerenciamento das cidades não é mais o indivíduo; é por esse motivo que a contestação da vigilância urbana pela via da privacidade individual perde força ao centrar o debate nessa figura disciplinar – o indivíduo – que não está mais em questão para o videomonitoramento urba-

no. Por mais que esta visão esteja proliferada pela mídia e pelo próprio sistema de monitoramento, por meio dos avisos de área monitorada, ou até mesmo pelos poucos grupos de contestação que insistem em seguir essa linha de argumentação, esta visibilidade trazida pelas câmeras não individualiza e não é para todos.

A sensação de estar visível gera de fato um ajuste comportamental nos indivíduos, sem dúvida alguma, mas o faz na medida em que o torna invisível, porque o força a integrar-se ao fluxo. Essa invisibilidade, contudo, é diferente do desaparecimento, que discuti anteriormente. Em outras palavras, em um sistema de videomonitoramento urbano como o de Curitiba, todos somos inicialmente invisíveis enquanto indivíduos. Será alvo da observação aquele que se destacar do fluxo, seja o mendigo deitado sobre a grama no parque, o usuário de drogas sentado em um banco, a prostituta parada na esquina, o grupo de jovens da periferia andando a esmo pelas ruas do centro. Nesse sistema de vigilância, são estes os casos que se tornam visíveis, não como erros que deverão ser corrigidos por um castigo exemplar, mas simplesmente como erros a serem eliminados, erros que devem, portanto, desaparecer.

> "Existia um problema muito grande naquela praça, uma grande concentração de pessoas paradas sem fazer nada lá. No início quando a gente colocou as câmeras, começava a perceber as coisas, chamava a viatura, a viatura ia lá... assim, não acabou com o problema, mas a Praça 19 de Dezembro, o que era uns anos atrás e o que ela é hoje tá bem diferente". (Entrevista com um dos gestores do sistema de monitoramento de Curitiba).

Esse efeito de desaparecimento dos desvios ao invés da correção dos mesmos é um fator muito importante a ser le-

/ O VIGIAR ESTÁ PRESENTE, MAS NÃO SE CONECTA TÃO DIRETAMENTE COMO ANTES AO PUNIR /

vado em conta quando analisamos as câmeras de vigilância enquanto dispositivos de poder, e é um fator também que distancia o videomonitoramento do sistema panóptico foucaultiano. Ainda assim, pela bibliografia levantada para a produção desta dissertação, são poucos os autores que voltaram sua atenção para essa questão, enquanto grande parte da literatura ainda mantém suas leituras limitadas ao modelo de Bentham e Foucault.

Por esse motivo, e pela minha própria experiência em campo, me parece muito mais produtivo aproximar-se da proposta de Kanashiro (2008) ao afirmar que o que se vê em campo não é um incentivo aos conflitos, como diria Koskela (2003), mas, ao contrário, um desaparecimento deles para tornar a cidade limpa e segura, e no caso de Curitiba, para manter a imagem de cidade modelo, moderna e homogênea. Nessa lógica do desaparecimento, não importa mais corrigir os desvios individuais. O que as novas tecnologias de monitoramento e controle põem em movimento é a eliminação do próprio desvio, o extermínio do erro através da exclusão e da restrição do acesso e da mobilidade.

As câmeras de videomonitoramento urbano fazem parte de outro regime de visibilidade, que não focaliza mais o indivíduo como nas sociedades disciplinares tão bem analisadas por Foucault. Elas fazem parte de um regime que focaliza o fluxo das pessoas, anônimas em meio à massa de transeuntes e não mais individualizadas e identificadas. Mais do que isso: se trouxermos as contribuições de Erving Goffman sobre a estigmatização de determinados grupos ao debate, podemos ver que as áreas monitoradas na cidade de Curitiba não são apenas – nem principalmente – os espaços totalmente elitizados, mas sim a região central, parques e pontos turísticos; em última instância, espaços marcados pelo que Goffman chama de *contatos mistos*.

Os sistemas de videomonitoramento urbano têm, nesse sentido, um papel essencial nesse processo, pois eles próprios são as ferramentas ideais para que se exerça um controle contínuo do fluxo de transeuntes, com o poder de atuar diretamente sobre a circulação, a permanência e a mobilidade dos cidadãos. Tal foco sobre a mobilidade articulado ao processo de revalorização e ressignificação do espaço público posto em prática pelo planejamento urbano de Curitiba aponta para o investimento de uma determinada elite da população para ampliar sua própria mobilidade, definir as fronteiras de seus espaços exclusivos, e protegê-los da violência, do crime e, principalmente, dos *indesejáveis*. Revela-se, assim, na capital paranaense, uma radicalização do desaparecimento do conflito e da diferença, que, dita de outra forma, torna-se realidade por meio do desaparecimento de certa parte da população, no limite, uma política de extermínio legitimada sim pelo discurso do medo da violência e do crime, mas marcada ainda mais profundamente pelo medo da diferença.

Na busca por segurança, aceitamos sem questionar a disseminação, numa velocidade assustadora, de câmeras de vigilância e outros recursos de monitoramento de informações. No entanto, o escopo das câmeras não se restringe a filmar apenas atividades criminosas, mas tudo que se passa sob o alcance de suas lentes. O fascínio pela técnica e pelas possibilidades da tecnologia é tamanho que supera os receios do que pode advir dos abusos e negligências de um sistema invasivo de vigilância e controle da informação.

É mais do que óbvia a importância da discussão sobre violência e segurança urbanas e sua relação com a vigilância e a informatização do cotidiano, mesmo porque são temas com o quais nos deparamos diariamente, seja através da mídia, cujo lucro baseia-se, em grande parte, no bombardeio constante dos jornais e noticiários com notícias sobre violên-

cia, seja pelo nosso próprio cotidiano que nos coloca sob o foco das câmeras e outros processos de vigilância em quase todas as nossas ações.[2]

JUSTIFICANDO A VIGILÂNCIA

É claro que o discurso da segurança e do medo está sempre presente quando se busca legitimar a instalação de quaisquer técnicas e dispositivos de securização urbana, mas, durante a pesquisa, tanto bibliográfica quanto empírica, pude estabelecer três objetivos principais relacionados especificamente às câmeras: o poder preventivo, o poder reativo e o poder de viés-probatório, assim classificados em função do tempo de um ato criminoso que venha a ser cometido sob o escopo das câmeras.

O primeiro deles é o chamado poder preventivo, aquele mais frequentemente enfatizado pela literatura sobre vigilância e que também é muito divulgado por aqueles/as que apoiam a instalação das câmeras. Esse poder preventivo relaciona-se à capacidade da mera presença das câmeras de evitar que um crime aconteça no futuro. De acordo com alguns autores/as, este seria o objetivo que as câmeras alcançam com mais eficiência, induzindo no criminoso a sensação de que ele está sendo continuamente vigiado e inibindo sua ação através de uma espécie de ajuste comportamental, visto que cometer um ato criminoso em uma área monitorada constitui um grande risco ao criminoso.

Ao mesmo tempo em que essa presença abstrata do olhar gera no criminoso essa sensação de risco, oferecendo ao "cidadão de bem" uma maior sensação de segurança, enquanto para este cidadão a presença das câmeras equivale à presença de um policial militar ou um guarda municipal que deve estar ali para manter a ordem e protege-lo dos "criminosos" e "marginais". Outro efeito ainda deste poder preventivo das

câmeras seria o ajuste comportamental dos próprios agentes de segurança, sejam da PM ou da GM que, ao atuar em uma área monitorada, tomarão mais cuidado ao realizar suas abordagens de forma adequada, evitando cometer abusos e violências desnecessárias.

> "Por parte do agente público, também ele sabe que ele tem que tomar uma ação adequada, correta legalmente, não é porque o cidadão tá cometendo um crime, que o cidadão tá numa situação de marginalidade que ele vai ser menos respeitado enquanto pessoa, então impõe ao agente público também que atue de forma correta". (Entrevista com um dos gestores do sistema de monitoramento de Curitiba).

Contudo, devo ressaltar aqui que, apesar de o discurso de alguns gestores alinhar-se ao debate teórico e apontar essa como a principal função das câmeras, o que se encontra na prática é um pouco diferente. De fato, as câmeras possuem a capacidade de exercer coercitivamente esse ajuste comportamental e esse poder preventivo, porém seus efeitos são mais evidentes no período imediatamente posterior à instalação das câmeras, enquanto tanto os criminosos, quanto os agentes públicos de segurança e os próprios cidadãos ainda não estão habituados com a presença desses dispositivos. Com o passar do tempo, tanto uns como outros se adaptam às câmeras, se acostumam e até mesmo esquecem-se de sua presença, desenvolvendo novas práticas e estratégias para conviver com elas, ou simplesmente ignorando sua existência.

O segundo objetivo relacionado à instalação das câmeras, e aquele do qual os operadores das mesmas mais se orgulham por serem os responsáveis diretos por sua execução, é o chamado poder reativo, o poder de agir em tempo real durante

uma ação criminosa. Assim, quando o poder preventivo falha e um crime é cometido sob o olhar dos vigilantes, as câmeras tornam-se uma extensão dos olhos dos policiais e guardas municipais e, apesar de não ter sido capaz de evitar o crime, é o videomonitoramento que permite acompanhar o deslocamento do criminoso e eventualmente realizar sua captura. É a vigilância que permite a identificação da atividade suspeita e a ação no momento presente, enviando alertas e coordenando a ação dos agentes nas ruas e impedindo que a ação criminosa seja concluída ou fique impune.

Apesar dos gestores do sistema enfatizarem, durante as entrevistas, mais os outros dois objetivos das câmeras – o preventivo e o de viés-probatório – durante a observação na sala de controle em Curitiba, esse foi com certeza o poder mais enfatizado pelos operadores, orgulhosos de serem os olhos por trás das câmeras capazes de pôr em prática esse poder onipresente. Repetidas vezes em nossas conversas eles comentavam sobre ações desse tipo em que estiveram envolvidos, coordenando a realização de prisões por meio do sistema de videomonitoramento, chegando inclusive a me mostrar as imagens registradas pelas câmeras dessas ações.

Paradoxalmente, esse é com certeza o objetivo em que o monitoramento se mostra menos eficiente, sendo raros os casos em que os criminosos são presos em flagrante graças ao uso das câmeras, e isso acontece por diversos motivos: pela impossibilidade dos operadores de monitorarem atentamente todas as câmeras durante todo o tempo, ou pela incapacidade dos agentes de segurança na rua de atenderem aos alertas emitidos pelo sistema de videomonitoramento imediatamente, e até mesmo pela própria adaptabilidade dos criminosos, atuando nos pontos cegos do sistema ou simplesmente fora das áreas monitoradas, de modo que as ocorrências mais frequentemente flagradas são casos de pi-

chações, usuários de drogas e, às vezes, pequenos traficantes ou furtos do interior de veículos.

O terceiro objetivo das câmeras é aquele chamado pelos entrevistados de poder de viés-probatório, que se relaciona ao tempo passado, a um crime que foi cometido e concluído sob o escopo das câmeras e que teve suas imagens registradas pelas mesmas, de forma que a polícia ou a guarda municipal consegue usar as imagens como documento e prova do crime construindo um banco de dados para investigação e identificação do criminoso. Este é um dos objetivos mais enfatizados pelos gestores do sistema de monitoramento em Curitiba, que afirmaram em entrevista que a maior contribuição do sistema, mais até do que a prevenção e a sensação de segurança, é o poder de responsabilizar o infrator por seus atos.

> "O que eu destaco do videomonitoramento não é tanto pela sensação de segurança que ele traz, mas pela questão da criminalização do marginal. Foi preso, tem a materialidade do crime, a imagem que prova que foi ele, então ele vai responder pelo crime que ele cometeu. Então hoje o que a gente mais fornece aqui são cópias, via judicial, para a criminalização do marginal e isso tem sido bastante significativo. Então o cara sabe que vai ser punido. A maior importância do sistema de videomonitoramento é que você tenha a gravação da imagem que possa servir de ferramenta jurídica para que você possa criminalizar o marginal. Então o marginal sabe que se ele for pego ele será responsabilizado. Vai ter aqui a prova material do crime que ele cometeu, tanto pra identifica-lo quanto pra criminaliza-lo, esse é o grande diferencial, é o que traz de positivo, o cara sabe que se ele foi pego lá não adianta ele dizer que foi isso ou foi aquilo". (Entrevista com um dos gestores do sistema de monitoramento de Curitiba).

OLHOS ELETRÔNICOS E OLHARES HUMANOS

> Para aqueles que promovem o videomonitoramento como uma panaceia para o crime e a desordem nas ruas de nossas cidades, assim como para aqueles que alertam para o espectro do estado distópico de vigilância, há uma concepção em comum: de que o videomonitoramento realmente produz os efeitos que lhe são atribuídos... Neste sentido, ambos compartilham uma tendência a um determinismo tecnológico: uma crença inquestionável no poder da tecnologia, seja ele benigno ou maligno. (Norris & Armstrong, 1999, p. 9, tradução nossa[3])

Como Norris e Armstrong apontam na citação acima, a maior parte dos estudos sobre vigilância, e especialmente sobre vigilância visual e videomonitoramento, está marcada por um determinismo tecnológico que limita a análise dos efeitos da presença das câmeras, assumindo de forma bastante ingênua que a sua operação se efetiva da maneira ideal para a qual foi planejada e ignorando o papel essencial do "elemento humano" por trás das lentes das câmeras.

Essa perspectiva de análise do videomonitoramento coloca os estudos de vigilância em uma posição normalmente teórica, quantitativa e estatística em suas observações e conclusões, e deixa de lado uma abordagem qualitativa da forma como os sistemas eletrônicos de vigilância são operados. A maioria dos autores parece se esquecer que as câmeras não atuam de forma autônoma nem são autoconscientes e só são efetivas na medida que são monitoradas pelos seus operadores, que nada mais são do que indivíduos em uma situação de trabalho, capazes de serem irracionais, disfuncionais e preconceituosos em seu olhar.

São esses operadores que irão observar, interpretar e responder às imagens geradas constantemente pelas câmeras de vigilância espalhadas pelas ruas e praças da cidade. De fato, podemos afirmar que, no limite, sem esse triplo processo de observação, interpretação e resposta, a videovigilância seria absolutamente fútil e completamente sem efeitos, tanto negativos quanto positivos.

Devido a esse privilégio dado às abordagens quantitativas sobre o videomonitoramento, relacionando seus efeitos a indicadores de violência e criminalidade urbanas, muito pouco foi produzido sobre o nível microssociológico dessas relações, e há uma relativa pobreza de dados empíricos sobre a real operação desses sistemas, daí a importância deste trabalho para somar ao campo de estudos da vigilância e através da comparação com os resultados que outros pesquisadores obtiveram em diferentes cidades e instituições para que seja possível generalizar alguns elementos e a partir daí construir teorizações capazes de analisar de forma menos determinista os impactos trazidos pelas câmeras de vigilância para o cotidiano.

PARA ONDE OLHAM AS CÂMERAS?

Ainda assim, existem alguns estudos empíricos que merecem destaque, que serviram como exemplos para a realização da minha pesquisa e como base de comparação para os resultados obtidos. Em primeiro lugar, os estudos de Norris e Armstrong realizados em 1997 e 1999 com sistemas de videomonitoramento em espaços públicos na Inglaterra demonstravam como, na maioria das situações observadas, era o preconceito dos operadores o que determinava quem seriam os alvos das câmeras, mais do que qualquer tipo de comportamento suspeito.

Os autores afirmam que os indivíduos eram vigiados principalmente por pertencerem a subculturas e grupos particulares cuja percepção dos operadores era negativa. Assim, a maior parte dos alvos da vigilância eram jovens do sexo masculino e especialmente negros, desproporcionalmente representados em comparação aos brancos. Além disso, também eram alvo frequente das câmeras os bêbados, moradores de rua e vendedores ambulantes, considerados "fora do lugar" nos espaços privilegiados para o consumo (Norris & Armstrong, 1997).

> O escopo das câmeras não cai igualmente sobre todos os usuários das vias públicas, mas sim sobre aqueles que são estereotipicamente predefinidos enquanto potencialmente desviantes, ou que pela aparência e comportamento, são apontados pelos operadores como irrespeitáveis. Dessa forma a juventude, particularmente aquela que já é social e economicamente marginalizada, pode ser sujeita a ainda maiores níveis de intervenção autoritária e estigmatização oficial, e, ao invés de contribuir para a justiça social através da redução da vitimização, CFTV (circuitos fechados de TV) tornam-se meramente uma ferramenta de injustiça por meio da amplificação de uma política diferenciada e discriminatória. (Norris & Armstrong, 1997, p. 8, tradução nossa).[4]

Outra pesquisa realizada por McCahill com sistemas de videomonitoramento de centros comerciais aponta também para a supervigilância exercida sobre indivíduos em grupo, especialmente jovens que eram observados pelo simples fato de estarem juntos, motivo pelo qual eram sumariamente considerados "causadores de problemas" e retirados do complexo comercial pela equipe de segurança (McCahill, 2002).

Na cidade de Curitiba, os mesmos padrões de observação foram reconhecidos, especialmente no que diz respeito à vigilância exercida sobre moradores de rua, prostitutas, usuários de drogas e grupos de jovens, especialmente membros de subculturas "*punk*" ou "*hip hop*" circulando pelos espaços de consumo da Rua XV de Novembro, no centro da cidade. O preconceito e a percepção negativa dos operadores em relação a esses grupos estavam claramente demarcados em suas falas e ações e, apesar do discurso oficial negar essa relação, a observação das práticas dos operadores tornou impossível ignorá-las.

Retomando o que foi dito no tópico anterior sobre os padrões de segregação socioespacial promovidos pelo planejamento urbano local e o conceito de "consumidores falhos" de Bauman que apontamos, fica clara a atuação do sistema de videomonitoramento urbano como uma ferramenta de manutenção dessa ordem social preestabelecida e de exclusão das diferenças para fora dos espaços de consumo, invisibilizando os conflitos e inviabilizando o encontro com o *outro*.

Outro ponto interessante levantado por Norris e Armstrong, e que traz uma questão de gênero ao debate, é em relação à vigilância sobre as mulheres, que em seus estudos era normalmente exercida apenas por razões voyeurísticas para satisfazer os operadores. Vale destacar aqui que nos casos que esses autores estudaram o ambiente da sala de controle dos sistemas de videomonitoramento era marcado pela exclusividade de operadores do sexo masculino.

A sala de controle em Curitiba, no entanto, não é tão homogênea nesse sentido, sendo que em um local onde trabalham 6 operadores durante o horário comercial, normalmente 2 ou 3 desses indivíduos são mulheres. Apenas no período da noite, quando apenas 4 operadores estão de serviço, é que a presença masculina se torna exclusiva.

Apesar dessa diferença, o olhar voyeurístico sobre as mulheres também se faz muito forte no caso curitibano e são comuns os *zooms* e comentários sobre os corpos femininos capturados pelas câmeras. Embora este não seja o foco desse artigo, é importante problematizar a apropriação dos corpos das mulheres por esses homens. Por mais invisíveis que estejam atrás das câmeras, eles exercem uma vigilância e um abuso sobre aqueles. A objetificação do corpo feminino está imbricada em uma relação de poder que foi culturalmente interiorizada, mas se torna necessário questionar por que esses indivíduos consideram tão "natural" falar, focar e valorar um corpo de mulher sem a sua permissão, mas com total permissividade.

Para compreender tal relação de poder, a pesquisadora Susan Amussen ressalta que nas sociedades ocidentais o homem cumpre um papel dentro de uma chave binária onde acredita que "os homens devem aprender a ser dominadores e ativos e as mulheres a serem submissas; se as mulheres devem ser castas, os homens devem conhecer os limites nos quais eles podem atentar contra esta castidade." (Amussen, 1980). É dentro dessa chave binária de performances que os operadores se colocam como os "analisadores", detentores do poder do olhar acima daquelas cidadãs, perpetuando nesse gesto uma sociedade que dá mais valor ao masculino do que ao feminino. Segundo Saffioti, a sociedade promove altos investimentos para naturalização desse projeto. Essa dominação, contudo, deve ser combatida, pois ela gera não só violências simbólicas como estas, mas é base de todas as violências de gênero (Saffioti, 1987).

A (DES)ATENÇÃO E O FATOR TÉDIO

Outro autor dos estudos de vigilância que traz enormes contribuições para este trabalho é Gavin Smith, que realizou sua pesquisa na sala de controle de videomonitoramento de uma instituição universitária e apontou para interessantes consi-

derações em relação ao trabalho dos operadores e sua relação com os "vigiados" por intermédio das câmeras (Smith, 2004). Uma das principais questões levantadas pelo autor é o que ele irá chamar de "fator tédio,"[5] que nasce de uma rotina monótona e repetitiva de longas horas de trabalho observando imagens sem áudio que mostram essencialmente nada, no interior de uma sala fechada, sem atributos marcantes, numa situação de trabalho com falta de incentivo e excesso de cobrança por resultados positivos.

Por vezes o trabalho dos operadores é tomado como fácil e que não exige esforço, afinal, basta sentar-se confortavelmente em frente ao computador e ficar assistindo as câmeras. No entanto, esse ambiente de trabalho é bem mais cansativo do que pode parecer, e a experiência da observação participante me permitiu não apenas observar mas também sentir os efeitos do fator tédio. Depois de poucas horas no interior da sala, mesmo a minha atenção, que não estava limitada às imagens das câmeras, acabava vagueando para outras questões que nada diziam respeito à observação. Assim, eu pude perceber e entender a situação cotidiana dos operadores.

Na sala de controle em Curitiba trabalham de 4 a 6 operadores, responsáveis pelo monitoramento de 47 câmeras na região central da cidade. A equipe é composta por 3 Guardas Municipais, sendo um supervisor, um Policial Militar, uma fiscal da Secretaria Municipal de Trânsito (SETRAN) e uma fiscal da Secretaria de Urbanismo – sendo que essas duas últimas trabalham apenas no horário comercial, enquanto os GM e PM trabalham em turnos que cobrem o monitoramento 24 horas por dia das câmeras. Os turnos dos operadores da Guarda Municipal – com quem eu trabalhei mais diretamente graças à sua relação privilegiada com o sistema de videomonitoramento urbano que é gerenciado pela Guarda – são de 12 horas por dia, sendo 6 horas na sala de controle e 6 horas em atividades externas.

Manter 6 horas de atenção exclusiva às câmeras de vigilância nesse ambiente apontado anteriormente é praticamente impossível, e, para lidar com a rotina e o tédio do seu trabalho, os operadores põem em prática diversas "estratégias" informais para "passar o tempo" que pude testemunhar durante minha observação.

Assim, era comum, por exemplo, as idas e vindas na sala de controle, enquanto os operadores frequentemente se retiravam de seus postos para fumar um cigarro, tomar um café ou simplesmente "esticar as pernas". Da mesma forma, a atenção dos operadores frequentemente era direcionada para outros objetos que não as câmeras de vigilância, enquanto liam o jornal, acessavam a internet em seus *notebooks*, estudavam para concursos públicos e até assistiam filmes e jogavam enquanto as câmeras eram deixadas em seu *tour* automático com pouca ou nenhuma atenção dedicada a elas.

Em algumas ocasiões, até mesmo a forma como o monitoramento era posto em prática estava mais no sentido de "passar o tempo" do que de fato de exercer a vigilância, como quando os operadores olhavam preços nas vitrines das lojas, acompanhavam situações inusitadas e pessoas conhecidas que passavam sob o escopo das câmeras, direcionavam as mesmas para vigiar seus próprios carros ou até "brincavam" com o sistema tentando abrir 20 câmeras simultaneamente no mesmo computador.

Algumas dessas "estratégias" também foram observadas por Smith em seu trabalho, e o autor argumenta que essas práticas podem ser interpretadas também como, além de uma simples forma de "passar o tempo", uma espécie de resistência dos operadores ao seu ambiente de trabalho, marcado pelas longas horas de trabalho rotinizado, baixos salários, pouco ou nenhum incentivo e motivação e grandes

cobranças por um monitoramento eficiente que não deixe nada passar despercebido.

A maior parte desses argumentos é facilmente transportado para a realidade dos operadores em Curitiba, com exceção do último ponto. Como pude confirmar pelas conversas que tive com os operadores sobre o seu trabalho e sua relação com as instituições envolvidas, ficou claro que de fato são baixos os salários e quase inexistentes os incentivos e o reconhecimento para o trabalho realizado pelos operadores. Porém, os gestores do sistema estão cientes de que o número de operadores é muito baixo para o número de câmeras que devem ser monitoradas (nos horários com maior número de operadores, são 6 pessoas para monitorar 47 câmeras), além do próprio sistema impor limitações ao trabalho dos operadores contando com várias câmeras que necessitavam de manutenção. Dessa forma, inexiste aqui o excesso de cobrança por resultados que Smith aponta em seu estudo.

E O RECONHECIMENTO FACIAL

Indo um pouco além das câmeras, vamos pensar a relação disso com o reconhecimento facial. As tecnologias de reconhecimento facial são desenvolvidas e comercializadas como uma conveniência, seja para desbloquear o celular ou acessar sua conta bancária, mas têm laços claros com a vigilância e o controle.

Teoricamente, os algoritmos utilizados por essas tecnologias seriam capazes de eliminar a subjetividade dos operadores das câmeras, fazendo uma análise objetiva dos dados. Mas, quando estamos falando de *machine learning* (aprendizado de máquina), dados gerados de forma enviesada tendem a levar a resultados enviesados.

Uma pesquisa recente desenvolvida no MIT demonstrou que os sistemas de reconhecimento facial disponíveis no mercado apresentam resultados preocupantes em suas taxas de erro de acordo com gênero e raça-etnia.

Enquanto a taxa de erro na identificação para homens brancos é de 0,8%, para mulheres negras as taxas de erro ficam na média de 20% a 34%. Para definir o gênero de pessoas negras de pele mais escura, a taxa de erro chegou a 46,8%. Basicamente, os softwares estavam atribuindo gênero aleatoriamente.

No contexto da segurança pública ou do sistema de justiça criminal, isso significa que as chances de uma pessoa negra receber um falso positivo, ou falso negativo, por um sistema de reconhecimento facial são muito maiores do que as de um homem branco.

Para concluir, a maior preocupação de pesquisadores e ativistas em relação a essas questões é sobre os possíveis abusos dessas tecnologias para coibir manifestantes, dissidentes e imigrantes (ilegais ou não), abrindo portas para eventuais casos de violações aos direitos humanos.

É claro que essas particularidades apontadas aqui não colocam em jogo o futuro e o potencial do *machine learning* ou dos *softwares* de reconhecimento facial, mas são questões preocupantes quando pensamos em suas possíveis consequências na justiça criminal.

As questões técnicas e sociais são separadas e interdependentes, os vieses técnicos podem ser resolvidos com soluções técnicas, mas mesmo com um reconhecimento facial totalmente funcional, um sistema tendencioso requer soluções culturalmente muito mais complexas. Basta lembrar da TayandYou, a inteligência artificial da Microsoft que em apenas um dia de exposição ao Twitter tornou-se racista e machista.

Precisamos estar abertos e abertas à possibilidade de que as tecnologias de vigilância mais avançadas talvez não sejam necessariamente as melhores em termos de garantias democráticas e de direitos civis.

NOTAS

1. Surveillance Studies Network, Surveillance Studies Centre e Surveillance Studies: Das Forschungsnetzwerk zu Überwachung, Technologie und Kontrolle.

2. A presença da vigilância em nosso cotidiano não se restringe aos sistemas de videomonitoramento ou aos Circuitos Fechados de TV (CFTV), mas estende-se também a cadastros biométricos, transações realizadas com cartões de crédito, rastreamentos via GPS e celular, bem como perfis de redes sociais, e-mails e atividades na internet em geral.

3. "For those who promote CCTV as the panacea to the crime and disorder on our city streets and for those who warn of the spectre of the dystopian surveillance state, there is a common assumption: CCTV actually produces the effects claimed for it … In this way, both share a tendency towards technological determinism: an unquestioning belief in the power of technology, whether benign or malevolent".

4. "The gaze of the cameras does not fall equally on all users of the street but on those who are stereotypically predefined as potentially deviant, or who through appearance and demeanour, are singled out by operators as unrespectable. In this way youth, particularly those already socially and economically marginal, may be subject to even greater levels of authoritative intervention and official stigmatization, and rather than contributing to social justice through the reduction of victimisation, CCTV will merely become a tool of injustice through the amplification of differential and discriminatory policing".

5. Boredom factor no original.

REFERÊNCIAS BIBLIOGRÁFICAS

Amussen, S. D. (1985). Féminin/Masculin: le genre dans l'Angleterre de l'époque moderne. In *Annales ESC*. Paris, vol. 40(2), mar./apr., 1985.

Bauman, Z. (1998). *O mal-estar da pós modernidade*. Jorge Zahar Editor.

Bentham, J. (2006). *O Panóptico*. Autêntica.

Botello, N. A. (2010). Orquestração da vigilância eletrônica: uma experiência de CFTV no México. In Bruno, F.; Kanashiro, M.; & Firmino, R. *Vigilância e visibilidade: espaço, tecnologia e identificação***.** Editora Sulina, pp. 17-35.

Bruno, F.; Kanashiro, M.; & Firmino, R. (2010). *Vigilância e visibilidade: espaço, tecnologia e identificação*. Editora Sulina.

Castro, R. B.; & Pedro, R. M. L. R. (2010). Redes de vigilância: experiência de segurança e da visibilidade articuladas às câmeras de monitoramento urbano. In Bruno, F.; Kanashiro, M.; & Firmino, R. (2010). *Vigilância e visibilidade: espaço, tecnologia e identificação*. Editora Sulina, pp. 36-60.

Corrêa, L; & Cunha, M. (2009). Câmeras no jornal: cartografando o discurso jornalístico sobre a vídeo-vigilância no Brasil. In VIGILÂNCIA, SEGURANÇA E CONTROLE SOCIAL NA AMÉRICA LATINA, Curitiba, *Anais*, Curitiba, Editora Universitária Champagnat, PUCPR, 2009, pp. 92-111.

Foucault, M. (2008). *Segurança, Território, População*. Martins Fontes.

Foucault, M. (2004). *Vigiar e Punir: Nascimento da prisão*. Vozes.

Huxley, A. (1993). *Admirável Mundo Novo*. Ed. Globo.

Kanashiro, M. M. (2008). Surveillance cameras in Brazil: exclusion, mobility regulation and the new meanings of security. *Surveillance & Society*, v. 5(3), pp. 270-289.

Leblanc, P. B. (2009). Composição para circuito de vídeo-vigilância. In VIGILÂNCIA, SEGURANÇA E CONTROLE SOCIAL NA AMÉRICA LATINA, 2009, Curitiba, *Anais*, Curitiba, Editora Universitária Champagnat, PUCPR, pp. 466-486.

Lissovsky, M.; & Bastos, T. (2010). A enunciação da vigilância nas fotografias da polícia política brasileira. In Bruno, F.; Kanashiro, M.; & Firmino, R. *Vigilância e visibilidade: espaço, tecnologia e identificação*. Editora Sulina, pp. 223-247.

Marx, G. T. (2002). What's new about the "new surveillance"? Classifying for change and continuity. In *Surveillance & Society,* v. 1(1), pp. 9-29.

McCahill, M. (2002). *The Surveillance Web.* The Rise of Visual Surveillance in an English City. Willan Press.

Melgaço, L. (2010). *Securização Urbana: da psicoesfera do medo à tecnoesfera da segurança*. 276 f. Tese (Doutorado em Geografia) Universidade de São Paulo e Universidade de Paris 1 – Panthéon Sorbonne.

Norris, C.; & Armstrong, G. (1999). *The Maximum Surveillance Society: The Rise of CCTV.* Berg.

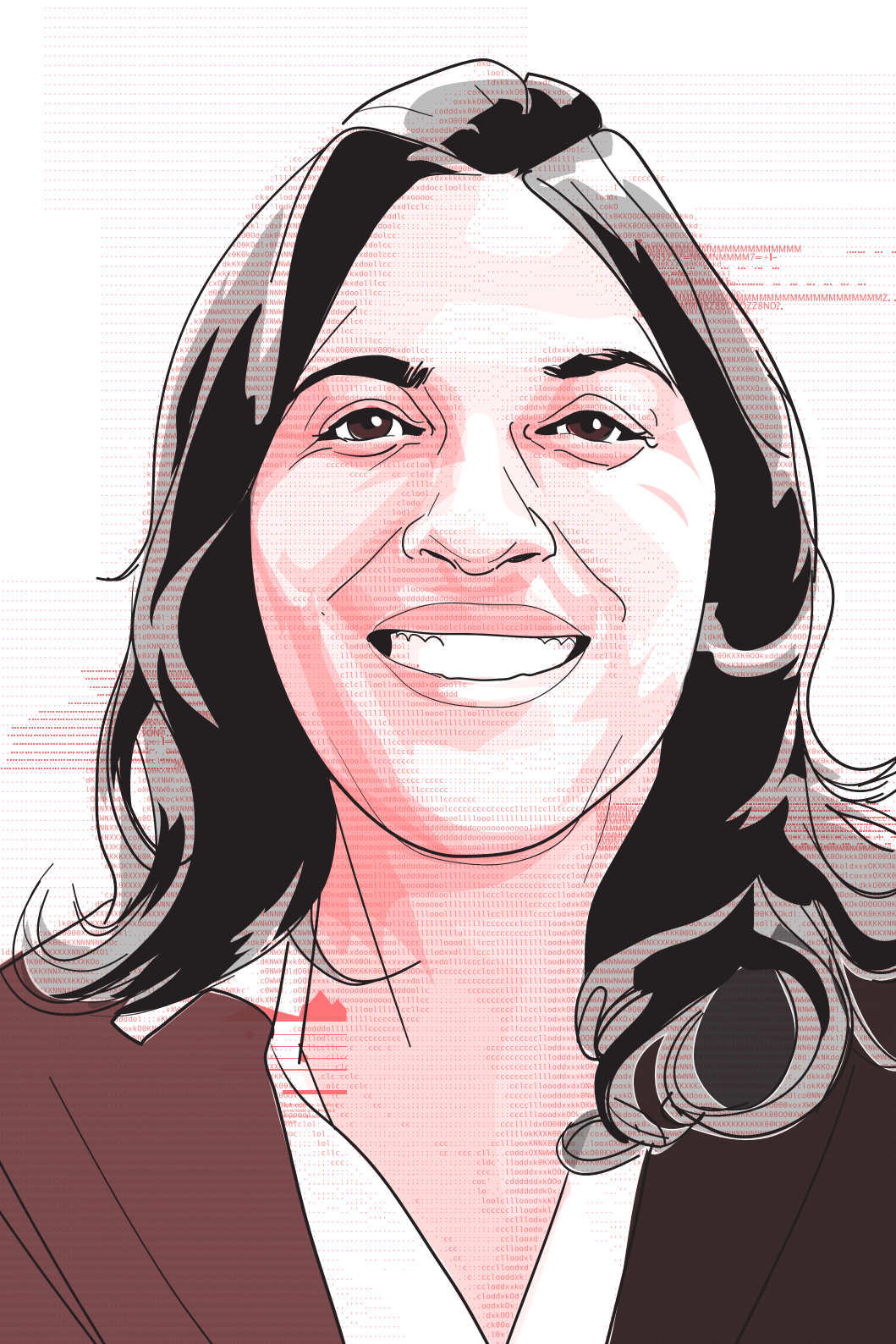
Norris, C.; & Armstrong, G. (1997). *The Unforgiving Eye: CCTV Surveillance in Public Space.* University of Hull.

Orwell, G. (2005). ***1984***. Ed. Nacional.

Rosa, M. (2006). *A reputação na velocidade do pensamento – Imagem e ética na era digital*. Geração Editorial.

Smith, G. (2004). Behind the screens: examining constructions of deviance and informal practices among CCTV control room operators in the UK. *Surveillance & Society*, v. 2(2/3), pp. 376-395.

Souza, M. M. (2008). *Sorria você está sendo filmado: a consolidação de uma sociedade de controle sobre o direito fundamental à privacidade e sobre as formas de interação espontânea e participação democrática nos espaços públicos e privados*. 133 pp. Dissertação (Mestrado em Ciências Jurídicas) – Departamento de Direito, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro.



08.

INFILTRAÇÕES VIRTUAIS: A ATUAÇÃO DE AGENTES DE INVESTIGAÇÃO EM REDES SOCIAIS E APLICATIVOS DE MENSAGENS

Fernanda Domingos[1]

1. A INTERNET E A MUDANÇA DE COMPORTAMENTO SOCIAL

A internet e os meios tecnológicos revolucionaram e continuam impulsionando mudanças no comportamento das pessoas e a forma como interagem entre si.

Diversos aspectos podem ser apontados, mas principalmente a facilidade na aproximação de pessoas, independentemente da distância física e de um conhecimento prévio a respeito da identidade do seu interlocutor, bem como a rapidez nessas interações, possibilitando a comunicação instantânea, inclusive com troca de documentos, entre duas pessoas ou um grupo muito maior de indivíduos.

As redes sociais trouxeram um novo padrão de divulgação de notícias, onde cada indivíduo tem a possibilidade de contar a sua história pessoal, o seu dia-a-dia, seu ponto de vista em relação a qualquer assunto, dando conhecimento disso a todos os demais usuários daquela rede, dando publicidade a um número enorme de dados e informações, acessíveis a qualquer um que queira buscá-los.

Por outro lado, as comunicações privadas, não importa se entre dois indivíduos ou entre um número maior de pessoas, receberam uma camada extra de proteção tecnológica para garantir a segurança da informação com a utilização das diferentes técnicas de criptografia, por exemplo.

Naturalmente, o mundo virtual passou a integrar o dia-a-dia de todos e tanto crimes passaram a ser cometidos por meios virtuais, como as fraudes bancárias mediante envio de *links* falsos por SMS para os *smartphones* para que atualizemos os dados cadastrais e bancários, aliciamento *online* de crianças em redes sociais para obtenção de *nudes* e atração para o cometimento de outros delitos no mundo real, bem como o uso da tecnologia para a comunicação imediata atra-

vés dos aplicativos de mensageria instantânea por meio dos quais são planejados os crimes em associação.

A presença das autoridades policiais no mundo virtual é um forte fator de prevenção da criminalidade da mesma forma que a patrulha no mundo real.

As redes abertas da *internet* se assemelham aos locais públicos do mundo real, porém, as comunicações em redes sociais fechadas e com o uso de aplicativos de mensageria instantânea com tecnologia de criptografia representam um desafio às autoridades públicas no combate às infrações penais.

Se antes as interceptações telefônicas eram o meio mais eficaz de investigação quando não havia mais outra forma de obter informações e desmantelar o conluio para o crime, atualmente a infiltração do agente policial desponta como uma importante técnica de investigação.

A infiltração do agente em organizações criminosas não é uma técnica simples, demandando certo tempo para convencimento do grupo acerca da fidelidade do novo membro, que muitas vezes se confronta com a necessidade de cometimento de infrações para continuar no papel de infiltrado.

A infiltração virtual é outra modalidade que se faz necessária demandando outras técnicas, já que, nas quadrilhas virtuais, muitas vezes os integrantes estão em diferentes locais e nem mesmo se conhecem pessoalmente.

Nesse cenário, a infiltração utilizando-se de meios tecnológicos como o *software* espião é uma alternativa que dispensa a atuação do agente, podendo ser utilizada mais rapidamente, já que depende menos de ganhar a confiança do grupo ou pessoas investigadas, embora ainda coloque muitas questões no tocante à legislação que a autoriza, bem como aos limites da medida e garantias da intimidade e privacidade que devem acompanhá-la.

2. CIBERPATRULHA E INVESTIGAÇÃO EM FONTES ABERTAS (OSINT)

A ciberpatrulha não está expressamente prevista em nosso ordenamento jurídico, mas tem fundamento no artigo 144 da Constituição Federal, que trata da Segurança Pública, tendo sido utilizada por diversos países.

O mundo virtual é um ambiente onde vigora a mesma lei vigente para o mundo real, já que a lei e o direito regulam as interações sociais, independentemente do meio em que elas ocorram. A sua importância é crescente, tendo passado a ser parte inerente do cotidiano das pessoas, nele ocorrendo interações sociais, financeiras, profissionais etc. e, por consequência, passando a ser cenário do cometimento de ilícitos.

A ciberpatrulha é a presença de agentes do Estado em locais virtuais públicos de forma preventiva para verificar o cometimento de infrações e a partir daí tomar as medidas judiciais cabíveis para sua repressão.

Ela não depende de autorização judicial porque ocorre em locais abertos da rede, isto é, acessíveis a qualquer pessoa. Mesmo que o acesso dependa de um cadastro para ser autorizado, se esse acesso é garantido a qualquer pessoa, o local virtual ainda é considerado público, não se caracterizando infiltração a exigir ordem judicial específica.

Recentemente, sua prática causou polêmica e discussões na Argentina, onde estaria sendo utilizada para "detectar humor social", prevenir saques ou delitos como aliciamento, mas sofreu críticas por supostamente poder afetar a liberdade de expressão ao trazer por consequência a autocensura.[2]

Claro que se presta apenas para que as autoridades tomem conhecimento da ocorrência do ilícito, sendo decorrentes do dever de vigilância das autoridades policiais. Estas somente estarão aptas a agir após o recolhimento de maiores dados, que podem ser buscados em fontes abertas e cruzados com

dados protegidos, sendo que estes somente serão obtidos após a devida autorização judicial para tanto.

Nos países da União Europeia é uma prática já consolidada internamente e em coordenação com a Europol, como se pode verificar na própria página *web* da Europol sobre *cyber-patrolling*.[3]

O recolhimento de dados e informações presentes nas redes sociais e em outras fontes abertas na internet para fins de investigação utilizando-se de simples verificação , mas também de ferramentas e técnicas especiais é o que se chama em inglês OSINT - Open Souce Intelligence, para dados abertos, e SOCMINT - Social Media Intelligence, para a análise das redes sociais.

Esse tratamento dos dados colhidos em ambiente aberto aponta relevantes conclusões que são fundamentais para o direcionamento da investigação de delitos, chegando a revelar informações que nem mesmo o próprio titular dos dados se dá conta de que estão disponíveis na rede aberta.

O mais conveniente é que essas práticas tenham algum tipo de previsão e regulação, ainda que *interna corporis*, para que, sendo práticas importantes para garantia da segurança pública e da própria liberdade de expressão *online*, não dêem ensejo ao cometimento de abusos para não comprometimento da validade das investigações.

Especificamente quanto à utilização de perfil falso pelo agente policial para atuar em ambiente virtual público, ela decorre do dever de vigilância inerente à função policial e, tendo em vista que ocorre em redes sociais abertas, não se caracteriza como infiltração, dispensando portanto prévia autorização judicial. Mesmo assim é importante ter atenção para não ocorrência do flagrante provocado, quando o agente policial acaba concorrendo para a ocorrência do ilícito. Nas palavras de Tourinho Filho.[4]

> Não se deve confundir o flagrante preparado com o denominado flagrante esperado. É preciso distinguir o agente provocador do funcionário policial que, informado previamente acerca de crime que alguém está praticando ou vai consumar, diligencie prendê-lo em flagrante, pois, em tal hipótese a intervenção da autoridade não provocou nem induziu o autor do fato criminoso a cometê-lo.

Após a ação de vigilância/ciberpatrulha, caso desnecessária autorização judicial para medidas invasivas, se o agente policial toma ciência de que está próxima a ocorrência de ilícito, deve atuar de forma a caracterizar-se o flagrante esperado, sem influir para a ação criminosa.

3. INFILTRAÇÃO DE AGENTES COMO TÉCNICA ESPECIAL DE INVESTIGAÇÃO – ART. 10 DA LEI 12.850/2013

A Lei 12.850/2013 trouxe a definição do que são as organizações criminosas, dispondo sobre a investigação criminal, os meios de obtenção da prova, as infrações penais correlatas e o procedimento criminal.

Ao tratar da investigação e dos meios de obtenção da prova, essa Lei tratou das Técnicas Especiais de Investigação, elencando no inciso VII do seu artigo 3º a infiltração por policiais em atividade de investigação.

Essa técnica já havia sido prevista na Lei 9.034/95, antiga lei de organizações criminosas, porém, a despeito de mencionar a necessidade de decisão judicial circunstanciada para a infiltração do agente policial ou de inteligência, não era tão específica e detalhada como a atual Lei 12.850/13.

Além disso, a possibilidade de infiltração por agente de inteligência foi excluída, já que manifestamente inconstitu-

cional, nos termos do artigo 144 da Constituição Federal que atribui a segurança pública às polícias.

Também a Lei de Drogas nº 10.409/2002 incluiu a infiltração de policiais em quadrilhas, grupos, organizações ou bandos como possibilidade de investigação de seus crimes (art. 33, I), possibilidade mantida pela atual Lei de Drogas, Lei 11.343/2006, no seu artigo 53, I, com a seguinte redação:

> Art. 53. Em qualquer fase da persecução criminal relativa aos crimes previstos nesta Lei, são permitidos, além dos previstos em lei, mediante autorização judicial e ouvido o Ministério Público, os seguintes procedimentos investigatórios.
> I- a infiltração por agentes de polícia, em tarefas de investigação, constituída pelos órgãos especializados pertinentes

A Lei 12.850/13 detalha o procedimento e as cautelas da infiltração de agente policial. Estatui que cabe ao delegado de polícia ou ao membro do Ministério Público representar por essa medida especial de investigação ao juiz, que decidirá motivadamente e detalhando as circunstâncias em que deverá ocorrer a infiltração e estabelecendo seus limites. Essa decisão é sigilosa, tanto para preservar a investigação quanto para a proteção do agente policial que irá desempenhar essa tarefa.

O prazo da infiltração é de até 6 meses, podendo ser prorrogado se comprovada a necessidade.

Importante destacar que os meios de obtenção da prova descritos na Lei 12.850/13 não se aplicam somente aos crimes cometidos por organizações criminosas conforme definidas nesta lei.

A definição de organização criminosa é "*a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracte-*

rizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional."

Ocorre que pode haver o cometimento de crimes por grupos de pessoas cuja associação não se encaixa na definição legal de organização criminosa, não havendo, porém, outro meio disponível para a produção da prova, nos termos do §2º do artigo 10 da Lei 12.850/13.

Nesse caso, se a infração penal estiver prevista em tratado ou convenção internacional e tiver caráter transnacional, isto é, quando a execução do crime tiver se iniciado no país e o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente, nos termos do §2º do artigo 1º da Lei , seus dispositivos também serão aplicáveis, a despeito de a atuação dos criminosos se encaixar perfeitamente no conceito de organização criminosa ou não. A consequência disso é a inexigibilidade de associação de 4 pessoas ou mais para que o delito transnacional cometido possa ser investigado mediante a utilização das Técnicas Especiais de Investigação.

O mesmo raciocínio deve ser feito para as organizações terroristas. Basta a leitura do §2º; que diz que a Lei se aplica também:

> §2º Esta Lei se aplica também:
> I- às infrações penais previstas em tratado ou convenção internacional quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;
>
> II- às organizações terroristas, entendidas como aquelas voltadas para a prática dos atos de terrorismo legalmente definidos.

O prazo da infiltração do agente policial é de até 6 meses, podendo ser renovado, sem prejuízo de eventuais renovações, desde que comprovada a sua necessidade.

Terminado o prazo da infiltração, relatório circunstanciado será apresentado ao juiz, mas no curso da investigação, a qualquer tempo, poderá ser requisitado relatório da atividade de infiltração.

Importante destacar que a infiltração não é medida corriqueira e de fácil implementação. Pelo contrário. Ela demanda tempo para que o agente ganhe a confiança do grupo no qual pretende se infiltrar, colocando em risco sua integridade física e mesmo sua vida, além de se ver em situações onde precisará cometer crimes, que precisam ser antevistos pelo juiz para que dê de antemão a autorização judicial pertinente.

4. INFILTRAÇÃO VIRTUAL DE AGENTES DE POLÍCIA — ART. 10-A A 10-D DA LEI 12.850/2013

No que toca à infiltração virtual de agentes de polícia, o chamado Pacote Anticrime, ou Lei nº 13.964/2019, incluiu os artigos 10-A a 10-D na Lei 12.850/2013 para prever a possibilidade expressa da infiltração de agentes de polícia em meio virtual para investigação dos mesmos crimes previstos na Lei 12.850/13.

A infiltração tradicional significa que o agente policial passará a fazer parte do círculo fechado dos criminosos, sendo necessário certo tempo para que ganhe a confiança dos mesmos e passe a integrar o grupo criminoso.

A infiltração virtual é necessária porque os crimes passaram à esfera virtual e os criminosos passaram a se encontrar e planejar as infrações em ambiente virtual também.

Nos termos do artigo 10-A, §3º, a infiltração virtual será admitida se houver indícios da prática de infração penal prevista no artigo 1º da Lei, isto é, nas mesmas hipóteses em que

se admite a infiltração real prevista no artigo 10 e observando-se que as provas não possam ser produzidas por outros meios disponíveis.

Note-se que a infiltração virtual é uma técnica especial de investigação que serve para investigar crimes praticados em meio real e em meio virtual, sendo cada vez mais percebida a necessidade da sua utilização, já que as redes sociais e mensageiros eletrônicos têm assumido papel recorrente no cenário da vida das pessoas e também na criminalidade.

Enfatizo mais uma vez que a infiltração não se restringe à investigação de crimes praticados por organizações criminosas definidas nos termos do §1º do artigo 1º da Lei. E mesmo antes da introdução dos artigos 10-A e 10-B, a infiltração virtual já era possível e foi autorizada em operações para investigação do crime de divulgação de pornografia infantil na internet,[5] artigo 241-A do ECA, dentre outros, nas hipóteses da Lei nº 12.850/13 mesmo não se tratando de organização criminosa na estrita definição legal e sim crime transnacional.

Tome-se como exemplo a investigação do crime de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza, previsto no artigo 20, §2º, da Lei nº 7.716/89, cuja pena máxima é de 5 anos.

É muito comum que usuários de redes sociais na internet, que não se conhecem e nem nunca se encontraram, passem a integrar grupos fechados de comunicação, tanto nas redes sociais quanto em grupos formados a partir de aplicativos de mensageria instantânea, com caráter transnacional, onde disseminam ideias de discriminação ou preconceito pelas razões elencadas no dispositivo legal.

Tal conduta está acordada em Tratado Internacional, qual seja, a Convenção Internacional das Nações Unidas para a Eli-

minação de todas as Formas de Discriminação Racial, de 1965, e ratificada pelo Brasil em 1969. Na ocorrência de transnacionalidade da conduta, isto é, quando iniciada a execução da conduta no país, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente, essa infração é elegível para ser investigada mediante infiltração virtual, mesmo que os integrantes desse grupo fechado não configurem uma organização criminosa, ou seja, uma associação de 4 ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas com o objetivo de obter qualquer vantagem. Nesse tipo de delito é comum grande número de participantes, porém sem uma divisão estruturada de tarefas. A investigação desse tipo de delito, no mais das vezes, necessita da infiltração virtual para a sua elucidação e encontra respaldo no §2º, inciso I, do artigo 1º da Lei.

O artigo 10-A estipula que a necessidade da infiltração virtual deve ser demonstrada, bem como indicados o alcance das tarefas dos policiais, os nomes ou apelidos dos investigados e, caso já conhecidos, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.

Evidentemente que, no curso da infiltração, outros suspeitos podem ser apontados e investigados se os indícios indicarem essa necessidade, sendo que toda a atividade constará de relatório da atividade de infiltração que pode ser requisitado a qualquer tempo pelo juiz, membro do Ministério Público ou delegado de polícia e ao final integrará o relatório circunstanciado da infiltração.

O artigo 10-C exclui explicitamente a antijuridicidade do ato cometido pelo agente policial que oculta sua identidade na internet para investigar autoria e materialidade dos crimes previstos no artigo 1º da Lei 12.850/13, respondendo, porém, por excessos se deixar de observar a estrita finalidade da lei e o quanto estipulado na ordem judicial.

Quanto ao prazo da infiltração virtual, é o mesmo da infiltração real, de até 6 meses, podendo ser renovado desde que haja necessidade e motivação. Porém, para a infiltração virtual foi estipulado o período máximo de 720 dias, este que já havia sido introduzido para a infiltração virtual específica para a investigação de infrações penais violadoras da dignidade sexual de criança ou de adolescente na Lei nº 13.441/2017, da qual falaremos adiante.

Como já dito, os limites da atuação do agente estatal devem estar bem claros na ordem judicial autorizadora da infiltração virtual a fim de coibir excessos.

5. INFILTRAÇÃO VIRTUAL DE AGENTES DE POLÍCIA PARA INVESTIGAÇÃO DE CRIMES CONTRA A DIGNIDADE SEXUAL DE CRIANÇA E ADOLESCENTE – LEI Nº 13.441/2017 INTRODUZIU OS ARTS.190-A ATÉ 190-E DA LEI 8.069/90 (ESTATUTO DA CRIANÇA E DO ADOLESCENTE- ECA), ARTS. 217-A, 218, 218-A E 218-B DO CÓDIGO PENAL E ARTIGO 154-A DO CÓDIGO PENAL

Antes da alteração havida na Lei nº 12.850/13 (das ORCRIMS) pelo Pacote Anticrime (Lei nº 13.964/2019) para a inclusão da expressa previsão do agente infiltrado virtual, a Lei nº 13.441/2017 incluiu os artigos 190-A a 190-E no Estatuto da Criança e do Adolescente (Lei nº 8.069/89) para regular a infiltração de agentes de polícia para a investigação de crimes contra a dignidade sexual de criança e de adolescente presentes no ECA (arts. 240, 241, 241-A, 241-B, 241-C e 241-D) e no Código Penal (arts. 217-A, 218, 218-A e 218-B) e a investigação dos crimes descritos no artigo 154-A também do Código Penal.

Primeiramente, é preciso destacar a inadequação da técnica legislativa que incluiu artigo de lei no Estatuto da

Criança e Adolescente, o qual traz autorização de técnica investigativa para delitos previstos em outro diploma legal, qual seja, o Código Penal.

Analisando-se a exposição de motivos do PLS 100/2010[6] que resultou nessa Lei, verifica-se que o objetivo foi possibilitar a investigação para repressão desses delitos contra a dignidade sexual da criança e do adolescente que tiveram no advento da internet uma explosão de ocorrências. A utilização da internet inclusive para a prática autônoma do aliciamento de criança com fim de com ela praticar ato libidinoso (art. 240-D do ECA) passou a ser prática corrente como crime antecedente para os delitos sexuais contra vulnerável previstos no Código Penal.

Com o aparecimento de comunidades virtuais, tanto em redes sociais da internet quanto em fóruns virtuais presentes na Deep Web - a internet não indexada, isto é, onde não é possível encontrar uma página virtual sem conhecer previamente o seu endereço - bem como grupos utilizando mensageiros instantâneos dedicados a troca de imagens de abuso sexual de crianças e adolescentes, revelando as evidências dos crimes reais de estupro e abuso perpetrados para a produção dessas imagens trocadas, não há outra maneira de descobrir esses delitos que não seja pela inserção do agente policial nesse meio onde, ganhando a confiança dos criminosos, poderá vir a descobrir os autores desses delitos.

Assim, no tocante ao Estatuto da Criança e do Adolescente, essa lei introduziu expressamente a figura da infiltração virtual de agentes de polícia para a investigação dos crimes de produção (art. 240) de cenas ou imagens que contenham cena de sexo explícito ou pornográficas envolvendo criança ou adolescente, venda ou exposição à venda (art. 241) de qualquer registro que contenha essas cenas, distribuição (art. 241-A) desse material por qualquer meio, inclusive por meio de sistema de informática ou telemático, aquisição, posse

ou armazenamento (art. 241-B) desse material, simulação da participação (art. 241-C) de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual, bem como o aliciamento, assédio, constrangimento(art. 241-D) de criança com o fim de com ela praticar ato libidinoso.

A possibilidade do uso dessa técnica de investigação também foi introduzida para os crimes sexuais praticados contra vulnerável previstos no Código Penal Brasileiro.

Dessa forma, a infiltração virtual é medida possível de ser determinada judicialmente para elucidar os crimes de estupro de vulnerável (art. 217-A), corrupção de menores (art. 218), satisfação de lascívia mediante presença de criança ou adolescente (art. 218-A) e favorecimento da prostituição ou de outra forma de exploração sexual de criança ou adolescente ou de vulnerável (art. 218-B).

A Lei nº 13.441/2017, portanto, identificou os delitos cometidos contra a dignidade sexual da criança e do adolescente previstos no Estatuto da Criança e do Adolescente e no Código Penal como graves o suficiente para permitirem a medida de infiltração virtual, que é uma técnica de investigação mais invasiva, já que o bem jurídico protegido a justifica, devendo estar demonstrada a sua necessidade e não sendo possível obter essa prova por outros meios.

A importância dessa lei para o descobrimento desses delitos é que ela não exige que o crime seja transnacional para a utilização da técnica de infiltração virtual, como na Lei nº 12.850/13. Tendo em vista que muitos desses grupos podem trocar mensagens apenas entre usuários dentro do território nacional, mesmo que utilizando a internet para tanto, e que a infiltração virtual é, na maior parte das vezes, a única forma de conseguir investigar, a possibilidade da sua utilização

/ OS LIMITES DA ATUAÇÃO DO AGENTE DEVEM ESTAR BEM CLAROS NA ORDEM JUDICIAL AUTORIZADORA DA INFILTRAÇÃO VIRTUAL A FIM DE COIBIR EXCESSOS /

para desbaratar os grupos nacionais foi um grande avanço no combate desse delito.

A medida de infiltração virtual deve ser autorizada por ordem judicial circunstanciada e fundamentada, estabelecendo os limites da infiltração para obtenção da prova.

Também repetido pela Lei nº 12.850/13, o alcance das tarefas deve estar definido, bem como os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.

O artigo 190-C do ECA, introduzido pela Lei nº 13.441/2017, exclui a antijuridicidade da conduta do policial que oculta sua identidade na internet para colher indícios de autoria e materialidade dos crimes descritos por essa lei. Esse dispositivo também se encontra na Lei nº 12.850/13, no artigo 10-C.

Quanto ao prazo da infiltração, ficou estabelecido que a infiltração não pode exceder 90 dias, com renovações motivadas pela autoridade judicial, não podendo exceder 720 dias.

A possibilidade de utilização dessa técnica especial de investigação para os crimes do artigo 154-A do Código Penal causa estranheza pelo fato de ter sido inserido em uma lei que visa aperfeiçoar a investigação dos delitos sexuais contra a dignidade da criança e do adolescente, já que o tipo penal do artigo 154-A não tem essa finalidade específica:

> Código Penal
>
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

No entanto, a infiltração do agente policial na internet sem dúvida é medida de investigação importante para a elucidação também desse crime de invasão de dispositivo informático, uma vez que os programas destinados a possibilitar essa invasão estão acessíveis online, bem como a associação para as fraudes digitais também acaba acontecendo no mais das vezes no ambiente virtual. Isto é, o ambiente propício para o cometimento de crimes migrou para o ambiente *online*, sendo desejável que os agentes policiais possam estar presentes nesse ambiente para combatê-los.

6. UTILIZAÇÃO DE MEIOS TECNOLÓGICOS – SPYWARE – PARA OBTENÇÃO DE FLUXO DE COMUNICAÇÕES E COMUNICAÇÕES ARMAZENADAS – LEI 9.296/96 E ARTIGO 7º DO MCI

Diferentemente da infiltração do agente policial é a infiltração do spyware, software desenvolvido para ser inoculado em dispositivo informático e capturar dados do usuário.

Segundo o *site Significados*, "*Spyware* é um *software* espião de computador, que tem o objetivo de observar e roubar informações pessoais do usuário que utiliza o PC em que o programa está instalado, transmitindo-as para uma fonte externa na internet, sem o conhecimento ou consentimento do usuário."[7]

Já de acordo com o site *Tecmundo*," *Spywares* são programas espiões, isto é, sua função é coletar informações sobre uma ou mais atividades realizadas em um computador."[8]

Há programas desse tipo que coletam dados pessoais dos usuários a fim de direcionar os anúncios publicitários que serão apresentados a esse possível consumidor, porém, isso somente pode ser feito de forma lícita mediante o consentimento do usuário.

Aqui estamos tratando de coisa diversa: de programa espião, instalado sem o conhecimento do usuário e obviamente sem seu consentimento.

Não há previsão legal explícita a esse respeito.

O projeto de lei do Pacote Anticrime trazia uma proposta de redação desse tipo de infiltração virtual por meios tecnológicos ao propor incluir na Lei de Interceptações - Lei nº 9.296/96, o artigo 9º- A para permitir a interceptação de comunicações por qualquer meio tecnológico disponível, desde que assegurada a integridade da diligência, podendo a ação incluir a apreensão do conteúdo de mensagens e arquivos eletrônicos armazenados em caixas postais eletrônicas.

Essa proposição não restou acolhida na redação da lei, porém, do ponto de vista da investigação criminal, essa proposição, além de desnecessária, era limitante às hipóteses de infrações penais descritas na Lei nº 9.296/96 às quais se aplicaria.

Note-se que tal proposição refere-se a duas situações distintas: a apreensão de conteúdo de mensagens e arquivos eletrônicos armazenados em caixas postais eletrônicas e a interceptação de comunicação eletrônica.

O Marco Civil da Internet, Lei nº 12.965/14, em seu artigo 7º, prevê nos incisos II e III, a forma de acesso a esses conteúdos:

> Lei nº 12.965/14
> Art.7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I- (...)
> II- inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial;
> III- inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> [. . .]

Tomando-se o artigo 7º, inciso II, vemos a proteção da inviolabilidade e do sigilo do fluxo das comunicações pela internet, cujo acesso só é obtido por ordem judicial, na forma da lei.

Ora, a lei mencionada só pode ser a Lei nº 9.296/96, que trata da interceptação de comunicações telefônicas e do fluxo de comunicações em sistemas de informática e telemática, e que traz em seu bojo os limites para que o acesso a tal conteúdo somente se dê nas situações e condições ali descritas.

Dessa forma, a Lei nº 9.296/96 já estabelece que a interceptação do fluxo das comunicações telefônicas e telemáticas só pode ocorrer se houver indícios de autoria ou participação em infração penal apenada com reclusão e se a prova não puder ser feita por outros meios disponíveis. Ainda, estabelece que o pedido de interceptação deve conter a demonstração de que a sua realização é necessária para a apuração da infração penal, com a indicação dos meios a serem empregados (artigo 4º da Lei nº 9.296/96), devendo a decisão ser fundamentada e indicar a forma de execução da diligência.

Os "meios a serem empregados" e a "forma de execução da diligência" já abarcam a possibilidade do uso de meios tecnológicos, como o *software* espião, para a interceptação do fluxo das comunicações.

Enquanto o agente virtual infiltrado é a forma para a investigação de redes sociais fechadas, ou grupos limitados de pessoas utilizando-se de aplicativos de mensagens, o uso do *software* espião é mais eficaz para obter essas mensagens sem a necessidade de atuação de um agente real, que precisa de tempo para ganhar a confiança dos demais usuários para ser admitido no círculo fechado dessas pessoas, estando sujeito a ser descoberto caso cometa algum deslize e muitas vezes sendo obrigado a cometer infrações penais, desde que autorizado judicialmente para tanto.

O *software* espião é, portanto, uma alternativa a ser utilizada quando não há tempo para que um agente real se imiscua no grupo criminoso de forma a ser aceito e passe a ter acesso à comunicação do grupo.

Com a tecnologia de criptografia ponta-a-ponta , o provedor dos serviços de mensageria instantânea também não tem acesso ao conteúdo das comunicações, sendo inócua a ordem dirigida a ele para que as entregue.

Assim, o software espião precisará ser instalado em um dos dispositivos eletrônicos que trocam as mensagens, onde terá acesso às mensagens enviadas antes que sejam criptografadas e onde a chave privada no dispositivo do usuário recipiente permite decodificar a mensagem criptografada recebida via aplicativo de mensageria.

A polêmica na utilização desse mecanismo tecnológico é o alcance e abrangência que uma interceptação dessa espécie possui.

Essa tecnologia permite invadir dispositivos informáticos, incluídos os *smartphones*, que usualmente trazem praticamente todas as informações do indivíduo.

O grau de invasão é muito alto, pois, além do acesso ao teclado do dispositivo, espionando o fluxo escrito das comunicações telemáticas, também permite o acesso ao áudio do dispositivo eletrônico, captando suas comunicações verbais, e à câmera de vídeo do dispositivo eletrônico, podendo flagrar toda a intimidade do investigado e de outras pessoas que estejam interagindo com este.

Tendo em vista essa possibilidade de desfraldamento quase total da vida privada e da intimidade do investigado, deveria a lei trazer uma salvaguarda detalhada, exigindo que a decisão judicial estabelecesse o limite da interceptação na medida da necessidade da prova.

Ainda que o artigo 9º da Lei esclareça que a gravação que não interessar à prova será inutilizada por decisão judicial, para o caso de interceptação telemática por meio de *software* espião, cujo grau de invasão da esfera privada do indivíduo pode ultrapassar o quanto bastaria à investigação criminal, a previsão legal quanto ao grau de invasão seria uma garantia ao indivíduo.

Na sua falta, deve a decisão judicial autorizadora de tal medida tomar o cuidado de estabelecer esse limite, já que tão moderna tecnologia apresenta a possibilidade de interceptar o fluxo da comunicação telemática sem obter a imagem da videocâmera, por exemplo, na hipótese de essa não ser uma informação imprescindível à investigação.

Por outro lado, a instalação de *software* espião que tenha acesso à câmera e áudio do dispositivo eletrônico pode configurar também uma medida de captação ambiental de sinais eletromagnéticos, ópticos ou acústicos, com previsão no artigo 8º-A da Lei nº 9.296/96, incluído pelo Pacote Anticrime.

O requerimento de tal medida deve descrever circunstanciadamente o local e a forma de instalação do dispositivo de captação ambiental, que deverá obedecer o prazo máximo de 15 dias, renovável conforme a sua indispensabilidade.

Assim, tanto o fluxo das comunicações telemáticas quanto a captação ambiental efetivados mediante a inserção de meio tecnológico diferenciado, qual seja , um software espião, podem ser efetivados e possuem arcabouço legal para tanto, sendo desnecessária a previsão expressa quanto ao meio empregado para sua efetivação, cabendo à decisão judicial estabelecer o alcance e os limites da medida.

No que toca ao artigo 7º, inciso III, temos a proteção e garantia do sigilo das comunicações privadas armazenadas, às quais somente se pode ter acesso mediante ordem judicial.

Logo, com relação ao acesso às mensagens eletrônicas privadas e documentos eletrônicos armazenados, mencionados na proposição não acolhida, o Marco Civil também já elenca essa a possibilidade e não a restringe para as hipóteses da lei de interceptações.

A ordem judicial, nesse caso, será lastreada no artigo 240 do Código de Processo Penal, dispositivo legal que permite a busca e apreensão de qualquer elemento a formar convicção, quando as mensagens eletrônicas privadas e os documentos eletrônicos estiverem armazenados em dispositivos informáticos que estejam ao alcance das autoridades, ou mesmo se estiverem armazenados em serviços de armazenamento remoto - em nuvem - mas esse conteúdo puder ser alcançado pelas autoridades a partir do dispositivo informático apreendido.

Na hipótese em que as comunicações e documentos eletrônicos estiverem armazenados em servidores de empresas que oferecem esse serviço remoto de armazenamento, as autoridades, cientes disso, podem determinar diretamente às empresas a entrega de cópia desses documentos eletrônicos, nos termos do artigo 7º, inciso III do Marco Civil, combinado como o artigo 234 do Código de Processo Penal, que disciplina a entrega de documento.

A hipótese a ser discutida aqui é se, no caso da busca e apreensão de comunicação ou documento eletrônico armazenados em dispositivo eletrônico, seria possível a busca e apreensão remota, mediante a utilização de *software* específico para isso, o que poderia ocorrer sem o conhecimento do investigado, ainda que com ordem judicial.

Veja-se que, numa busca e apreensão tradicional, o investigado ou a pessoa presente no local são interpelados presencialmente pela autoridade policial que vai até o local da diligência. O investigado ou a pessoa presente no local é cien-

tificado da ordem judicial, consubstanciada no mandado de busca e apreensão, e acompanha a diligência.

No caso de uma busca e apreensão remota mediante o uso de meio tecnológico específico para tal, o investigado pode nunca ter ciência de que suas informações foram copiadas pelas autoridades, já que, caso o material copiado na busca remota não traga elementos suficientes ao oferecimento de uma acusação criminal, essa diligência não chegará ao conhecimento do investigado em invasão da esfera privada do indivíduo.

Por outro lado, fazendo-se um paralelo com a lei das interceptações telefônicas e telemáticas, Lei nº 9.296/96, seu artigo 9º determina que aquilo que não interessar ao processo será destruído. Nessa situação, indivíduos cujas conversas também foram interceptadas, mas não interessaram ao processo, também não terão ciência do ocorrido.

> Lei nº 9.296/96
> art. 9º. A gravação que não interessar à Prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada.

De toda sorte, embora entendamos que o presente arcabouço jurídico permita tal medida, a sua execução precisa ser cercada de garantias para que não seja considerada eivada de nulidade e em afronta ao princípio da inviolabilidade da intimidade, da vida privada, da honra e da imagem insculpido no inciso X do artigo 5º da Constituição Federal.

Assim, uma medida de busca e apreensão remota, realizada por meio tecnológico que dispense a presença física da autoridade no local da busca, deve ser autorizada por decisão judicial circunstanciada e motivada, com estabelecimento de

limites quanto a sua extensão e regras procedimentais que garantam a autenticidade e integridade do conteúdo copiado, bem como quanto ao destino desse material, caso não venha a integrar o processo.

Deve-se ainda ter em mente que a busca e apreensão remota, em verdade, não "apreende" o conteúdo buscado, podendo apenas fazer uma cópia desse conteúdo. Porém, existe ainda a possibilidade de apagamento desse material, remotamente, se assim determinado pelo juiz, caso se entenda danosa a permanência de conteúdo ilícito na posse do criminoso, após feita a cópia com as técnicas que garantam a autenticidade e integridade do material, podendo servir de prova que possa ser auditada mediante a perícia técnica.

Outro tópico a ser levantado na questão da busca e apreensão de dispositivo informático, remota ou não, é a possibilidade de busca de conteúdo que esteja armazenado em outro dispositivo informático que não o alvo da medida constritiva de busca e apreensão, porém a ele conectado remotamente.

Em nossa visão, essa possibilidade deve ser levada em consideração pelas autoridades requerentes e deferentes da medida de busca e apreensão de conteúdo digital em dispositivos informáticos, uma vez que a tecnologia digital permite a conexão entre diversos dispositivos informáticos que partilham o mesmo conteúdo que pode estar armazenado em um deles ou em pasta virtual de serviço remoto, de sorte que é prudente tal possibilidade de apreensão estar prevista pela ordem judicial.

Todas essas questões se apresentam aos operadores do direito face ao vertiginoso desenvolvimento tecnológico e precisam ser bem equacionadas para que não provoquem a paralisação das atividades de investigação de crimes e persecução penal, uma vez que a criminalidade não vê barreiras que possam cerceá-la. Pelo contrário, tiram proveito dos avanços tecnológicos.

Sendo assim, há que se aplicar o arcabouço jurídico existente, assegurando-se que em cada caso concreto as garantias da intimidade, da vida privada e do sigilo das comunicações estejam presentes, observando-se o devido processo legal, presentes a motivação e fundamentação das decisões judiciais que afastam essas garantias.

Analisando-se a legislação comparada, é possível encontrar semelhanças com a nossa legislação e outras soluções adotadas.

A Estônia, embora seja o país mais moderno do mundo em termos de digitalização do serviços governamentais e das informações dos cidadãos[10], em termos de legislação se compara ao Brasil, já que o arcabouço jurídico existente para as medidas processuais de busca e apreensão de evidências digitais são as mesmas utilizadas para a medida tradicional, observando-se as peculiaridades em cada ordem judicial emanada com esse fim.[11]

No artigo de Anna-Maria Osula, Remote search and seizure: Estonia case study, é mencionado, além do arcabouço jurídico estoniano, o tratamento existente na Nova Zelândia (página 364) que também é adotado em outros países. É feita a diferenciação entre a natureza da busca e apreensão remota e a interceptação telemática do fluxo das comunicações.

Enquanto a interceptação do fluxo das comunicações telemáticas é tida para os neozelandeses como uma medida sigilosa, o entendimento é no sentido de que a busca e apreensão remota guarda a mesma essência da busca e apreensão tradicional, não se tratando de uma medida subreptícia. Pelo contrário: a exemplo da busca e apreensão tradicional, que é executada com a ciência e acompanhamento do investigado ou da pessoa responsável presente no local, o investigado, alvo de uma busca e apreensão remota, deve ser notificado da medida invasiva.

Tendo em conta a peculiaridade do conteúdo digital objeto da busca, a notificação do investigado acerca da medida

deve ser feita em momento adequado a não prejudicar as investigações, a notificação *a posteriori*.

A legislação belga, também mencionada no estudo, prevê expressamente a possibilidade de copiar, tornar inacessível ou apagar informações em uma busca e apreensão remota, e deixa clara a distinção entre a busca tradicional e a remota. Na busca e apreensão de um dispositivo informático, imediatamente o agente policial deve deixar o aparelho em modo avião para evitar que ele se conecte automaticamente a qualquer outro dispositivo ou servidor não previamente listado na ordem de busca, como uma conta de *email*, por exemplo.[12]

CONCLUSÃO

A partir da breve explanação, é possível concluir que o meio virtual e as novas formas de comunicação pelas redes sociais e mensageiros instantâneos apresentam novos desafios às investigações criminais.

Os métodos tradicionais de investigação não são eficazes face à transposição das ações do meio real para o meio virtual. Nesse contexto, a infiltração virtual é uma técnica de investigação especial importante para o combate à criminalidade, tanto real como virtual.

A infiltração tradicional não é um método que pode ser banalizado, pois é lento e traz sérios riscos à integridade física do agente policial. A infiltração virtual, embora também seja lenta, minimiza esses riscos e é eficaz para as redes virtuais, onde nem sempre há um grupo organizado; ou seja, muitas vezes, embora o ambiente seja restrito, os próprios integrantes não se conhecem pessoalmente.

A possibilidade de infiltração virtual com a utilização de meio tecnológico como um programa espião acelera e amplia as possibilidades de investigação no meio virtual. Isso ocorre

principalmente no caso de ser necessária a interceptação do fluxo da comunicação telemática criptografada, tecnologia que impede métodos tradicionais de interceptação e também torna inócua a ordem de entrega dessas mensagens para os provedores desses serviços, os quais também não possuem acesso às mensagens no caso da utilização de criptografia ponta-a-ponta, a menos que façam modificações técnicas para atender às necessidades das autoridades.

Conforme explanado, existe já arcabouço jurídico a embasar esses métodos de infiltração virtual tanto por agente quanto pela utilização de *software* específico, cabendo à autoridade judiciária detalhar na ordem a ser emitida o alcance e os limites da infiltração para que sejam salvaguardadas as garantias da intimidade e vida privada do indivíduo, de forma a que o Estado atue somente na medida do necessário à garantia da segurança pública.

NOTAS

1. Procuradora da República do Ministério Público Federal. Coordenadora do Grupo de Apoio sobre Criminalidade Cibernética da Câmara Criminal da PGR.

2. Santoro, D. (mar. 2020). Coronavirus en Argentina: polémica por el "ciberpatrullaje" de las fuerzas de seguridad en las redes sociales. *Clarín Política*. https://bit.ly/2UFf219

3. Europol (2017). *Cyber-patrolling Week*. https://bit.ly/3ftSDMB

4. Tourinho Filho, F. da C. (1999). *Código de Processo Penal Comentado*, Vol. 1. (4ªedição). Saraiva, p. 530.

5. Operação Underground II - anterior à Lei nº 13.441/2017, que introduziu a infiltração virtual específica para os delitos de pornografia infantil na internet. Cf. Supremo Tribunal Federal, Conflito de Competência nº 167.746-SP (2019/0242461-9), Min. Reynaldo Soares da Fonseca. https://bit.ly/3e2rVu6.

6. Projeto de Lei do Senado nº 100/2010. https://bit.ly/30Ga7kz.

7. Significados (2014). *Significado de Spyware*. https://bit.ly/3frpTnF.

8. Xavier, A. (2008). O que é spyware? Tecmundo. https://bit.ly/2AzpUHe.

9. "A criptografia de ponta-a-ponta (end-to-end encryption ou E2EE) é um recurso de segurança que protege os dados durante uma troca de mensagens, de forma que o conteúdo só possa ser acessado pelos dois extremos da comunicação: o remetente e o destinatário. Usada atualmente em aplicativos como o Telegram e o WhatsApp, a ferramenta é uma implementação da criptografia assimétrica e garante que as informações não sejam interceptadas. Ninguém mais além dos envolvidos na conversa deve ter acesso ao conteúdo transmitido por meio da criptografia de ponta-a-ponta, nem mesmo as empresas dos apps." Coutinho, M. (12 jun. 2019). *O que é criptografia de ponta-a-ponta? Entenda o recurso de privacidade*. TechTudo. https://glo.bo/30I9qqW.

10. Ferrara, Y. (18 out. 2018). *Visita ao governo da Estônia: o mais moderno do mundo*. https://bit.ly/3foZlmR.

11. Osula, A. (2016). *Remote search and seizure in domestic criminal procedure: Estonian case study*. International Journal of Law and Information Technology, Volume 24(4), pp. 363-364, https://doi.org/10.1093/ijlit/eaw010.

12. Osula, A. (2016). Remote search and seizure in domestic criminal procedure: Estonian case study. International Journal of Law and Information Technology, Volume 24(4), pp. 363-364, https://doi.org/10.1093/ijlit/eaw010.

BIBLIOGRAFIA

Projeto de Lei do Senado nº 100/2010. https://bit.ly/30Ga7kz.

Ucciferri, L. (29 out. 2018). *Seguidores que no vemos - Una primera aproximación al uso estatal del Open-source intellingence (OSINT) y Social media intelligence (SOCMINT)*. Asociación por los Derechos Civiles. https://bit.ly/37u5lCu.

Buffon, J. A. (2018). *Agente Infiltrado Virtual.* In Crimes Cibernéticos - Coletânea de Artigos. Volume. 3. 2ª Câmara de Coordenação e Revisão, Brasília - MPF.

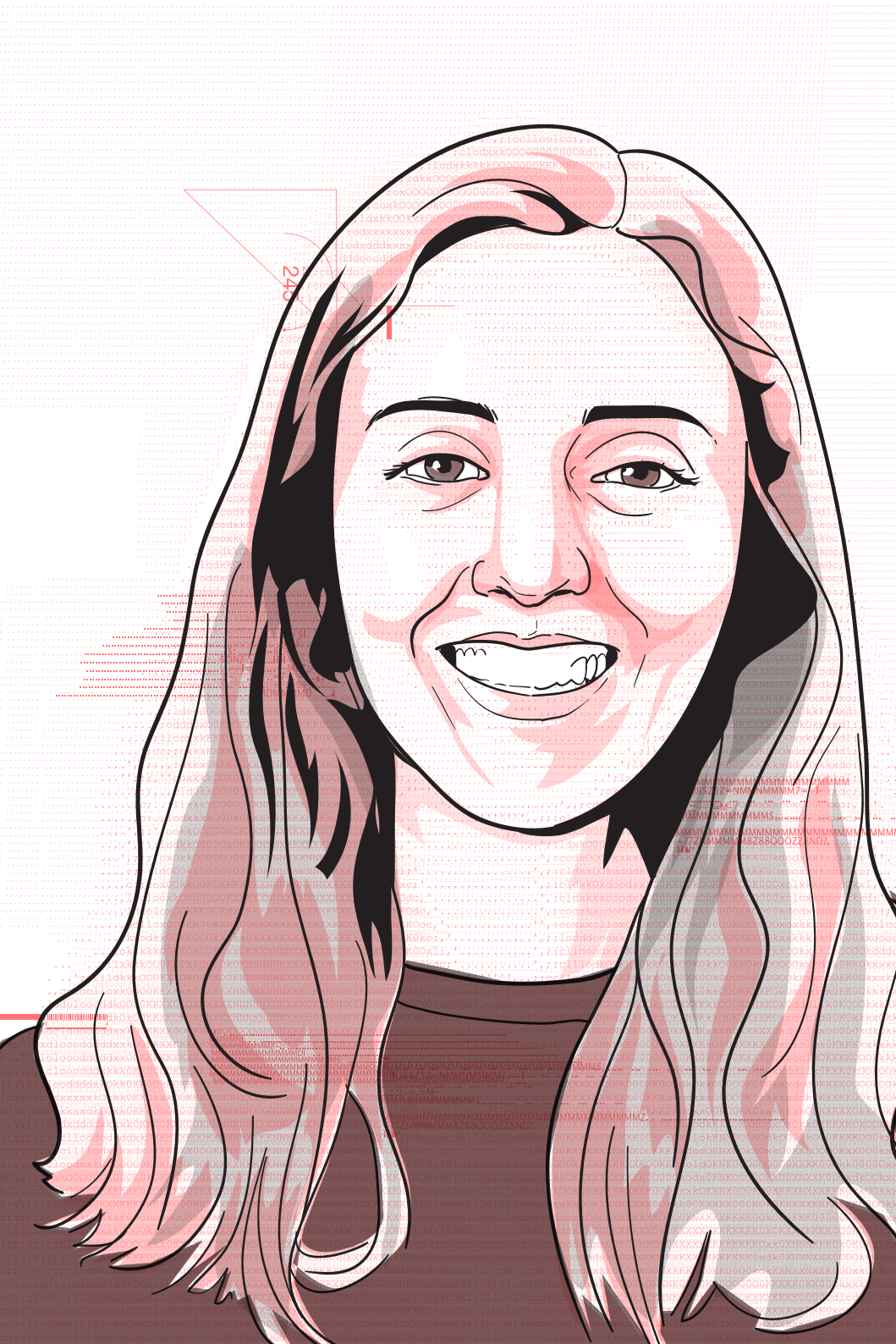
Council of Europe. *Convention on Cybercrime (ETS Nº185).Protocol on Xenophobia and Racism. Explanatory Reports and Guidance Notes.* https://bit.ly/2B7srbw.

Godoy, L. R. U. de. (2016). *A evolução tecnológica e o monitoramento de sinais: uma nova regulamentação jurídica***.** Tese de Doutorado em Direito. Pontifícia Universidade Católica de São Paulo - PUC-SP. https://bit.ly/2YFzosG.

Hoffman, H. (jan. 2019). *Lei 13.441/17 instituiu a infiltração policial virtual.* Jus.com.br. https://bit.ly/30N1Onf.

Osula, A. (2016). *Remote search and seizure in domestic criminal procedure: Estonian case study.* International Journal of Law and Information Technology, Volume 24(4), pp. 363-364. https://doi.org/10.1093/ijlit/eaw010.

Tourinho Filho, F. da C. (1999). *Código de Processo Penal Comentado*, Vol. 1. (4ªedição). Saraiva, p. 530.



09.

INFILTRAÇÕES VIRTUAIS NO DIREITO BRASILEIRO: MAPEANDO O CENÁRIO

Jacqueline Abreu

A presente apresentação[1] oferece um panorama do quadro normativo hoje em vigor sobre o tema das infiltrações policiais virtuais no Brasil. Tentando mapear a discussão, partirei de uma concepção ampla de "infiltrações". Para fins didáticos, esse tema pode ser dividido em três categorias, baseados em dois tipos de critério: (i) o elemento da interação: se a polícia está interagindo de alguma maneira com pessoas que estão sendo investigadas; e (ii) o elemento do espaço: em que tipo de espaço em que está ocorrendo a infiltração.

Então temos: (a) infiltrações que envolvem interação e se desenrolam tanto em fóruns públicos e privados, envolvendo um agente encoberto que assume a identidade falsa (o "agente infiltrado"); (b) infiltrações não interativas, em que a polícia não interage diretamente se comunicando com aqueles que está investigando, mas faz coleta de dados em uma fonte aberta para análise de informações (atividades de inteligência e investigação em fontes abertas); e (c) infiltrações não interativas por meio de invasão em um domínio privado (hacking estatal).

AGENTES INFILTRADOS

Quando pensamos em infiltrações policiais, é difícil não pensar no que é retratado em filmes como "Os Infiltrados" (2006) e "Infiltrado na Klan" (2018). Essa é a concepção mais clássica de "agente infiltrado". É o policial que passa a se envolver com determinada pessoa ou grupo, que é alvo de investigação, e tenta ganhar a sua confiança, para que assim ele possa colher informações privilegiadas sobre aquele grupo, repassar para a polícia e permitir uma investigação apurada. Como existe esse elemento de conseguir a confiança do investigado (e até de tolerância a crimes presenciados), há também por isso um elemento de fraude – uma certa falsidade em que o Estado permite que a polícia se engaje nesses casos específicos em que haveria um interesse relevante para fins de investigação.

Esse tipo de infiltração é interativa e envolve todos os tipos de espaço. Se a polícia desenvolveu uma relação com as pessoas que ela está investigando, ela está se comunicando e colhendo informações tanto em fóruns públicos como em ambientes privados – incluindo nas comunicações de grupo na internet, WhatsApp etc. –, porque a pessoa faz parte daquele grupo agora, em termos de confiança.

O que a gente tem do quadro jurídico aqui? Desde 2006 há uma menção simples e genérica a esse tipo de infiltração policial no art. 53[2] da Lei de Drogas (Lei nº 11.343/2006) como procedimento investigatório disponível para investigar os crimes punidos por aquela lei. Nesse momento não existiu nenhum estabelecimento de critérios de regulamentação específica sobre quais são os parâmetros e qual é o rito.

Em 2013, veio a Lei das Organizações Criminosas (Lei nº 12.850/2013) com uma previsão semelhante no seu art. 10 e alguma regulamentação: é necessário que haja autorização judicial, indícios de que os alvos que estão sendo investigados por infração penal de organização criminosa e demonstração da necessidade desse tipo de prova. Também se impôs limite de seis meses (com possibilidade de renovação) e a elaboração de relatórios circunstanciado sobre tudo aquilo que é feito e apurado. Há ainda um regime de responsabilização por excessos (art. 13), caso o policial se engaje em algum tipo de crime, durante a infiltração, que seja entendido como excesso, além daquilo que ele deveria ter feito ou poderia ter feito para manter a sua identidade naquele grupo. Aos agentes são também resguardados certos direitos (art. 14), como o de fazer cessar a atuação infiltrada.

Por sua vez, em 2017, foi incluído o art. 190-A[3] no Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), que pela primeira vez faz uma menção explícita à infiltração de agentes de polícia *na internet*, como uma medida investigativa possí-

vel para todos os crimes lá elencados – a maioria relacionada a abuso infantil, sendo um deles também o art. 154-A do CP, o crime de invasão de dispositivos. Então, nesses casos, há previsão legal expressa de que um agente de polícia possa se engajar em infiltração virtual. Estão previstos os seguintes elementos: exigência de autorização judicial, delimitação do escopo do que se pode fazer, demonstração de necessidade, limitação temporal (nem tão limitada assim – dois anos), exigência de relatório circunstanciado e etc.

Um comentário pertinente a esse tipo de infiltrações é que, também por conta dessa redação da alteração do ECA com foco em infiltrações *na internet*, levanta-se a dúvida de se a infiltração policial prevista na Lei de Drogas e na Lei das Organizações Criminosas incluiria também autorização para infiltração *virtual* de agentes de polícia. Como pontuei, a categoria de infiltração aqui analisada se refere a infiltrações de agentes policiais em que há elemento de engajamento interativo, voltado a estabelecer relações de confiança, em qualquer tipo de fórum. Como apontei, me parece natural que agentes infiltrados f*isicamente* em grupos também exerçam essa infiltração pela internet – como extensão da mesma identidade falseada. A dúvida, portanto, era/é o quanto desse tipo de engajamento seria permitido através da criação de identidades falsas e estabelecimento de relações com investigados em fóruns quase-públicos (como redes sociais, em que é necessária a criação de perfil para acesso ou de autorização do administrador) ou privados (chats em aplicativos de mensagens) *unicamente ou preponderantemente online*, sem o contato presencial. Nesse aspecto, uma atualização legislativa recente foi trazida pela Lei nº 13.964/2019, que alterou a Lei das Organizações Criminosas para dispor explicitamente sobre infiltrações policiais virtuais (arts. 10-A a 10-D), estando disponível para "investigar os crimes previstos nesta Lei e a

eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas".

INTELIGÊNCIA E INVESTIGAÇÃO EM FONTES ABERTAS

Há também um tipo de infiltração policial virtual que não é interativo com pessoas que se está investigando. O que se faz nesse tipo de infiltração é coletar e analisar comunicações e dados que estão disponíveis abertamente, em uma fonte aberta em fóruns públicos ou quase-públicos.

No final de 2018 saiu uma notícia de que a Polícia Civil de São Paulo faria algo chamado de *cerca eletrônica*[4]: uma raspagem dos dados disponíveis publicamente em redes sociais, a partir de recortes de publicações em regiões ou certas palavras chave, a pretexo de fazer "campana virtual" e até para começar investigações. Então, por exemplo, raspam-se todos os tuítes com a palavra "arma" ou "assalto" em São Paulo e aí se provoca o engajamento da Polícia Militar para certa área e/ou efetivamente começar uma investigação. Isso conversa bastante com a palestra da professora Margaret Hu na abertura do congresso, em que ela estava dizendo que hoje a polícia faz análise de big data.

O que temos aqui é um tipo de infiltração que consiste em uma grande operação de coleta e análise de informações – inclusive pessoais. Coleta-se um grande volume de dados, que passa a ser analisado a partir de critérios definidos pela própria polícia e então se chega a quem e ao quê se vai investigar. Essa atividade envolve uma reversão da lógica do processo penal, que é partir não de um suspeito ou de um fato criminoso sobre os quais se quer produzir provas, mas de grandes volu-

mes de dados para então chegar em um suspeito, então chegar em algum fato criminoso que você vai passar a investigar.

Esse tipo de atuação infiltrada é frequentemente associado com "campanas policias" comuns, de policiamento ostensivo (como se faz na reportagem citada), para se pontuar que não precisa atender a requisitos materiais e formais específicos. De fato, esse tipo de atividade escapa de um regramento mais específico por duas razões: seu cunho preventivo (em detrimento de repressivo) e a afetação de dados pessoais (mas não propriamente de interesses de privacidade).

Quanto ao primeiro ponto, vale observar que esse é um tipo de infiltração virtual que é inserido principalmente em atividades de inteligência policial. Em outras palavras, não é uma atividade com ênfase investigativa propriamente dita, voltada à repressão de uma conduta criminosa. Quanto a atividades de "agentes de inteligência" – e ao modo como se contrastam com os agentes infiltrados da categoria anterior, vale mencionar uma distinção a que recorreu o STF em uma decisão recente da 2ª Turma (HC 147.837, de 26.02.2019, rel. Min. Gilmar Mendes): "a distinção entre agente infiltrado e agente de inteligência se dá em razão da finalidade e amplitude de investigação. Enquanto "agente de inteligência" tem uma função preventiva e genérica, buscando informações de fatos sociais relevantes ao governo, o "agente infiltrado" possui finalidades repressivas e investigativas, visando à obtenção de elementos probatórios relacionados a fatos supostamente criminosos e organizações criminosas específicas."

Como já se sinalizou, entretanto, uma atividade de inteligência pode se tornar uma atividade investigativa. A partir do momento em que há direcionamento para apuração de um fato concreto e finalidade repressiva, já se está diante de atividade com cunho investigativo. Na ausência do engajamento (interação para conquista de confiança), pode-se falar em

/ A ATIVIDADE ENVOLVE A REVERSÃO DA LÓGICA DO PROCESSO PENAL: PARTIR DE GRANDES VOLUMES DE DADOS PARA CHEGAR A UM SUSPEITO, A UM FATO CRIMINOSO /

"agente disfarçado" – categoria que pressupõe atuação investigativa passiva e que não possui um regramento particular.[5] Caso a atuação evolua para as características vistas na categoria anterior, atrai-se o regramento aplicável (visto na categoria anterior). De fato, como decidiu o STF nesse caso, uma atividade de inteligência (de um policial militar), que começou para simplesmente obter informações para orientar as estratégias de atuação durante a Copa do Mundo e monitoramento de manifestações, logo passou a ser voltada a efetivamente investigar conduta de um grupo concreto de pessoas, estabelecendo-se relações de confiança com eles com o propósito de obter provas (para inquérito da Polícia Civil). Nesse sentido, a prova obtida e usada contra tais pessoas seria ilícita por não ter obedecido aos requisitos legais para infiltrações policiais.[6]

Quanto ao segundo ponto, cabe observar que a atividade de coleta e análise em si de informações em fontes abertas não é considerada invasiva de interesses de privacidade (que supõe interferência em âmbito privado) – sendo, na verdade, tratável sob a perspectiva da proteção de dados pessoais. Nesse sentido, não está sujeita a um regramento abrangente, que estabeleça balizas e salvaguardas nenhuma em termos de devido processo legal. Com efeito, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), além de ainda não estar vigor, tem o âmbito de aplicação recortado: o seu art. 4º, III dispõe que não se aplica a tratamentos e operações para a segurança pública em investigações. O ponto aqui então é que nós precisamos avançar em uma discussão sobre uma legislação específica para esse assunto e finalmente criar uma autoridade nacional competente para a área.

HACKING

O terceiro tipo de infiltração a ser comentado é de tipo não interativo e envolve intrusão em domínio privado. Uma notí-

cia que ilustra esse tipo de medida, ou pelo menos a pretensão de executá-la, é essa: "PF quer instalar vírus em telefone grampeado para copiar informações."[7] Publicada em 2015, é interessante observar como ela é da mesma época em que o WhatsApp realmente ganhou popularidade. Demonstra como autoridades policiais passaram a se preocupar com o fato de que agora não conseguiam mais, com o mesmo tipo de efetividade, obter informações através de interceptações telefônicas. Nesse sentido, tentaram forçar empresas de telefonia a instalar vírus em telefones celulares, para assim conseguir acesso aos aplicativos que têm instalados naquele celular e inclusive aos dados dentro desses aplicativos, portanto, o Whatsapp e as mensagens etc. Esse é um tipo de atuação policial que envolve um elemento de hacking (exploração de vulnerabilidades de computadores e sistemas, contaminando-os com programa malicioso).[8]

Quais são os critérios e as balizas para esse tipo de diligência? Neste primeiro momento, a polícia dizia que uma ordem judicial baseada na Lei de Interceptações (Lei nº 9.296/96) era o suficiente. E, com base nessa tese, tentavam forçar as empresas a instalarem esse vírus espião.

Essa tese tem, entretanto, problemas e, para ilustrá-los, cabe mencionar uma decisão recente do STJ. Trata-se do RHC 99.735 (j. 12.12.2018, rel. Min. Laurita Vaz), que envolvia também o WhatsApp, mas não exatamente o uso de software espião. Nele, a autoridade policial apreendeu momentaneamente o celular de uma pessoa, fez o espelhamento pelo WhatsApp Web, com o QR Code. Assim, puxaram todas as mensagens para o computador e a seguir devolveram o celular para a pessoa, que seguiu em frente. A partir do que tinha obtido pelo WhatsApp Web, a polícia conseguiu ter acesso a diversas comunicações que estavam no histórico daquela pessoa, salvas ainda no celular dela.

Ao analisar a licitude da prova assim obtida, o STJ entendeu que havia características específicas aqui: esse tipo de medida (i) envolve um acesso aos dados armazenados historicamente, não só comunicações em tempo real; e (ii) implica a capacidade da polícia de deletar e editar mensagens, justamente porque ela tem a interface do próprio usuário. Essas duas características distinguem a medida de uma interceptação telefônica ou telemática tradicional – em que só se tem acesso a comunicações em tempo real, sem capacidade de intervir/editar. Seria uma medida que não comporta analogia com a Lei nº 9.296/96, e por isso esse tipo de prova, obtida dessa maneira, é ilegal até que seja passado algum tipo de legislação específica que aprove algo nesse sentido. Entendo que esse mesmo raciocínio se aplica a questões de hacking – não temos regramento específico para isso e, até termos, não é possível executar como meio lícito de obtenção de prova.

Então é esse o estado em que nós estamos. Existe um interesse de autoridades investigativas em autorizar isso, reconhecendo em lei. Foram propostas mudanças na Lei nº 9.296/96 nesse sentido no projeto de lei anticrime.[9] Não foi, entretanto, acolhida a proposta nesse ponto.

NOTAS

1. O presente texto se baseia em apresentação oral feita no painel "A atuação de agentes de investigação em redes sociais e aplicativos de mensagem" do III Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em parceria com a FDUSP em agosto de 2019. A autora agradece aos organizadores e às organizadoras pelo convite e pela oportunidade de também registrar as reflexões por essa via. O texto foi revisto em junho de 2020, quando se fez pequenos ajustes para remover maiores oralidades e atualizar comentários.

2. Lei nº 11.343/2006, Art. 53: "Em qualquer fase da persecução criminal relativa aos crimes previstos nesta Lei, são permitidos, além dos previstos em lei, mediante autorização judicial e ouvido o Ministério Público, os seguintes procedimentos investigatórios: I - a infiltração por agentes de polícia, em tarefas de investigação, constituída pelos órgãos especializados pertinentes;"

3. Lei nº 8.069/1990, Art. 190-A, caput: "A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), obedecerá as seguintes regras: (Incluído pela Lei no 13.441, de 2017)"

4. Cerca eletrônica da polícia na internet ajuda a resolver crimes, *O Estado de São Paulo*, 10 de novembro de 2018, https://bit.ly/2ZpiFLx.

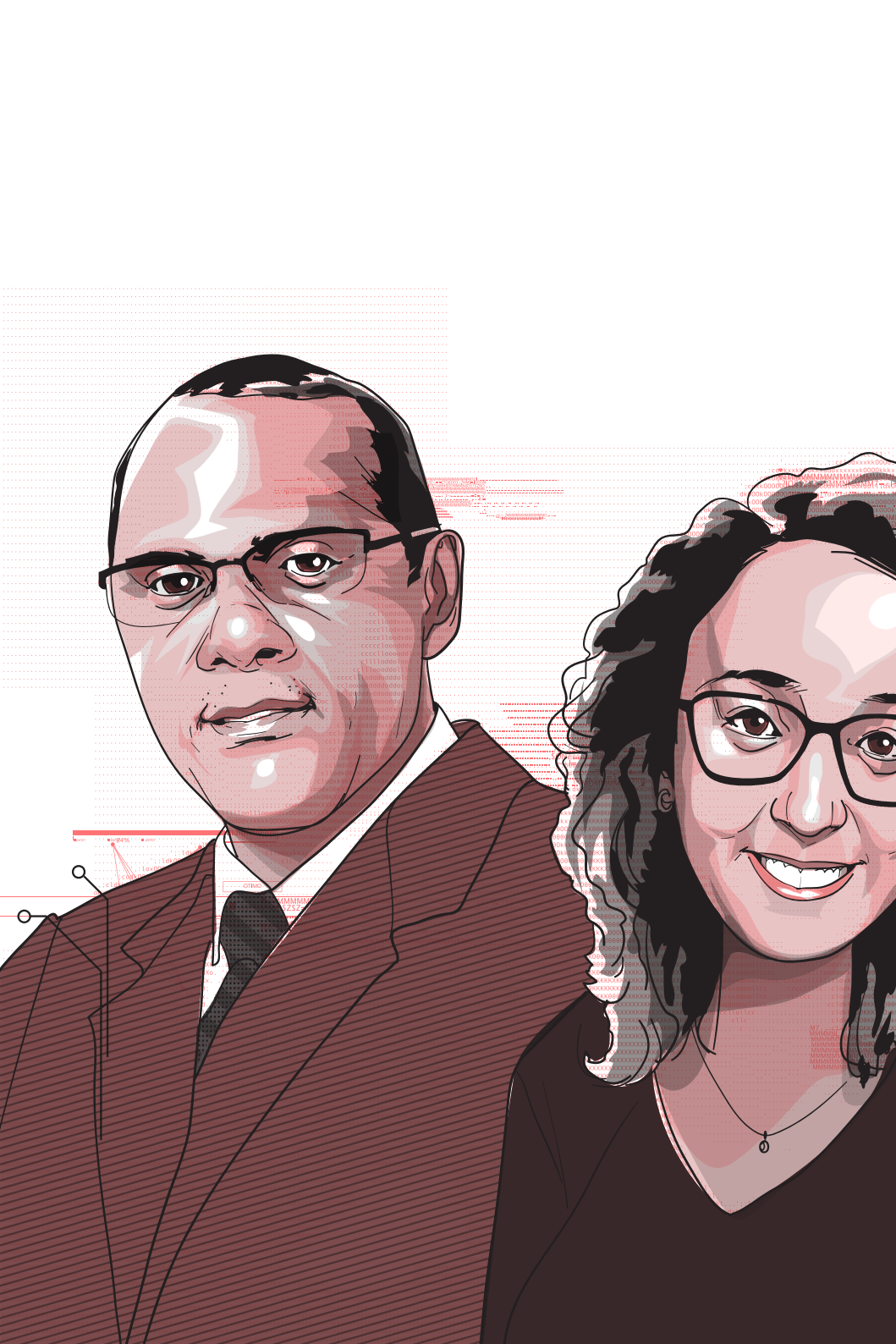
5. A Lei nº 13.964/2019 (Anticrime) faz menção da figura do agente policial disfarçado em alterações à Lei nº 10.826/2003 (arts. 17 e 18) e à Lei nº 11.343/2006 (art. 33), no sentido de que a venda de armas ou drogas para um agente policial disfarçado ainda caracterizaria crime quando haja "elementos probatórios razoáveis de conduta criminal preexistente". Não há, entretanto, maior regulamentação da atuação em si. Para discussão sobre tal figura e como se diferencia de um agente *provocador*, ver LINS, C.; SOUZA, R.; CUNHA, R. (2020). "A nova figura do agente disfarçado". In: Ministério Público Federal. *Inovações da Lei nº 13.964 de 24 de dezembro de 2019*. Brasília: MPF.

6. Para discussão sobre a decisão do STF, ver ROMÃO, L. (2019, dezembro). Agente Infiltrado e agente de Inteligência: distinções a partir de estudo de caso julgado pelo Supremo Tribunal Federal. *Revista Brasileira de Inteligência*. Brasília: Abin, n. 14.

7. Folha de São Paulo, 27 de abril de 2015, https://bit.ly/2OyZybX.

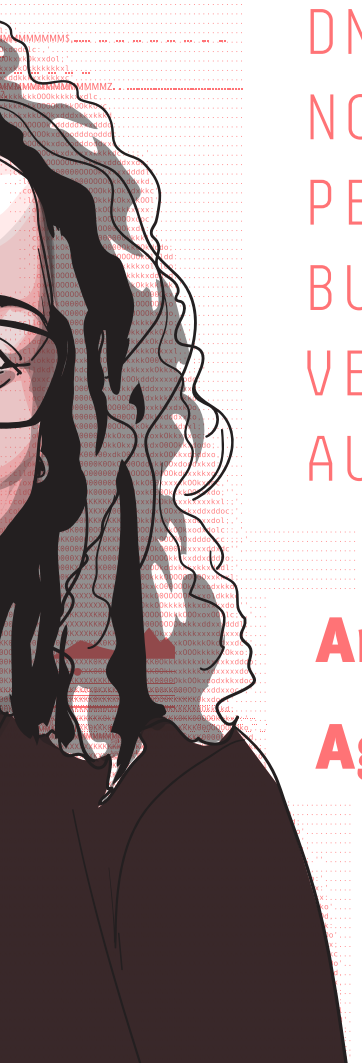
8. Para referência introdutória sobre o assunto, ver ABREU, J.; ANTONIALLI, D. (2017). E quando a polícia vira hacker? Blog do InternetLab. https://bit.ly/3iX25dL.

9. O PL 882/2019 chegou a contar com a proposta de inserir na Lei nº 9.296/1996 dispositivo que previa: "Art. 9º-A. A interceptação de comunicações em sistemas de informática e telemática poderá ocorrer por qualquer meio tecnológico disponível desde que assegurada a integridade da diligência e poderá incluir a apreensão do conteúdo de mensagens e arquivos eletrônicos já armazenado em caixas postais eletrônicas".



10.

DNA COMO PROVA NO PROCESSO PENAL: DA BUSCA PELA VERDADE À NÃO AUTOINCRIMINAÇÃO



André Luiz Nicolitt

Agatha Rosa

[...] E se todos os outros aceitassem a mentira imposta pelo Partido – se todos os registros contassem a mesma história –, a mentira tornava-se história e virava verdade. "Quem controla o passado controla o futuro; quem controla o presente controla o passado", rezava o lema do Partido. E com tudo isso o passado mesmo com sua natureza alterável, jamais fora alterado. Tudo o que fosse verdade agora fora verdade desde sempre, a vida toda. [...]

1984, George Orwell

INTRODUÇÃO

A possibilidade de se determinar a identidade de uma pessoa a partir do seu DNA se tornou um dos grandes marcos científicos do século XX. Toda a informação genética que um ser vivo possui, além de subsídio para seus traços físicos, performa também profícua fonte para a sua individualização, isto é, para o seu reconhecimento numa população de semelhantes.

Variabilidade é uma característica natural da molécula de DNA. Salvo os casos de gêmeos univitelinos, nunca duas pessoas compartilharão as mesmas informações genéticas. Partindo-se desse fato, os avanços do conhecimento biológico e de novas tecnologias possibilitaram que o DNA fosse acessado, compreendido e, posteriormente, manipulado. Esse arcabouço foi preponderante para o estabelecimento da sua análise como uma técnica eficiente para identificação humana.

Assim, além de contribuir em diferentes áreas de pesquisa, como, por exemplo, no estudo de doenças genéticas e na produção de medicamentos personalizados, desde a década de 1980 as análises de DNA foram transformadas também

em ferramenta das investigações criminais, ganhando amplo uso nesse campo.

Para se alcançar um resultado, as análises de genética forense necessitam de uma comparação entre o perfil genético de um suspeito e o perfil apresentado pelo vestígio biológico encontrado na cena do crime ou na própria vítima. Havendo identidade, torna-se possível estabelecer um vínculo entre ambas as amostras, transparecendo, num primeiro momento, o envolvimento da pessoa sob investigação com o crime.

Esse tipo de busca pode tanto contribuir para determinar a ausência de uma pessoa na cena de um crime, possibilitando a sua consequente absolvição por inexistência de vínculo genético entre os perfis, quanto, por outro lado, convencer sobre o envolvimento de um suspeito em um delito, contribuindo para a sua condenação. Nessa segunda hipótese, como veremos, confirmar o envolvimento de alguém com determinado crime implica, necessariamente, a convergência de outras provas para trazer robustez à hipótese acusatória. Isso porque, a mera presença do DNA pode ter outras explicações.

Ademais, por ser um tipo de prova produzida, em regra, fora do processo, utilizando de conhecimentos técnico-científicos praticamente ininteligíveis ao operador do direito, acaba sendo revestida com um manto de veracidade e inquestionabilidade, que atinge o imaginário dos operadores jurídicos, ganhando importância tamanha no processo a ponto de velar qualquer discussão acerca da sua capacidade para provar.

A perspectiva analítica do trabalho é de realçar o seguinte: no processo penal a dúvida é suficiente para uma decisão absolutória e isso demonstra que a utilização dos exames de DNA com o fim de provar a inocência pode ter seu uso alargado e mais tranquilo, não sendo poucos os casos de condenações revertidas em decorrência da superveniência de análise

de DNA. Por outro lado, as decisões condenatórias exigem um *standard* probatório mais rigoroso, de modo que mesmo as análises de DNA não podem ser admitidas ou valoradas sem as devidas cautelas.

Outro aspecto a se pensar sobre o tema é o fato de a análise de DNA reclamar a comparação com o perfil genético da pessoa suspeita, isto é, demandar que ela colabore ativamente com a investigação. Nesse tocante, entendemos que tal procedimento também deve possuir como fundamento os limites da dignidade da pessoa humana e da não autoincriminação, aspectos do Estado Democrático de Direito.

Deste modo, o objetivo deste trabalho é realçar a necessidade de cuidados na admissão e valoração das análises de DNA, bem como apontar a dignidade humana e o *nemo tenetur se detegere*, como limites impostos a atividade probatória, com destaque às intervenções corporais voltadas à coleta de material genético nas pessoas suspeitas, investigadas ou mesmo condenadas.

1. O DNA NO PROCESSO PENAL

A capacidade humana de ler e interpretar as informações contidas na molécula de DNA consubstanciou um dos avanços científicos de maior importância no século XX. Como exemplos podemos citar o estudo mais profundo de doenças genéticas e a elaboração de medicamentos personalizados, o desenvolvimento de organismos geneticamente modificados, desde a produção de insulina em larga escala até os plantios resistentes a determinadas pragas, e, mais recentemente, o fato de ter aproximado a antes utópica chance de se editar os genes de um organismo de forma precisa e controlada.[1]

Não obstante, as análises de DNA também se tornaram importante instrumento de auxílio à justiça. Não só no reconhecimento de paternidade e identificação de vítimas de

grandes acidentes (quando há a perda da identidade física), como também na determinação de culpa ou inocência de indivíduos suspeitos de terem cometido determinados crimes.

A Biologia Molecular é o ramo científico que se dedica ao estudo do dogma central da Biologia. Melhor dizendo, ela se ocupa dos processos imbricados na transformação da informação genética contida no DNA em proteína, estrutura metabolicamente ativa. A Genética Molecular, de maneira mais específica, se debruça sobre o estudo da estrutura e função desses trechos de informação (genes), lançando mão de técnicas que permitam o acesso de forma direta ao material genético. Ainda, vale dizer que a Ciência Forense trata de compilar ambos os conhecimentos com o objetivo de auxiliar o sistema de justiça criminal, contribuindo efetivamente para a materialização de prova a ser utilizada no processo penal.

Por muito tempo as proteínas, notadamente aquelas que compõem os grupos sanguíneos, foram utilizadas pelos procedimentos de identificação humana, possivelmente porque também podem ser encontradas em outros fluidos corporais além do sangue, como no sêmen.[2] Entretanto, a limitada variabilidade impedia uma identificação mais precisa.

Dessa forma, partindo-se do pressuposto de que o DNA é uma molécula de grande variabilidade e, portanto, altamente informativa para fins de individualização, os avanços das técnicas de biologia molecular possibilitaram que, desde a década de 1980, os processos de identificação genética figurassem como uma ferramenta biológica revolucionária para a identificação de pessoas,[3] atuando em colaboração às práticas mais tradicionais do meio criminal, como a datiloscopia, por exemplo.

No campo legal, vale destacar que os crimes ditos permanentes são aqueles que deixam vestígios, elementos sensíveis aos sentidos, na cena do crime. Nossa lei processual penal exige que nesses casos seja realizado o exame de corpo de

delito (art. 158 do CPP). Ou seja, através dessa apreciação, os diferentes vestígios[4] encontrados no local podem ser convertidos em provas no processo penal.

As análises de DNA, ou DNA forense, possibilitam a identificação do vestígio biológico que compõe o corpo de delito do crime. Através de um procedimento comparativo entre dois perfis genéticos obtidos de diferentes amostras biológicas – uma de origem conhecida, obtida da pessoa sob a qual recaem as suspeitas de autoria, e outra, recolhida do ambiente no qual ocorreu o delito (cuja autoria se busca conhecer) –, é possível a determinação de coincidência e compatibilidade entre elas.[5]

O DNA pode ser extraído dos mais variados elementos biológicos, como sangue, sêmen, pelos, dentes, fezes, urina etc., que sejam encontrados na cena do crime ou no corpo da vítima. Um tipo de evidência que tem se tornado particularmente importante para a pesquisa forense é o "DNA de toque", cuja molécula pode ser recuperada de frações mínimas de componente biológico, praticamente imperceptíveis, como de células descamadas da epiderme que são transmitidas pelo toque de uma pessoa a um objeto.[6] Basta que seja possível a extração de material genético do vestígio – isso depende que ele seja corretamente manuseado para não dar azo à degradação – para que se tenha fonte de pesquisa de identidade.

Assim, sempre que for necessária a determinação da identidade de alguém, o DNA será fonte riquíssima de pesquisa. É, portanto, num pequeno indício que podemos encontrar grande informação.

Diante do exposto, e considerando-se que o presente trabalho objetiva situar as análises de DNA no contexto de investigações criminais, reputamos relevante traçar uma breve nota sobre as principais características dessa molécula, que acabaram por forjar o seu amplo uso na prática forense.

1.1. DNA: ASPECTOS ESTRUTURAIS E FUNCIONAIS

De início, não nos custa retomar a conhecida informação de que todos os seres vivos possuem DNA, ácido desoxirribonucleico, como material genético, e que todo DNA apresenta variabilidade inter e intraespecífica.[7] A partir desse fato, depreendemos que nenhum organismo possui exatamente o mesmo conteúdo molecular informativo que outro.

Ele está contido nos cromossomos das células humanas e apresenta todas as informações transmissíveis por hereditariedade, perfazendo o código da vida. Nele, cada segmento responsável pela síntese de uma proteína é chamado de gene, isto é, uma sequência portadora de informação que codifica o arranjo de aminoácidos para a construção de uma proteína. Esta, por sua vez, concretiza a forma ou função do organismo,[8] sendo o produto da expressão gênica.

A molécula de DNA entrou nos holofotes da ciência quando um químico suíço descobriu o ácido nucleico na segunda metade do século XIX[9] durante suas pesquisas sobre os componentes nucleares de leucócitos. Já no começo dos anos 1920 os pesquisadores haviam adquirido uma compreensão mais robusta sobre a estrutura desse composto, notadamente quanto aos seus componentes fundamentais: pentose, fósforo e bases nitrogenadas (adenina – A, guanina – G, citosina – C e timina – T). Entretanto, além desses detalhes rudimentares, nada se sabia sobre a estrutura ou função do DNA.[10]

Nesse ponto precisamos apresentar duas informações cruciais: os supracitados elementos se estruturam num arranjo molecular chamado nucleotídeo, cada um com uma base específica; depois, estes nucleotídeos se organizam de maneira seriada formando cadeias poliméricas. O DNA é formado por uma grande cadeia polinucleotídica (duas, como veremos) e cada gene possui uma sequência de nucleotídeos específica, variável de pessoa a pessoa.

Ato contínuo, na primeira metade do século XX a academia procurou determinar qual seria a molécula portadora das informações genéticas. Uma corrente defendia as proteínas, tidas como mais estáveis e com maior variabilidade do que o ácido desoxirribonucleico, visto como frágil e de pouca complexidade, mas que, ainda assim, ocupou o segundo polo.[11:12]

Apesar desse período conter uma belíssima história científica, composta pelos mais sofisticados e delicados experimentos laboratoriais,[13] cabe-nos apenas mencionar que a segunda corrente saiu vencedora: o DNA foi determinado como a molécula genética primordial.

Após esse momento, as pesquisas tomaram o rumo da elucidação da estrutura do DNA, cuja informação permitiria o início da compreensão da expressão gênica. Assim, calcando-se em todas as informações disponíveis até o momento, em especial à imagem de difração de raio X produzida por Rosalind Franklyn, em 1953 James Watson e Francis Crick propuseram a teoria da dupla-hélice[14] como a estrutura do DNA, composta por duas cadeias polinucleotídicas entrelaçadas em forma helicoidal. Vale um destaque acerca da disposição dos seus componentes fundamentais:

> [...] O "D" do DNA representa o açúcar desoxirribose (NA = ácido nucleico). Os grupos de açúcar desoxirribose, separados por moléculas de fosfato, formam a espinha dorsal da molécula de DNA. Ligado a cada açúcar há um composto chamado base (como em oposição ao ácido). São quatro as variedades de bases [...], as quais costumam ser representadas pelas respectivas iniciais: A, C, G e T. A base de uma fita se liga a uma base na outra, conectando as duas fitas como os degraus de uma escada. Mas A só pode se ligar a T (e vice-versa) e C a G (e vice-versa).[15]

O curto trecho acima colacionado traz uma importante concepção em suas duas últimas frases. Essa forma tão específica de ligação entre as bases nitrogenadas define o caráter de complementariedade entre as duas cadeias que formam a dupla-hélice, isto é, estando ambas unidas, foi possível perceber que a informação contida em uma fornece o subsídio para a complementação da cadeia que forma o seu par. Assim, por exemplo, se um trecho do DNA é formado em um cadeia pela sequência ATTCGATCC, na cadeia complementar a informação será TAAGCTAGG.

De posse dessa referência foi possível a determinação dos mecanismos conectados à primeira etapa do dogma central, a replicação do DNA.[16] De maneira resumida, a replicação inicia com a abertura da dupla-hélice pela ação de uma enzima específica e a partir de então cada cadeia passa a servir de molde para que um novo arranjo polinucleotídico seja complementado a ela pela ação da DNA polimerase,[17] por uma enzima que atua criando um polímero de nucleotídeos a partir do reconhecimento da ligação específica de bases.

Nessa esteira, o progresso científico possibilitou que os princípios da replicação fossem aplicados na amplificação artificial de trechos de DNA: as sequências-alvo de interesse poderiam ser acessadas e aumentadas em quantidade suficiente para análises posteriores. Em meados de 1980 uma técnica molecular capaz de levar ao crescimento exponencial dessas sequências de maneira mais rápida e menos trabalhosa chegou aos laboratórios com o nome de PCR (reação em cadeia da polimerase, em português).[18]

Feita essa breve introdução acerca da estrutura e função da molécula mestra, precisamos dedicar algum espaço para falar das sequências que a compõem.

Os genes que integram o genoma[19] humano correspondem apenas a uma pequena porção do DNA, o que nos leva à

conclusão de que a maior parte dele é, na verdade, formada por trechos de sequências que não carreiam qualquer informação para a produção de proteínas (mas que, como se considera, também não deixam de ter sua função biológica). Essas sequências se localizam em regiões intergênicas (entre genes) e são compostas por arranjos de repetições nucleotídicas (ex.: ACTACTACTACTACTACTACT...) decorrentes de uma falha natural na maquinaria de replicação.[20]

Já mencionamos que a variabilidade do DNA consta na singularidade do arranjo nucleotídico, mas apesar de estarmos falando de sequências repetitivas, elas também são fonte de informação bastante valiosa para fins de identificação, particularmente porque são hipervariáveis no que tange à quantidade de vezes que aparecem nas pessoas. Ou seja, cada indivíduo acaba possuindo um tamanho específico, maior ou menor, dessas sequências. Em outros termos, temos que o núcleo repetitivo (no exemplo acima seria ACT) acaba se revelando numa quantidade específica e, assim, exsurge como um verdadeiro marcador molecular, como um ponto de referência no genoma que pode ser comparado entre duas amostras de DNA para fins de identificação.

Nesse contexto, para o estabelecimento de vínculo genético entre o suspeito e o material biológico coletado na cena do crime é preciso, antes, que se faça uma extração de DNA e que a região genômica que inclua o marcador molecular de escolha seja amplificada pela técnica de PCR em ambas as amostras. Posteriormente, os produtos dessa amplificação serão submetidos a uma técnica específica que permita a visualização e consequente comparação de tamanho.

Quanto maior a quantidade de marcadores em análise, mais pontos de comparação entre ambas as amostras teremos, o que enseja um aumento da sensibilidade do procedimento e de sucesso na identificação forense. Atualmente, podem ser

/ O RESULTADO DA ANÁLISE PODE ATÉ SER VERDADEIRO, MAS O MATERIAL GENÉTICO NÃO REFLETE A OCASIÃO DO FATO DELITUOSO /

/ É PRECISO QUE SE MANTENHA UM MECANISMO DE RASTREAMENTO DA EVIDÊNCIA PARA DEMONSTRAR A IDONEIDADE DA PROVA NO PROCESSO /

encontrados no mercado kits para identificação de pessoas e alguns podem amplificar até 16 regiões, isto é, 16 marcadores genéticos, em uma única PCR.[21]

Vale ressaltar que a partir dessa amplificação, cria-se o perfil de DNA ou DNA *fingerprinting*, em alusão à tradicional técnica de identificação pelas impressões digitais (*fingerprint*).[22]

Acabamos de mencionar uma das técnicas mais tradicionais de identificação genética da praxe forense, a qual procuramos citar para fins de contextualização e buscando deixar tal explanação à margem da técnica típica da área. Contudo, outras ferramentas moleculares também podem ser utilizadas atualmente no processo de identificação de pessoas por meio de seu DNA, como SNP, RFLP, sequenciamento, análises epigenéticas, entre outras.[23] Aprofundar o tema, contudo, se mostra desnecessário aos fins para os quais nos voltamos nesse momento.

1.2. FALIBILIDADE DA PROVA DE DNA

Não obstante as informações que trouxemos da seção anterior, especificamente acerca do potencial identificador do material genético de uma pessoa, não é possível que apresentemos o DNA forense como uma *conditio sine qua non* das investigações criminais.

Se pararmos para refletir um pouco, veremos que o procedimento de identificação se limita tão somente a criar um vínculo entre duas amostras genéticas, isto é, ele diz a quem pertence o perfil genético do vestígio coletado na cena do crime, mas, por outro lado, não tem a capacidade de conferir mais informações acerca do momento (antes, durante ou depois do evento criminoso) ou sobre como (transferência direta ou indireta) o DNA foi lá deixado.[24]

À título de exemplo, podemos citar o caso de Lukis Anderson,[25] um sem-teto norte-americano, que foi preso em de-

zembro de 2012 acusado de ter assassinado Raveesh Kumra, um milionário do Vale do Silício, na Califórnia. A única prova da qual havia se desincumbido a acusação foi demonstrar a presença do DNA de Anderson no local do crime, e apenas com ela possivelmente pediria a pena de morte. Apesar do cenário, o rapaz não era culpado e tinha o forte álibi de ter sido hospitalizado na data do crime e ter permanecido sob constante supervisão médica naquele dia. Posteriormente, a equipe jurídica que o defendia percebeu que o DNA de Anderson havia sido deslocado do hospital para a cena do crime por meio dos próprios médicos que chegaram à casa de Kumra: eram os mesmos que haviam tratado de Anderson naquela manhã e, inadvertidamente, acabaram "plantando" as evidências na cena do crime.

Esse caso real demonstra a capacidade de o DNA forense confirmar uma falsa realidade. Isso porque o resultado da análise pode até ser verdadeiro – realmente o perfil genético do suspeito coincide com o perfil encontrado na cena do crime –, mas o material genético extraído do vestígio não reflete a ocasião do fato delituoso. Acabou sendo detectado porque lá apareceu por outras circunstâncias.

Essa discussão ganha ainda mais força num cenário no qual o perfil genético da evidência é comparado aos perfis de bancos de dados de DNA mantidos pelas instâncias governamentais de persecução, o que amplia sobremaneira o alcance do erro.

Nessa seara, insta mencionar alguns apontamentos trazidos por Peter Gill em publicação intitulada "Misleading DNA evidence: reasons for miscarriages of Justice."[26] Aduz o autor que, apesar de a sensibilidade das tecnologias de análise de DNA estarem aumentando progressivamente, há um paralelo com o também aumento da detecção de perfis genéticos não necessariamente associados com o fato criminoso. Isso ocor-

re, basicamente, porque as moléculas de DNA podem ser encontradas em qualquer lugar, bem como podem ser transferidas para a cena do crime de forma ativa ou passiva. Portanto, a fim de garantir a confiabilidade da análise, ele determina:

> To avoid false associations leading to false deductive logic, it is necessary for scientists to actively consider all possible methods of transfer: before the crime-event – innocent transfer or background contamination; after the crime-event – investigator-mediated contamination.[27]

A compreensão das variáveis relacionadas à transferência de DNA no contexto de investigações criminais é um tema sob o qual vasta literatura se debruça. Em recente artigo de revisão, Roland Oorschot e colaboradores[28] buscaram compilar informações sobre o assunto e lançar luzes acerca da necessidade de todas as pessoas que interagem com a evidência terem conhecimento das possibilidades de transferência de DNA após a atividade criminosa, procurando limitar os riscos de contaminação ou perda do material genético.

Diante dessas informações, resta-nos claro que contaminações no material genético coletado na cena do crime podem ocorrer, contribuindo para que se chegue a um resultado verdadeiro com base numa falsa percepção da realidade.

Isso nos faz compreender duas questões de grande importância relativas à valoração da prova e cadeia de custódia. A dependência exclusiva de provas de DNA pelo sistema de justiça criminal, muitas vezes tratadas como infalíveis, na verdade são capazes de ensejar risco significativo para a condenação de pessoas. Daí a necessidade de sermos cautelosos quanto ao uso e apresentação desse tipo de prova de maneira isolada no processo, o que nos faz ressaltar que elas devem sempre vir acompanhadas de outras provas para que se con-

dene uma pessoa. Precisamos ser de certa forma mais céticos e conceber a existência de um desgaste na confiança do DNA forense como prova inequívoca.

Em segundo lugar, temos que o contexto exposto também nos alude quanto a uma premente necessidade de que haja gerência sobre os processos empregados na custódia dessas evidências, desde a coleta até o seu uso pelo tribunal, procedimento que tem a aptidão de criar um controle sobre eventuais interferências externas, daí a relevância da chamada cadeia de custódia da prova do que cuidaremos adiante.

Uma última nota sobre o tema da falibilidade consiste no fato de nos situarmos num sistema composto por operadores do direito com conhecimentos superficiais sobre as análises de DNA e cuja compreensão acaba sustentando tal prova como carreadora de um caráter técnico e identificador de valor superior às demais provas.[29]

2. DNA COMO PROVA CIENTÍFICA E PRESUNÇÃO DE VERDADE

Como tentamos demonstrar inicialmente, a prova de DNA é materializada por meio de conhecimentos técnico-científicos próprios das ciências biológicas, que são experimentais. Agora precisamos discutir o motivo pelo qual recai sob ela um costumeiro manto de inquestionabilidade.

É consenso no mundo moderno que o conhecimento depreendido pelo método científico alcança a verdade através da comprovação empírica.[30] Assim, a vasta experimentação que segue a validação ou refutação de uma determinada hipótese acaba funcionando como base sólida para confirmar o resultado ao qual se chega. Seja positivo ou negativo, ele foi testado na prática, de modo a ser reduzido qualquer espaço para dúvidas.

Como bem aponta Aury Lopes Jr,[31] determinadas provas, como aquelas obtidas por análise de DNA, possuem uma cer-

ta pretensão de evidência, servindo como verdadeiro atalho para a obtenção da verdade. Segundo o autor, são provas que acabam por sedar os sentidos e anular o contraditório porque se fundamentam em mecanismo de autorreferência, bastando-se por si próprias.

No mesmo sentido, há trabalhos da literatura especializada que apontam o fato das provas obtidas por métodos científicos receberem um grande peso na visão dos jurados, o que revela a dita sedação dos sentidos. A análise de DNA é, inclusive, tida como o padrão ouro em relação a outras provas utilizadas no processo, levando, consequentemente, a uma maior probabilidade de condenação após a sua apresentação do que quando comparadas a um cenário no qual elas não tenham sido utilizadas. Percebe-se, pois, que tal tipo de prova recebe uma imagem impenetrável e intimidante devido ao rigor científico aplicado por um especialista que a interpreta. Dessa forma, apesar de ser circunstancial, o DNA forense ganha muita força e capacidade de influenciar pessoas leigas (leia-se aqui leigos em relação à produção probatória científica) quando da tomada de suas decisões.[32]

Interessante também ressaltar a dificuldade que cerca a apresentação de uma evidência produzida por um especialista a uma pessoa comum. Na seara das análises de DNA, por exemplo, temos que os jurados concebem a palavra "*match*" como indicadora de forte associação entre o suspeito e a evidência encontrada no local do crime. Por outro lado, os especialistas entendem o mesmo termo como uma associação mais fraca do que outros como "individualização" e "identificação"[33]

Isso denota que, além da problemática quanto à contaminação, o resultado fornecido por um especialista pode ainda ser mal interpretado a depender da forma como apresentado.

Pelo exposto, é mais certo que estejamos diante de um processo de deferência cognitiva por parte dos operadores do

Direito, que, diante da ignorância quanto aos métodos aplicados para a materialização da prova, preferem a ela prestar toda a credibilidade, considerando que foi produzida por um perito, técnico no assunto.

Nesse cenário, importa que a prova científica tenha valor em si e que essa qualidade possa ser efetivamente sopesada, não havendo espaço para que seja utilizada como argumento de autoridade, ou em outras palavras, como um instrumento retórico para o convencimento do julgador.[34] É preciso que a busca pela verdade possível no processo não se esconda por detrás de uma alusão à inquestionabilidade da prova de DNA.

3. OS LIMITES DA VERDADE NO PROCESSO

Sabemos que as provas são levadas ao processo para a formação da convicção do julgador, mas, não raro, elas são transformadas em instrumentos de uma insana busca pela verdade dos fatos. Ainda paira no entendimento de alguns que um julgamento justo é aquele no qual a decisão tenha se baseado na verdade e, por isso, pretendem reconstituir o passado através de pequenos fragmentos dele. O resultado, no entanto, será sempre comparável à tentativa de se juntar os pedaços de um espelho quebrado: é impossível possuirmos novamente uma imagem íntegra e sem distorções porque ora fragmentos serão perdidos e ora será impossível encaixá-los perfeitamente.

Dessa forma, o momento no qual a pretensão de evidência do DNA forense se entrecruza com a busca pela famigerada verdade real no processo pode acabar criando um ambiente propício para que questionamentos relevantes sejam olvidados em prol do alcance de uma efetividade processual calcada em provas irrefutáveis, o que, de certo, não se presta à persecução penal pelo Estado. Ou seja, durante o contraditório, momento de legitimação das provas, a pretensão de evidência seda os sentidos e a "certeza" é sobrelevada ao grau

máximo de importância, impedindo que questões relativas à confiabilidade do DNA forense sejam discutidas.

Considerando tudo o que foi dito até o presente momento, temos que a análise de DNA serve perfeitamente a essa sede de demonstração da verdade, haja vista a alta sensibilidade em termos de identificação, mas não podemos nos deixar inebriar com os seus resultados, que tampouco podem ser tidos como verdades absolutas.

Segundo afirma Susana Kappler,[35] as análises de DNA não podem ser tidas como prova plena porque não são infalíveis: elas resultam na inequívoca presença do sujeito no lugar do fato, mas somente por elas não se pode aferir a autoria do crime, o que, por certo, depende do sopesamento com outros elementos de prova. Não obstante a certeira visão, ousamos somente ajustá-la quanto a possibilidade de que o acusado nem mesmo tenha estado na cena do crime, como visto acima.

Nesse ponto, cumpre-nos realizar algumas breves observações acerca do conceito de verdade. Primeiro, precisamos pontuar que a realidade se coloca independentemente do homem, ao passo que a verdade pertence à ordem do discurso ou da representação. Assim, através da linguagem almejamos criar uma correspondência entre inteligência e realidade.[36] Ou seja, buscamos demonstrar a verdade de uma realidade passada por meio de um processo de cognição.

A obtenção da verdade pode variar desde a credulidade cega até o ceticismo. No que tange ao segundo termo, temos que o espírito humano não é capaz de alcançar, com certeza, qualquer verdade de ordem geral ou especulativa,[37] abrindo espaço para se "praticar a dúvida."[38] Partindo-se do ceticismo, o norte deve ser que qualquer hipótese pode estar errada.

Já numa visão pragmática, a verdade é essencialmente dependente dos resultados práticos para o homem.[39] Nesse contexto Nietzsche se destaca e afirma que a concepção de verda-

de absoluta é falsa e está vinculada a interesses, a vontade de poder.[40] Aqui podemos encaixar perfeitamente a busca pela verdade no processo penal.

Interessa-nos, nesta altura, destacar o falibilismo como uma doutrina filosófica que dita a impossibilidade de termos a certeza de qualquer forma de conhecimento. Aquele que se diz falibilista não incide nem no ceticismo radical, isto é, não afirma que nenhuma forma de conhecimento seja válida, e nem no relativismo radical, porque também não admite a validade de qualquer forma de conhecimento. Para ele, existem, de fato, formas de conhecimento mais válidas, legítimas e frutíferas que outras, mesmo que não tenhamos certeza delas.

O falibilismo trata da busca pela verdade em condições de incerteza. Nele se encontra a negação da possibilidade de demonstração absoluta da verdade, embora também não negue absolutamente a possibilidade da verdade.[41] É nesse contexto que deve ser enquadrada a prova de DNA, eis que possível a sua falha em determinar a culpabilidade de alguém.

Mesmo diante de tantas questões em torno da obtenção da verdade, causa-nos espécie a associação que ainda se faz do processo penal com a chamada busca da verdade material, ou real.

Lamenta-se que nosso Código de Processo Penal ainda possua a previsão do art. 156[42] que para muitos é a base de um (inexistente) princípio da verdade. Este dispositivo transforma o juiz em investigador e acusador, na medida em que ao invés de mantê-lo inerte e em posição processual de equidistância entre as partes, destoante da regra constitucional do *in dubio pro reo*, direciona o juiz à suprir a atividade probatória (supostamente) deficiente dos órgãos de investigação e acusação, determinando, de ofícios, diligências investigatórias e probatórias.

Para Geraldo Prado, os laços que a prova estabelece entre os fatos e o direito pautam a busca da verdade e legitimam o

processo penal conforme os paradigmas do Estado de Direito.[43] Vale advertir que partimos do referencial teórico do Garantismo Penal. Daí observamos o impacto das garantias processuais, como o contraditório, igualdade de armas, presunção de inocência etc., sobre a verdade processual, que será sempre probabilística da verdade factual,[44] uma verdade relativa, mínima. Em outras palavras, na perspectiva do garantismo, a verdade perseguida pelo processo encontra eco na verdade aproximação, e não na verdade correspondência.[45]

Desta forma, ao abraçarmos o garantismo como teoria do direito, renunciamos à verdade máxima, de cariz inquisitorial, cuja satisfação desta "vontade de verdade", na expressão de Nietzsche, muitas vezes não ocorrerá sem recorrer-se às intervenções corporais, e, para tanto, recorrer-se-ia a elas ainda que necessário fosse o emprego da força física. Por outro lado, a verdade mínima recomendada pela teoria do garantismo e pela democracia constitucional, que limita a vontade majoritária, pode prescindir do recurso à violência para a obtenção da verdade.

Portanto, a prova de DNA deve funcionar somente como mais uma dentre todas aquelas que podem firmar a convicção do julgador, devendo recair sobre todas elas uma valoração conjunta. Assim como um pedaço de espelho quebrado, a evidência de DNA é apenas uma pista circunstancial que remete a um evento passado.[46]

4. CONTRADITÓRIO, AMPLA DEFESA E A CADEIA DE CUSTÓDIA DA PROVA

Contraditório e ampla defesa são dois conceitos altamente relacionados, mas que não se confundem. Enquanto o primeiro pode ser determinado pela organização dialética do processo, possibilitando que as partes se manifestem sobre cada um dos atos processuais, traduzido no binômico ciência

e possibilidade de resistência, o segundo se revela através da autodefesa e da defesa técnica.[47]

A ampla defesa, de fato, se utiliza do procedimento contraditório para se efetivar. Como exemplo, temos que a defesa técnica sempre se manifesta por último.

Sendo a legitimação da prova resultado do contraditório durante o processo, a imprescindibilidade de que haja paridade de armas e conhecimento integral das fontes de prova obtidas durante a investigação é termo crucial para a formação de um conhecimento amplo e articulado para o concreto exercício do direito de defesa.[48]

Imaginemos, pois, hipótese na qual o DNA forense chegou a determinado resultado sem lastro na realidade do fato criminoso, isto é, após ter ocorrido algum evento de contaminação durante o processo de materialização da prova. Nesse caso, o contraditório legitimará a prova da mesma forma, mas sequer poderíamos utilizar tal termo porque estaríamos diante de uma interrupção no controle de racionalidade da evidência, o que, em verdade, é causa para a sua inadmissibilidade. Precisamos ter em mente que uma alteração pode enfraquecer ou destruir o valor probatório de uma evidência.[49]

Por certo, corremos o risco de legitimar uma prova calcada em inverdade quando não temos o total controle de sua materialização no campo extraprocessual. Ficamos sujeitos a transformar uma mentira em verdade porque entorpecidos com a beleza de uma aparente idoneidade, mas que pode estar veladamente maculada. Como tentamos expor, uma mentira perpetrada acaba virando verdade, e reveste o resultado de indiscutibilidade.

Portanto, é preciso que se mantenha um mecanismo de rastreamento da evidência para demonstrar a idoneidade da prova no processo, isto é, para demonstrar que não houve

qualquer interferência externa ou degradação do material genético antes, durante e depois da análise. A título de exemplo, como diz Geraldo Prado, sem esse rastreamento, a identificação do vínculo eventualmente existente entre uma prova aparentemente lícita e outra, anterior, ilícita, de que a primeira é derivada, dificilmente será revelado.[50]

Considerando-se o exposto, é notório que as investigações requeiram protocolos mais afetos às boas-práticas procedimentais e que previnam a contaminação de quaisquer ferramentas afetas ao manuseio das evidências pelos investigadores na cena do crime ou já no laboratório. A cadeia de custódia é ferramenta hábil para tanto.

Girlei Marinho define esse instrumento nos seguintes termos:

> A cadeia de custódia da prova pericial é constituída por uma série de atos interligados, sem deixar lacunas, visando a segurança e a confiabilidade do processo em que os vestígios estão submetidos. Todos os atos podem ser registrados com os nomes dos profissionais que preservaram o local e os que manusearam os vestígios, desde sua fixação, busca, coleta, transporte, envio, recebimento pelos órgãos de Perícia Oficial e armazenamento. Toda história pode ser catalogada situando todo processo de produção no tempo e no espaço.[51]

Trata-se de uma garantia da plena eficácia da fonte de evidência. Isso porque a validade do meio de prova depende de a sua fonte ter permanecido inalterada desde a comissão dos fatos até o julgamento, incluindo, por óbvio, a análise laboratorial.[52] Assim, como pressuposto epistemológico de fiabilidade da prova, a cadeia de custódia assegura a autenticidade da evidência e garante que a prova examinada seja a mesma

relacionada com o fato criminoso, trazendo, nesses termos, o conceito de "mesmidade" da prova.[53]

Vale ressaltar que, com a possibilidade de situar o procedimento de materialização da prova no tempo e no espaço, eventuais erros nesse percurso, incluindo contaminações, podem ter sua origem perquirida na documentação que consubstancia a cadeia de custódia, desde que, é claro, todo o procedimento legal seja posto em prática, zelosamente.

No Brasil, a cadeia de custódia da prova tomou seu devido lugar no Código de Processo Penal somente após o advento da Lei nº 13.964/2019, que incluiu os artigos 158-A a 158-F para regulamentar a matéria, definindo seus contornos e etapas, que vão desde a preservação da cena do crime até o descarte da evidência. Antes disso, tratava-se de assuntou sobremaneira afeto às discussões doutrinárias, salvo pela existência da Resolução nº 82/2014 da Secretaria Nacional de Segurança Pública.

Interessante aspecto trazido por esta resolução é o fato dela dividir a cadeia de custódia em duas etapas, uma externa e outra interna, sendo a chegada do vestígio ao órgão pericial o limiar entre ambas. Dessa informação podemos extrair que os procedimentos realizados internamente pela perícia, notadamente a análise pericial propriamente dita, também devem ser suscetíveis de controle.

Sob esse aspecto, é importante frisar que, para que haja a minimização do risco de contaminação e a concomitante manutenção da integridade do material a ser analisado – principalmente porque estamos falando de material biológico, que pode ser degradado a depender das vicissitudes com as quais tenha contato –, verdadeiras medidas técnico-científicas devem ser observadas para assegurar a preservação das amostras e posterior confiabilidade da prova.

Um exemplo dessas medidas é o Procedimento Operacional Padrão (POP) de Perícia Criminal elaborado pela Secreta-

ria Nacional de Segurança Pública (Ministério da Justiça) em 2013.[54] Esse documento dita quais devem ser as estratégias adotadas para a coleta de material biológico de pessoas vivas e em locais de crime, bem como aquelas que devem ser utilizados para a coleta do vestígio biológico e o seu envio para a unidade de análise. Ele dita também as regras de recebimento do material, armazenamento e análise do DNA. Enfim, é um documento que deve ser observado junto à cadeia de custódia, seja na sua fase externa ou interna.

Pelo exposto, percebemos que a cadeia de custódia, de maneira simples, funciona como mecanismo de redução da perpetração de inverdades no processo penal porque se trata de autêntico controle epistêmico da prova, permitindo como fim último um contraditório legítimo, cujo aspecto dialógico se perfaça sobre prova hígida desde a sua fonte vestigial.

5. DIGNIDADE DA PESSOA HUMANA E *NEMO TENETUR* SE DETEGERE

Outro aspecto de suma relevância compreendido pela prova de DNA é a polêmica quanto à contribuição do investigado para a sua formação.

Como já mencionado, o DNA forense exige que se obtenha amostra biológica do investigado para dela se extrair o perfil genético que será comparado com o perfil encontrado na evidência do local do crime. É preciso, portanto, haver uma intervenção corporal na pessoa sob investigação, isto é, uma a ingerência sobre o corpo vivo de uma pessoa de modo a possibilitar afetação a seus direitos fundamentais,[55] maculando sua integridade física em nome da *persecutio criminis*.

Sob outro prisma, temos que a dignidade humana faz da pessoa fundamento e fim da sociedade e do Estado, conferindo unidade de sentido e de concordância prática ao sistema de direitos fundamentais.[56] Em nosso ordenamento é

tratada como verdadeiro fundamento da República (art. 1º, CRFB/88), mostrando-se como importante guia do processo penal, haja vista ser a raiz das garantias constitucionais que devem inspirar a atividade jurisdicional do Estado, notadamente no que tange às dimensões relativas à individualidade, à liberdade, à autonomia frente ao poder público e à igualdade de tratamento normativo.[57]

Determinar o conteúdo desse conceito, porém, nunca se mostrou tarefa das mais fáceis. Com o intuito de trazer maior clareza ao tema, Canotilho[58] nos forneceu a teoria dos cinco componentes, a partir dos quais seria possível definir positivamente a dignidade humana. Resumidamente, os componentes da teoria são: a) a integridade física e espiritual do homem (aspectos irrenunciáveis de sua individualidade); b) o livre desenvolvimento de sua personalidade; c) as condições mínimas existenciais (proporcionadas por um atuar estatal); d) a consagração da autonomia individual (pela limitação dos poderes públicos); e, por fim, e) a igualdade de tratamento normativo.

Outra definição sobre a dignidade da pessoa humana advém da fórmula-objeto de Dürig, que, partindo de uma perspectiva negativa do conceito, aduz que a dignidade é violada sempre que o homem deixar de ser visto como pessoa para ocupar uma posição reificada. Segundo Kloepfer, teremos a violação da dignidade da pessoa humana quando essa for tratada como mero objeto da ação estatal.[59]

Ao que aqui importa destacar, temos que a integridade física e corporal da pessoa humana é o primeiro dos cinco componentes que moldam a sua dignidade e, ao que entendemos, somente a esta pessoa cabe o julgamento quanto a tal violação, se relevante ou não.[60] Já com espeque na segunda definição, a pessoa humana não pode ser degradada a ponto de se tornar um mero instrumento contra si própria e em favor da persecução, ou melhor, a dignidade humana impede que o Estado-

-juiz, no afã de seguir com à persecução penal, se olvide da condição de pessoa com a qual se reveste todo ser humano, impossibilitando, por conseguinte, que o processo penal lance mão de certos meios de prova que afrontem tal qualidade.

Lado outro, o princípio *nemo tenetur se detegere* se apresenta como uma garantia do acusado, permitindo que ele não seja obrigado a produzir provas contra si mesmo. Não é, contudo, a compreensão do princípio que implica em dificuldades, mas sim o entendimento do seu alcance.[61] Essa adversidade aumenta à medida que nos aproximamos da zona fronteiriça entre a condição de sujeito da investigação que sustenta a pessoa e a *persecutio criminis* estatal no que tange à produção probatória. Entendemos que estando amparado pela presunção de inocência e pelo direito de defesa, o investigado pode se recusar com qualquer colaboração não voluntária relativamente à investigação ou instrução.[62]

Dessa forma, diante de possível colisão de interesses, deve o julgador optar por aquele que melhor efetive a dignidade da pessoa humana, como dito, fim do próprio Estado. Assim, toda a atividade estatal voltada à persecução penal deve estar lastreada na realização e respeito a tal condição, seja na investigação, no exercício da ação penal ou no curso do processo. Não pode o Estado, em nome da necessidade de buscar a satisfação de um fim coletivo, sacrificar interesses individuais, que possuem esteio em direitos fundamentais.[63]

As intervenções corporais não consentidas se mostram como limitações aos direitos fundamentais da pessoa investigada, podendo alcançar, inclusive, violação à dignidade humana. Afirmamos, nesse ponto, que não há qualquer norma na Constituição da República que autorize a restrição do direito à inviolabilidade e à integridade corporal, e tampouco dos direitos de defesa, da presunção de inocência ou da garantia contra a autoincriminação.[64] Pelo contrário, apenas

encontramos dispositivos que vedam ofensa à integridade física e psíquica (art. 5º, caput e inc. X), havendo ausência de previsão quanto a obrigatoriedade de fornecer amostra biológica (art. 5º, II) e a proibição de utilização de provas obtidas ilicitamente (art. 5º, LVI), que, por conseguinte, servem de supedâneo para a recusa do investigado em colaborar, e que não pode ser vencida por coação estatal.

Vale ressaltar, ainda, que o investigado não pode ser levado, seja por fraude ou coação, a contribuir com a investigação, isto é, não pode ser dirigido à produção de provas contra sua defesa. Ele, de fato, não se encontra em posição afeta por um dever de colaboração, tampouco por um dever de verdade.[65]

Com efeito, entendemos que a não contribuição do investigado para a realização das análises de DNA tem plena fundamentação legal, e se escora no amplo espectro que compõe sua defesa, incluindo a não produção de prova contra si mesmo. Nesse caso, serão outras as provas que devem corroborar para se chegar à verdade possível no processo, não se incluindo aquela capaz de dizer a identidade genética do vestígio.

Sem prejuízo, comparações de perfis genéticos poderão ocorrer a partir de amostras desprendidas do corpo desde que não provenham de métodos enganosos proscritos pela doutrina[66] e pela jurisprudência[67]. De modo geral, não se trata de inviabilizar a investigação, pois é possível a produção de prova sem exigir a colaboração obrigatória do suspeito ou acusado.[68]

Ademais, vale lembrar que o STF tem se mantido firme na efetivação do *nemo tenetur se detegere* como se extrai de inúmeros julgados. No HC 83.096-0 afirmou o direito ao silencio destacando que o réu não está obrigado e não pode ser fisicamente compelido a fornecer padrões vocais para confronto com escutas telefônicas. No HC 93.916 decidiu que a recusa em participar de exame de dosagem alcóolica não pode gerar conclusões desfavoráveis ao suspeito ou acusado. Nesta linha

aponta (STF, HC 77.135) ainda que o réu não é obrigado a fornecer padrões grafotécnicos.

CONCLUSÃO

Procuramos traçar ao longo desse texto os principais aspectos relativos à análise de DNA como elemento probatório no processo penal. Por conta do potencial individualizador da molécula e do alto grau de sensibilidade na identificação de pessoas, o DNA forense se tornou uma ferramenta bastante utilizada para tal finalidade.

Porém, como vimos, a materialização da prova de DNA a partir da evidência encontrada na cena do crime pode ter sua confiabilidade esfacelada por interferências externas que rompam a idoneidade do material sob análise.

A partir de tal contestação, destacamos a importância da cadeia de custódia da prova para permitir a admissão e fiabilidade do material probatório.

Ademais, apresentamos a dignidade humana e o *nemo tenetur se detegere* como princípios que limitam as intervenções corporais não consentidas, através das quais se pretenda colher material genético do corpo do suspeito, investigado, acusado e mesmo do condenado.

NOTAS

1. CRISPR é uma ferramenta de engenharia genética que tem se mostrado bastante promissora na edição de DNA pela precisão molecular em adicionar ou retirar informações, permitindo, assim, que um organismo expresse um gene exógeno ou deixe de expressar um gene que seja deletério (silenciamento gênico). As possíveis aplicações circundam as áreas de terapia gênica humana, destruição de patógenos, agropecuária etc. Para mais informações ver: Doudna, J.; Charpentier, E. (2014). Genome editing. The new frontier of genome engineering with CRISPR-Cas9. *Science*, v. 346 (6213), pp. 1.077-1.086. DOI: 10.1126/science.1258096.

2. Decanine, D. (2016). O papel de marcadores moleculares da genética forense. *Revista Brasileira de Criminalística*, v. 5(2), pp. 18-27. DOI: https://doi.org/10.15260/rbc.v5i2.123.

3. O primeiro caso criminal a utilizar análise de DNA para sua resolução ocorreu em 1986, no Reino Unido. Jobling, M.; Gill, P. (2004). Encoded evidence: DNA in forensic analysis. *Nature Reviews Genetics*, v. 5 (10), pp. 739–751. DOI: doi:10.1038/nrg1455.

4. Vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal (art. 158-A, § 3º do CPP).

5. Navarro, C. (2015). La cadena de custodia de las muestras biológicas. In C. Navarro, *La cadena de custodia en el processo penal*. Edisofer s.l., p. 108.

6. Smith, P. (2016). When DNA Implicates the Innocent. *Scientific American*, v. 314(6), pp. 11–12. DOI: 10.1038/scientificamericano616-11.

7. Jobling & Gill, (Op cit.)

8. Mukherjee, S. (2016). *O gene: uma história íntima*. Companhia das Letras, p. 197.

9. O ácido nucleico foi descoberto por Friedrich Miescher em 1869, contudo, a molécula de DNA (ácido desoxirribonucleico) não deve ser confundida com a de RNA (ácido ribonucleico). Ambas compõem o grupo dos ácidos nucleicos, porém possuem estrutura e funções diferentes. Em suma: enquanto o DNA é uma molécula mais estável, localizada no núcleo e responsável por armazenar a informação genética, o RNA tem um caráter mais transitório, formado a partir da transcrição da informação constante no DNA e cuja função principal é levar tal mensagem do núcleo para o citosol (região extranuclear), ambiente no qual será traduzido pelos ribossomos e a informação inicial resultará, então, na produção de uma proteína. Ademais, além de outras divergências estruturais, o RNA é eminentemente uma molécula de fita simples enquanto o DNA se apresenta numa estrutura de dupla fita.

10. Mukherjee, S., op. cit., p. 166.

11. Watson, J. et al. (2015). *Biologia Molecular do Gene* (7. ed.). Artmed, p. 21.

12. Este pode parecer um questionamento inocente, mas vale lembrar que, apesar de os cromossomos serem as estruturas já sabidamente relacionadas com a hereditariedade, a única certeza que se tinha à época era a de que sua composição continha tanto DNA quanto proteínas, o que suscitava a possibilidade do ácido nucleico funcionar apenas como uma estrutura de suporte para os verdadeiros genes proteicos.

13. Como não possuímos espaço para discuti-los aqui, vale uma breve digressão, com a imprecisão inerente a uma alusão simplista: a) Griffith realizou experimentos que demonstraram que bactérias não patogênicas poderiam ser geneticamente transformadas a partir de bactérias patogênicas previamente inativadas

pelo calor (1928); b) Avery conseguiu demonstrar que a substância capaz de transformar as bactérias no experimento anterior era o DNA (1944); c) Hershey e Chase, a partir de experimentos com bacteriófagos (tipo de vírus) marcados radioativamente, conseguiram demonstrar que é o DNA o componente viral introduzido na célula e que vai possibilitar a multiplicação da partícula (1952); d) Chargaff demonstrou que o DNA de todo e qualquer ser vivo possuía as quatro bases nitrogenadas e que elas se apresentavam sempre numa proporção determinada (A/T e C/G) (1949); e) Franklyn e Wilkins realizam estudos com difração de raio X que acabaram demonstrando que o DNA é formado por uma estrutura helicoidal e composta por mais de uma cadeia (1953). Informações retiradas de: Watson, J. et al., op. cit., pp. 5-41.

14. Watson, J., op. cit., p. 81.

15. Francis, R. (2015). E*pigenética: como a ciência está revolucionando o que sabemos sobre hereditariedade*. Zahar, p. 31.

16. A replicação ocorre na fase correspondente à duplicação dos cromossomos dentro do ciclo celular e possibilita que a novas células recebam, cada qual, o mesmo número de cromossomos que a célula-mãe.

17. Louten, J. (2016). *Essential human virology.* Elsevier/Academic Press, p. 37.

18. Mullis, K. et al. (1986). Specific enzymatic amplification of DNA in vitro: the polymerase chain reaction. *Cold Spring Harbour Symposia on Quantitative Biology*, v. 51(1), pp. 263-273. DOI:10.1101/sqb.1986.051.01.032.

19. Genoma é o termo que se refere ao conjunto de todas as informações hereditárias de um organismo, incluindo os genes, regiões intergênicas e DNA mitocondrial.

20. Watson, J., op. cit., pp. 205-7, 315.

21. Decanine, D., op. cit..

22. Watson, J., op. cit., p. 160.

23. Decanine, D., op. cit..

24. Fonneløp, A. et al. (2016). Contamination during criminal investigation: detecting police contamination and secondary DNA transfer from evidence bags. *Forensic Science Int.*: Genetics, v. 23, pp. 121–129. DOI: 10.1016/j.fsigen.2016.04.003.

25. Smith, P., op. cit..

26. Gill, P. (2016). *Misleading DNA Evidence: Reasons for Miscarriages of Justice.* Elsevier.

27. Para se evitar associações falsas que levem a uma lógica dedutiva falsa, é necessário que os cientistas considerem ativamente todos os métodos possíveis de transferência: antes do evento criminoso - transferência inocente ou contaminação por DNA no ambiente; após o evento criminoso - contaminação mediada pelo investigador.

28. Van Oorschot, R. et al. (2019). DNA transfer in forensic science: a review. *Forensic Science International: Genetics*, v. 38, pp. 140-166. DOI: 10.1016/j.fsigen.2018.10.014.

29. Navarro, C., op. cit., p.108.

30. Tonet, I. (2013). Método científico: uma abordagem ontológica. Instituto Lukács, p. 75.

31. Lopes Jr, A. (2018). *Direito processual penal* (15ª ed). Saraiva, p. 439.

32. Lynch, M. (2003). God's signature: DNA profiling, the new gold standard in forensic science. Endeavour v. 27(2), pp. 93-97, 2003. DOI: 10.1016/s0160-9327(03)00068-1; Briody, M. (2003). The effects of DNA evidence on homicide cases in court. *Aust. N. Z. J. Criminol*, v. 37(2), pp. 231-252. DOI: https://doi.org/10.1375/acri.37.2.231; Curley, L. et al. (2020). An inconvenient truth: More rigorous and ecologically valid research is needed to properly understand cognitive bias in forensic decisions. Forensic Sci. Int.: Synergy, v. 2, pp. 107-109. DOI: 10.1016/j.fsisyn.2020.01.004.

33. Eldridge, H. (2019). Juror comprehension of forensic expert testimony: a literature review and gap analysis, *Forensic Sci. Int.: Synergy,* v.1, pp. 24-34. DOI: https://doi.org/10.1016/j.fsisyn.2019.03.001.

34. Azevedo, Y.; Vasconcelos, C. R. (2017). *Ensaios sobre a cadeia de custódia no processo penal brasileiro.* Empório do Direito, p. 76.

35. Kappler, S. Á. de N. (2008). *La prueba de DNA en el proceso penal*. Editorial Comares, p. 60.

36. Clément, E., et al. (1999). *Dicionário Prático de Filosofia*. Edição Original: Paris, Hatier, 1994. 2ª edição portuguesa: Terramar, p. 389.

37. Alves, M. dos S. (1989). *História da Filosofia*. Porto Editora, p. 44.

38. Clément, E. et al., op. cit., p. 56.

39. Alves, M. dos S., op. cit., p. 141.

40. Giacoia Junior, O. (2002). *Nietzsche & Para Além de Bem e Mal*. Jorge Zahar Editor, p. 18.

41. Schorn, R. (2008). *O Problema da Verdade do Conhecimento no Racionalismo Crítico*. Tese de Doutorado apresentada no Programa de Pós-Graduação em Filosofia da Faculdade de Filosofia e Ciências Humanas da Pontifícia Universidade Católica do Rio Grande do Sul, p. 254.

42. Acreditamos que esse artigo foi tacitamente revogado pelo advento da Lei nº 13.964/2019, especificamente por conta da previsão elencada no art. 3º-A do CPP: O processo penal terá estrutura acusatória, vedadas a iniciativa do juiz na fase de investigação e a substituição da atuação probatória do órgão de acusação. O citado dispositivo se encontra suspenso por força de medida cautelar em ADI exarada pelo STF em janeiro de 2020.

43. Prado, G. (2014). *Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos* (1ª ed). Marcial Pons.

44. Ferrajoli, L. Garantias. In *Revista do Ministério Público*. Ano 22º, janeiro-março, 200, pp. 15-16.

45. Ferrajoli, L. (2002). *Direito e Razão*. Tradução: P. Zomer, F. Hassan Choukr, J. Tavares e L. Flavio Gomes. Revista dos Tribunais, pp. 38-42, 434 e 440.

46. Smith, P., op. cit..

47. Nicolitt, A. (2020). Manual de Processo Penal (10. ed.). D'Plácido, p. 183.

48. Prado, G. (2014). *Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos* (1ª ed.). Marcial Pons, p. 59.

49. Osterburg, J., et al. (1992). *Criminal investigation: a method for reconstructing the past.* Anderson Publish, p. 180 apud Prado, G. (2014). *Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos* (1ª ed.). Marcial Pons, p. 81.

50. Prado, G., op. cit., p. 79.

51. Marinho, G. V. (2014). Cadeia de custódia da prova pericial: uma exigência no mundo contemporâneo. In Revista Segurança, Justiça e Cidadania/Ministério da Justiça (ano 6, n. 9). Secretaria Nacional de Segurança Pública (SENASP), p. 11.

52. Tabuenca, P. L. (2015). La cadena de custodia en el proceso penal español: revisión normativa. In Navarro, C. *La cadena de custodia en el processo penal.* Edisofer s.l., p. 21.

53. Prado, G. (set. 2014). Ainda sobre a "quebra da cadeia de custódia das provas". Boletim IBCCrim, nº 262, pp. 16-17.

54. Brasil. (2013). Secretaria Nacional de Segurança Pública. *Procedimento operacional padrão: perícia criminal.* Ministério da Justiça. https://bit.ly/2B1PwfV.

55. Nicolitt, A.; Wehrs, C. (2015). *Intervenções corporais no processo penal e a nova identificação criminal* (lei 12.654/2012) (2. ed.). Revista dos Tribunais, p. 29.

56. Miranda, J. (2000). *Manual de Direito Constitucional* (3. ed.). Coimbra (t. IV), pp. 180-181.

57. Nicolitt, A., op. cit., p. 914.

58. Canotilho, J. J. G. (2003). *Direito Constitucional e Teoria da Constituição* (7. ed.). Almedina, pp. 248-249.

59. Kloepfer, M. (2009). *Vida e Dignidade da Pessoa Humana*. Trad. R. Dostal Zanini. In Sarlet, I. W. (organizador). *Dimensões da Dignidade*. Livraria do Advogado, p. 164.

60. Nicolitt, A. & Wehrs, op. cit., p. 154.

61. Andrade, M. da C. (1992). *Sobre as proibições de prova em processo penal*. Coimbra Ed., p. 127.

62. Nicolitt, A., op. cit., p. 222.

63. Nicolitt, A., op. cit., pp. 145 e 171.

64. Nicolitt &Wehrs, op. cit., p. 143.

65. Andrade, M. da C. (1992). *Sobre as proibições de prova em processo penal*. Coimbra, p. 121.

66. Andrade, M. da C. (1992). *Sobre as proibições de prova em processo penal.* Coimbra, pp. 233-234.

67. STF, HC 80.949.

68. STF, HC 77.135.

BIBLIOGRAFIA

Alves, M. dos S. (1989). *História da Filosofia*. Porto Editora.

Andrade, M. da C. (1992). *Sobre as proibições de prova em processo penal*. Coimbra Ed.

Azevedo, Y.; & Vasconcelos, C. R. (2017). *Ensaios sobre a cadeia de custódia no processo penal brasileiro*. Empório do Direito.

Brasil. (2013). Secretaria Nacional de Segurança Pública. *Procedimento operacional padrão: perícia criminal.* Ministério da Justiça. https://bit.ly/2B1PwfV.

Briody, M. (2003). The effects of DNA evidence on homicide cases in court. *Aust. N. Z. J. Criminol*, v. 37(2), pp. 231-252. DOI: https://doi.org/10.1375/acri.37.2.231.

Canotilho, J. J. G. (2003). *Direito Constitucional e Teoria da Constituição* (7. ed.). Almedina.

Clément, E., et al. (1999). Dicionário Prático de Filosofia. Edição Original: Paris, Hatier, 1994. 2ª edição portuguesa: Terramar, Janeiro, 1999.

Curley, L., et al. (2020). An inconvenient truth: More rigorous and ecologically valid research is needed to properly understand cognitive bias in forensic decisions. *Forensic Sci. Int.: Synergy*, v. 2, pp. 107-109. https://www.sciencedirect.com/science/article/pii/S2589871X20300048?via%3Dihub.

Decanine, D. (2016). O papel de marcadores moleculares da genética forense. *Revista Brasileira de Criminalística*, v. 5(2). https://doi.org/10.15260/rbc.v5i2.123.

Doudna, J.; Charpentier, E. (2014). Genome editing. The new frontier of genome engineering with CRISPR-Cas9. Science, v. 346 (6213), pp. 1.077-1.086. https://science.sciencemag.org/content/346/6213/1258096

Eldridge, H. (2019). Juror comprehension of forensic expert testimony: a literature review and gap analysis, *Forensic Sci. Int.: Synergy*, v.1, pp. 24-34. DOI: https://doi.org/10.1016/j.fsisyn.2019.03.001.

Ferrajoli, L. *Garantias*. In Revista do Ministério Público. Ano 22º, Janeiro-março, 200.

Ferrajoli, L. (2002). *Direito e Razão*. Tradução: P. Zomer, F. Hassan Choukr, J. Tavares e L. Flavio Gomes. Revista dos Tribunais.

Fonneløp, A. et al. (2016). Contamination during criminal investigation: detecting police contamination and secondary DNA transfer from evidence bags. *Forensic*

Science Int.: Genetics, v. 23, pp. 121–129. https://www.fsigenetics.com/article/S1872-4973(16)30059-X/fulltext

Francis, R. (2015). *Epigenética: como a ciência está revolucionando o que sabemos sobre hereditariedade.* Zahar.

Giacoia Junior, O. (2002). *Nietzsche & Para Além de Bem e Mal*. Jorge Zahar Editor.

Gill, P. (2016). Misleading DNA Evidence: Reasons for Miscarriages of Justice. Elsevier.

Jobling, M.; Gill, P. (2004). Encoded evidence: DNA in forensic analysis. *Nature Reviews Genetics*, v. 5 (10), pp. 739–751. https://www.nature.com/articles/nrg1455

Kappler, S. Á. de N. (2008). *La prueba de DNA en el proceso penal*. Editorial Comares.

Kloepfer, M. (2009). *Vida e Dignidade da Pessoa Humana*. Trad. R. Dostal Zanini. In Sarlet, I. W. (organizador). *Dimensões da Dignidade.* Livraria do Advogado.

Louten, J. (2016). *Essential human virology***.** Elsevier/Academic Press.

Lopes Jr, A. (2018). *Direito processual penal* (15ª ed.). Saraiva Educação.

Lynch, M. (2003). God's signature: DNA profiling, the new gold standard in forensic science. *Endeavour* v. 27(2), pp. 93-97. https://www.sciencedirect.com/science/article/abs/pii/S0160932703000681?via%3Dihub

Marinho, G. V. (2014). Cadeia de custódia da prova pericial: uma exigência no mundo contemporâneo. In *Revista Segurança, Justiça e Cidadania* /Ministério da Justiça (ano 6, n. 9). Brasília: Secretaria Nacional de Segurança Pública (SENASP).

Miranda, J. (200). *Manual de Direito Constitucional* (3. ed.). Coimbra (t. IV).

Mukherjee, S. (2016). *O gene: uma história íntima*. Companhia das Letras.

Mullis, K. et al. (1986). Specific enzymatic amplification of DNA in vitro: the polymerase chain reaction. *Cold Spring Harbour Symposia on Quantitative Biology,* v. 51(1), pp. 263-273. http://symposium.cshlp.org/content/51/263

Navarro, C. (2015). La cadena de custodia de las muestras biológicas. In Navarro, C. *La cadena de custodia en el processo penal***.** Edisofer s.l.

Nicolitt, A.; & Wehrs, C. (2015). *Intervenções corporais no processo penal e a nova identificação criminal* (lei 12.654/2012) (2. ed.). Revista dos Tribunais.

Nicolitt, A. (2020). *Manual de Processo Penal* (10. ed.). D'Plácido.

Prado, G. (2014). *Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos* (1ª ed). Marcial Pons.

Prado, G. (2014). Ainda sobre a "quebra da cadeia de custódia das provas". *Boletim IBCCrim*, nº 262, setembro de 2014.

Schorn, R. (2008). O Problema da Verdade do Conhecimento no Racionalismo Crítico. Tese de Doutorado apresentada no Programa de Pós-Graduação em Filosofia da Faculdade de Filosofia e Ciências Humanas da Pontifícia Universidade Católica do Rio Grande do Sul. Porto Alegre: 2008.

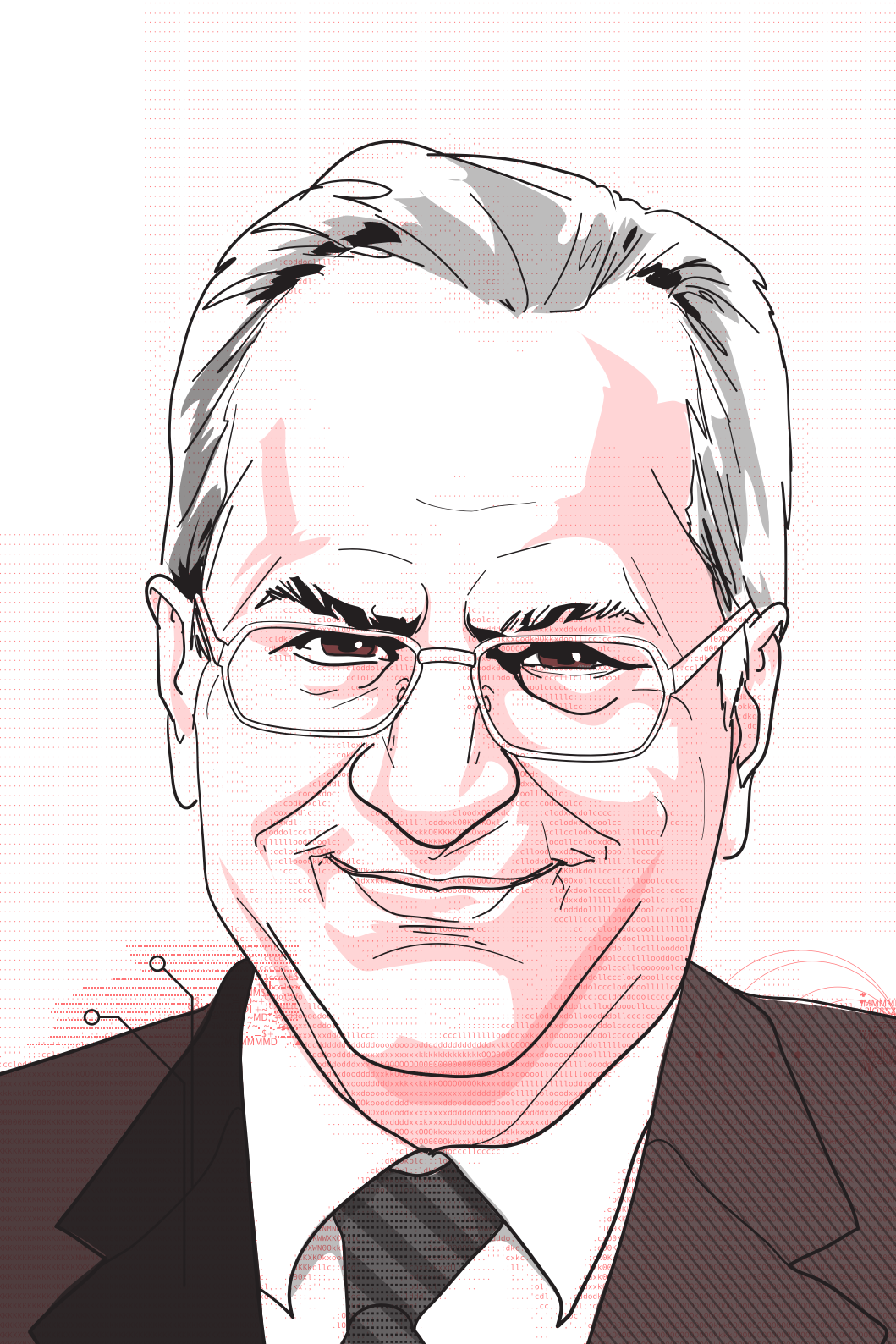
Smith, P. (2016). When DNA Implicates the Innocent. *Scientific American*, v. 314(6), pp. 11–12. https://www.scientificamerican.com/article/when-dna-implicates-the--innocent/

Tabuenca, P. L. (2015). La cadena de custodia en el proceso penal español: revisión normativa. In Navarro, C. *La cadena de custodia en el proceso penal.* Edisofer s.l.

Tonet, I. (2013). *Método científico: uma abordagem ontológica*. Instituto Lukács.

Van Oorschot, R. et al. (2019). DNA transfer in forensic science: a review. *Forensic Science International*: Genetics, v. 38, pp. 140-166. https://www.fsigenetics.com/article/S1872-4973(18)30395-8/fulltext

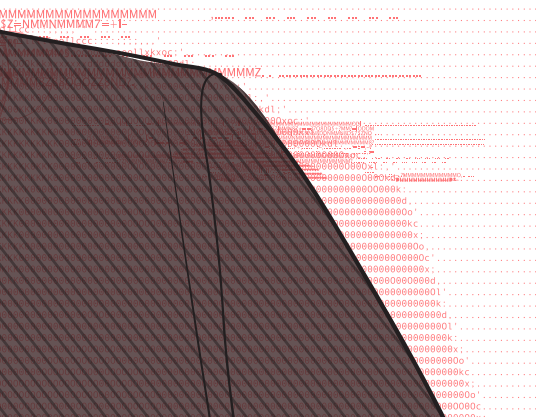
Watson, J. et al. (2015). *Biologia Molecular do Gene* (7. ed.).Artmed.



11.

UTILIZAÇÃO DE DADOS DE DNA NA JUSTIÇA CRIMINAL

Antônio Magalhães Gomes Filho



Queria cumprimentar e agradecer ao Dennys e à Marta, pelo convite para participar desse debate e dizer da minha satisfação de ter aqui ouvido às exposições tão importantes e tão argutas do André Nicolit, da Norma Bonaccorso e da Dora Cavalcanti, as duas últimas minhas alunas na graduação, e dizer que esse efetivamente é um tema que suscita muitas dúvidas, muitas discussões que estão longe de ser resolvidas. Eu me lembrava que a Dora mencionou um caso de DNA há 20 anos... Eu acho que há mais de 20 anos eu participei de um debate na FMU, em que havia um professor norte-americano, e um professor brasileiro. Esse professor brasileiro afirmou a certa altura que a prova de DNA levava a resultados 100% corretos, ao que o professor norte-americano fez uma intervenção dizendo que, mesmo nos Estados Unidos, naquela época eles só acreditavam que pudesse levar a 99% de acerto. O nosso professor brasileiro respondeu: "Bom, 100% quando a prova é bem feita".

Então, nós vemos o problema que existe em relação à prova científica; ela traz ao juiz e ao processo informações que estão além do conhecimento geral. O juiz não teria acesso a essas informações de outra forma. Elas são, evidentemente, úteis, mas, exatamente porque existe essa ideia de que podem ser provas infalíveis, absolutas e definitivas é que temos que tratá-las com algum cuidado. E o teste DNA é o exemplo mais evidente da utilização de provas com essa característica no processo. Tanto do Processo Civil, a Norma lembrou muito bem a questão da investigação de paternidade, como no Processo Penal, em que em inúmeros casos os testes de DNA podem ser utilizados tanto para fazer prova do crime, prova para condenação, como também para fazer a prova que afasta a culpabilidade do réu de uma forma clara e definitiva. Por isso, é importante que essas várias cautelas sejam tomadas no âmbito do processo. Tanto com

/ EM UMA VISÃO DEMOCRÁTICA DO PROCESSO PENAL NÃO PODEMOS ACEITAR ESSA OBTENÇÃO COMPULSÓRIA DO MATERIAL GENÉTICO /

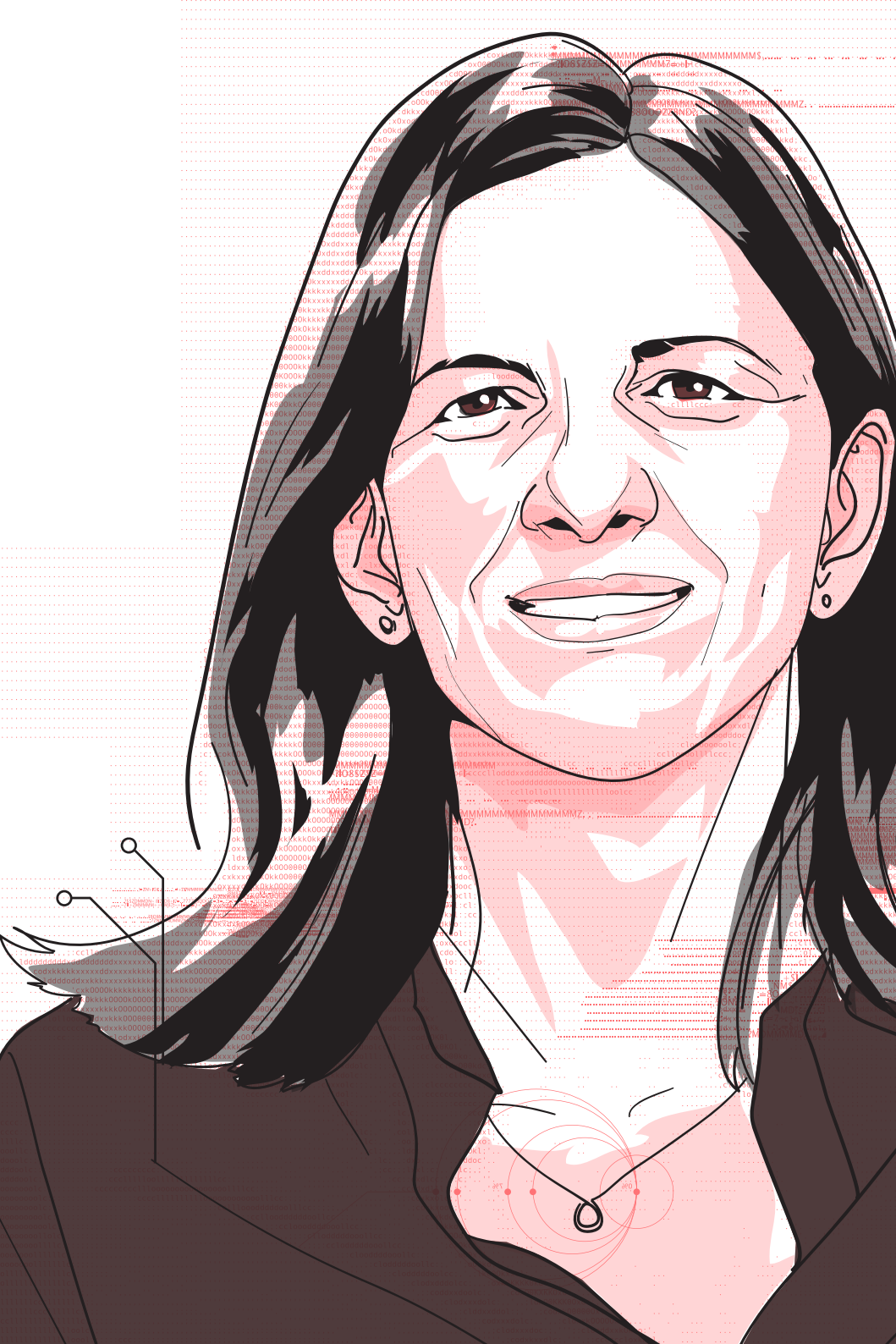
relação ao juiz, como com relação à possibilidade que tem as partes de discutir essas provas.

Há algum tempo, até 2008, nós não tínhamos a figura do assistente técnico no processo penal. Então, muitas vezes a afirmação do perito era uma afirmação definitiva. Hoje, em benefício do contraditório, existe a possibilidade dos assistentes técnicos que irão apontar ao juiz e às partes as deficiências e as insuficiências em relação a qualquer uma dessas provas. Assim, nós evoluímos também no nosso direito, de alguma forma, para poder aceitar com maior tranquilidade a prova do DNA.

Um ponto que foi aqui levantado e que também me parece muito importante é o da possível obrigatoriedade para o acusado, para o suspeito, e para o investigado de fornecer material para o exame de DNA, um material biológico, porque uma das características do DNA, a Norma me corrija se eu estiver errado, é que ele está presente em todos os tecidos humanos. Então, é possível identificar o DNA tanto no sangue, como na saliva, como numa célula, na pele etc. Então, por isso, sempre que houver a necessidade de se fazer a prova de DNA, é necessário (ou seria necessário) saber se esse material está disponível. Muitas vezes, o material é encontrado nas roupas, no local do crime, no próprio corpo da vítima, então nesse caso não teríamos esse problema; mas há situações em que surge a necessidade de que o próprio suspeito forneça esse material. Nesse caso, trata-se de uma situação praticamente insolúvel ao meu ver, que só pode ser equacionada de acordo com uma orientação ideológica do processo penal, uma situação em que o acusado seria constrangido a fornecer material biológico e, inclusive, contra a sua vontade. Daí a caracterização dessa situação como uma inconstitucionalidade, na medida em que a Constituição assegura não só o direito ao silêncio, como direito a permanecer calado, mas também o

direito à presunção de inocência, que inclui a necessidade de que a acusação traga as provas da culpabilidade, e não que o acusado traga as provas da sua inocência.

Nesse caso, em uma visão democrática do processo penal, uma visão que respeite os direitos individuais, não podemos aceitar essa obtenção compulsória do material genético. Ao contrário, se nós temos uma orientação autoritária do processo penal, como bem lembrou o professor André, uma visão que, infelizmente, é a visão que hoje prevalece embora, nós tenhamos, como ele lembrou, toda uma jurisprudência do Supremo Tribunal Federal no sentido de que o acusado não pode ser constrangido a fornecer provas contra si mesmo. Nós sabemos que isso, na prática, nem sempre é observado e nem sempre também a própria opinião pública comunga desse entendimento. Então essas são as minhas observações corroborando aqui as brilhantes exposições feitas anteriormente.



12.

UTILIZAÇÃO DE DADOS DE DNA NA JUSTIÇA CRIMINAL

Norma Sueli Bonaccorso

O DNA foi meu motor dentro da perícia. Um dos motores. O primeiro foi a toxicologia. Fiquei dez anos trabalhando com drogas, saí das drogas e fui para o DNA. No DNA, nós montamos o laboratório da Polícia Científica de São Paulo, que hoje se tornou o maior laboratório da América Latina voltado ao crime. A tarefa é muito difícil. Em contraste, o processo de identificação do DNA voltado à elucidação de paternidade, por exemplo, trabalha com matéria viva, sangue vivo. Agora, trabalhar com ossos, com restos mortais, vestígios de locais de crime nem sempre bem preservados é um desafio tecnológico. E nós conseguimos fazer isso, a partir de 1998. A SENASP – Secretaria Nacional de Segurança Pública, através da Polícia Federal, queria fazer um banco de dados genéticos, aos moldes do sistema de banco de dados genéticos norte-americano, denominado CODIS - *Combined DNA Index System*, que é uma base de dados de DNA fundada pelo FBI (*Federal Bureau of Investigation*). Então, a SENASP investiu muito nesta área. Se não fosse o governo federal, não teríamos o que temos hoje.

Para podermos ter bancos de dados genéticos funcionando bem, há de se ter muitos dados neles inseridos. Então, o banco nacional de dados genéticos precisa ser alimentado pelo país inteiro. Para que isto ocorresse, foi preciso equipar os laboratórios de todas as polícias. E quem gera a maioria dos dados genéticos criminais são as Polícias Científicas. Assim, a SENASP precisou aprimorar e/ou equipar laboratórios e propiciar conhecimento técnico na área do DNA forense para peritos, em todos os estados interessados na introdução da técnica no Brasil. Hoje em dia, nós temos 20 laboratórios de diferentes estados que geram dados genéticos criminais e a Polícia Federal coordena a utilização nacional desses dados.

Para que esse banco de dados genéticos criminais pudesse funcionar, haveria de se ter uma lei federal que o regulasse. Contudo, a comissão de estudos estabelecida pela SENASP

para dar subsídios técnicos para a elaboração desta lei não contemplava estudiosos do direito e da ética, mas apenas peritos da área da genética, em sua maioria leigos em direito, principalmente quanto aos direitos dos investigados criminalmente.

Preocupada com tal situação, fiz meu mestrado acerca deste tema. Peço desculpas por estar sendo um pouco personalista e ficar falando nisso, mas é porque eu fiz alguma coisa voltada a solucionar esta lacuna nos estudos legais e éticos da questão. A minha dissertação de mestrado foi algo voltado para o uso de DNA na elucidação de crimes. O meu doutorado, eu o fiz pensando numa futura lei que regulasse o banco de dados genéticos um pouquinho melhor. Essa tese eu a terminei em 2009 e a lei saiu em 2012. Em resumo, meus trabalhos falavam: "Olha, tem que discutir! Tem que ter a ponderação de valores, não é?"

O que acontece? O nosso sistema de banco de dados é semelhante ao CODIS dos Estados Unidos. O sistema jurídico deles é o anglo-saxão, onde quase tudo é pela coletividade. E o nosso sistema é mais pela individualidade, pelos direitos individuais. Lá, eles colocam todo mundo no banco de dados. Se você está dirigindo e a sua carteira de habilitação está vencida, você doa material para o exame de DNA e pode ficar no banco de dados para sempre. Eles acham isso normal. Aqui não. Mas importamos essa ideia para regular nosso banco de dados genéticos nacional.

Então, eles fizeram essa lei péssima. Sem muito discutir, sem que ninguém que estivesse ali abraçasse importantes questões legais. Foi, então, o que eles fizeram. Eles pegaram essa lei, que é a Lei 12.654 de 2012, que altera as Leis 12.037, de 2009, e 7.210, de 1984 - Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal.

Eles pegaram a Lei de Identificação Criminal e colocaram lá como se o DNA, que é realmente uma outra forma de iden-

tificação, fosse uma exceção da identificação civil. Então, se uma pessoa for civilmente identificada, mas eles tiverem alguma dúvida em relação a ela, ela pode ceder material para exame de DNA.

Só que, como o professor que me antecedeu falou: "isto serve para dizer José é José." O que eles acham que podem com esta modificação legal dizer é: "José é José e vamos ver também se ele é um estuprador". Não podem! Isso é um absurdo! Eles pegaram e deram um jeitinho na lei. Na outra parte da Lei 12.654, eles pegaram a Lei de Execuções Penais e introduziram lá a coleta compulsória dos condenados por crime praticado, dolosamente, com violência de natureza grave contra pessoa, ou por qualquer dos crimes hediondos.

Então, para se ter uma ideia, nós temos hoje 750 mil pessoas detentas, presas. Fizeram um estudo em 2018, que aponta que desses 750 mil, 137.600 condenados estão em condições de doar compulsoriamente o material. Pelo fato de não se arrancar sangue destes condenados, pois o método de extração é indolor, feito com um suabe (cotonete), eles deduzem que não há qualquer violação de direitos. Só que estão levando toda informação genética, o genoma completo de um cada deles nos cotonetes.

Tudo bem que as regiões que nós estudamos para elucidação de crimes são regiões que não dizem respeito às características físicas dos sujeitos. Os exames de DNA rotineiramente feitos nas Polícias Científicas não são voltados para dizer se a pessoa tem câncer ou se a pessoa é negra, amarela, ou azul... Não falam nada disso. Só que no material biológico coletado há também outras regiões do DNA que podem revelar se a pessoa tem leucemia, se tem tendência para ficar louca ou esquizofrênica. Este material poderá me falar quase tudo sobre o indivíduo, dependendo do tipo de estudo genético feito com ele. Inclusive, mesmo para as regiões usual e legalmente

estudadas (perfis genéticos que não revelam traços somáticos ou comportamentais das pessoas, exceto a determinação genética de gênero), quando inseridas em banco de dados, dependendo do tipo de busca no confronto entre os perfis lá existentes, pode-se chegar a identificação de familiares da pessoa que está sendo investigada. Certamente, leis e decretos controlam o acesso e o uso das informações genéticas sigilosas, mas é de se alertar para a potencialidade informativa do material genético coletado *in totum*, bem como para a geração superlativa de informações, que transcendem o indivíduo investigado, a depender do tipo de busca feita nos bancos de dados genéticos.

É certo que existem freios legais para a geração e utilização destas informações, mas dado seu grande potencial de utilização além das divisas da investigação criminal, é de se prestar muita atenção aos modos de pesquisa destes bancos e reforçar o controle de quem efetivamente toma conta deles.

Pois bem, voltando aos dados, nós temos aí 137 mil condenados que se encaixam nas categorias citadas. Já foram "tipados" cerca de 18 mil perfis genéticos, até este momento. Com isto, o Ministério da Justiça vai liberar mais de 2 milhões de reais para aumentar a automatização das análises para obtenção dos perfis genéticos. Eles querem chegar até o final do ano a um número bem maior que isso. Querem chegar a 65 mil perfis.

E como funcionam esses bancos de dados? A gente tem um banco de dados para apuração criminal e ele se divide em crimes sexuais e outros crimes, normalmente crimes contra o patrimônio e crimes contra a pessoa. Depois têm uma parte desse banco de identificação de pessoas. Em junho, saiu o 10º Relatório do Comitê Geral dos Bancos de Dados da RIBPG - Rede Integrada de Bancos de Perfis Genéticos. Esses bancos estão sendo alimentados desde 2013. Estamos em 2019. Esse

relatório revela que, em nível nacional, já foram introduzidos nesses bancos por volta de 27 mil perfis. Destes, nove mil são perfis que foram encontrados em locais de crime; 18 mil perfis de condenados; 545 perfis de identificação criminal e 167 perfis por decisão judicial. Disto tudo, qual é o resultado? Vamos ver quanto que isso ajudou. Segundo o relatório, 852 investigações foram auxiliadas nisso tudo. Em outro tópico, o relatório indica que perfis de 146 vestígios (de casos não resolvidos, 59% deles relativos a crimes contra o patrimônio e 41% relativos a crimes sexuais) foram confrontados com perfis de indivíduos que já estavam cadastrados nos bancos de dados. Qual o significado disto? Como isto tem ajudado efetivamente na investigação criminal?

Então, para se ter uma ideia disso, eu fiz um pequeno levantamento no estado de São Paulo. Aqui nós temos por volta de 15 mil ocorrências de crimes sexuais por ano. A Polícia Científica colhe material dos vestígios relativos a todos esses casos. Porém, não é em todos os casos que se chega a um resultado positivo para espermatozoides. Assim, nem todos eles chegam lá ao laboratório de DNA. Para se ter uma ideia, desses 15 mil casos por ano, vejamos o que a investigação policial trouxe ao nosso laboratório de DNA em termos de casos fechados (vestígios contendo espermatozoides e material biológico do suspeito). No primeiro trimestre de 2018, chegaram ao laboratório 13 casos fechados. Isto significa que os resultados das investigações chegam a menos de 1%. Ainda mais, destes 13 casos fechados, apenas seis deles resultaram em inclusão dos suspeitos.

Então, agora voltando ao banco de dados, nos 146 perfis dos vestígios que foram colocados nos bancos genéticos, não havia notícias do perpetrador. São tidos como perfis de desconhecidos. Após inseridos e confrontados com outros perfis já existentes nos bancos de dados, foram encontradas coinci-

/ ESTE MATERIAL PODERÁ ME FALAR QUASE TUDO SOBRE O INDIVÍDUO, DEPENDENDO DO TIPO DE ESTUDO GENÉTICO FEITO COM ELE /

/ MAS É DE SE
ALERTAR PARA
A POTENCIALIDADE
INFORMATIVA
DO MATERIAL
GENÉTICO COLETADO
IN TOTUM /

dências destes perfis com outros já existentes e decorrentes de outras investigações policiais. Vê-se, então, que os bancos de dados são um bom instrumento para se encontrar vínculos de vestígios entre si e entre indivíduos de diferentes ocorrências. Frente às estatísticas de ocorrências policiais, isto é ainda incipiente, mas promissor. Quando nós começamos a inserir perfis genéticos no banco de dados aqui no estado de São Paulo, eu já não estava mais nas bancadas do laboratório de DNA, mas sim na direção da Polícia Científica. As meninas do laboratório disseram: "Olha nós encontramos o perfil genético de um mesmo estuprador em casos diferentes. Eram casos antigos, um de Santo Amaro e o outro de Santana." Vejam o que aconteceu. Eu falei com o Secretário da Segurança da época, mas acredito não ter sido muito clara. Então, eu disse: "Vamos ligar para o Delegado de Santana." Este falou: "Eu não posso fazer nada com o de Santo Amaro. Eu não tenho lá também a minha jurisdição. Eu não alcanço." Entenderam? Ainda tinha esse tipo de problema. Como fazer isso para ir atrás? É uma coisa nova, como é que quem vai investigar isso?

O que eu quero ressaltar com isto, então, é que a perícia nesta área deixou de ser apenas reativa. Isto porque a perícia era assim, dava apenas resposta para aquilo a que era instada: "Veja se o perfil genético do suspeito corresponde ao do perfil retirado do corpo da vítima". Com os bancos de dados, a perícia passou a ser também proativa, com a possibilidade indicar vínculos genéticos inimagináveis entre diferentes ocorrências.

Ainda sobre os resultados apresentados no relatório da RIBPG, foram relatadas 780 coincidências entre vestígios já cadastrados, sendo 59% deles referentes a crimes sexuais, 35% relativos a crimes contra o patrimônio e o restante relativo a outros crimes. Sobre pessoas desaparecidas, o relatório indica que no total o banco nacional possui 3.625 perfis genéticos, sendo 1.730 de familiares; 1.855 de restos mortais de desco-

nhecidos; 18 perfis obtidos de fonte direta dos desaparecidos e 22 perfis de pessoas vivas com identificação conhecida. Com a ajuda destes perfis, 32 vínculos foram estabelecidos, ou seja, 32 pessoas foram identificadas por esse banco de dados.

São Paulo contribuiu bastante para esse banco de dados nacional, tendo já inserido mais de 2.900 perfis genéticos. A maioria deles é oriunda de locais de crime e o restante, mais de 1.000 perfis, relativo a crimes sexuais. Já inserimos também mais de 2.500 perfis de condenados, com pretensão de alcançar a inserção de 10.000 perfis com a automação prometida pela SENASP. Estes dados inseridos não são nenhuma glória, mas estamos falando como em São Paulo, infelizmente, tem isso.

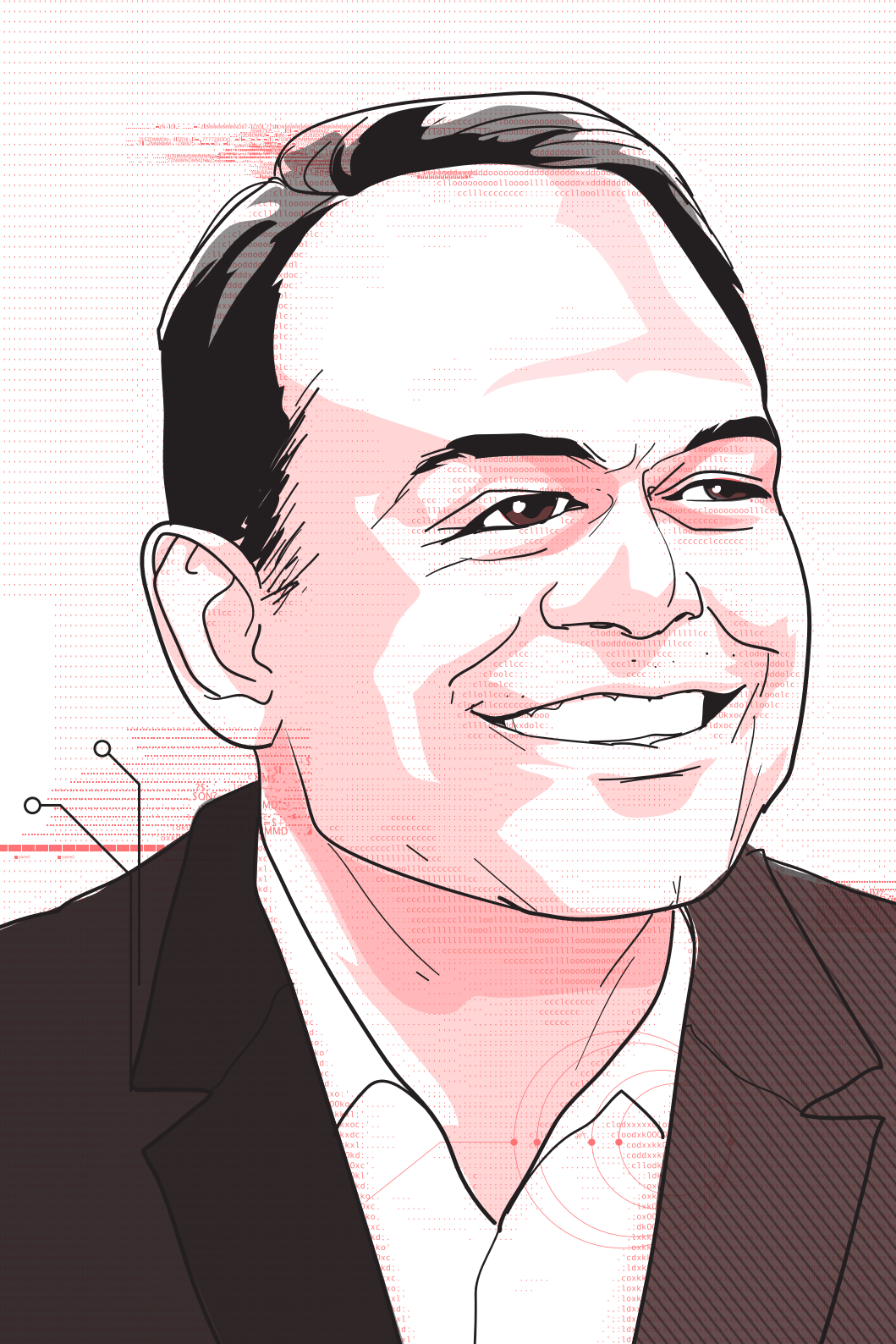
E em relação aos crimes sexuais aqui no estado, nós temos, desde 2012, um programa que se chama Bem-me-quer, voltado ao atendimento exclusivo às vítimas de crimes sexuais. Nós estamos fazendo análise retrospectiva de materiais que foram retirados das vítimas e que deram resultado positivo para espermatozoide, mas não houve investigação por falta de suspeitos. Nós temos um *backlog* de mais de 6 mil suabes para analisar até o ano de 2012. Então, nós iremos inserir mais de 6 mil perfis no banco nacional e esperamos com isso achar e condenar mais pessoas que estejam praticando crimes sexuais.

Uma outra coisa aqui e já encerro a minha fala: em relação ao Decreto de Lei 7.950/2013, que instituiu o Banco Nacional de Perfis Genéticos e RIPG, na verdade ele também regulou a composição do Comitê Gestor. Conversando com um pessoal que faz parte deste comitê, eles sentiram muito a ausência dos membros que deveriam ser convidados: o pessoal do Ministério Público, da Defensoria. Não tinha a representação da OAB e da Comissão de Ética. Então, o que é que acabou acontecendo? Muitas das regras que eles colocaram, que eles pautaram, as resoluções que eles fizeram, fizeram assim, só

os peritos. Os membros não ajudaram a definir tudo aquilo, porque você tem a necessidade de um respaldo jurídico e ético nas questões de coleta; da análise, da inclusão do perfil ou não, quanto tempo fica, do armazenamento, da manutenção dos perfis. Isso tudo deveria ter sido discutido e não foi! Só agora o pessoal do DEPEN está tendo uma participação efetiva, em função da coleta de material dos condenados. Estão fazendo a coleta dos presos.

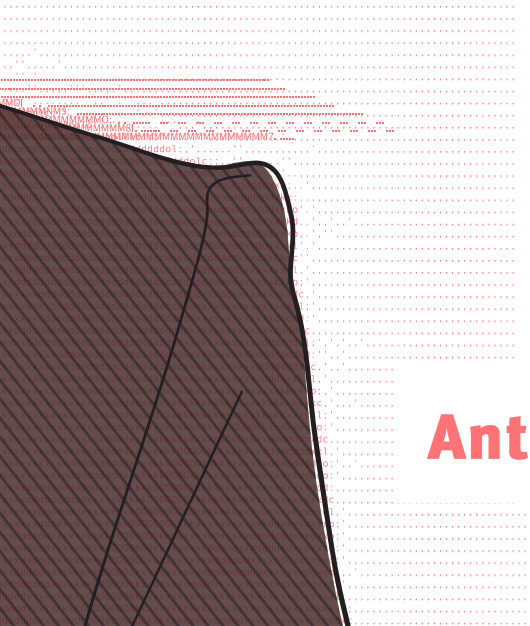
Bem, para terminar mesmo, é preciso falar dos projetos de lei da área. Nós temos alguns expansionistas, como o Projeto de Lei 882/2019 que prevê a exclusão do perfil genético e por outro lado cria o Banco Nacional Multibiométrico (íris, face e voz), o que é assustador! E só para lembrar que bancos totais são proibidos constitucionalmente na Espanha, por exemplo. Isso é um absurdo, porque você tem domínio total sobre as pessoas. Temos aqui também o projeto do Senador Cássio Cunha Lima, que é o Projeto de Lei 67/2018, que já começa com uma deficiência na descrição dos vestígios, mas, ao menos, não prevê a coleta compulsória de amostras.

É isso aí, trouxe esses dados para se ter uma ideia da efetividade dos bancos de dados genéticos. Obrigada.



13.

A CADEIA DE CUSTÓDIA NA INTERCEPTAÇÃO TELEFÔNICA



Antonio Santoro

INTRODUÇÃO

A Constituição de 1988 adotou de forma clara um modelo garantista, assim compreendido o sistema concebido por Luigi Ferrajoli (2014, p. 91 e ss.) que, em sua conhecida obra "Direito e Razão: teoria do garantismo penal", elaborou um modelo teórico baseado em apenas dez axiomas básicos, dos quais quatro são aplicáveis ao processo penal.

Tal concepção foi corroborada pela ratificação em 1992 de alguns tratados internacionais sobre direitos humanos, como o Pacto Internacional sobre os Direitos Civis e Políticos, que teve seu texto aprovado no âmbito interno do Brasil por meio do Decreto Legislativo no 226/91, entrou em vigor no dia 24 de abril de 1992 e foi promulgado pelo Decreto no 592, de 6 de julho de 1992 e, em especial, a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), que entrou em vigor no Brasil quando o governo depositou a carta de adesão em 25 de setembro de 1992, e foi promulgada pelo Decreto no 678, de 6 de novembro de 1992.

Assim, os quatro axiomas processuais penais básicos do garantismo foram contemplados expressamente pela Constituição e pelos diplomas internacionais referenciados: (1) qualquer pessoa só pode ser julgado por um juiz, independente e imparcial, (2) diante de uma acusação clara, objetiva e previamente conhecida formulada por um órgão de acusação distinto do órgão de julgamento, (3) acusação esta que deve ser provada e (4) garantido o direito de defesa e de contraditório.

Assim, toda acusação deve ser provada, de tal forma que a decisão condenatória depende da verificação da descrição dos fatos imputados pela acusação ao réu. Vale dizer, em um sistema processual penal inserido no âmbito de um Estado Democrático de Direito, a condenação à perda da liberdade, de direitos ou dos bens está condicionada à verificabilidade empírica da acusação.

Nesse contexto a atividade probatória ganha força e relevo. Todo ato que pretenda gerar dados a serem submetidos à valoração judicial deve obedecer a um procedimento definido por lei (meio de prova ou meio de obtenção de prova) que respeite os direitos e garantias fundamentais.

Um dos mais relevantes meios de obtenção de prova é a interceptação telefônica, que, de acordo com o Conselho Nacional de Justiça, ultrapassa o número de 300.000 (trezentas mil) interceptações por ano no Brasil (Santoro & Tavares, 2019, p. 116).

Um dos grandes problemas é: como garantir que as gravações de conversas são seguras e confiáveis, que não foram alteradas até chegar aos autos? Secundariamente: quais as consequências processuais penais de não existir um mecanismo que garanta a integridade do elemento de prova?

Parte-se da hipótese de que o mecanismo existente para garantia da confiabilidade das gravações que se convertem em elementos de prova é a cadeia de custódia, cuja violação implica na violação dos princípios e garantias do devido processo legal.

Para tanto, trabalhar-se-á metodologicamente com fontes bibliográficas sobre a cadeia de custódia, com o objetivo de perquirir o seu conceito, sua importância, bem como a quebra e seus efeitos, uma análise sobre sua positivação pela Lei nº 13.964/2019, bem como far-se-á uma análise do funcionamento da operação de interceptação telefônica, para então verificar o papel da cadeia de custódia nesse meio de obtenção de prova e na estrutura garantista do processo penal brasileiro.

1. A CADEIA DE CUSTÓDIA

1.1. CONCEITO

A cadeia de custódia pode ser definida como o conjunto de procedimentos que devem ser adotados com o objetivo de proteger a prova penal, desde o momento do acesso às fon-

tes de prova e colhimento dos vestígios no local da prática criminosa até o trânsito em julgado da sentença penal condenatória. Trata-se do mecanismo de proteção da autenticidade do material que se tornará prova durante o processo penal, visando à adequada identificação e o registro do caminho percorrido durante as investigações, garantindo, assim, sua segurança, rastreabilidade e licitude.

Manifesta-se, portanto, "o instituto da cadeia de custódia com o objetivo de garantir a todos os acusados o devido processo legal, bem como os recursos a ele inerentes, como a ampla defesa, o contraditório e principalmente o direito à prova lícita." (Menezes, Borri & Soares, 2018, p. 281).

Segundo Geraldo Prado (2014, p. 80), a cadeia de custódia seria, de forma simplificada, o dispositivo que objetiva assegurar os elementos probatórios em sua integridade. Trata-se de uma garantia constitucional contra a prova ilícita. Nas palavras do professor:

> O filtro processual contra provas ilícitas depende do rastreio das provas às fontes de prova (elementos informativos) e a ilicitude probatória, direta ou por derivação, é mais facilmente detectável na sequência desse rastro produzido entre as fontes de prova e os elementos (meios) probatórios propriamente ditos. (Prado, 2014, p. 57)

No entendimento do pesquisador Jefferson Lemes Carvalho, a cadeia de custódia seria constituída como um

> conjunto de procedimentos técnicos e científicos que irão oferecer conhecimento aos operadores do Direito, permitindo-se avaliar se aquela prova que está no tribunal, e que representa a materialidade de um ato criminoso, foi tratado com o devido rigor técnico-científico legal

> desde sua origem de colheita no local da infração penal. (Carvalho, 2016, p. 373)

Nas instituições periciais oficiais nacionais e internacionais, a cadeia de custódia assegura um "meio que se possa garantir a confiança, autenticidade e integridade das amostras (vestígios); desde o isolamento do local da infração penal – perícias externas até perícias internas aos laboratórios forenses." (Carvalho, 2016, p. 371)

Para Aury Lopes Jr (2017, p. 412), "A cadeia de custódia exige o estabelecimento de um procedimento regrado e formalizado, documentando toda a cronologia existencial daquela prova, para permitir a posterior validação em juízo e exercício do controle epistêmico."

É preciso manter o registro da sucessão de eventos desde a coleta do dado até o trânsito em julgado "de forma a proteger a integridade de um vestígio do local crime ao seu reconhecimento como prova material." (Dias Filho, 2002, p. 404)

O início da cadeia de custódia se daria logo após a prática criminosa, com a devida preservação do lugar da infração penal (Carvalho, 2016, p. 376).

Desde o cometimento da infração penal até o fim do processo judicial, faz-se necessária a demonstração de todas as etapas para assegurar o "rastreamento" e a "continuidade" da evidência desde o local do crime até a sala do tribunal. (United Nations Office on Drugs and Crime, 2010)

O "tema de provas exige a intervenção de regras de 'acreditação', pois nem tudo que ingressa no processo pode ter valor probatório: há que ser 'acreditado', legitimado', valorado desde sua coleta até a sua produção em juízo para ter valor probatório."(Lopes Júnior, 2017, p. 412) Para tanto, requer-se ainda a identificação de todos os envolvidos na custódia do material (Marinho, 2011).

É possível, portanto, garantir a idoneidade do caminho que a amostragem percorreu em todas as fases processuais a partir da observação de um protocolo legal, fazendo memória dessas etapas. Esse referido protocolo, que é a cadeia de custódia, é um rigoroso procedimento de coleta e conservação das evidências, a fim de evitar a contestação das provas (Lopes, Gabriel & Bareta, 2006).

Na visão de Carlos Edinger, a cadeia de custódia pode ser compreendida como uma sucessão de elos, e "um elo é qualquer pessoa que tenha manejado esse vestígio", sendo necessário identificar cada elo para garantir "a possibilidade de se indicar fontes de prova, de se exigir que elas venham ao processo." (Edinger, 2016, p. 242) Portanto, só se pode falar em cadeia de custódia íntegra quando se fala em sucessão de elos provados.

1.2. IMPORTÂNCIA DA CADEIA DE CUSTÓDIA

Geraldo Prado esclarece que a cadeia de custódia discute a concreta possibilidade de ocorrer indevida manipulação do elemento probatório. Sua importância está no fato de ser o adequado mecanismo que "visa assegurar a memória de todas as fases do processo, constituindo-se e mantendo assim um protocolo legal que permita garantir a idoneidade do resultado e rebater as possíveis contestações dúbias." (Carvalho, 2016, p. 371)

A relevância de tal instituto decorre da impossibilidade de "controlar os mecanismos de convencimento psicológico do juiz", daí porque "o controle da decisão judicial em um Estado democrático de direito deve se dar através de sistemas de controles epistêmicos, mediante critérios objetivos, inclusive na fase da produção da prova, para garantir a qualidade da decisão judicial." (Moraes, 2017, p. 136)

Cumpre ressaltar que a cadeia de custódia não pretende questionar a credibilidade da prova colhida pela autorida-

de policial, mas garantir que aquela prova possa ser acreditada, ou seja, "demonstre que tais objetos correspondem ao que a parte alega ser." (Lopes Júnior, 2017, p. 412) Trata-se da segurança de que o Estado cumprirá com sua obrigação de conservação da prova, visando garantir sua integridade e confiabilidade. Geraldo Prado define tal posicionamento como "mesmidade", isto é, a garantia de que a prova colhida é a mesma que a projetada em juízo. (Prado, 2014, pp. 16-17)

Por fim, tem-se que "saber se as informações são empiricamente verificáveis implica, antes de mais nada, poder confiar que os dados armazenados e submetidos à valoração judicial guardam fidedignidade e não foram manipulados ou que não foram passíveis de manipulação." A cadeia de custódia se apresenta, portanto, como "a única maneira de assegurar a integridade do procedimento probatório." (Santoro, Tavares & Gomes, 2017, p. 620) Em outras palavras, deve ser preservada a cadeia de custódia para permitir o rastreio às fontes de prova.

1.3. A PREVISÃO NORMATIVA DA CADEIA DE CUSTÓDIA NO ORDENAMENTO JURÍDICO BRASILEIRO E A LEI Nº 13.964/2019

A cadeia de custódia, como instituto da teoria das provas, "deve ser vista como direito subjetivo das partes, visto que a garantia de uma prova idônea e preservada é um desdobramento da garantia ao devido processo legal." (Azevedo, 2017, p. 106)

Dessa forma, a cadeia de custódia se fundamenta em diversos dispositivos constitucionais, especialmente nos princípios do contraditório e da ampla defesa (da paridade de armas), da presunção de inocência, da inadmissibilidade das provas obtidas ilicitamente, previstos no artigo 5º, incisos LV, LVII, LVI da Constituição Federal, respectivamente, bem como do

princípio do sistema acusatório, com a separação de funções, iniciativa probatória das partes e imparcialidade do julgador.

Portanto, o respeito ao instituto é a maneira pela qual se pode garantir a aplicabilidade de importantes princípios constitucionais no processo penal, os quais tornam essencial a manutenção da higidez da cadeia de custódia como forma de garantir tratamento igualitário entre as partes, possibilitando o conhecimento integral da imputação criminal e da produção probatória.

Em que pese a importância da cadeia de custódia decorrer também da adequada observação da previsão constitucional, como anteriormente demonstrado, havia no ordenamento jurídico brasileiro pouca normatização referente ao instituto, de forma específica, até a entrada em vigor da Lei nº 13.964/2019. Vejamos a situação normativa antes e depois do referido diploma legal.

O Código de Processo Penal não contemplava regulamentação objetiva sobre a conceituação e a documentação da cadeia de custódia. Entretanto, Gustavo Badaró sugeria uma interpretação sistemática do referido diploma legal, indicando alguns dispositivos que apontavam e ainda apontam para a sua necessidade. Exemplifica-se com o artigo 6º, especialmente os incisos I e II do Código de Processo Penal, que impõe à autoridade policial a preservação do local do crime até a chegada dos peritos e a apreensão dos objetos após a liberação pelos *experts*.

Há a exigência, ainda, conforme prevê o artigo 158 do Código Processo Penal, da obrigatoriedade da realização de exame de corpo de delito quando houver sinais indicativos da ocorrência de infração penal.

Ainda no mesmo diploma legal, prevê o artigo 170: "Nas perícias de laboratório, os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que con-

veniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos os esquemas." (Brasil, 1941)

Dessa forma, a prova pericial no processo penal brasileiro é a regra, cuja ausência pode acarretar o desaparecimento de todos os vestígios da infração. "É exigido que o laboratório criminal guarde material suficiente para contraprova pericial, satisfazendo assim o princípio constitucional do contraditório e da ampla defesa do acusado." (Carvalho, 2016)

Com a reforma realizada no processo penal brasileiro a partir da Lei 11.690 de 2008, tem-se a figura do assistente técnico, o qual poderá apresentar parecer técnico corroborando ou se contrapondo ao laudo pericial oficial, o que só pode acontecer se os vestígios forem preservados, garantindo-se a cadeia de custódia da prova e viabilizando o direito de defesa e ao contraditório.

Tal previsão vinha se mostrado de grande valia para as partes exercerem o controle e garantir a confiabilidade da cadeia de custódia no manuseio das evidências. Pontua Jefferson Lemes Carvalho que "é possível explicar que a prática de alguns advogados de questionar o manuseio de evidências ganha força com a figura do assistente técnico no processo penal e esse procedimento será enormemente explorado como argumento de defesa." (Carvalho, 2016, p. 378)

A partir de tudo mostrado, pode-se inferir que o Código de Processo Penal não regulamentava diretamente a cadeia de custódia de forma pormenorizada, tratando, todavia, de especificar no meio de prova pericial (artigos 154 a 184 do Código de Processo Penal) providências que podiam ser compreendidas como uma garantia à cadeia de custódia.

Com efeito, conforme determina a Portaria nº 82, de 16 de julho de 2014, da Secretaria Nacional de Segurança Pública, cadeia de custódia é o "conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica

do vestígio, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte." (Brasil, 2014) A referida norma considera que a cadeia de custódia "é fundamental para garantir a idoneidade e a rastreabilidade dos vestígios, com vistas a preservar a confiabilidade e a transparência da produção da prova pericial até a conclusão do processo judicial." (Brasil, 2014) Por fim, ela "confere aos vestígios certificação de origem e destinação e, consequentemente, atribui à prova pericial resultante de sua análise, credibilidade e robustez suficientes para propiciar sua admissão e permanência no elenco probatório." (Brasil, 2014)

Considerando ser imprescindível a garantia aos elementos de prova documentados nos autos do procedimento persecutório penal para se identificar a preservação da cadeia de custódia, o Supremo Tribunal Federal se debruçou a respeito da matéria e consolidou a Súmula Vinculante nº 14, a qual "garante ao defensor a possibilidade de conhecer os elementos angariados em desfavor de seu constituinte." (Menezes, Borri & Soares, 2018, p. 290) Determina a referida súmula: "É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa." (Brasil, 2018)

Decorre desse entendimento a compreensão da Suprema Corte sobre o acesso aos elementos informativos da investigação (chamados pela súmula de "elementos de prova") como constituição de vetor de controle da cadeia de custódia da prova, especialmente no que se refere ao conhecimento das fontes de prova. "Qualquer tipo de filtro realizado na prova – quer seja por ocultação, destruição ou agregação de conteúdo -, é incompatível com o 'acesso amplo aos elementos de prova', justamente por corresponder à parte de um todo." (Machado & Jezler Júnior, 2016, pp. 8-9)

/ RECONHECIDA E COMPROVADA DE FORMA PERICIAL, A QUEBRA DA CADEIA DE CUSTÓDIA DESAFIA A APLICAÇÃO DE SANÇÕES PROCESSUAIS /

A partir do que foi apresentado, tem-se que "os princípios constitucionais limitadores do poder punitivo estatal, as normas processuais penais e o entendimento sumular possibilitam o reconhecimento da cadeia de custódia como mecanismo hábil a conferir fidelidade à prova, permitindo o conhecimento pela defesa de eventual manipulação, adulteração ou supressão da prova provocando consequências." (Menezes, Borri e Soares, 2018, p. 291)

Todavia, com a entrada em vigor da Lei nº 13.964/2019, foram introduzidos os artigos 158-A a 158-F no Código de Processo Penal, cujo objetivo foi regulamentar a cadeia de custódia. Porém, a cadeia de custódia foi regulamentada apenas para o meio de prova pericial.

O art. 158-A do CPP define cadeia de custódia como "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte". Estabelece que o início da cadeia de custódia se dá com a preservação do local, cuja responsabilidade é do agente público que reconhecer um elemento como de potencial interesse para a investigação. E define vestígio como "todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal."

O art. 158-B define as etapas da cadeia de custódia e o significado de cada uma delas. São etapas legais da cadeia de custódia: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte.

Os dispositivos seguintes definem que o perito oficial é responsável pela coleta do material e determina a criação de uma central de custódia em todos os institutos de criminalística, a qual deve guardar e controlar os vestígios.

Ficou definido também que a responsabilidade pela cadeia de custódia é de diferentes órgãos conforme as etapas da cadeia. O funcionário que identificar um elemento potencial terá uma responsabilidade que termina antes da coleta. O perito é responsável pela coleta, bem como por todo o período em que o vestígio estiver sob sua guarda, e a central de custódia é responsável pelo guarda e controle dos vestígios, bem como pelo registro de entrada e saída do vestígio no órgão, devendo identificar todas as pessoas que tiveram acesso, com registro de data e hora. Toda tramitação dos vestígios na central de custódia deve fazer constar a identificação do responsável pelas ações, com registro da destinação, data e hora da ação.

A cadeia de custódia se mostra, portanto, como instituto indispensável e de fundamental importância ao processo penal brasileiro. Faz-se necessária, portanto, a análise da quebra da cadeia de custódia e das consequências decorrentes desse rompimento para o processo penal brasileiro.

2. A QUEBRA DA CADEIA DE CUSTÓDIA E SEUS REFLEXOS NO PROCESSO PENAL BRASILEIRO

Como já demonstrado, o instituto da cadeia de custódia "abarca todo o caminho que deve ser percorrido pela prova até a sua exata análise e escorreita inserção no processo, sendo que qualquer interferência durante o trâmite processual pode resultar na sua imprestabilidade." (Menezes, Borri & Soares, 2018, p. 281)

Dessa forma, conforme entende Alberi Espindula:

> Claro está que a finalidade em se garantir a cadeia de custódia é para assegurar a idoneidade dos objetos e bens escolhidos pela perícia ou apreendidos pela auto-

> ridade policial, a fim de evitar qualquer tipo de custódia quanto à sua origem e caminho percorrido durante a investigação criminal e o respectivo processo judicial. (Espindula, 2009, p. 165)

Estabelecido o conceito de cadeia de custódia, faz-se necessária a discussão sobre a falta ou insuficiência da documentação do referido instituto. Tal advertência é importante porque "não se viola a sucessão de pessoas que teve contato com a coisa, mas a documentação que atesta essa realidade." (Badaró, 2018, p. 254) Em outras palavras, "o fato de inexistir o registro das pessoas que mantiveram contato com a fonte de prova não significa assentir que houve violação da cadeia de custódia." (Menezes, Borri & Soares, 2018, p. 282)

A regulamentação da cadeia de custódia é relevante porque três principais argumentos podem ser suscitados para questionar a validade do referido instituto: a) a falsidade da prova; b) a insuficiência da prova da cadeia de custódia da prova; e c) a falsidade da prova da cadeia de custódia da prova. Apenas o primeiro e o terceiro itens poderiam ser resolvidos através do incidente de falsidade documental, mantendo-se as demais controvérsias quanto a cadeia de custódia insuficiente, segundo Dallagnol & Câmara (2016, p. 437).

O valor probatório da evidência ou do documento, portanto, será validado caso não sejam discutidas sua origem e sua tramitação. Alberi Espindula diz que:

> Muitas situações já são conhecidas sobre fatos dessa natureza, nas quais é levantada a suspeição sobre as condições de determinado objeto ou sobre a própria certeza de ser aquele o material que de fato foi apreendido ou periciado. Assim, o valor probatório de uma evidência ou documento será válido se não tiver sua origem e tramitação

> questionada. Qualquer questionamento acarretará prejuízo para processo como um todo. (Espindula, 2009, p. 165)

Assim, "qualquer interrupção na cadeia de custódia pode causar a inadmissibilidade da evidência. Mesmo se admitida, uma interrupção pode enfraquecer ou destruir seu valor probatório. A regra é ter o menor número possível de pessoas lidando com a evidência." (Osterburg & Ward, 1992, p. 180). Em outras palavras, tem-se que:

> A ausência de observância de um procedimento específico no momento da produção do elemento probatório pode gerar a quebra da cadeia de custódia da prova e, por consequência sua ilicitude. Sendo assim, necessário se faz que o detentor da fonte de prova, na maioria das vezes o Estado-acusação, tenha o devido cuidado na coleta, manipulação e transporte do objeto que, posteriormente, será um elemento probatório, a fim de preservar a cadeia de custódia e garantir a integridade da prova. (Menezes, Borri & Soares, 2018, p. 284)

Entende Geraldo Prado que a questão relacionada à cadeia de custódia, antes tratada apenas em sua relevância estritamente técnica no estudo das perícias, "transcende esta dimensão para gozar de status constitucional, pois que se relaciona com a garantia contra a prova ilícita." (Prado, 2014, p. 82)

Acrescenta Prado que a análise sobre a ocorrência de provas ilícitas "depende do rastreio das provas às fontes de prova (elementos informativos) e a ilicitude probatória, direta ou por derivação, é mais facilmente detectável na sequência deste rastro produzido entre as fontes de prova e os elementos (meios) probatórios propriamente ditos. (Prado, 2014, p. 57)

Tem-se evidente que a falha na preservação dos elementos probatórios, que configura a quebra da cadeia de custódia, pode influenciar na interpretação de todo o conjunto probatório, considerando a natureza persuasiva das provas. (Prado, 2014, p. 82) A referida ruptura, portanto, terá reflexos diretos no entendimento final do magistrado, bem como guiará as alegações da acusação e da defesa, podendo resultar em um julgamento injusto, violando os princípios constitucionais do contraditório e da ampla defesa.

Segundo Geraldo Prado "A destruição dos elementos informativos, comprovada por perícia no processo, inviabiliza o exercício do direito de defesa e a própria fiscalização judicial, relativamente ao caráter de confiabilidade dos demais elementos..." (Prado, 2014, p. 83)

Entende Carlos Edinger que a quebra da cadeia de custódia gera também a quebra da rastreabilidade das provas, resultando na perda da credibilidade do referido lastro probatório, afinal, argumenta o autor, "se eu desconheço a proveniência daquela prova, se eu desconheço por quem aquela prova passou e o que foi feito com ela, nada impede que seja ela objeto da manipulação e seleção unilateral das provas, realizada por agentes do Estado ou, até, por eventuais corréus" (Edinger, 2016, p. 251)

Reconhecida e comprovada de forma pericial, a quebra da cadeia de custódia desafia a aplicação de sanções processuais, visto sua gravidade, e "configura prova ilícita, pois não há como sujeitá-lo, adequadamente, aos procedimentos de comprovação e refutação." (Prado, 2014, p. 87)

Para Aury Lopes Jr., a consequência da quebra da cadeia de custódia "sem dúvida deve ser a proibição de valoração probatória com a consequente exclusão física dela e de toda a derivada." (Lopes Júnior, 2017, p. 414)

Na mesma linha, Geraldo Prado entende que com a ruptura da cadeia de custódia "uma vez reconhecida sua ilicitude,

de forma definitiva, haverá o desentranhamento e sua inutilização" (Prado, 2014, p. 57), seja porque foram violados os cuidados no aspecto de correspondência entre a prova colhida e aquela trazida ao feito ("mesmidade"), seja na perspectiva do significado da prova que acarreta a falta de confiabilidade do elemento probatório, impedindo sua valoração.

Cumpre ressaltar que, em sentido contrário aos entendimentos apresentados, Gustavo Badaró entende que a quebra da cadeia de custódia não implica em ilicitude da prova, sendo certo que a problemática deve ser solucionada no momento da valoração das provas, a partir da análise do magistrado. Adverte o autor que, mesmo em situações de maior gravidade, mediante existência de questionamento sobre a integridade e a autenticidade da prova, tal fato repercutirá em seu valor. (Badaró, 2018, p. 535)

Todavia, prevalece na doutrina o entendimento de que

> deve-se verificar as consequências jurídicas oriundas da quebra da cadeia de custódia da prova entendendo-se como adequada e harmônica a Constituição Federal a compreensão de ilicitude probatória, enodando todos os elementos derivados, conforme a teoria dos frutos da árvore envenenada. (Prado, 2014, p. 296)

Não se pode ignorar que a regulamentação sobre a cadeia de custódia inserida pela Lei nº 13.964/2019 padece de dois problemas: (1) dirige-se apenas ao meio de prova pericial; (2) não traz nenhuma disposição sobre a consequência para a validade ou valor dos elementos de prova.

Começando pelo segundo ponto, os artigos 158-A a 158-F do CPP não dispõem sobre a ilicitude da prova, sobre a obrigatoriedade de desentranhamento ou sobre a obrigatoriedade de não valoração. Apenas afirma no §2º do art. 158-C do

CPP que a entrada em locais isolados e a remoção de vestígios antes da liberação pelo perito responsável, implica na tipificação de fraude processual.

Isso mostra que a Lei nº 13.964/2019 teve a preocupação de criminalizar condutas que violassem a cadeia de custódia, mas não tipificou com a devida sanção processual os elementos probatórios de um meio cuja cadeia de custódia tenha sido violada.

Nesse sentido, compreendemos como a doutrina que "verificada a quebra da cadeia de custódia das provas, todos os demais elementos colhidos a partir da quebra estarão contaminados e igualmente não serão válidos." (Prado, 2014, p. 91) Observando a norma processual penal brasileira, notadamente o artigo 157 do Código de Processo Penal, já explicado, a contaminação gerada pela quebra da cadeia de custódia estabelece a "inadmissibilidade das provas derivadas das ilícitas, salvo quando houver rompimento do nexo de causalidade entre umas e outras." (Prado, 2014, p. 92). A quebra da cadeia de custódia, portanto, é capaz de gerar provas ilícitas, inclusive por derivação, devendo ocorrer o desentranhamento e completa inutilização das mesmas.

No centro dessa discussão está o contraditório, como bem observa Prado, para quem a verificabilidade do meio probatório, como função do contraditório, "apenas é viável se for possível determinar a integridade das fontes de prova", sendo esse o papel do princípio da "mesmidade". (Prado, 2019, p. 134)

Quanto ao segundo problema, qual seja, a Lei nº 13.964/2019 ter regulado a cadeia de custódia apenas quanto à prova pericial, importa observar o que ensina Geraldo Prado sobre as cautelares probatórias, entre as quais se encontra a interceptação telefônica. Para Prado, se impõe a definição e concreção de métodos de manutenção dos elementos infor-

mativos obtidos com o empregos desses meios, bem como a instituição de práticas fiscalizadoras destes elementos (Prado, 2019, p. 135).

Portanto, conquanto a Lei nº 13.964/2019 só tenha definido regras sobre a cadeia de custódia dos vestígios da prova pericial, propõe Prado que seu estudo, inspirado nos princípios constitucionais e convencionais estruturantes do processo penal no Estado de Direito, continue a fornecer subsídios para o enfrentamento deste tema em relação às cautelares probatórias. Acrescente-se, por oportuno, que as bases normativas da cadeia de custódia da prova pericial podem e devem ser aplicadas por analogia para as cautelares probatórias, especialmente a interceptação telefônica.

Nesse sentido, apresentaremos os pontos relevantes sobre a interceptação telefônica, especialmente sobre o funcionamento prático das medidas e principais funcionalidades que geram importantes implicações sobre a cadeia de custódia.

3. INTERCEPTAÇÃO TELEFÔNICA E OS SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO (TI) QUE CAPTAM E ARMAZENAM OS DADOS COLHIDOS DOS MONITORAMENTOS DAS COMUNICAÇÕES

3.1. TERMINOLOGIAS DA PROVA: INTERCEPTAÇÃO TELEFÔNICA COMO MEIO DE OBTENÇÃO DE PROVA ATÍPICO

Ponto fundamental à compreensão do problema diz respeito à compreensão terminológica referente ao tema probatório. Sabe-se que o termo prova é usado de forma indiscriminada para designar uma variada gama de significados, daí a sua natureza polissêmica tanto no trato comum como no discurso jurídico.

Entretanto, faz-se necessário realizar algumas distinções para efetiva compreensão da proposta de pesquisa realizada neste trabalho. A primeira é a compreensão do que vem a ser *elemento de prova e resultado da prova*.

Elementos de prova, no inglês evidence, são os "(...) dados objetivos que confirmam ou negam uma asserção a respeito de um fato que interessa à causa" (Gomes Filho, 2005, p. 307) e sobre os quais o juiz vai realizar um procedimento inferencial para chegar a alguma conclusão sobre os fatos. São as informações valoráveis pelo juiz. Já o resultado da prova, no inglês *proof*, é a própria conclusão que o julgador extrai dos diversos elementos de prova existentes, por meio de um procedimento intelectual para estabelecer a veracidade ou não dos fatos alegados. Estes fatos alegados são chamados de objeto de prova.

Há que se distinguir, ainda, *fonte de prova, meio de prova e meio de investigação de prova*.

Fonte de prova são as pessoas ou coisas que podem fornecer uma informação apreciável sobre o objeto de prova, ou seja, os fatos alegados. Daí porque as fontes podem ser reais (documentos *lato sensu*) ou pessoais (testemunhas, acusado, vítima, perito, assistentes técnicos).

Meios de prova são instrumentos ou atividades endoprocessuais que se desenvolvem perante o juiz, com conhecimento e participação das partes, pelos quais as fontes de prova introduzem elementos de prova no processo. Diferenciam-se dos meios de investigação de prova, também chamados meios de pesquisa da prova ou meios de obtenção de prova, que são atividades extraprocessuais, que podem ser produzidos na fase investigatória, sem a participação do investigado, baseado no fator "surpresa" (Tonini, 2002, p. 242) e não podem ser repetidos.

Nosso Código de Processo Penal não distingue entre meios de prova e meios de investigação de prova. O *Codice*

di Procedura Penale[1] italiano distingue no Livro III, Título II os meios de prova (testemunhal, confronto ou acareação, reconhecimento, reprodução judicial, pericial e documental) e no Título III os meios de pesquisa da prova (inspeções, buscas, sequestros e interceptações das conversas ou comunicações).

Todavia, a Lei nº 12.850/2013 adotou claramente esta nomenclatura e fez um elenco dos meios de obtenção de prova admitidos nas investigações no seu art. 3º e regulamentou algumas delas.

A interceptação das comunicações telefônicas, conquanto esteja no rol dos meios de obtenção de prova da Lei nº 12.850/2013, está regulada pela Lei nº 9.296 de 1996. De fato, a interceptação telefônica é um meio de investigação ou de pesquisa ou de obtenção da prova, cuja aptidão para levar ao processo elementos probatórios deve ser analisada cuidadosamente.

Em primeiro lugar, há que se distinguir se a interceptação das comunicações telefônicas é um meio de investigação de prova típico ou atípico. Neste ponto é importante pontuar que meios típicos não se caracterizam meramente por estarem previstos em lei, pois, como pontua Antonio Scarance Fernandes, apoiado na lição de Antonio Laronga, "a prova típica é aquela prevista e dotada de procedimento próprio para sua efetivação; a prova atípica, por conseguinte, é aquela que, prevista ou não, é destituída de procedimento para sua produção." (Scarance Fernandes, 2012, p. 15)

Nesse sentido seriam típicos aqueles meios cuja previsão e procedimento estão regulamentados, seja o procedimento próprio ou por remissão. De outro lado, não estando previsto o meio ou, ainda que previsto, se seu procedimento não estiver regulamentado ou for objeto de remissão, está-se diante de um meio atípico.

Ora, o art. 50 da Lei no 9.296 de 1996 prevê não apenas que a decisão que defere a medida deve ser fundamentada, mas que o juiz deve indicar "a forma de execução da diligência".

Dessa forma, como observou Geraldo Prado, quando a legislação silencia sobre o procedimento probatório, a exigência de motivação da "decisão que defere o emprego de métodos ocultos de investigação importa" não apenas na indicação dos elementos que convencem acerca da sua adequação, mas "ainda, na definição dos meios de sua execução e fiscalização" (Prado, 2014, p. 78).

Isso significa que o procedimento da interceptação das comunicações telefônicas não é regulamentado, sendo deixado ao juiz, no ato decisório, fazê-lo. Isso implica em que a interceptação das comunicações é um meio de investigação de prova atípico.

Daí surge um questionamento: os elementos de prova obtidos pelos meios de prova atípicos são de regra admitidos porque submetem-se ao contraditório judicial, mas os meios de investigação de prova atípicos são aptos a obter elementos de prova ou apenas a descobrir e resguardar a fonte de prova?

A resposta de Scarance Fernandes merece transcrição:

> O problema da ilicitude coloca-se mais em relação aos meios de investigação ou de obtenção de prova. Como, quase sempre, eles importam restrição ou ameaça de restrição a direitos individuais, a regra deve ser a tipicidade, dependendo a obtenção da fonte de prova de lei que indique as hipóteses em que a restrição será possível e os limites em que será permitida. Somente quando o meio de investigação de prova atípico não interfira em direito individual será possível a sua utilização. (Scarance Fernandes, 2012, pp. 28-29)

A interceptação das comunicações telefônicas é um meio de investigação de prova atípico, vez que carece de uma regulamentação metodológica de obtenção, que interfere diretamente no direito individual à inviolabilidade das comunicações, à privacidade e à intimidade.

Essa omissão legislativa pode implicar na adoção de uma alternativa epistemológica autoritária pela aplicação de um subjetivismo inquisitivo (Ferrajoli, 2013, pp. 46-47), a menos que se definam mecanismos de estabelecimento prévio das "regras do jogo", às quais todos os atores do sistema penal, inclusive o juiz, devam se submeter.

Segundo Geraldo Prado, na ausência de regulação legal, cabe ao juiz fazê-lo (Prado, 2014, p. 78). Essa foi a técnica utilizada pelo legislador pátrio no que concerne ao procedimento para execução da diligência. Basta ver que a Lei no 9.296/96, que regulamentou o art. 5º, XII, da CRFB/88 para tratar dos casos de autorização da interceptação telefônica e telemática como meio de obtenção de prova no processo penal brasileiro, dispôs no art. 5o que cabe ao juiz, na decisão que defere ou determina a medida, definir "a forma de execução da diligência".

De se observar que é a autoridade policial quem deve conduzir os procedimentos de interceptação, cientificando o Ministério Público, que poderá acompanhar a sua realização, segundo o art. 6o da referida lei.

Assim, inobstante não se possa deixar de relembrar o atropelo dos princípios do contraditório e da imparcialidade da jurisdição, estão definidas as posições (porém não totalmente as tarefas de cada um) dos atores tradicionais do sistema penal, com o devido alijamento da defesa.

A novidade é que a Lei no 9.296/96 traz à cena dois novos atores para este subsistema probatório: (1) as concessionárias

de serviço público de telefonia e provedores de acesso e (2) o sistema de tecnologia da informação (TI) que trata os dados colhidos dos monitoramentos das comunicações (e seus operadores privados). Isso ocorre, respectivamente, no artigo 70 e no parágrafo 10 do art. 60, ambos da Lei no 9.296/96.

O art. 70 afirma que a autoridade policial (não a autoridade judicial, nem o Ministério Público) poderá requisitar serviços e técnicos especializados às concessionárias de serviço público.

O parágrafo 10 do art. 60 apenas afirma que "no caso de a diligência possibilitar a gravação da comunicação interceptada, será determinada sua transcrição". Muito embora este dispositivo nada fale sobre sistemas de TI, quando faz menção à possibilidade de gravação, torna esse procedimento obrigatório sempre que tiver sido possível. Acontece que em 1996, quando a lei entrou em vigor, poderia não ser possível em todos os casos, mas hoje, com o avanço tecnológico, isso é sempre possível e entra em cena o sistema de TI utilizado para realizar a tarefa como parte da engrenagem probatória no processo penal.

Todavia, essas parcas menções legais às concessionárias de serviço público de telefonia e ao sistema de tecnologia da informação que trata os dados colhidos dos monitoramentos das comunicações não são suficientes para descrever com precisão o papel que devam desempenhar. Falta regulamentar de maneira uniforme os procedimentos de execução dessas medidas invasivas, incluindo a atividade de cada um dos atores do sistema penal e dos novos atores desse subsistema probatório.

3.2. IDENTIFICAÇÃO DOS SISTEMAS DE RECEPÇÃO E ARMAZENAMENTO DE DADOS

Pelo que se tem notícia, há, no Brasil, basicamente três sistemas de TI utilizados para recepção e armazenamento dos dados objetos de monitoramento: o Sistema Guardião, de-

senvolvido e comercializado pela empresa Dígitro Tecnologia Ltda., o Sistema Sombra, desenvolvido e comercializado pela empresa Federal Tecnologia de Software Ltda.-EPP, e o Sistema Wytron, desenvolvido e comercializado pela empresa Wytron Technology Corp. Ltda.

Dados colhidos do Processo no 0.00.000.001328/2012-95, que tramitou junto ao Conselho Nacional do Ministério Público e se tratava de um Pedido de Providência formulado pelo Conselho Federal da Ordem dos Advogados do Brasil, consistente no requerimento de auditoria e inspeção nos sistemas de escuta e monitoramento de interceptações telefônicas utilizados pelas unidades do Ministério Público brasileiro[2], mostram que, a partir das consultas feitas às 30 unidades do Ministério Público brasileiro, 8 (oito) adquiriram o Sistema Guardião (o Ministério Público Federal e o Ministério Público dos estados de Goiás, Mato Grosso, Rio Grande do Norte, Rio Grande do Sul, São Paulo, Santa Catarina e o Distrito Federal); 6 (seis) adquiriram o Sistema Wytron (o Ministério Público dos estados de Alagoas, Amapá, Ceará, Maranhão, Pará e Rondônia); 3 (três) adquiriram o Sistema Sombra (o Ministério Público dos estados da Bahia, Mato Grosso do Sul e Paraíba); 4 (quatro) utilizam o Sistema Guardião disponibilizado ou cedido por órgãos do Poder Executivo (o Ministério Público dos estados do Espírito Santo, Minas Gerais, Amazonas e Tocantins); 9 (nove) não possuem ou não têm acesso a qualquer um desses sistemas (o Ministério Público Militar, o Ministério Público do Trabalho e o Ministério Público dos estados de Sergipe, Pernambuco, Acre, Paraná, Piauí, Roraima e Rio de Janeiro).

Portanto, das 30 (trinta) unidades do Ministério Público, 21 (vinte e uma) adquiriram ou utilizam sistemas de TI que se destinam a receber e armazenar dados obtidos de interceptações telefônicas ou de dados. Destas 21 (vinte e uma) unidades que operam sistemas de monitoramento de comu-

nicações, 12 (doze) "não dispõem de ato normativo versando sobre procedimentos e rotinas adotadas"[3] e 18 (dezoito) recorrem a policiais civis e/ou militares na operação.

No que se refere à aquisição desses sistemas pelos Departamentos de Polícia Federal dos Estados não há dados tão precisos quanto esses constantes do processo que tramitou no Conselho Nacional do Ministério Público, mas dados do Portal da Transparência do governo federal demonstram que as empresas Dígitro Tecnologia Ltda., Federal Tecnologia de Software Ltda.-EPP e Wytron Technology Corp. Ltda. comercializaram com o Departamento de Polícia Federal, sendo, ademais, amplamente divulgada a contratação do Sistema Guardião pelas Superintendências da Polícia Federal de Santa Catarina, Paraná, São Paulo e Rio de Janeiro.

3.3. A OPERAÇÃO DA INTERCEPTAÇÃO

Quanto à operação desses sistemas, a Dígitro e a Federal afirmam que seus sistemas, Guardião e Sombra, respectivamente, não permitem a interceptação telefônica sem a participação das operadoras de telefonia, portanto só realizam monitoramento passivo. Assim, são as operadoras de telefonia que encaminham as informações interceptadas ao sistema de monitoramento.

Na prática, as operadoras "abrem um *link*" de tal forma que a chamada telefônica ou o fluxo de dados seja desviado para um outro canal de recepção diverso do destinatário e o direciona para o sistema de TI utilizado para recepção e armazenamento dos dados objetos de monitoramento (Guardião, Sombra ou Wytron, por exemplo).

Assim, se o interlocutor A (não interceptado) liga para o interlocutor B (interceptado), esta ligação irá se completar, mas o fluxo se duplicará em dois *links*, um para o interlocutor, outro para o sistema de TI responsável pelo monitoramento.

Aqui está um primeiro, porém muito grave problema. É que diversamente do que dispõe a legislação, quem verdadeiramente conduz a interceptação não é a autoridade policial, como determina o art. 60 da Lei no 9.296/96, mas a operadora de telefonia. São precisamente as concessionárias de serviço público de telefonia ou os provedores de acesso (no caso de desvio de dados, como e-mail e VOIP) que controlam quem será objeto de interceptação e qual a duração, pois, uma vez que os sistemas de monitoramento são passivos, é a operadora que abre e fecha o *link* e, portanto, determina o tempo de interceptação.

Diante das informações prestadas pelas empresas desenvolvedoras dos sistemas de TI responsáveis pelo monitoramento das comunicações, as operadoras de telefonia e os provedores de acesso desempenham, na prática, um papel proeminente na execução das medidas cautelares de interceptação. No entanto, o sistema legal ignora esse novo ator desse subsistema probatório, não dispensando sequer uma única regulamentação para sua atuação, muito menos discutindo a adequação ou inadequação da sua posição protagonista na coleta de informações dentro da investigação penal.

Ademais, as operadoras de telefonia também não fazem o desvio da chamada para o canal de recepção do sistema de TI dedicado ao monitoramento das comunicações sem o auxílio de uma ferramenta. Há um sistema chamado Vigia, desenvolvido pela empresa Suntech, que gerencia "todo o processo de interceptação legal e retenção de dados para qualquer serviço ou subsistema de comunicação de qualquer tecnologia ou vendedor". De acordo com o desenvolvedor, "com o Vigia é possível interceptar a comunicação em praticamente todos os tipos de rede e reter dados de comunicação sem notificar os assinantes ou prejudicar o serviço".[4]

Desta forma, o Sistema Vigia e os sistemas de TI dedicados ao monitoramento e armazenamento das comunicações

(Guardião, Sombra ou Wytron) não se sobrepõem, ao contrário, são complementares. Na verdade, o Sistema Vigia é o sistema ativo, ele é quem de fato realiza a interceptação e o desvio da chamada para o sistema passivo que recebe e armazena os dados.

Importa ressaltar que os sistemas passivos de TI que recebem, monitoram e armazenam os dados interceptados são adquiridos e operados pelas autoridades públicas responsáveis pela investigação (Ministério Público, Polícia Federal, secretarias de segurança dos estados, etc.), ao passo que o Sistema Vigia tem como clientes exatamente as operadoras de telefonia (Claro, Oi, Vivo, Tim, Nextel, Embratel, GVT, Movistar), o que aliás é divulgado em seu sítio eletrônico na internet.[5] Isso apenas corrobora o fato de que operadoras de telefonia e provedores de acesso são atores do sistema penal e precisam ser assim compreendidos para que suas ações sejam excluídas ou regulamentadas.

É ainda imprescindível que se compreenda quais as possibilidades de que os operadores das empresas desenvolvedoras desses sistemas (aqui leia-se todos eles, Vigia, Guardião, Sombra, Wytron, ou qualquer outro com a mesma funcionalidade), que prestam serviços de suporte técnico, tenham acesso aos mecanismos de funcionamento e aos dados armazenados. Isso porque qualquer um que possa ter acesso, inclusive remoto, ao sistema para solucionar eventual problema técnico precisa ser devidamente conhecido para configuração da cadeia de custódia.

3.4. FUNCIONAMENTO E ALGUMAS FUNCIONALIDADES DOS SISTEMAS DE RECEPÇÃO E ARMAZENAMENTO DE DADOS

A pesquisa se baseou no acesso ao Manual de Configuração e Operação do Sistema Guardião (Versão Release 1.6.8 e Ver-

são do Aplicativo 3.2.8.78 – julho de 2013) da empresa Dígitro Tecnologia Ltda, obtido diretamente junto à empresa em formato impresso.

Importa dizer que este trabalho não pretende fazer qualquer apanhado sobre o funcionamento do sistema informático, mas apenas traçar em linhas gerais algumas funcionalidades que interessam para garantia do direito fundamental à prova e ao contraditório, bem assim estabelecer bases importantes para compreensão da cadeia de custódia da interceptação telefônica.

Assim, as chamadas direcionadas pela operadora de telefonia ou os dados desviados ingressam na plataforma que realiza a gravação em um determinado suporte (HD) e as informações referentes àquela chamada são armazenados em um banco de dados relacional, que podem ser acessados e manipulados. Em outras palavras, o *Hard Disk* (HD) em que ficam armazenados os áudios é diverso daquele em que estão armazenados os dados (metadados), mas são relacionados de tal forma que para cada áudio há os correspondentes dados dos metadados que, quando acionados remetem por *hiperlink* diretamente ao áudio vinculado.

Isso implica em que, malgrado se afirme que não é possível fazer exclusão de um áudio do sistema, qualquer alteração de dados na base gera um apagamento lógico, ou seja, não havendo mais relação entre dados e áudio o acionamento do *hyperlink* não será direcionado ao áudio e, portanto, o áudio fisicamente existe, mas não é encontrado.

Ademais, o módulo de *backup* do sistema permite alguns tipos de *backup* (manual ou por agendamento), mas se não for gerado é possível que haja sobrescrição, ou seja, a gravação por cima, o que implica também na possibilidade de perda definitiva de áudios. Isso fica muito claro quando, no início do Manual, a Dígitro informa que não se responsabiliza por

perdas de informações, devido a não observação, por parte do cliente, de procedimentos de *backup*, orientando para que regularmente armazene os dados também em mídia eletrônica (CD, DVD, etc.), de forma a possuir contingência externa.

É possível inserir no sistema durante a operação alguns dados cadastrais, como os alvos do monitoramento, os telefones monitorados, os alvarás judiciais que autorizam a interceptação com a data da expedição, o período e a data de validade.

Todavia, esse cadastro, como já dito antes, não torna o sistema ativo, porquanto ele não irá captar as chamadas de determinados alvos e telefones, que continuam a depender do desvio a ser realizado pela operadora de telefonia.

O problema é que o cadastro de alvará judicial não permite ao sistema bloquear a gravação das chamadas após o término do período de validade da autorização judicial, de tal sorte que esta gestão do período de interceptação fica a cargo exclusivo das operadoras de telefonia.

Há no sistema a possibilidade de ter acesso aos *logs* de eventos que, segundo o manual, se selecionada essa opção, será apresentada uma janela com informações estratégicas da execução do programa, recolhidas durante a utilização do Guardião, que são utilizadas para que se possa fazer a telemanutenção do sistema.

Essa funcionalidade, embora não tenha finalidade de controle da utilização do sistema para rastreamento dos agentes que manusearam ou manipularam a prova, deveria ser utilizada para tal. Alie-se essa ferramenta aos logs de gravação, que fornecem o histórico de gravações e revelam qualquer problema no processo de conversão das gravações, bem como ao histórico de *backup*, teremos um rastreamento pelo próprio sistema.

Há dois problemas: o primeiro é que esse rastreamento só forneceria informações até o *backup* e o segundo é que não há

sequer notícia de uma única autorização judicial conhecida que dê à defesa (ou seus eventuais assistentes técnicos) acesso ao sistema de logs do sistema de TI.

Com efeito, rastrear apenas até o *backup* é insuficiente quando nos deparamos com perda de áudios nas medidas cautelares de interceptações telefônicas e nos obriga a voltar à questão da cadeia de custódia. Em outras palavras, ainda que o sistema de TI responsável pela recepção e armazenamento das ligações telefônicas ou dados interceptados permita rastrear as etapas da operação até a geração do *backup* para assegurar a integridade do procedimento probatório, é imprescindível que, após a geração, seja criada uma rotina por lei ou fixada na decisão que defere a interceptação para permitir à defesa do acusado rastrear as fontes de prova e exercer o seu direito ao contraditório e à defesa. A não observância da rotina implica na quebra da cadeia de custódia e, por conseguinte, na perda da prova.

Ainda que a exata rotina de custódia da fonte de prova fosse definida, seria imprescindível que o acesso ao sistema de TI responsável pela recepção e armazenamento das ligações telefônicas ou dados interceptados fosse garantido à defesa. No entanto, ao argumento de que não se pode dar acesso à defesa por colocar em risco o sistema e o sigilo de outras operações em andamento (numa presunção de má-fé da defesa e seus eventuais assistentes técnicos), nega-se tal direito sem sequer conceber a criação de mecanismos que possam garantir esse acesso sem prejuízo dos demais interesses envolvidos.

CONCLUSÃO

Ao fim, verifica-se possível responder aos problemas iniciais de pesquisa, quais sejam: como garantir que as gravações de conversas são seguras e confiáveis, que não foram alteradas até chegar aos autos? Secundariamente: quais as consequ-

ências processuais penais de não existir um mecanismo que garanta a integridade do elemento de prova?

Parece muito claro que não há outra forma de garantir a segurança e confiabilidade das conversas gravadas senão pela cadeia de custódia da prova. É esse o mecanismo que garante a "mesmidade", ou seja, que aquela conversa gravada é exatamente a mesma do início ao fim, desde a gravação até seu ingresso nos autos do processo.

A regulamentação da cadeia de custódia no Código de Processo Penal introduzida pela Lei nº 13.964/2019 foi insuficiente, na medida em que se dirigiu apenas aos vestígios usados na prova pericial.

Todavia, a falta de regulamentação não afasta a necessidade de garantir a cadeia de custódia da prova nas cautelares probatórias, conhecidas como meios de obtenção de prova, e sua quebra deve implicar na consequência da inadmissibilidade. Trata-se de prova ilícita, que não garante a integridade, integralidade e "mesmidade" e, portanto, sua quebra implica na impossibilidade de ser admitida ou, se já constante dos autos, na sua exclusão física.

Como se verificou, é preciso adotar um procedimento detalhadamente registrado, fixados os elos entre as fases e as pessoas envolvidas em cada uma delas que servem para garantir a "mesmidade" do vestígio levado à condição de elemento de prova, a rastreabilidade e a confiabilidade, permitindo o exercício da defesa e do contraditório, inclusive a realização de eventual contraprova.

A única possibilidade no âmbito da interceptação telefônica é o acesso ao sistema de logs do sistema de TI. Todavia, importa reconhecer que essa é uma providência que só garante a cadeia de custódia até o *backup*. A partir daí, é preciso que exista um órgão responsável pela guarda e armazenamento das gravações, que seja obrigado a manter a identificação das

pessoas que tiveram acesso aos elementos, bem como registro de acesso com data e hora.

Assim, a não existência desse mecanismo conhecido como cadeia de custódia ou a quebra (também conhecido como ruptura) inviabiliza garantir o exercício dos direitos de defesa e do contraditório, de tal forma que o devido processo legal se mostra vulnerado em essência.

A consequência é a ilicitude da interceptação telefônica, tanto direta, devendo ser desentranhada para evitar a valoração pelo juiz dos elementos obtidos sem confiabilidade.

NOTAS

1. https://bit.ly/2XJKIDg

2. Disponível em https://bit.ly/2XHGoVd.

3. Decisão proferida no Processo 0.00.000.001328/2012-95, que tramitou junto ao Conselho Nacional do Ministério Público. Disponível em https://bit.ly/2TKUtQH.

4. Disponível em https://bit.ly/3dl1xel. Essa página hoje está desativada, mas a informação a respeito do sistema pode ser obtida na página da Câmara dos Deputados, disponível em https://bit.ly/2AilHqT.

5. Disponível em https://bit.ly/3gz4JoW. Veja comentário na nota anterior.

REFERÊNCIAS

Azevedo, Y. (2017). A importância da cadeia de custódia das provas para o devido processo legal. In Prado, G.; & Malan, D. (orgs.). *Ensaios sobre a cadeia de custódia das provas no processo penal brasileiro*, p. 106. Empório do Direito.

Badaró, G. (2018). A cadeia de custódia e sua relevância para a prova penal. In Sidi, R.; & Lopes, A. B. *Temas atuais da investigação preliminar no processo penal.* D'Plácido.

Brasil. (2014). *Portaria nº 89, de 28 de julho de 2014*. Ministério da Justiça. Secretaria Nacional de Segurança Pública. https://bit.ly/2AinBI3.

Brasil. (2012). *Diagnóstico da perícia criminal no Brasil***.** Ministério da Justiça. Secretaria Nacional de Segurança Pública. https://bit.ly/36NpjNN.

Brasil. (2018). Súmula vinculante 14. É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa. Supremo Tribunal Federal. In Supremo Tribunal Federal. *Aplicação das Súmulas no STF*. https://bit.ly/3di8DR8.

Carvalho, J. L. (2016). Cadeia de custódia e sua relevância na persecução penal. *Brazilian journal of forensic sciences, medical law and bioethics*, v. 5 (4), pp. 371-382. https://bit.ly/2AmqokS.

Chasin, A. A. da M. (2001). Parâmetros de confiança analítica e irrefutabilidade do laudo pericial em toxicologia forense. *Revista Brasileira de Toxicologia*, v. 14(1), pp. 40-46.

Dallagnol, D. M.; & Câmara, J. A. S. R. (2016). A cadeia de custódia da prova. In Salgado, D. de R.; & Queiroz, R. P. de (orgs.). *A prova no enfrentamento à macrocriminalidade* (2. ed.). Juspodium.

Dias Filho, C. R. (2002). Cadeia de custódia: do local do crime ao trânsito em julgado; do vestígio à evidência. In Moura, M. T. R. de A.; & Nucci, G. de S. (orgs.). *Doutrinas essenciais: processo penal*, 3. Revista dos Tribunais.

Edinger, C. (maio/jun. 2016). Cadeia de custódia, rastreabilidade probatória. *Revista brasileira de ciências criminais*, 120, pp. 237-257.

Espindula, A. (2009). *Perícia criminal e cível: uma visão geral para peritos e usuários da perícia* (3. ed.), p. 165. Millenium.

Ferrajoli, L. (2014). *Direito e razão: teoria do garantismo penal* (4a ed.). Zomer Sica, A. P.; Hassan Choukr, F; Tavares, J.; & Gomes, L. F. (tradutores). Revista dos Tribunais.

Gomes Filho, A. M. (2005). Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In Yarshell, F. L.; & Zanoide de Moraes, M. (orgs.). *Estudos em homenagem à Professora Ada Pellegrini Grinover*. DPJ.

Lopes, M.; Gabriel, M. M.; & Bareta, G. M. S. (jun. 2006). Cadeia de custódia: uma abordagem preliminar. *Visão Acadêmica, 7* (1). https://bit.ly/2yIMzzS.

Lopes Júnior, A. (2017). *Direito processual penal* (14. ed.). Saraiva.

Machado, V. P.; & Jezler Junior, I. (nov. 2016). A prova eletrônica-digital e a cadeia de custódia das provas: uma (re)leitura da Súmula Vinculante 14. *Boletim IBCCRIM*, 24(288), pp. 8-9.

Marinho, G. V. (2011). *Cadeia de custódia da prova pericial*. [Dissertação de Mestrado, Escola Brasileira de Administração Pública e de Empresas, Centro de Formação Acadêmica e Pesquisa, Rio de Janeiro].

Menezes, I. A..; Borri, L. A..; & Soares, R. J. (jan./abr. 2018). A quebra da cadeia de custódia da prova e seus desdobramentos no processo penal brasileiro. *Revista brasileira de direito processual penal*, 4(1), pp. 277-300. https://bit.ly/2AheF5U.

Moraes, A. L. Z. de. (jun. 2017). Prova penal: da semiótica à importância da cadeia de custódia. *Revista Brasileira de Ciências Criminais*, 132, pp. 117-138.

Osterburg, J. W.; & Ward, R. H. (1992). *Criminal investigation: a method for reconstructing the past*. Anderson Publish.

Prado, G. (set. 2004). Ainda sobre a "quebra da cadeia de custódia das provas". *Boletim IBCCRIM*, 22(262), pp. 16-17.

Prado, G. (2014). *Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos*. Marcial Pons.

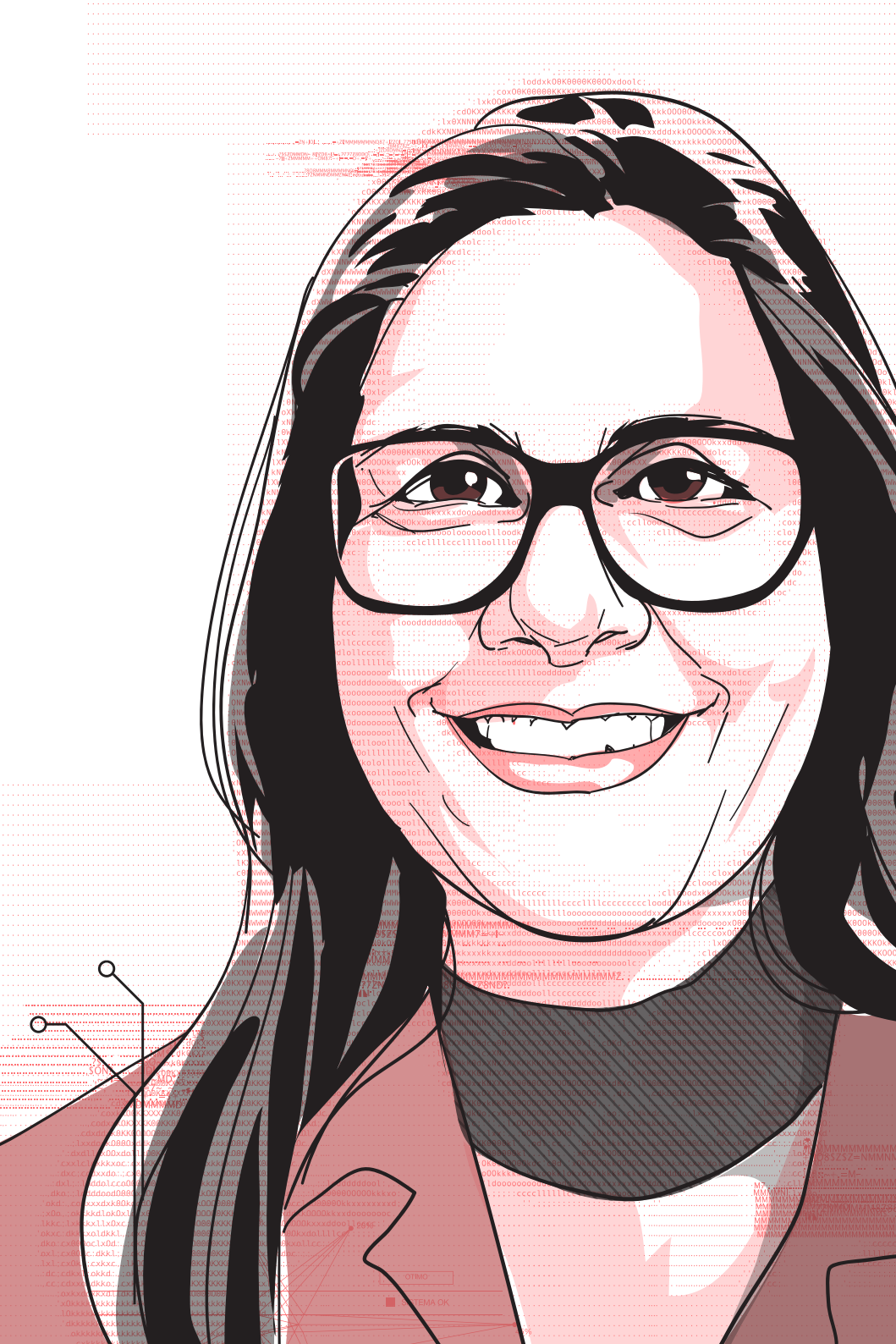
Santoro, A. E. R.; Tavares, N. L. F.; & Gomes, J. C. (mai./ago. 2017). O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia. *Revista Brasileira de Direito Processual Penal*, 3(2), pp. 605-632. https://bit.ly/2TSnOIV.

Santoro, A. E. R.; Tavares, N. L. F. (nov. 2019). Diagnóstico sobre o uso da interceptação telefônica no Brasil: uma análise quantitativa e comparativa dos dados até 2018. *Revista Brasileira de Ciências Criminais*, 161(27), pp. 101-130.

Scarance Fernandes, A. (2012). Tipicidade e sucedâneos de prova. In Scarance Fernandes, A.; Gavião de Almeida, J. R.; & Zanoide de Moraes, M. (coords.). *Provas no Processo Penal: estudo comparado*. Revista dos Tribunais.

Tonini, P. (2002). A prova no processo penal italiano. Martins, A. & Mróz, D (tradutoras). Revista dos Tribunais.

United Nations Office on Drugs and Crime. (2010). *Conscientização sobre o local de crime e as evidências materiais em especial para pessoal não-forense*. Nações Unidas. https://bit.ly/3cgkIF5.



14.

A NECESSIDADE DE VALORAÇÃO DAS PROVAS CIENTÍFICAS COMO GARANTIA MÍNIMA DE JUSTIÇA PROCESSUAL

Evanilda Godoi

INTRODUÇÃO

Ante os avanços tecnológicos e científicos, cada dia mais os magistrados necessitam de auxílio técnico para melhor compreender os fatos do litígio e, então, formar sua convicção acerca da verdade ou da falsidade dos enunciados probatórios trazidos ao processo. Neste contexto, é inegável que as relações entre processo e ciência estejam ainda mais estreitas, evidenciando um caminho sem volta. Assuntos inerentes particularmente ao campo da genética (*forensic science*), tais como investigação biológica de paternidade, problemas de identidade, análises de amostras biológicas (sangue, saliva, esperma, pelo) etc., são questões com as quais os juízes têm que lidar rotineiramente. Não por outra razão, a colaboração da ciência (levada ao processo judicial pelas provas científicas) para a formação do juízo do julgador é um fator que ganha cada vez mais importância na atividade probatória. Entretanto, na mesma proporção da sua inegável importância, cresce também a preocupação de que as decisões probatórias apoiadas em provas científicas se assumam como inquestionáveis ou irrefutáveis, encobrindo o risco de os juízes acreditarem que não seja necessário valorar esse tipo de prova, tampouco motivar as decisões judiciais delas decorrentes, de modo que bastaria seguir o que apontam os dados e justificar que houve prova científica.

Contudo, ao se analisar as provas científicas tendo a cadeia de custódia da prova como pressuposto, torna-se ainda mais preocupante a atuação do juiz na condução do processo. Isso porque sendo a cadeia de custódia o instituto que visa a garantia do acusado de que os procedimentos legais e seus direitos fundamentais foram devidamente observados durante todo o processo de obtenção dos elementos probatórios que instruem a acusação, imprescindível se faz um controle de admissibilidade desse tipo de provas.[1] Como se pretende demonstrar ao longo deste texto, caso as provas científicas

sejam admitidas sob o véu da infalibilidade, qualquer quebra da cadeia de custódia das provas tornar-se-ia imperceptível.

É preciso fixar a premissa de que a valoração das provas é uma das mais árduas tarefas dos magistrados, muitas vezes negligenciada por eles. Mas é também o cerne do processo judicial. Perguntas como "o que dizem os dados?", "o que deve ser acreditado?", são perguntas incipientes, mas cruciais. Naturalmente, os juízes não são seres capazes de dominar todos os assuntos técnicos que chegam para sua análise, por isso recorrem aos peritos, especialistas e cientistas. Mas como valorar o que dizem esses especialistas se o juiz necessita do especialista exatamente porque não domina o tema? Deve-se crer no perito/especialista baseado no argumento de autoridade? E mais, os argumentos baseados na autoridade do perito/especialista podem ser questionáveis? Ou, ainda, falaciosos? Todas essas questões exercem relevante impacto no processo de tomada de decisão dos juízes.

Para respondê-las, um importante passo é a desmistificação da prova científica ou da prova técnica de um modo geral.

SOBRE O MITO DA INFALIBILIDADE DA PROVA CIENTÍFICA

Ainda que nem sempre seja possível alcançar a verdade dos fatos, a averiguação dos enunciados fáticos no processo judicial deveria estar orientada à busca da verdade. É nesse sentido que Taruffo certa vez afirmou que "a ciência e o processo têm um objetivo em comum: a investigação da verdade" (2005, p. 1285). O emprego cada vez mais frequente da prova científica acaba por representar o emprego da ciência "como instrumento para a verificação da verdade sobre os fatos que devem ser analisados no contexto processual" (Taruffo, 2005, p. 1286). E, por tal razão, muitas vezes é concebida como determinante para a elucidação do caso.

Neste contexto, as provas científicas têm desempenhado um papel de destaque no desenvolvimento do processo. A chamada *forensic science* tem obtido avanços espetaculares e, por conseguinte, contribuído em muito para a resolução de numerosos problemas judiciais. Cite-se, como exemplo, a prova de DNA, que desde sua implementação tem desempenhado um papel de grande importância na atividade probatória, possibilitando elucidar casos que de outro modo seriam difíceis de solucionar.[2]

Entretanto, apesar da extraordinária contribuição que esse tipo de prova tem atribuído à atividade probatória, há que se adotar uma série de cautelas quanto à admissibilidade e valoração das provas científicas, em especial devido à ideia bastante equivocada de infalibilidade que se tem atribuído a essas provas. Essa ideia, por conseguinte, tem levado à propagação de uma prática de "beatificação desse universo probatório" (Gascón, 2010, p. 96). Em certo sentido, tanto a ideia de infalibilidade como a prática de beatificação dessas provas são assim porque, como explica Taruffo:

> a ciência está envolta em uma espécie de aura mitológica, e representa o símbolo do conhecimento certo e da verdade objetiva em torno a qualquer tipo de acontecimento. Simboliza também coisas que se supõem que estão além do nível natural de conhecimento das pessoas 'normais', como os advogados e os juízes. (Taruffo, 2005, p. 1287)

Esses símbolos do conhecimento, da certeza, da confiabilidade, são símbolos que se encontram muito presentes no imaginário popular, o que tem conduzido a certa falta de cautela e de controles sobre esse tipo de prova. Como bem explicam Marina Gascón e J.J. Molina,

> precisamente pelo fato de apresentarem-se como 'científicas' estas provas têm sido acompanhadas de uma aura de infalibilidade que tem freado, quando não claramente impedido, qualquer tentativa de revisão ou reflexão crítica sobre as mesmas. (Gascón Abellan & Lucena Molina, 2010, p. 96)

Há que se desfazer a crença de que as provas científicas não precisariam ser valoradas por estarem apoiadas em leis universais aplicadas de acordo com uma metodologia científica e que, por tal razão, "seus resultados podem ser considerados inquestionáveis ou fora de toda dúvida" (Gascón Abellan & Lucena Molina, 2010, p. 97). Com base nessas concepções (equivocadas), essas provas seriam admitidas no processo como provas dedutivas, dispensando-lhes qualquer inferência, é dizer, não necessitariam ser estruturadas mediante um raciocínio indutivo.

Com tudo, essa convicção de certeza absoluta é errônea e traz como consequência a perigosa propagação da crença de que "as decisões probatórias apoiadas em provas científicas se assumem como inquestionáveis ou irrefutáveis e, por conseguinte, desobriga o juiz de fazer um especial esforço para fundamentar racionalmente a decisão" (Gascón Abellán, 2007, p. 2).

As conclusões da literatura jurídica recente caminham no sentido de que a validade das provas científicas e a confiabilidade de seus resultados é algo que não se pode dar por certo, mas, sim, que depende de vários fatores.

O primeiro fator está relacionado à validade científica e metodológica da prova. Esse fator é de primordial importância e deve ser observado com rigor, pois as provas científicas podem ser realizadas por métodos científicos diferentes que nem sempre gozam do mesmo crédito na comunidade cien-

tífica, de modo que o grau de confiabilidade dessas provas pode aumentar ou diminuir de acordo com as técnicas ou métodos empregados.

Outro fator do qual depende diretamente a validez e confiabilidade das provas científicas refere-se à qualidade técnica, ou seja, a correta realização da prova no laboratório, que pode estar relacionada tanto à correção técnico-procedimental, como à correção técnico-científica. A correção técnico-procedimental representa todo o processo de análise da prova, desde o registro do vestígio ou da amostra até sua análise laboratorial. A correção técnico-científica diz respeito à sua correta realização no laboratório e seu grau de confiabilidade está diretamente relacionado aos controles e protocolos de realização da prova. De acordo com Gascón, "a coleta de evidências há que ser feita com sumo cuidado e a manutenção da cadeia de custódia é fundamental para que os indícios não percam seu valor probatório" (Gascón Abellan & Lucena Molina, 2010, p. 98).

Ainda, existem os riscos cognitivos inerentes a certas provas técnicas que tradicionalmente "têm um forte componente comparativo que os deixa inteiramente sob a supervisão de um especialista" (Gascón Abellan & Lucena Molina, 2010, p. 99), como impressões digitais e testes gráficos. Este também é o caso da psicologia forense que, da mesma forma que as outras ciências, experimentou um aumento expressivo nos últimos anos, especialmente no que diz respeito a casos que envolvem testemunhos. Ademais, há uma questão que certamente é clara, mas deve ser lembrada: o mito da infalibilidade das provas científicas oculta o risco de o juiz achar que não é necessário justificar sua decisão.

Pode-se afirmar, sem muito esforço, que a validade de uma prova científica e a confiabilidade de seus resultados depende diretamente da validade científica do método utilizado, da adoção de tecnologia apropriada e da observância de rigo-

rosos controles de qualidade. De resto, o juiz também deve sempre ter claro que "as leis científicas nas quais essas provas se baseiam são, na maioria dos casos, de natureza probabilística, e os resultados das mesmas devem ser interpretados usando estatísticas" (Gascón Abellan & Lucena Molina, 2010, p. 99), o que significa que "o resultado de uma prova científica é apenas uma simples probabilidade, por mais alta que seja" (Gascón Abellan & Lucena Molina, 2010, p. 99).

Desse modo, quando são realizadas em condições empíricas ótimas e utilizando-se de métodos cientificamente adequados, o grau de confiabilidade dos resultados daquela prova aumentam. A *contrario sensu*, se o ambiente empírico, o método ou as técnicas utilizadas, não são apropriados ou indicados pelos protocolos científicos, o grau de confiabilidade dessa prova diminui, quando não se anula.

Precisamente pelas considerações acima, pode-se dizer que certamente o problema mais importante que afeta a validade das provas científicas é a falta de controle processual da validade científica dessas provas. De fato, a falta de um controle sério sobre a validade ou confiabilidade dessas provas permite a entrada no processo da chamada *junk science*, elementos probatórios levados ao processo sem qualquer fundamento científico. Nas palavras de Marina Gascón, "verdadeiro lixo sem fundamento científico algum que às vezes é usado por especialistas e laboratórios como um interessante negócio" (Gascón Abellan & Lucena Molina, 2010, p. 99). As consequências podem ser desastrosas: erros judiciais, inocentes condenados, erros de identificação, etc.

O problema da confiabilidade das provas científicas foi trazido ao debate no famoso *Agente Orange Case* e nas diversas causas de amianto e Bendectina nos Estados Unidos. Conhecidos como *mass toxic torts*, esses processos foram importantes para deixar claro que

> os dados científicos podem ser pouco confiáveis ou insuficientes para apoiar uma conclusão acerca dos fatos em litígio, as provas periciais podem estar equivocadas ou ser confusas, os peritos podem não ser imparciais tampouco ter credibilidade, os juízes e jurados podem ser enganados na valoração dos dados científicos, as provas científicas podem ser aplicada de maneiras pouco apropriadas etc. (Taruffo, 2008, p. 98-99)

Taruffo resume de forma bastante didática as principais preocupações e os principais perigos inerentes a esse tipo de prova. É possível identificar nesse excerto que, mais uma vez, a necessidade de mudanças de paradigmas quanto à concepção de infalibilidade da prova científica e técnica se impõe. E essa necessidade urge não apenas quanto aos juízes, mas também em relação aos jurados, formados originalmente por pessoas 'comuns' da comunidade. Já houve um tempo em que fora proposto um júri formado apenas por especialistas para os casos em que essas provas fossem requeridas. Christian Dahlman (2015) relata que, em 1901, o juiz Hand publicou um artigo defendendo a posição de que esse tipo de situação (valorar a prova pericial ou o testemunho do expert) seria praticamente impossível para os membros do júri, de modo que, para solucionar esse problema, ele acreditava que o jurado deveria ser composto por especialistas. Assim, o procedimento de seleção deveria assegurar-se de que os membros do jurado fossem escolhidos entre pessoas com expertise no campo da controvérsia jurídica (Dahlman, 2015, pp. 4-5).

A normatização de critérios técnicos-científicos para auxiliar o juiz a avaliar as provas que chegam até ele seria uma possibilidade para amenizar o problema. Critérios tais como uma certificação de aptidão ou certificado de garantia de qualidade (controle de qualidade) atestando a qualidade interna

/ O PROBLEMA MAIS IMPORTANTE QUE AFETA A VALIDADE DAS PROVAS CIENTÍFICAS É A FALTA DE CONTROLE PROCESSUAL DA SUA VALIDADE CIENTÍFICA /

e externa do laboratório; as metodologias admitidas para o exame e que devem ser adotadas pelos laboratórios; a capacidade técnica dos especialistas que assinam o relatório final; os requisitos para a elaboração do laudo técnico; a definição de critérios mínimos de qualidade, dentre outros critérios. O objetivo seria estabelecer regras garantidoras da segurança jurídica das partes, da cadeia de custódia das provas mediante a devida preparação dos laboratórios e peritos responsáveis pelos exames, bem como o controle sobre as técnicas e métodos utilizados.

Por outro lado, a prova científica não pode ser transformada em um tipo de 'prova legal' que se sobrepõe ao princípio do livre convencimento motivado do juiz, ou seja, a referência à ciência não pode excluir a avaliação da prova, porque "a natureza científica da prova, por si só, não encerra a questão de seu valor probatório, que deve ser resolvido pelo tribunal em cada caso em virtude do princípio da livre valoração" (Gascón Abellan & Lucena Molina, 2010, p. 104). O juiz pode considerar confiável o resultado da prova científica e as conclusões alcançadas pelo perito, mas não basta a simples menção ao laudo. Deve-se demonstrar, ainda, seu raciocínio jurídico até a decisão final.

No processo judicial, a distinção entre a tarefa do perito e a do juiz consiste em o primeiro expressar o que os dados dizem, e a do juiz em avaliar esses dados à luz de outros dados e provas disponíveis no processo. Em outras palavras, a avaliação dos elementos probatórios deve levar em consideração todo o conjunto probatório trazido ao conhecimento do juiz pelo processo. O juiz deve ser o *gatekeeper* da prova científica no processo, ou seja, ele deve ser responsável pelo controle processual de admissibilidade. No contexto atual, o juízo de admissibilidade ainda é um dos principais problemas apresentados pelas provas científicas.

Historicamente, a tentativa de estabelecer um controle sobre a prova científica se deu pela primeira vez no caso *Daubert vs. Merrel Dow Pharmaceuticals, Inc.*[3] em 1993, pela Corte Suprema dos Estados Unidos. Naquela ocasião, o juiz Blackmum ditou "um sintético tratado de epistemologia, com a finalidade de apontar os critérios aos quais deveria o juiz se deter para admitir ou excluir os meios de prova científica apresentados pelas partes" (Taruffo, 2008, p. 283). Na realidade, a Corte americana tentou implantar critérios para guiar o juiz na seleção preliminar das provas científicas, a fim de permitir a admissibilidade unicamente daquelas baseadas na 'boa ciência'.

Esses critérios constituem o denominado *Daubert Test* e são, basicamente: a contrastabilidade e a falseabilidade da teoria ou da técnica aplicada; o conhecimento da *ratio de error* real ou potencial; a publicação de artigos ou dados em revistas científicas com *peer-review*; a aceitação geral de tais dados por parte da comunidade científica relevante; e, ainda, somente deveriam ser admitidas no processo quando relevantes para a decisão sobre os fatos em litígio (Taruffo, 2008, p. 99). Os critérios formulados no caso Daubert foram confirmados por outras resoluções da Corte Suprema dos Estados Unidos, o que culminou na emenda à regra 702 das *Federal Rules of Evidence*, nos Estados Unidos.

Os desafios e tarefas pendentes no campo da prova científica ainda são muitos. Um dos caminhos a ser trilhado é tentar estabelecer uma 'orientação' que possa ser observada na realização das provas científicas, e que também possa ajudar o juiz a interpretar e a valorar os dados aportados ao processo por essas provas, tendo em vista evitar o risco da má interpretação ou de sobrevaloração das provas científicas.

Mas como valorar? Como estabelecer a verdade?

Como já tivemos a oportunidade de nos manifestar em outras oportunidades,[4] a valoração das provas científicas (e

das provas de um modo geral) é tarefa que traz consigo um legítimo dilema: o juiz necessita buscar respostas entres os especialistas (*experts*), já que não possui conhecimento técnico para julgar o caso que é colocado à sua frente, mas esbarra no problema de ter que distinguir entre as chamadas *good Science e junk Science*. Como o juiz fará a valoração da prova se não possui conhecimentos técnicos ou científicos para julgá-la? Como ele vai trabalhar com a categoria da verdade?

A VALORAÇÃO RACIONAL DAS PROVAS

Uma vez afastada a ideia de infalibilidade das provas científicas, é preciso pensar em como analisar referidas provas. O primeiro passo é ter clareza de que as provas científicas não são portadoras de uma verdade absoluta que vá revelar os fatos do mundo real. Mas o que se deve entender por valoração racional das provas?

Para Nieva Fenoll, a valoração das provas seria "a atividade de percepção por parte do juiz dos resultados da atividade probatória que se realiza em um processo" (Nieva Fenoll, 2010, p. 34). Marina Gascón entende que seria a

> verificação dos enunciados fáticos introduzidos no processo através dos meios de prova, assim como no reconhecimento aos mesmos de um determinado valor ou peso na formação da convicção do julgador sobre os fatos que se julgam (Gascón Abellán, 2010, pp. 140-141).

A seu turno, Taruffo acredita que a atividade de valoração das provas judiciais tem por objetivo "estabelecer a conexão final entre os meios de prova apresentados e a verdade ou falsidade dos enunciados sobre os fatos em litígio" (Taruffo, 2008, p. 132).

Embora a valoração das provas seja o núcleo essencial do processo de tomada de decisão judicial, esse objeto esteve ao largo das investigações acadêmicas por bastante tempo, dado o desinteresse da teoria do direito pela análise probatória. Mas como muito bem colocado por William Twining,

> a investigação e o exame dos fatos, bem como a argumentação sobre questões de fato controvertidas nos diferentes contextos jurídicos requerem tanta atenção e tanta exigência intelectual como as questões de interpretação e argumentação sobre questões de Direito (Twining, 2009, p. 318).

Atualmente, já é possível encontrar diversos pesquisadores se dedicando ao tema. Ao se debruçar sobre a temática, Christian Dahlman (2015) propõe um método para a avaliar a confiabilidade dos argumentos dos experts, chamado por ele de *expertology*, a partir de critérios que podem ser utilizados por pessoas que não têm conhecimento científico ou técnico sobre o tema em litígio. Apesar de o esse método ter sido pensado para o modelo judicial estadunidense, em que o perito é ouvido como testemunha, acredita-se que possa ser também aplicado ao modelo brasileiro.

Em apertada síntese, defende o autor que a *expertology* pode ser utilizada para avaliar argumentos de autoridade do perito e argumentos que questionam essa autoridade. A confiabilidade de um perito pode ser questionada por diversos motivos, tais como a falta de competência ou capacidade técnica, a parcialidade e falta de justificação. O autor sugere a utilização da Fórmula de Bayes (Dahlman, 2015, pp. 8-11) para aclarar os diferentes efeitos sobre a confiabilidade do perito, o que, a princípio, e pensando na realidade brasileira, tornaria o processo de análise probatória ainda mais penoso.

Mas Dahlman oferece um método ou esquema avaliativo perfeitamente aplicável a qualquer situação, não apenas quando se fala em provas científicas, a partir de argumentos *ad hominem*. O autor chama de argumentos *ad hominem* positivos ao referir-se a argumentos sobre a confiabilidade do perito. Esses argumentos podem ser divididos em duas categorias principais: as relacionadas à competência e as relacionadas à motivação do perito. Os atributos que se relacionam com a competência seriam os relativos à formação acadêmica, formação profissional, experiência. Por sua vez, os atributos relacionados com as motivações seriam a objetividade e dedicação do perito. Segundo Dahlman (2015, pp. 5-6), um argumento *ad hominem* positivo afirma que o atributo faz com que a pessoa seja mais confiável. A contrario sensu, um argumento *ad hominem* negativo afirma que o atributo faz com que a pessoa seja menos confiável. Tomando emprestado o exemplo utilizado pelo autor, pode-se afirmar que o argumento de que uma pessoa é confiável como expert em temas de medicina porque tem um título universitário em medicina é um exemplo de um argumento *ad hominem* positivo. O argumento de que ela não é confiável como um expert em relação aos efeitos secundários de um determinado medicamento porque ela é empregada da companhia farmacêutica que fabrica o referido medicamento, é um argumento *ad hominem* negativo. Em *expertology*, segue o autor, "argumentos *ad hominem* positivos podem fazer referência aos diplomas e postos de trabalho, enquanto os argumentos *ad hominem* negativos podem indicar uma parcialidade ou más referências de desempenho (Dahlman, 2015, p. 6). Alguns argumentos *ad hominem* são sólidos, enquanto outros são falácias, como por exemplo, nos casos em que o atributo é irrelevante para a confiabilidade da pessoa, bem como nos casos em que o atributo é relevante, mas seu efeito sobre a confiabilidade da pessoa é exagerado.

A seu turno, Marina Gascón, afirma que "o juiz há de ser livre para valorar discricionariamente a prova, mas não pode ser livre para deixar de observar uma metodologia racional na fixação dos fatos controvertidos" (Gascón Abellán, 2010, p. 144). Seguindo esse raciocínio, a busca por modelos de valoração racional das provas há de pressupor a busca por técnicas ou esquemas que funcionem como diretivas para os juízes. É dizer, há que se buscar metodologia ou esquemas (ou esquemas argumentativos, esquemas de atributos, de questões) que sejam mais adequados para se alcançar a finalidade da atividade probatória. E, ainda, que permita determinar o grau de probabilidade aceitável no raciocínio probatório e exercer, posteriormente, o controle sobre as decisões tomadas em matéria probatória.

Nesse cenário, tem-se o modelo de probabilidade lógica ou indutiva como modelo de valoração racional das provas. De acordo com esse modelo, a probabilidade de um certo enunciado de fatos ser verdadeiro é determinada em razão do grau de confirmação que os elementos probatórios lhe atribuem. De acordo com Ferrer Beltrán, "a probabilidade que um elemento de análise aporta à uma hipótese é uma relação lógica entre duas proposições, ou seja, o grau em que uma preposição implica em outra" (Ferrer Beltrán, 2007, p. 95). Dito de outro modo, a probabilidade de uma hipótese se baseia em sua conexão lógica com as provas, com o conjunto probatório, e mede o apoio indutivo que essas provas proporcionam às hipóteses. Trata-se de esquemas de confirmação nos quais a probabilidade de uma hipótese depende do apoio que lhe proporcionam as provas aportadas ao processo. Pode também ser visto como um modelo de racionalização de análise do conjunto probatório baseado em um procedimento de eliminação de hipóteses.

Afirmar que uma hipótese é provável significa que ela é demonstrável, que é possível encontrar a hipótese mediante

inferências a partir das provas disponíveis. No entanto, não basta que o conjunto probatório proporcione alto grau de apoio à hipótese. É necessário que esse mesmo conjunto probatório permita excluir hipóteses alternativas. A partir desta condição, propõe-se a utilização de esquemas valorativos baseados no grau de confirmação. Nessa proposta, a probabilidade de um enunciado de fatos ser verdadeiro se verifica em razão do grau de confirmação que os elementos de prova lhe atribuem. A probabilidade é medida em termos de apoio indutivo ou graus de confirmação e necessita de dois requisitos básicos, o da confirmação e da não refutação.

Nos moldes do requisito da confirmação, "uma hipótese *h* vem confirmada por uma prova *p* se existe um nexo causal ou lógico entre ambas que faça com que a existência desta última constitua uma razão para aceitar a primeira" (Gascón Abellán, 2005, p. 159). Esse grau de confirmação de veracidade da hipótese, aumenta ou diminui a partir de algumas variantes ou elementos: (i). o fundamento cognoscitivo e o grau de probabilidade expresso pelas regras utilizadas (quanto mais seguro e preciso o tipo de conexão entre a hipótese e as provas, maior será o grau de confirmação daquela hipótese); (ii). a qualidade epistêmica das provas que a confirmam; (iii). o número de passos inferenciais que compõem a cadeia de confirmação (quanto maior o número de passos inferenciais que separam a hipótese das provas que a confirmam, menor será a probabilidade de confirmação desta hipótese) e (iv). a quantidade e variedade de provas ou confirmações (quanto mais variadas sejam as provas, maior será o grau de confirmação da hipótese, pois a variedade de provas proporciona uma imagem mais completa dos fatos).

O requisito da não refutação, como o próprio nome já indica, determina que para que uma hipótese seja aceita como verdadeira é necessário que, além de confirmada, não seja refutada por quaisquer das demais provas disponíveis. Aqui re-

side um argumento forte em favor da obrigação de motivação das decisões judiciais no que se refere à valoração das provas.

Todos esses critérios para a valoração das provas são de fundamental importância para auxiliar o juiz na árdua tarefa de decidir sobre o fatos, mas no que se refere às provas científicas, deve o juiz, do mesmo modo, adotar a perspectiva racionalista de valoração das provas, que como bem explica Taruffo,

> não implica na negação da liberdade ou da discricionariedade na valoração pelo juiz, o que representa o núcleo do princípio da livre convicção, mas impõe que o juiz efetue suas valorações segundo uma discricionariedade guiada por regras da ciência, da lógica e da argumentação racional. (Taruffo, 2005, pp. 1296-1297)

A NECESSIDADE DE MOTIVAÇÃO DAS DECISÕES COMO GARANTIA PROCESSUAL DO ACUSADO

Todo o processo de análise e raciocínio probatório dos juízes só poderá ser externado e submetido ao controle, ao mesmo tempo em que garante às partes o seu direito recursal, mediante a motivação ou justificação das decisões judiciais. Exigência constitucional em nosso ordenamento jurídico, muitas vezes burladas por alguns profissionais do judiciário, ela é a real garantia do acusado de que foi submetido a uma análise e julgamento justos.

A motivação ou justificação da decisão judicial é instrumento para garantir que a decisão não seja arbitrária, para garantir que o poder discricionário que possui o juiz para interpretar e aplicar o direito seja exercido racionalmente. Motivar uma decisão consiste em justificá-la, consignando as razões que permitam entendê-la como correta ou aceitável. Tem por finalidade facilitar o controle público da decisão (pela

sociedade); facilitar o controle interno das decisões judiciais (pelas partes, para exercer o direito de recurso / de contraditório e ampla defesa) e teria ainda uma função preventiva em relação à atuação do juiz (inibindo uma atuação arbitrária). A exigência de fundamentação das decisões judiciais, explica Aarnio, "não pode mais ser interpretada apenas como um requisito formal, mas como um requisito de justificação e imparcialidade" (Aarnio, 1991, p. 26).

Uma das características das constituições contemporâneas é que elas geralmente incluem, explícita ou implicitamente, normas vinculativas para a argumentação do juiz, que estabelecem o dever de fundamentar suas decisões, sob pena de nulidade. Esta é precisamente a obrigação de motivar publicamente as decisões judiciais. Como explica Gascón, remetendo à Bentham, "a motivação, como manifestação 'pública' das razões da decisão, ajuda a garantir sua racionalidade" (Gascón Abellán, 2010, pp. 178-179) e possibilita reconstruir o raciocínio jurídico e controlar sua racionalidade na fase recursal.

Ao justificar um enunciado normativo utilizado, o juiz deve proporcionar argumentos, razões, que permitam sustentar a validez e correção da sua decisão. Na mesma esteira, quando se defende a justificação também da matéria fática, é esperado do juiz que ofereça razões que permitam sustentar que determinado enunciado fático é verdadeiro ou provável. A decisão justificada em matéria fática há de trazer os atos de prova, de todas as provas do processo, os critérios de valoração utilizados (porque acreditou nas testemunhas A e B e não acreditou na C, por exemplo) e os resultados dessa valoração.

Como explica Aarnio, essa exigência de fundamentação de todas as decisões judiciais implica, inclusive, uma redefinição da própria ideia de certeza no Direito, pois já não é mais interpretada unicamente como uma exigência formal de previsibilidade, mas também como um requisito de justificabili-

dade e imparcialidade. Nas palavras do autor, “a expectativa de segurança jurídica *stricto sensu* significa que todo cidadão tem o direito de esperar proteção jurídica; em outras palavras: o tribunal ou outro órgão adjudicante tem a obrigação legal de dar uma resposta ao cidadão que solicita proteção jurídica. E este é um direito legal básico de todo cidadão na sociedade” (Aarnio, 1991, p. 26). Ainda segundo o autor,

> em uma sociedade moderna, as pessoas exigem não apenas decisões dotadas de autoridade, mas também exigem razões. A responsabilidade do juiz se tornou cada vez mais a responsabilidade de justificar suas decisões. A base para o uso do poder pelo juiz reside na aceitabilidade de suas decisões e não mais na posição formal de poder que ele possa ter. Nesse sentido, a responsabilidade de oferecer justificações é, especificamente, uma responsabilidade de maximizar o controle público da decisão. Assim, a apresentação da justificação é sempre também um meio de garantir, de forma racional, a existência de segurança jurídica na sociedade.” (Aarnio, 1991, p. 26).

No que diz respeito à justificação dos fatos, significa especificamente que a prova "admitida e praticada é levada em consideração para justificar a decisão que se adote" (Ferrer Beltrán, 2003, p. 29). Ao, por exemplo, adotar o modelo de probabilidade lógica ou indutiva como modelo de valoração da prova, o juiz deve reconhecer a obrigação discursiva de fundamentar de modo completo e conclusivo a probabilidade da hipótese aceita por ele como comprovada no caso em disputa.

A obrigação de motivar refere-se tanto aos enunciados de fato que se declarem provados como quanto aos que se declarem não provados. Apenas mediante uma declaração pública

e completa de todas as razões para aceitar como provado ou não provado um determinado fato é que se pode considerar completo o processo de justificação da decisão judicial e, portanto, cumprida a exigência constitucional de motivação de todos os atos de autoridade, inclusive as decisões discricionárias dos magistrados.

A importância da obrigação de motivar as decisões judiciais, principalmente em relação aos fatos, que é onde o juiz tem um maior poder de discricionariedade (ou arbitrariedade, imbuído pela adoção do princípio da livre valoração em sua concepção mais subjetiva), reside em razões de ordem extraprocessual, vinculadas ao controle externo ou público da decisão; e em razões endoprocessuais, vinculadas à necessidade de estabelecer também controle interno ou processual da racionalidade da decisão, controle esse a ser exercido por meio de recursos.

Nas palavras de Andrés Ibáñez, "efetivamente, a exigência de motivação responde a uma finalidade de controle do discurso, neste caso probatório, do juiz, com objetivo de garantir, na medida do possível, a racionalidade de sua decisão, dentro do marco da racionalidade jurídica" (Andrés Ibáñez, 1992, p. 292). Para tanto, o juiz deve fazer um exame detalhado das provas e explicar por que deu relevância a cada meio probatório, justificando "por que acreditou em dois testemunhos e deixou de acreditar em três ou por que deu mais credibilidade a um laudo pericial que a outro (Andrés Ibáñez, 1992, p. 293). Em suma, o juiz precisa fazer muito mais do que um simples registro dos dados no processo judicial.

CONSIDERAÇÕES FINAIS

Mesmo as provas científicas, que geralmente gozam de um status privilegiado na argumentação jurídica (mas não deviam), precisam ser explicitamente justificadas em conso-

nância com os critérios de racionalidade igualmente aplicáveis às provas de um modo geral. Deve o juiz contextualizar as conclusões do perito com as demais provas carreadas ao processo, interpretando as provas científicas como um meio de prova cuja força reside na racionalidade de suas conclusões e não meramente no argumento de autoridade.

Os desafios e tarefas pendentes no campo das provas científicas são desafiadores. Faz-se necessário desenvolver metodologias, técnicas, esquemas argumentativos que possam auxiliar na valoração da prova científica, na análise de sua admissibilidade, na sua interpretação e motivação, de modo a possibilitar ao juiz identificar situações em que a prova científica não deva ser admitida no processo. Um dos primeiros parâmetros para atingir esse objetivo, como dito, é ter consciência de que as provas científicas não são portadoras de uma verdade absoluta, que vai desnudar os fatos e desvelar a verdade. Há que se ter em conta as falibilidades dessas provas, pois são 'construídas' por pessoas (em nosso sistema de *civil law*, por um terceiro estranho ao processo), sendo, por conseguinte, suscetíveis ao erro humano.

O juiz tem que continuar sendo o titular da (e responsável pela) decisão sobre os fatos, não se podendo deixar substituir pelo perito. A correta valoração das provas e a sua subsequente justificativa são, em conclusão, condições de legitimidade e validade de toda e qualquer decisão judicial. Desse modo, objetiva-se contribuir para uma decisão mais acertada, na medida em que uma das exigências mais importantes de uma sociedade verdadeiramente democrática é justificação racional das decisões judiciais.

NOTAS

1. Sobre a cadeia de custódia da prova veja-se, por todos: Prado, G. (2019). *A cadeia de custódia da prova no processo penal.* Marcial Pons.

2. Veja-se, a modo de exemplo, o excepcional trabalho desenvolvido pelo *Innocence* Project, organização engajada em reverter a condenação de inocentes com a produção de novas provas obtidas a partir de exames de DNA. https://bit.ly/3eB16gv.

3. Daubert vs. Merrel Dow Pharmaceuticals, Inc., 509, U.S. 579 (1993).

4. Sobre a valoração das provas científicas, consultar Godoi Bustamante, E. N. (2015). Provas científicas e teorias da verdade: análise introdutória acerca da necessidade de uma mudança de paradigmas. In *Processo penal democrático* (1ª ed.), v. 1, pp. 10-31. Fórum.; e Godoi Bustamante, E. N. (2016). Pruebas científicas: sobre el mito de infalibilidad y la búsqueda por parámetros para su valoración. In Villanueva, R.; Marciani, B.; Lastres, P. (orgs.). *Ensayos sobre prueba, argumentación y justicia*, (1ed.), pp. 139-156. Fondo Editorial, PUC del PERU. Sobre a busca por parámetros de valoração racional da prova no proceso judicial, consultar Godoi Bustamante, E. N. (2013). *Decidir sobre los Hechos: un estudio sobre la valoración racional de la prueba judicial*, (1ª ed.). Bubok.; e Godoi Bustamante, E.N. (2014). A valoração racional das provas no processo judicial: uma aproximação do tema. In Hermenêutica [Recurso eletrônico on-line] XXII Encontro Nacional do CONPEDI / UNINOVE, 1ª ed., v. 1, pp. 407-428. Funjab.

REFERÊNCIAS BIBLIOGRÁFICAS

Aarnio, A. (1991). *Lo racional como lo razonable: un tratado sobre la justificación jurídica*. Centro de Estudios Constitucionales.

Andrés Ibáñez, P. (1992). Acerca de la motivación de los hechos en la sentencia penal. *DOXA Cuadernos de Filosofía del Derecho*, v. 12. Marcial Pons.

Dahlman, C. (2015). Appeal to Expert Testimony – A Bayesian Approach. In Bustamante T.; & Dahlman C. (Orgs.). *Argument Types and Fallacies in Legal Argumentation*. Springer.

Gascón Abellan, M.; & Lucena Molina, J.J. (nov. 2010). Pruebas científicas: la necesidad de un cambio de paradigma. *Jueces para la democracia*, vol. 69.

Gascón Abellán, M. (2010). *Los hechos en el derecho* (3. ed.). Marcial Pons.

Gascón Abellán, M. (2007). Validez y valor de las pruebas científicas: la prueba del ADN. *Cuadernos Eletrónicos de Filosofía del Derecho*, vol. 15, p. 02.

Gascón Abellán, M. (2005). Sobre la posibilidad de formular estándares de prueba objetivos. *Doxa, Cuadernos de Filosofía del Derecho*, vol. 28. Marcial Pons.

Godoi Bustamante, E. N. (2016). Pruebas científicas: sobre el mito de infalibilidad y la búsqueda por parámetros para su valoración. In Villanueva, R.; Marciani, B.; & Lastres, P. (Orgs.). *Ensayos sobre prueba, argumentación y justicia* (1ª ed.), pp. 139-156. Fondo Editorial, PUC del PERU.

Godoi Bustamante, E. N. (2015). Provas científicas e teorias da verdade: análise introdutória acerca da necessidade de uma mudança de paradigmas. In *Processo penal democrático* (1ed.), vol. 1, pp. 10-31. Fórum.

Godoi Bustamante, E.N. (2014). A valoração racional das provas no processo judicial: uma aproximação do tema. Hermenêutica [Recurso eletrônico on-line] XXII Encontro Nacional do CONPEDI / UNINOVE (1ª ed.), vol. 1, pp. 407-428. Funjab.

Godoi Bustamante, E. N. (2013). *Decidir sobre los Hechos: un estudio sobre la valoración racional de la prueba judicial* (1ª. ed.). Bubok.

Nieva Fennol, J. (2010). *La valoración de la prueba*. Marcial Pons.

Prado, G. (2019). *A cadeia de custódia da prova no processo penal*. Marcial Pons.

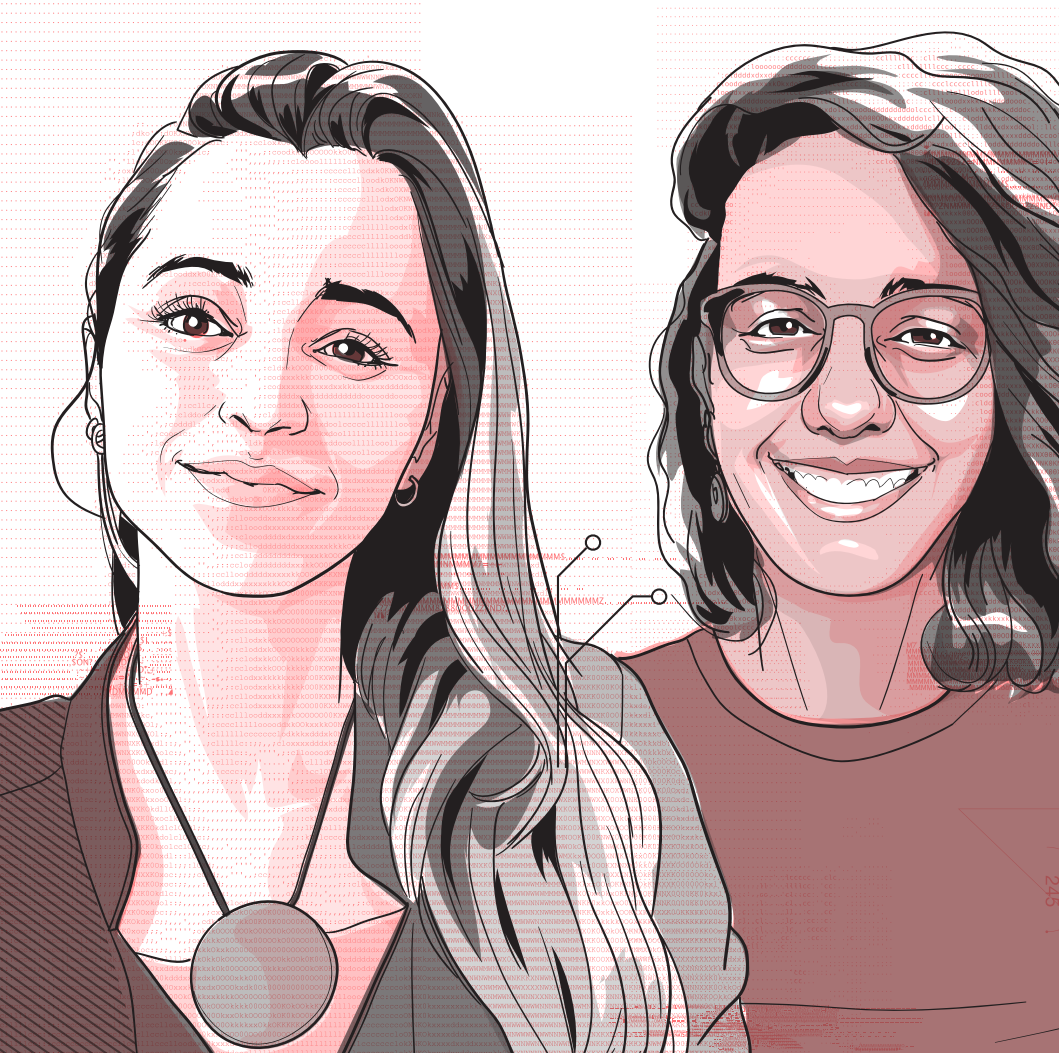
Taruffo, M. (2008). *La Prueba*. Marcial Pons.

Taruffo, M. (2005). Conocimiento Científico y estándares de prueba judicial. Carbonell, M.; & Salazar, P. (tradutores). *Boletín Mexicano de Derecho Comparado*, ano XXXVIII (114).

Ferrer Beltrán, J. (2007). *La valoración racional de la prueba*. Marcial Pons.

Ferrer Beltrán, J. (2003). Derecho a la prueba y racionalidad de las decisiones judiciales. *Jueces para la Democracia*, nº 47.

Twining, W. (2009). De nuevo, los hechos en serio. *DOXA Cuadernos de Filosofía del Derecho*, nº 32, pp. 317-340. Marcial Pons.



15.

A LEI ANTICRIME E O PROCESSAMENTO DE DADOS GENÉTICOS E BIOMÉTRICOS PELO ESTADO BRASILEIRO: UM PROJETO EM EXPANSÃO

Nathalie Fragoso

Clarice Tavares

Nos últimos anos, o Brasil investiu esperança e recurso público na adoção e disseminação de novas tecnologias à rotina de suas agências penais. Investimentos na expansão da Rede Integrada de Bancos de Perfis Genéticos,[1] na disponibilização de ferramentas para a integração[2] e análise massiva de dados de segurança pública e na utilização de tecnologias biométricas[3] são exemplos desses esforços, todos mobilizados sob a justificativa de ganho em eficiência na prevenção, investigação e processamento de crimes. A adesão a tais métodos, no entanto, é incrementada, e em alguns casos inaugurada, antes que se estabeleça e amadureça o debate sobre o tratamento de dados pessoais pelo poder público, quando em questão a segurança pública e a administração da justiça criminal.

No plano normativo, questões sensíveis foram recentemente alteradas pela chamada Lei Anticrime, a Lei nº 13.694/2019. O projeto do qual herdou a alcunha, proposto pelo então ministro da Justiça e da Segurança Pública, Sérgio Moro, e amalgamado ao projeto do anterior ministro da Justiça, Alexandre de Moraes, apostou no fortalecimento das capacidades de vigilância das autoridades de investigação por meio da tecnologia, entre elas a criação e expansão de bancos de dados sensíveis para a identificação de pessoas.[4]

O presente artigo pretende abordar: (i) as principais alterações promovidas pela Lei nº 13.964/2019, no que tange ao processamento de dados biométricos e genéticos na prevenção, investigação e processamento de crimes; e (ii) delinear questões problemáticas no trato de dados biométricos e genéticos[5] na rotina da segurança pública e da justiça criminal.

1.

A coleta de DNA, para a identificação do perfil genético de um indivíduo, relacionada a propósitos criminais foi inserida na legislação brasileira com a aprovação da Lei 12.654/2012,

passando a constar na Lei de Identificação Criminal (Lei 12.037/2009) e na Lei de Execução Penal - LEP (Lei 7.210/1984). Na Lei de identificação Criminal, está condicionada à demonstração da sua essencialidade para a investigação criminal e à autorização judicial, alinhando-se ali, portanto, ao propósito da fixação da autoria delitiva. No caso da LEP, o dispositivo foi inserido no capítulo da "classificação" e se aplica a todos os condenados pelo cometimento doloso de crimes com grave violência contra a pessoa e hediondos.

O propósito, nesse último caso, não responde à instrução processual no caso concreto; mas à alimentação do banco de perfis genéticos, que poderá ser acessado para instruir investigações futuras, em havendo inquérito instaurado (art. 9-A, §2º, da Lei 7.210/84), e para a identificação de pessoas desaparecidas (Decreto 7.950/13). O projeto de lei anticrime pretendia alterar o art. 9º-A da Lei de Execução Penal, tornando compulsória a identificação de todos os condenados por quaisquer crimes dolosos, independente do trânsito em julgado – e da gravidade da conduta, portanto. Durante a tramitação das Casas Legislativas, a alteração do caput foi afastada. Contudo, outros pontos problemáticos da lei foram sancionados, como o dispositivo que estabelece que a recusa em se submeter ao procedimento de identificação do perfil genético constitui falta grave (art. 9º-A, §8º e art. 50, VIII, da LEP).

Quanto à proteção desses dados, o §1º do art. 9º-A da LEP prevê que a regulamentação deverá fazer constar garantias mínimas de proteção de dados genéticos, deixando de abordá-las na lei. Dois parágrafos que dispunham sobre o uso destes dados — limitando o uso único e exclusivo da coleta de dados para fins de identificação de perfil genético (art. 9º-A, §5º) e prevendo o descarte da amostra coletada, uma vez identificado o perfil genético, para impedir que o dado coletado seja usado para fim diverso (art. 9º-A, §6º) — sofreram veto presidencial.

Na Lei da Identificação Criminal, a lei anticrime modificou o termo de exclusão do perfil genético. Segundo a redação proposta e aprovada para o art. 7º-A, a exclusão está condicionada à absolvição ou ao requerimento da/o afetada/o, passados vinte anos desde o cumprimento da pena; quando antes estava condicionada ao término do prazo de prescrição do delito, independentemente de solicitação.

Além desses dispositivos, regulam o processamento de dados genéticos no Brasil o Decreto 7.950/2013 e as resoluções do Comitê Gestor da Rede Integrada de Bancos de Perfis Genéticos, documentos com status infralegal. Na Resolução 10/2018, consta o procedimentos de coleta obrigatória de material biológico; a Resolução 12/2019 regulamenta as auditorias dos bancos; na Resolução 14/2019, o Manual de Procedimentos Operacionais da RIBPG.[6] A Lei da Identificação Criminal estabelece ainda limites quanto às informações passíveis de armazenamento (art. 5-A da Lei 12.037/2009)

Outra novidade da Lei Anticrime foi a criação do Banco Nacional Multibiométrico e de Impressões Digitais, para o armazenamento de dados de registros biométricos, de impressões digitais, íris, face e voz, para subsídio de investigações criminais (art. 7-C, § 1º, da Lei 12.037/2009). Nos termos da lei, constarão do banco registros colhidos em investigações criminais ou por ocasião da identificação criminal (art. 7-C, § 2º da Lei 12.037/2009), os dados de presos provisórios ou condenados (art. 7-C, § 3º da Lei 12.037/2009), e dados de bancos geridos por órgãos dos Poderes Executivo, Legislativo e Judiciário das esferas federal, estadual e distrital, inclusive pelo Tribunal Superior Eleitoral e pelos Institutos de Identificação civil (art. 7-C, §4º da Lei 12.037/2009).

No caso de bancos de dados de identificação de natureza civil, administrativa ou eleitoral, a integração fica limitada a impressões digitais e às "informações necessárias para iden-

/ A LEI ANTICRIME EXPANDE AS BASES DA IDENTIFICAÇÃO DE PESSOAS NA ADMINISTRAÇÃO DA JUSTIÇA CRIMINAL E NA SEGURANÇA PÚBLICA /

/ A LEI INTENSIFICA O TRATAMENTO DE DADOS, ARREFECE CONTROLES, NÃO ENDEREÇA AS LACUNAS LEGAIS /

tificação do seu titular". A integração depende da realização de acordo ou convênio com a unidade gestora do respectivo banco (art. 7-C, § 6º) e sua regulamentação, quanto à formação, gestão e o acesso são incumbidas ao Poder Executivo Federal (art. 7-C, § 11).

O banco é sigiloso e o acesso de autoridades policiais e do Ministério Público, no caso de inquérito ou ação penal instauradas, poderá ser concedido pelo juiz competente (art. 7-C, § 10).

2.

A lei anticrime expande as bases sobre as quais se opera a identificação de pessoas na administração da justiça criminal e na segurança pública, avançando no objetivo da integral identificação biométrica da população brasileira e de integração das bases de dados constituídos para finalidades diversas. O faz sobretudo no que diz respeito ao banco multibiométrico, que aproveita dados de outros bancos, e incide sobre o tratamento de dados pessoais sensíveis, para fins de investigação criminal, sem que precisem incidir as causas que tradicionalmente justificam a identificação criminal, operada hoje através da identificação dactiloscópica, fotográfica – e, excepcionalmente, genética. Convém lembrar, aliás, que a tendência já vinha antecipada na Lei 13.444/2017, que criou a base de dados da Identificação Civil Nacional – ICN e previu a integração de dados biométricos do cadastro eleitoral com as bases de dados de identificação criminal (artigo 3º, § 2º da Lei 13.444/2017).[7]

Segundo a Constituição Federal, o civilmente identificado não será submetido à identificação criminal, salvo nas hipóteses previstas em lei (artigo 5º, inciso LVIII da Constituição Federal), isto é, quando não houver outra forma segura e suficiente de identificação do suspeito presumido inocente. As normas mais recentes, entre elas a lei anticrime, instauram o processo de identificação biométrica para além dos limi-

tes e da finalidade da identificação criminal. Expandem-se as hipóteses de tratamento de dados biométricos, alarga-se o termo de armazenamento de perfis genéticos, faculta-se a integração de outros bancos de dados.

É certo que, por um lado, o processamento de dados biométricos é hoje feito para finalidades diversas da criminal no Brasil. O TSE inaugurou a coleta de dados biométricos ainda em 2008, amparado na Resolução nº. 22.688/2007.[8] Desde então, a coleta obrigatória foi expandida a todos os eleitores (Resolução nº. 23.335/2011) e, hoje, é condição de regularidade eleitoral. Por outro lado, os dados a esse modo e sob tal justificativa coletados são aproveitados, i.e. retornam, para o fim específico da identificação criminal, driblando as limitações constitucionais e os termos da Lei de Identificação Criminal. Registra-se, a título de exemplo, o compartilhamento de do TSE dados com a Polícia Federal,[9] MPF[10] e com o CNMP.[11]

Especificamente quanto à coleta de dados genéticos, além das normas inseridas ou modificadas pela Lei Anticrime, e dos demais marcos normativos mencionados, cumpre mencionar o debate em curso no Supremo Tribunal Federal, no âmbito do RE 973837. Nele é questionada a constitucionalidade do artigo 9-A da LEP, e a consequente coleta obrigatória do material genético imposta a todos os condenados por crimes com violência ou hediondos, sem que haja uma finalidade probatória concreta ou qualquer necessidade de justificativa quanto à sua utilidade, e sem que no âmbito desta lei estejam previstos os termos de exclusão.[12] O dispositivo, conforme argumenta o autor, violaria a garantia contra a autoincriminação, e o princípio da legalidade.

3.

As questões suscitadas acima tocam o debate mais amplo da proteção de dados pessoais diante das atividades de trata-

mento realizadas pelo poder público, nesse caso, referidas à prevenção, identificação, processamento de crimes.

A esse respeito, convém lembrar dois movimentos correntes, relevantes e em tensão. Por um lado, a edição do Decreto 10.046/2019, que, além de criar um Cadastro Base para a consolidação de atributos biográficos e biométricos sobre cidadãos brasileiros, ampliou significativamente as hipóteses de compartilhamento de dados entre órgãos e entidades da administração pública federal.[13] O Decreto, expande hipóteses autorizativas, dispensa a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para o compartilhamento de dados entre órgãos e entidades da administração pública federal e os demais Poderes da União, e está em aparente tensão com o que dispõe a Lei Geral de Proteção de Dados em seus princípios de proteção de dados pessoais listados no art. 6º, como finalidade, adequação, necessidade, livre acesso ao titular, transparência etc.[14] Por outro, há o julgamento da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393, no qual o STF por larga maioria suspendeu a eficácia da MP 954/2020 e reconheceu status constitucional à proteção de dados pessoais e dela desdobrou obrigações como a transparência, proporcionalidade, garantia de segurança aos titulares de dados.

Embora haja, de fato, uma pendência no que diz respeito à edição de normas para a proteção de dados na segurança pública e investigações criminais, elementos das "garantias analógicas" e o debate internacional sobre proteção de dados e tratamento de dados sensíveis pelas agências penais[15] indicam os riscos a que estão expostos os titulares de dados afetados pelas medidas comentadas. A lei anticrime promove a intensificação do tratamento, arrefece controles, não endereça as lacunas legais relacionadas à especificação dos propósitos (finalidade) e limitação do uso de dados (necessidade), nem

trata da segurança dos dados e responsabilização dos responsáveis pelo tratamento. Tampouco trata da reparação dos direitos das/os afetadas/os por danos decorrentes de vazamentos ou uso abusivo. Tal contexto não inspira preocupação apenas a "quem tem algo a esconder", mas também a quem receia confiar dados a um Estado mal preparado para seu tratamento.

O caminho para endereçamento dessas questões passa pela renovada investigação sobre a efetiva necessidade de tratamento de dados sensíveis para fins de segurança pública e investigações criminais e a regulação, por lei, dessa atividade de maneira precisa, contida ao mínimo, prevendo dispositivos que previnam acesso e transmissão indevidas, anonimização ou dissociação dos dados, controle externo do tratamento e, em se tratando, da coleta de dados genéticos controle judicial da pertinência concreta da coleta, descarte da amostra, exclusão do perfil. Em se tratando de dados biométricos, a medida hiperbólica de constituição de um banco totalizante que inclua potencialmente dados de todos os brasileiros parece falhar no primeiro passo da avaliação. 

NOTAS

1. https://bit.ly/306ppNt

2. https://bit.ly/306ppNt

3. https://bit.ly/300SmdO

4. ANTONIALLI, D.; FRAGOSO, N.; MASSARO, H. (2019). "Da investigação ao encarceramento: as propostas de incremento do uso da tecnologia no Projeto de Lei Anticrime". https://bit.ly/33nuBQx.

5. Tratamos simultaneamente de dados genéticos e biométricos, apesar de especificidades regulatórias, por serem dados sensíveis, nos termos da LGPD e da regulação internacional sobre o tema e permitirem a identificação única dos indivíduos a que se referem.

6. Resoluções disponíveis em: https://bit.ly/2DEyvcU

7. Há ainda outros exemplos, como a Portaria 248/2018 do Ministério da Saúde, que determinou a identificação palmar de todos os recém-nascidos e a identificação biométrica da mãe.

8. Sobre o processo, cf.: LOUREIRO, M. F. B. (2014). *Biometria e tutela jurídica da privacidade*: caso do TSE. Anais das Jornadas de Iniciação Científica, v. 1, p. 58-79.

9. https://bit.ly/38Vp5Fe e https://bit.ly/3exPLNT

10. https://bit.ly/32eaoxp

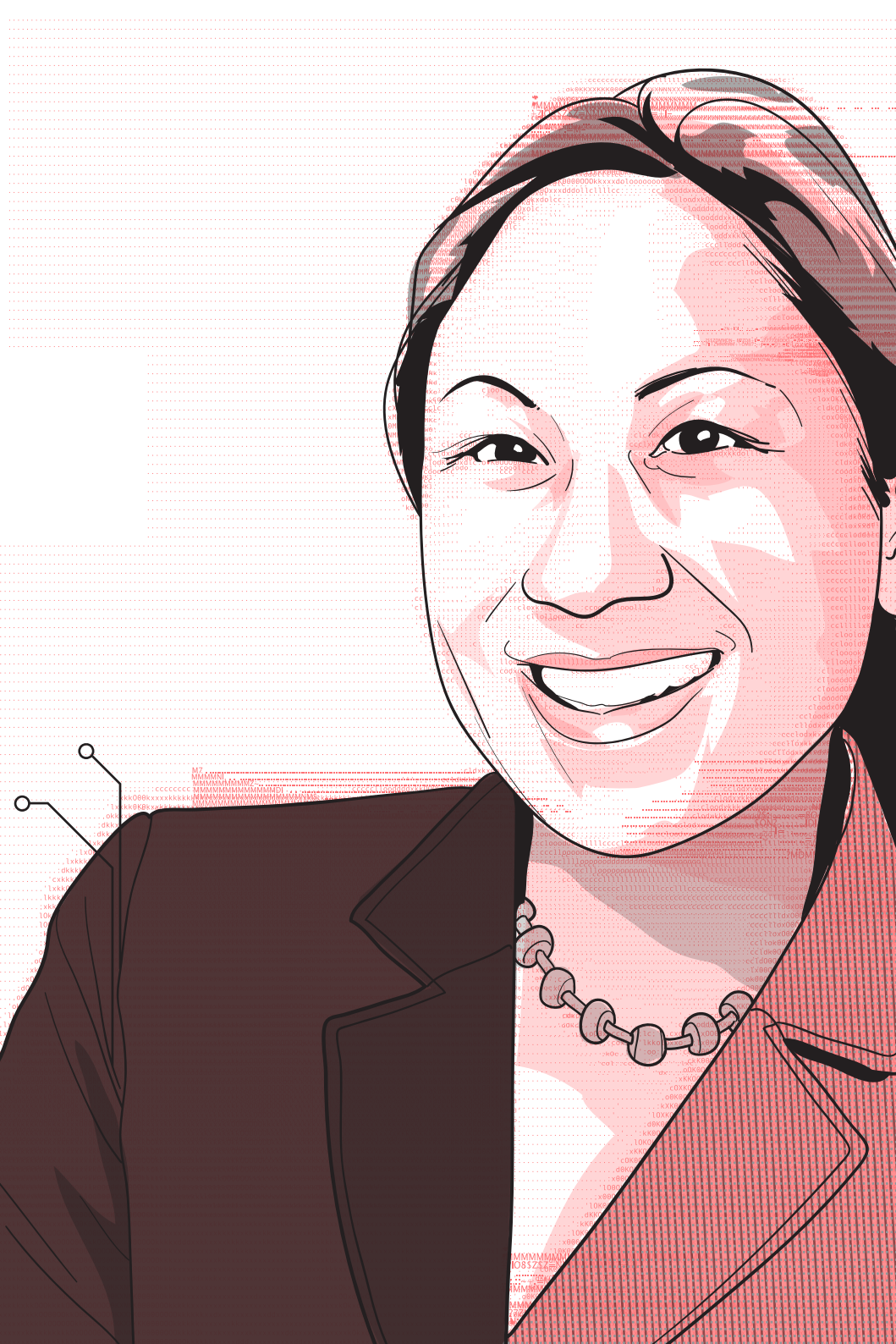
11. https://bit.ly/32eaoxp

12. CARVALHO, D. (2014). *As Intervenções Corporais no Processo Penal*: entre o desprezo, o gozo e a limitação de direitos fundamentais. Rio de Janeiro: Lumen Juris, pp. 147-150.

13. FRAGOSO, N.; MASSARO, H. (2019). *Cadastro Base e amplo compartilhamento de dados pessoais: a que se destina?* https://bit.ly/3eqGRRZ

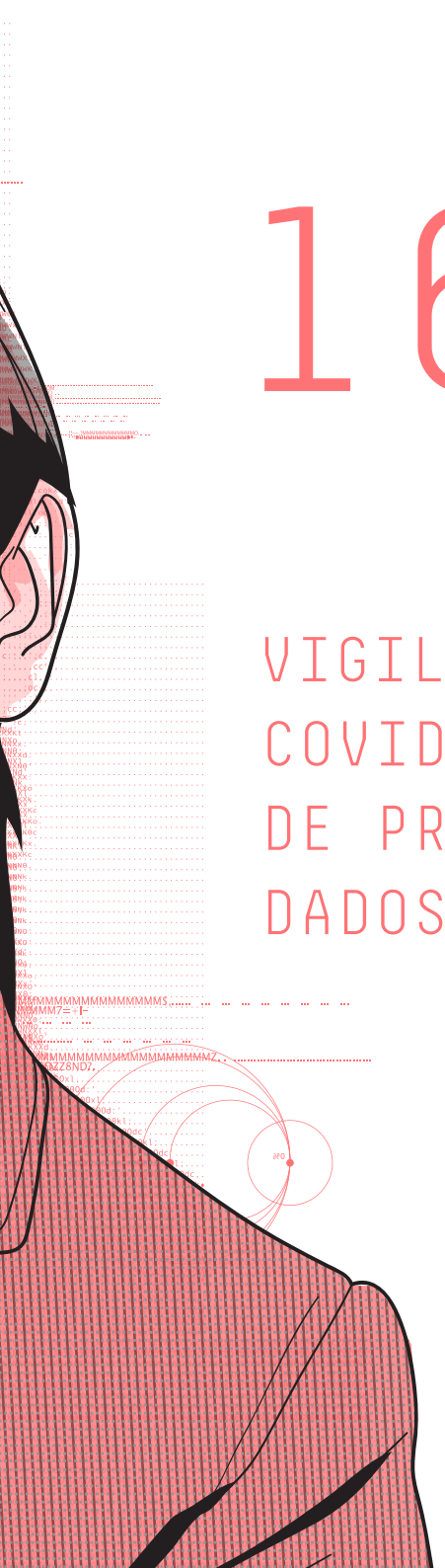
14. FRAGOSO, N.; MASSARO, H. (2019). *Cadastro Base e amplo compartilhamento de dados pessoais: a que se destina?* https://bit.ly/3eqGRRZ

15. Cf. Establishing Best Practice for Forensic DNA databases (2017). Disponível em: https://bit.ly/30d30mS



16.

VIGILÂNCIA, COVID-19 E LEI DE PROTEÇÃO DE DADOS DO BRASIL[1]



Margaret Hu

INTRODUÇÃO

Como o COVID-19 infectou milhões globalmente no início de 2020, várias empresas de tecnologia ofereceram apoio para ajudar a combater a propagação da doença. No Brasil, um país particularmente impactado pela rápida expansão do COVID-19, uma startup brasileira de tecnologia avançou em parceria com o governo. A InLoco, sediada no Porto Digital de Pernambuco, na cidade de Recife, tem acesso a 60 milhões de smartphones no Brasil.[2] A empresa oferece serviços de segmentação de varejo e tecnologia de anúncios por meio de rastreamento de localização geográfica de smartphones e outras vigilâncias agregadas do comportamento do consumidor.[3]

No final de março de 2020, a InLoco havia se unido ao governo da cidade de Recife para rastrear os dados geográficos de 700.000 usuários de smartphones na cidade, a fim de impedir a propagação do vírus.[4] O prefeito de Recife, Geraldo Júlio, explicou que a startup de tecnologia permitiu à cidade "monitorar bairros com dados coletivos para saber se o bloqueio está funcionando."[5] As respostas aos dados incluíram notificações por meio de alto-falantes, smartphones e outras comunicações públicas.[6] O CEO da InLoco, André Ferraz, explicou que a startup "foi inundada com pedidos de autoridades em todo o Brasil que desejam usar o sistema".

Em todo o mundo, as empresas de tecnologia se ofereceram para coletar dados para ajudar os governos nos esforços de redução de pandemia. Os objetivos parecem convincentes. A tecnologia também parece aderir a amplos princípios epidemiológicos, como rastreamento de contatos. A tecnologia é apresentada como replicação de protocolos históricos praticados por profissionais de saúde, como rastreadores de contato humanos. A parceria público-privada parece fazer sentido. Os governos estão buscando informações sobre a melhor forma de proteger os cidadãos da disseminação do coronavírus.

As empresas de tecnologia oferecem métodos de coleta de dados em massa e modos de comunicação em massa que eles afirmam ajudar no avanço de metas críticas de saúde pública.

Especialistas em privacidade, no entanto, alertaram que as soluções tecnológicas oferecidas por algumas empresas de tecnologia podem violar o espírito e a letra das leis de privacidade de dados. Na União Europeia (UE), por exemplo, o Regulamento Geral de Proteção de Dados (GDPR, sigla em inglês) se esforça para proteger os direitos de privacidade das informações dos cidadãos da UE. O Brasil seguiu o GDPR, por meio da promulgação da *Lei Geral de Proteção de Dados Pessoais* (LGPD), para proteger os direitos de privacidade de dados dos cidadãos brasileiros. Contudo, a LGPD, embora promulgada, está enfrentando atrasos na implementação.

Os Estados Unidos (EUA), no entanto, como muitas nações, carecem de um plano uniforme de proteção de dados. Não existe uma lei federal abrangente nos EUA que regule a coleta, o armazenamento e o processamento de dados pessoais.[7] Ao invés disso, as leis federais de privacidade de dados promulgadas nos EUA geralmente designam proteção para áreas específicas de dados, como a proteção da saúde e dos dados do paciente sob a Lei de Portabilidade e Responsabilidade do Seguro de Saúde (HIPAA, sigla em inglês). Estados individuais dos EUA promulgaram proteções mais amplas de privacidade de dados, por exemplo, o Califórnia Consumer Privacy Act (CCPA).[8] Leis federais como a Lei de Privacidade de Comunicações Eletrônicas de 1986 moldam a estrutura de privacidade dos EUA de maneira mais limitada.[9]

No contexto do processo criminal, a Quarta Emenda da Constituição dos EUA protege contra buscas e apreensões irrazoáveis sem mandado e, cada vez mais, é usada para proteger os cidadãos de buscas cibernéticas. As proteções de privacidade de dados oferecidas pela Quarta Emenda, no entanto,

são limitadas. Primeiro, o potencial protetor da Quarta Emenda é limitado apenas às ações do governo. E, por se relacionar apenas a procedimentos criminais, limita-se a ações governamentais que ocorrem durante o curso da aplicação da lei, como policiamento ou investigações, ou ação de segurança nacional. Segundo, não é uma autoridade explícita de privacidade ou proteção de dados. Isso contrasta com as garantias explícitas de privacidade de dados da Constituição Brasileira. A Quarta Emenda protege os cidadãos de uma busca e apreensão sem mandado pelo governo dos EUA. Terceiro, na era digital, a capacidade da Quarta Emenda de proteger contra intrusões cibernéticas ainda não está clara. Em 2018, no caso *Carpenter vs. Estados Unidos*, foi solicitado à Suprema Corte dos EUA que decidisse se agências penais poderiam, sem ordem judicial, realizar a vigilância, isto é obter informações de localização de antena de celular mantidas por empresas privadas de telecomunicações.[10] Antes de *Carpenter*, o governo havia argumentado que os dados de localização de antena de celular podiam ser acessados sem um mandado. As agências penais antes da decisão do caso *Carpenter*, haviam argumentado que os dados de geolocalização de antena de celular eram considerados um registro comercial de dados que não eram privados: o consumidor havia compartilhado voluntariamente dados de geolocalização emitidos pelo telefone celular ou smartphone com a empresa de telecomunicações.[11] Em *Carpenter* se considerou que os dados de localização geográfica eram particularmente sensíveis e que haveria uma expectativa razoável de privacidade na proteção dos dados de localização de antena de celulares contra buscas e apreensões sem ordem judicial.[12]

Como os EUA não oferecem uma lei abrangente de proteção de dados e o alcance protetor da Quarta Emenda em privacidade de dados pode ser limitado em sua aplicação aos

programas de rastreamento de dados COVID-19, a discussão abaixo concentra sua atenção na UE e no Brasil. Este capítulo oferece uma perspectiva comparada sobre as tecnologias de vigilância COVID-19 e possíveis pontos de conflito na lei de proteção de dados da UE e do Brasil. Primeiramente, fornece uma breve pesquisa sobre os tipos de tecnologias de vigilância pandêmica que foram introduzidas até agora. A seguir, descreve a estrutura protetora básica do GDPR da UE e da LGPD do Brasil. Por fim, explora como os atuais desafios enfrentados pelo GDPR podem ser aplicáveis à futura vigência da LGPD. Conclui que nem o GDPR, nem a LGPD provavelmente oferecerão proteção suficiente à privacidade de dados contra as formas de tecnologias de vigilância de dados que foram introduzidas para fins de vigilância na pandemia.

VISÃO GERAL DAS TECNOLOGIAS DE VIGILÂNCIA COVID-19

Em 31 de dezembro de 2019, autoridades de saúde de Wuhan, China, informaram que estavam tratando dezenas de pacientes com sintomas de um tipo de pneumonia.[13] Os meios de comunicação oficiais chineses informaram a primeira morte decorrente do novo coronavírus em 11 de janeiro de 2020.[14] Mais tarde chamado de "COVID-19", o vírus se espalhou com velocidade meteórica para quase todos os continentes. Os países do leste asiático foram os primeiros a ver a propagação da infecção.[15] No final da primavera (no hemisfério norte) de 2020, milhões foram infectados e as mortes globais do COVID-19 atingiram centenas de milhares.

Vários países da Ásia adotaram imediatamente métodos de vigilância em massa para inibir a transmissão e ajudar a resposta dos governos ao COVID-19. A China exigiu que os cidadãos residentes em Wuxi, Hangzhou e Wuhan baixassem aplicativos de código sanitário em smartphones.[16] Os apli-

cativos permitiram ao governo chinês rastrear movimentos populacionais.[17] Outras ferramentas de vigilância incluíam imagens térmicas através de sistemas de Circuito Fechado de TV (CFTV) para detectar altas temperaturas e febres,[18] e o uso de drones para transmitir anúncios de saúde pública e implementar normas de saúde.[19] Taiwan, Coréia do Sul e Cingapura logo seguiram a China nas ferramentas de rastreamento digital em massa adotadas como parte de sua resposta ao COVID-19.[20]

Em março de 2020, Cingapura incentivou os cidadãos a instalar um aplicativo chamado "TraceTogether" em seus smartphones, permitindo que o Bluetooth transmita e receba identificadores anônimos entre as pessoas que executam o aplicativo nas proximidades[21]. O "TraceTogether" "permite que as pessoas compartilhem voluntariamente suas informações e rastreia outras pessoas, com quem entram em contato, via Bluetooth."[22] Se um usuário do "TraceTogether" for infectado pelo o COVID-19, o governo de Cingapura e todos os usuários que entraram em contato com esse indivíduo serão notificados.[23]

Da mesma forma, até o momento, mais de 1 milhão de sul-coreanos baixaram o aplicativo "Corona 100m", permitindo que o governo sul-coreano notifique os usuários de que foram expostos em um raio de 100 metros a um paciente diagnosticado com COVID-19.[24] Os usuários também recebem os dados de nacionalidade, idade, sexo e geolocalização do paciente.[25] Os dados de localização geográfica dos pacientes com COVID-19 na Coréia do Sul foram compilados por meio da agregação de vários bancos de dados com novos conjuntos de dados, incluindo "imagens de CFTV, históricos de cartões de crédito e históricos de localização."[26] Taiwan usa dados de rastreamento de localização geográfica de smartphones para monitorar a conformidade com as medidas de quarentena e chamar os cidadãos diretamente.[27] Hong Kong exigiu que

novos visitantes fizessem o download do aplicativo "StayHomeSafe", emparelhado com uma pulseira de geofencing, para impor uma quarentena obrigatória de duas semanas.[28] A Índia usa um aplicativo centralizado chamado “Aarogya Setu”, que atualmente é o aplicativo de rastreamento de contatos mais popular em todo o mundo, com mais de 50 milhões de downloads.[29] Ao mesmo tempo em que várias nações asiáticas começaram a experimentar ferramentas de rastreamento de dados digitais para notificar os cidadãos sobre o risco de exposição ao COVID-19 e reforçar a conformidade com pedidos de permanência em casa; agências governamentais, instituições acadêmicas e empresas nos EUA e na UE exploraram métodos para conter o COVID-19 por meios tecnológicos. Um grupo internacional de especialistas em saúde e tecnologia começou a incentivar publicamente a Apple e o Google a desenvolver uma tecnologia de "rastreamento de contatos" que pudesse funcionar de maneira semelhante ao aplicativo "TraceTogether" de Cingapura, mas com mais proteções de privacidade de dados incorporadas ao sistema.[30] Alguns especialistas argumentaram que isso replicaria em uma escala muito mais ampla o rastreamento de contatos tradicional, baseado em humanos. Historicamente, o rastreamento de contatos baseado em humanos realizado por profissionais de saúde qualificados envolve entrevistar pacientes de doenças infecciosas para determinar com quem eles podem estar em contato e quem pode estar em risco de infecção por exposição[31].

Em 10 de abril de 2020, Apple e Google anunciaram sua colaboração em uma plataforma comum para aplicativos para habilitar o “rastreamento de contatos” ou “rastreamento de proximidade” (rastreamento digital) acionado por Bluetooth.[32] As empresas de tecnologia explicaram que pretendiam alterar o sistema operacional dos iPhones e telefones Android para permitir aos desenvolvedores de aplicativos de

rastreamento digital COVID-19 o acesso contínuo ao Bluetooth. À luz das preocupações de privacidade levantadas pelos esforços anteriores de rastreamento digital, Apple e Google enfatizaram que sua nova plataforma liderava um esforço internacional para "descentralizar" o rastreamento de contato digital.[33] Para proteger melhor a privacidade e os dados dos usuários, a Apple e o Google anunciaram que exigiriam explicitamente que os dados coletados dos aplicativos de rastreamento digital criados em sua plataforma precisassem ser mantidos no telefone individual do usuário, e não em um banco de dados central.[34]

RASTREAMENTO DIGITAL CENTRALIZADO VERSUS DESCENTRALIZADO

O conceito de rastreamento digital descentralizado versus centralizado é essencial para entender as preocupações de privacidade por trás das várias ferramentas de vigilância digital que foram implantadas em todo o mundo para combater o COVID-19. Uma das abordagens tecnológicas de rastreamento digital envolveu "a vigilância do governo e a coleta central de grandes quantidades de dados pessoais."[33] Os sistemas centralizados geralmente coletam informações como: sinais de GPS, feeds de CFTV ou dados geográficos, usando aplicativos de rastreamento de contatos digitais, pulseiras eletrônicas e outros dispositivos. Os dados coletados desses sistemas são armazenados em um banco de dados central controlado e acessado pelo governo local ou nacional. Ao gerenciar a vigilância pandêmica e o rastreamento digital dessa maneira, o objetivo pretendido é que as autoridades de saúde do governo possam "rastrear o histórico de localização dos cidadãos para determinar quando duas pessoas estão no mesmo local ao mesmo tempo[36]". Variantes dessa abordagem centralizada foram adotadas pela China, Cingapura, Hong Kong, Taiwan, Índia e Israel.[37]

Vários países europeus, incluindo França, Noruega e Reino Unido, estão atualmente projetando e testando aplicativos de rastreamento digital centralizados.[38] A França expressou decepção porque a Apple e o Google não apoiaram o esforço francês de combater o COVID-19 por meio de uma abordagem centralizada.[39] E explicou que seu aplicativo de rastreamento digital de coronavírus "é uma solução temporária, voluntária e valiosa."[40] As autoridades francesas argumentaram que o alcance do aplicativo é limitado: "O aplicativo não solicita absolutamente nenhum dado pessoal ao usuário: nem o nome, nem o endereço e nem número do celular."[41]

Por outro lado, os defensores e apoiadores de uma abordagem descentralizada do rastreamento de contatos incluem o rastreamento de contatos automatizado privado do MIT,[42] o "COVID-Watch" de Stanford[43] e o grupo de rastreamento de proximidade descentralizado de preservação de privacidade ("DP-3T").[44] Um modelo descentralizado incentiva o desenvolvimento de sistemas de identificação anônima que podem operar aplicativos de rastreamento digital com uma conexão Bluetooth. Os sistemas descentralizados suportam a retenção de dados no telefone de um usuário com IDs anônimos, mantidos localmente em smartphones. Por meio de um aplicativo que retransmite os dados para um servidor, o sistema, por exemplo, pode baixar um banco de dados de IDs anônimos, e o telefone combina o usuário com outras pessoas que podem ter sido infectadas pelo COVID-19.[45] O "servidor back-end está apenas no loop para retransmitir informações aos dispositivos."[46] O Parlamento Europeu apoia a descentralização, alertando que qualquer aplicativo de rastreamento digital desenvolvido na UE deve descentralizar o armazenamento de dados.[47] Além disso, o órgão declarou que os dados gerados por aplicativos de rastreamento de contatos digitais "não devem ser armazenados em bancos

de dados centralizados, propensos a possíveis riscos de abuso, perda de confiança e que podem comprometer a aceitação em toda a União."[48]

Ambos os modelos têm seus riscos de segurança. Os sistemas centralizados sofrem o risco de que as pessoas possam ser desanonimizadas. "[Se] o banco de dados é invadido, o anonimato fornecido pelos pseudônimos rotativos é anulado e os indivíduos podem ser rastreados com mais facilidade.[49] Com protocolos e aplicativos centralizados, os especialistas se preocupam com a inevitabilidade da vigilância do estado e a probabilidade de violação de dados.[50] Os modelos descentralizados carregam um risco semelhante, embora sejam considerados mais protetores da privacidade, eles ainda aproveitam a coleta centralizada e a troca de identificação anônima de indivíduos que testaram positivo.[51] Em outras palavras, os indivíduos que fazem o download do aplicativo de rastreamento digital ainda podem ser desanonimizados, mesmo que tudo o que eles estão centralizando sejam suas informações de identidade anônimas rotativas geradas a partir de sinais Bluetooth emitidos por um smartphone. Além disso, permanece a preocupação de que a limitação da quantidade de dados coletados e disponibilizados às autoridades de saúde pública possa diminuir a utilidade do aplicativo e tenha um impacto adverso em sua capacidade de ajudar a impedir a propagação do vírus.[52]

SISTEMAS DE RASTREAMENTO DE PROXIMIDADE COM BASE EM BLUETOOTH

Os proponentes dos sistemas de rastreamento de proximidade com base em Bluetooth estão imersos em um debate sobre a utilização de um modelo centralizado ou descentralizado para coleta de dados.[53] Alguns protocolos propostos que adotam a abordagem centralizada visam a armazenar todos os

dados do usuário coletados de aplicativos de rastreamento digital em um servidor de agência governamental, além de centralizar a análise de dados e o rastreamento de contatos com a agência governamental. Em 1 de abril de 2020, uma coalizão de cientistas e tecnólogos da UE anunciou a formação de um consórcio europeu, o Rastreamento de Proximidade Pan-Europeu de Preservação de Privacidade (PEPP-PT). O PEPP-PT apoia abordagens centralizadas para coleta de dados através de um sistema digital de rastreamento de contato digitalizado baseado em Bluetooth.[54]

Um modelo centralizado para rastreamento digital baseado em Bluetooth propõe o upload de todos os dados coletados pelo aplicativo para identificar todas as correspondências possíveis com outros contatos de proximidade baseados em Bluetooth.[55] O PEPP-PT promove esse modelo centralizado como uma opção de "preservação da privacidade."[56] Sob um sistema centralizado, argumenta o PEPP-PT, o acesso aos dados é cuidadosamente controlado e protegido pela agência governamental relevante, por exemplo, uma agência de saúde pública. Os defensores dessa abordagem centralizada explicam que ela "permite que as autoridades de saúde usem o banco de dados para reunir uma visão da rede de contatos, possibilitando insights epidemiológicos adicionais, como a revelação de grupos e super espalhadores."[57]

A Apple e o Google, no entanto, declararam sua intenção de respeitar uma abordagem descentralizada do rastreamento de proximidade digital. Por meio de uma conferência de imprensa conjunta realizada em 20 de maio de 2020, as empresas de tecnologia anunciaram seu novo sistema, chamado de "Interface de programação de aplicativos de notificação de exposição" ("API"). A plataforma API está sendo lançada para usuários do iPhone e Android na forma de uma atualização de software.[58] Durante a conferência de imprensa, a Apple e

o Google explicaram que o sistema foi projetado para ajudar as autoridades de saúde pública no desenvolvimento de aplicativos que podem oferecer suporte ao rastreamento digital baseado em Bluetooth.[59] O esforço conjunto das empresas exigiu o desenvolvimento da tecnologia necessária para evitar o consumo de bateria.[60] Como o sistema de API precisa ser executado constantemente em segundo plano no telefone de um usuário, a Apple e o Google explicaram que o novo sistema reduz os problemas de drenagem e segurança da bateria.[61]

A Apple e o Google revelaram ainda que, sob o sistema da API de notificação de exposição, um smartphone ou dispositivo iOS e Android "transmite regularmente uma sequência aleatória de caracteres que serve como pseudônimo para outros telefones usando a especificação de baixa energia do Bluetooth para o envio de dados."[62] A cada quinze minutos, o telefone altera a sequência de caracteres para anonimizar ainda mais o usuário. À medida que o telefone passa perto de outros telefones, ele registra as sequências de caracteres de outras pessoas, "além de informações sobre a intensidade do sinal para estimar o quão próximas elas estão"[63] também conhecidas como "handshake Bluetooth". Se um usuário fizer o download voluntário do aplicativo de rastreamento de contatos baseado em Bluetooth e se o usuário for diagnosticado com COVID-19, poderá consentir em publicar no banco de dados do aplicativo o histórico recente de pseudônimos por meio de "Bluetooth handshake."[64]

Em uma abordagem descentralizada, outros telefones individuais, em oposição às autoridades de saúde do governo, têm a capacidade de "baixar esse banco de dados, compará-lo com o histórico de encontros e alertar os usuários se eles foram expostos à pessoa infectada por tempo suficiente para colocá-los em risco de infecção."[65] Portanto, se um usuário do aplicativo atualizar seu status para "positivo" para o CO-

/ OS INDIVÍDUOS QUE FAZEM O DOWNLOAD DO APLICATIVO DE RASTREAMENTO DIGITAL AINDA PODEM SER DESANONIMIZADOS /

/ A FALTA DE ORIENTAÇÃO INTERPRETATIVA PARA A LGPD É UM DESAFIO NA DETERMINAÇÃO DE COMO OS APLICATIVOS DE RASTREAMENTO DIGITAL PODEM OPERAR /

VID-19, o sistema da API poderá "notificar anonimamente outros usuários que entraram em contato com essa pessoa"[66] sem compartilhar ou armazenar informações de geolocalização identificáveis do "indivíduo positivo" ou aqueles que ele ou ela infectou.

Os executivos da Apple e do Google listaram vários ajustes feitos no sistema de APIs durante o desenvolvimento "após ampla consulta com autoridades de saúde pública, defensores da privacidade, acadêmicos e agências governamentais de todo o mundo."[67] Os representantes da empresa enfatizaram que o modelo da API, diferentemente de outros designs de rastreamento digital, "não exigiria que as informações fossem armazenadas em um banco de dados central, mas permitiria que os usuários vissem em seus próprios smartphones se foram expostos a alguém com a doença"[68]. A API também permite que as autoridades de saúde pública entrem em contato com usuários expostos com base em "uma combinação da API e dos dados que os usuários escolheram voluntariamente inserir no aplicativo"[69]. A plataforma Apple-Google permite a coleta opcional de dados adicionais, incluindo códigos postais e números de telefone do usuário. Esse recurso permite que as autoridades de saúde pública coletem informações adicionais de usuários expostos e realizem divulgação[70]. Segundo as empresas, esses dados opcionais são compartilhados apenas se os usuários derem permissão expressa.

A Apple e o Google afirmam que o sistema cria importantes proteções de privacidade no design da API. As empresas afirmam que não é obrigatório para os usuários e depende do usuário fazer o download voluntário do aplicativo de rastreamento digital apropriado.[71] A plataforma também requer o consentimento expresso do usuário para relatar um diagnóstico positivo para o COVID-19 por meio do aplicativo.[72] Diferentemente de uma abordagem centralizada, Apple e Google

afirmam que, sob a nova API, os dados de geolocalização não são retidos pelo sistema.[73] As empresas planejam tornar a plataforma API Apple-Google acessível apenas às autoridades de saúde pública que executam aplicativos de rastreamento digital.[74] O design da plataforma também concede controle significativo às autoridades locais de saúde pública, porque "[o] sistema foi projetado para funcionar com um aplicativo por região, como um país ou estado, para evitar a fragmentação."[75] Cada região ou país individual tem autonomia para criar seu próprio aplicativo e cada um pode definir parâmetros para o que constitui uma exposição ao COVID-19, medindo fatores como o tempo gasto próximo a outro usuário ou a distância entre os usuários.[76]

Vários estados dos EUA e mais de vinte e dois países até agora manifestaram interesse em usar a plataforma API Google-Apple para realizar rastreamento digital entre os iPhones e Androids de seus cidadãos.[77] Alguns estados dos EUA, como Dakota do Norte, já haviam tentado lançar seus próprios aplicativos sem o suporte da Apple e do Google, e o fizeram com pouco sucesso.[78] Em Dakota do Norte, o aplicativo "Care19" segue as localizações de GPS dos usuários, contando com torres de celular e Wi-Fi, mas os dados de localização acabaram sendo "irregulares, já que vinte por cento da população não tem banda larga em casa."[79] Diante de questões de funcionalidade, o estado agora adotou a abordagem Apple-Google e está construindo dois aplicativos separados - um para rastreamento digital baseado em localização e outro no sistema Apple-Google "mesmo que [as autoridades estaduais] temam que isso leve à diminuição da adesão, a uma maior confusão e a atrasos na produção de dados que salvam vidas."[80]

Até o momento, mais da metade dos estados membros da UE fez parceria com empresas de telecomunicações para adotar ferramentas de rastreamento de dados com objetivo de en-

dereçar o problema da COVID-19.[81] Em 27 de maio de 2020, a Suíça se tornou o primeiro país a lançar um aplicativo de rastreamento digital baseado no padrão Apple-Google API.[82] O aplicativo suíço, chamado "SwissCovid", estava inicialmente limitado ao exército, funcionários de hospitais e funcionários públicos, e agora é liberado para uma população maior.[83] A Alemanha apoiou inicialmente o PEPP-PT e o modelo centralizado.[84] No entanto, em resposta a críticas generalizadas aos riscos de privacidade associados a esses protocolos centralizados, a Alemanha adotou posteriormente o modelo descentralizado proposto pelo Google e pela Apple.[85]

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS DA UE

Seja centralizado ou descentralizado, os aplicativos de rastreamento digital dependem fundamentalmente da coleta e uso de dados, incluindo a identificação do dispositivo e informações de saúde de indivíduos. Os desenvolvedores de aplicativos em todo o mundo devem trabalhar para atenuar os problemas de privacidade criados por essa coleta de dados e garantir que qualquer solução cumpra as leis de privacidade e proteção de dados aplicáveis. O Regulamento Geral de Proteção de Dados (GDPR) estabelece um conjunto único de desafios para desenvolvedores de aplicativos e autoridades de saúde que lidam com dados de cidadãos da UE.

O GDPR foi promulgado com o seguinte objetivo: ser "a lei de privacidade e segurança mais difícil do mundo."[86] Ela decorre do direito à privacidade, previsto na Convenção Européia de Direitos Humanos de 1950, que afirma que "todos têm o direito ao respeito da sua vida privada e familiar, seu lar e sua correspondência."[87] Em 1995, a UE aprovou a Diretiva Européia de Proteção de Dados, que impunha padrões mínimos de privacidade e segurança de dados.[88] O advento

da era da Internet estimulou a aprovação do GDPR[89]. O regulamento entrou em vigor em 2016 após a aprovação do Parlamento Europeu, e todas as organizações europeias foram obrigadas a estar em conformidade com ele a partir de maio de 2018.[90] O GDPR foi originalmente redigido e aprovado na UE e impõe obrigações às entidades que tratam os dados de indivíduos em toda a UE.[91] O regulamento também impõe multas pesadas contra os infratores e se esforça para alcançar "uma abordagem abrangente sobre proteção de dados pessoais."[92]

GDPR: ESCOPO, DEFINIÇÕES PRINCIPAIS E SANÇÕES

O GDPR se aplica a entidades que processam os dados pessoais de cidadãos ou residentes da UE ou a entidades que oferecem bens ou serviços a esses indivíduos, independentemente de a entidade estar ou não localizada na UE.[93] A lei define dados pessoais como "qualquer informação relacionada a uma pessoa física identificada ou identificável ('titular dos dados'); uma pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador."[94] Os dados pessoais incluem nomes e endereços de e-mail, bem como "dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular ". O GDPR refere-se a usuários ou visitantes do site como "titulares de dados", indivíduos cujos dados são processados. O tratamento de dados é definido amplamente como qualquer "operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não", como coleta, gravação, organização, armazenamento, uso ou exclusão de dados.

As multas por violar o GDPR podem ser significativas, chegando a dezenas de milhões de euros. A lei estabelece "dois níveis de penalidades, que atingem no máximo 20 milhões de euros ou 4% da receita global (o que for maior)."[95] Além disso, os titulares dos dados têm o direito de solicitar uma indenização por danos.

DIREITOS DE PRIVACIDADE, CONSENTIMENTO E SEGURANÇA DE DADOS NO GDPR

O GDPR reconhece vários direitos de privacidade explícitos para os titulares dos dados. Um objetivo importante do GDPR é dar às pessoas mais controle sobre os dados que são fornecidos às entidades. Alguns direitos importantes de privacidade previstos pelo GDPR incluem: direito de ser informado; direito de acesso; direito à retificação; direito de apagar; direito de restringir o processamento; direito à portabilidade de dados; direito de objetar; e direitos relacionados à tomada de decisão e perfilização automatizadas.[96] O GDPR lista ainda as condições em que uma entidade pode processar dados pessoais. Pelo menos uma das justificativas previstas no GDPR (também chamadas de bases) deve ser atendida: o titular dos dados deve conceder consentimento inequívoco para processar os dados para a entidade; o processamento é necessário para executar ou se preparar para celebrar um contrato do qual o titular dos dados é parte; a entidade precisa processar os dados para cumprir uma obrigação legal; a entidade precisa processar os dados para salvar a vida de alguém; o processamento é necessário para executar uma tarefa de interesse público ou para desempenhar alguma função oficial; e a entidade tem interesse legítimo em processar os dados pessoais.[97] Os “direitos e liberdades fundamentais do titular dos dados” se sobrepõem aos interesses da entidade, especialmente

se envolver dados de uma criança.[98] Depois de determinar a base legal para o processamento de dados, a entidade deve documentar essa base e notificar o titular dos dados para garantir a transparência. Se a entidade decidir posteriormente alterar sua justificação, ela deve ter um bom motivo, documentar esse motivo e notificar o titular dos dados.

A lei contém padrões estritos para o que constitui consentimento de um sujeito de dados para o processamento de suas informações por uma entidade. Primeiro, o consentimento deve ser "dado livremente, específico, informado e inequívoco". Além disso, os pedidos de consentimento devem ser "claramente distinguíveis dos outros assuntos" e apresentados em "linguagem clara e simples". Os titulares dos dados podem retirar o consentimento previamente fornecido a qualquer momento e a entidade deve respeitar sua decisão. Nesse caso, a entidade não pode simplesmente alterar a base jurídica do processamento para uma das outras justificativas. Finalmente, a entidade deve manter evidências documentais de consentimento.

Uma entidade que processa dados deve fazê-lo com segurança, implementando "medidas técnicas e organizacionais apropriadas". As medidas técnicas podem incluir, por exemplo, exigir que "os funcionários usem a autenticação de dois fatores em contas em que os dados pessoais são armazenados ou a contratação de fornecedores de nuvem que usam criptografia de ponta a ponta."[99] Exemplos de medidas organizacionais incluem "treinamentos da equipe, adicionando uma política de privacidade de dados ao manual do funcionário ou limitando o acesso a dados pessoais apenas aos funcionários da organização que precisam deles."[100] No caso de uma violação de dados, a entidade deve informar os titulares de dados dentro de 72 horas após a violação ou sofrerá penalidades.

LEI BRASILEIRA DE PROTEÇÃO DE DADOS: LGPD (LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS)

A recém-promulgada lei de proteção de dados do Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), é muito semelhante ao GDPR em escopo e origem. Os rascunhos iniciais do que acabaria por se tornar a LGPD foram publicados pela primeira vez em 2015.[101] A LGPD foi sancionada pelo Presidente Michel Temer em 14 de agosto de 2018; no entanto, a implementação e aplicação foram postergadas.[102] A lei possui princípios e disposições semelhantes ao GDPR, ela executa muitas das mesmas funções, regulando a coleta, o processamento e a proteção de dados.[103] Enumera os propósitos de proteger os direitos fundamentais de liberdade e privacidade (art. 1º, LGPD).

A base da regulação brasileira de privacidade é de natureza constitucional. A Constituição Federal enumera os principais direitos fundamentais no Artigo 5, incluindo o direito à privacidade. Além do direito à privacidade, a Constituição brasileira inclui o direito ao sigilo de correspondências e comunicações e remédios para violações da privacidade.[104] A Constituição brasileira também oferece fortes garantias à liberdade de expressão, como o direito ao acesso à informação e as proibições contra a censura.[105]

O Brasil também promulgou várias leis de privacidade antes da LGPD. O Código do Consumidor, o Código Civil e o Marco Civil da Internet criam uma rede de leis de proteção e direitos de privacidade para os cidadãos brasileiros.[106] O Código Civil concede certos direitos mínimos de privacidade no Brasil, enquanto o Código de Defesa do Consumidor confere direitos de privacidade, exigindo o uso responsável e o armazenamento de dados em um esforço de boa-fé, viabilizando a aplicabilidade desses direitos na ausência de uma lei brasileira específica.[107] O Marco Civil da Internet (Marco Civil da

Internet) estabelece regras e direitos para a Internet no Brasil, incluindo proteção de dados, ao mesmo tempo em que reforça os direitos constitucionais dentro da lei da Internet.[108] A LGPD visa unificar as fontes dispersas de proteção e regulamentação em uma lei abrangente, semelhante aos objetivos do GDPR na UE.

PRINCIPAIS DIFERENÇAS ENTRE O GDPR E A LGPD

Embora a LGPD tenha muitas semelhanças com o GDPR, e seu efeito prático provavelmente seja muito semelhante, distinções importantes podem produzir uma diferença em sua implementação. Várias diferenças, por exemplo, limitam o processamento de dados de algumas maneiras, enquanto outras permitem maiores liberdades. A definição de dados pessoais na LGPD difere da do GDPR.[109] A LGPD define dados pessoais como "informações sobre uma pessoa singular identificada ou identificável" e dados pessoais sensíveis como "dados pessoais sobre origem racial ou étnica, crença religiosa, opinião política, filiação sindical ou religiosa, filosófica ou política, dados relativos à saúde ou vida sexual, dados genéticos ou biométricos, quando relacionados a uma pessoa natural (art. 5º da LGPD)."

A LGPD enumera nove direitos para titulares de dados diante dos controladores de dados. Esses direitos de privacidade incluem: direito de ser informado da sobre o tratamento; direito de acesso; direito à retificação; direito ao anonimato; direito à portabilidade de dados; direito de eliminação; direito a informações sobre compartilhamentos; direito a informações sobre como negar consentimento e consequências; direito de revogar o consentimento (art. 18, LGPD). A LGPD apresenta várias justificativas e bases legais para o tratamento de dados pessoais: o titular dos dados dá consentimento

para tratar dados pessoais; o tratamento é necessário para o cumprimento de uma obrigação legal ou regulamentar; o tratamento é para administração pública, para execução da lei ou para contratos; o tratamento é necessário para estudos de entidades de pesquisa; o processamento é necessário para a execução de um contrato do qual o titular dos dados é parte, a pedido do titular; o tratamento é necessário para procedimentos judiciais, administrativos ou de arbitragem; tratamento é necessário para salvar vidas; é necessário tratamento para proteger a saúde, se usado por profissionais ou entidades de saúde; o tratamento é necessário para um controlador de dados cumprir uma obrigação legal; e o tratamento é necessário para a proteção do crédito.[110]

A implementação da LGPD continua pendente, pois foi adiada. Sem diretrizes publicadas para implementação, os requisitos de conformidade permanecem incertos.[111] Por exemplo, o texto da LGPD exige que os incidentes de segurança que possam causar riscos ou danos aos titulares de dados sejam comunicados à autoridade dentro de um prazo razoável, no entanto, não fornece especificações explícitas (art. 48, LGPD). Enquanto a agência nacional de proteção de privacidade, a Autoridade Nacional de Proteção de Dados (ANPD), poderá emitir orientações e regulamentos futuros, a partir do texto atual da LGPD, os requisitos para notificações de violação aguardam elaboração.[112]

APLICAÇÃO DO GDPR AOS APLICATIVOS DE RASTREAMENTO DIGITAL

Os especialistas em privacidade de dados identificaram vários problemas-chave nos aplicativos de rastreamento digital COVID-19 e possíveis problemas de conformidade com o GDPR. As orientações oficiais da UE demonstram como os desenvolvedores de aplicativos devem cumprir as diretrizes

divulgadas para permanecer dentro dos requisitos de proteção de dados do GDPR. O Conselho Europeu de Proteção de Dados (EDPB, sigla em inglês) enfatizou que a flexibilidade do GDPR pode permitir uma resposta eficiente à pandemia, ao mesmo tempo em que "protege os direitos e liberdades humanos fundamentais."[113] O EDPB observou que "como o vírus não conhece fronteiras, parece preferível desenvolver uma abordagem europeia comum em resposta à atual crise."[114]

O Parlamento Europeu concordou, recomendando "uma abordagem comum da UE para o uso de aplicativos [de rastreamento digital]."[115] O EDPB afirmou que o GDRP e a ePrivacy Directive[116] permite o uso responsável de dados anônimos ou pessoais para apoiar as autoridades públicas durante uma crise de saúde.[117] Para definir o escopo de tal uso responsável, no entanto, o EDPB emitiu diretrizes em abril de 2020 para "esclarecer as condições e os princípios do uso proporcional de dados de localização e ferramentas de rastreamento de contatos". Essas diretrizes ("as diretrizes de rastreamento") enfatizaram que o uso de aplicativos de rastreamento digital deve ser voluntário, anônimo, seguro e não deve se basear no rastreamento de movimentos individuais, mas em informações de proximidade dos usuários."[118] O EDPB também adotou diretrizes de processamento de dados no contexto de aplicativos de rastreamento digital ("as Diretrizes de Pesquisa Científica").[119]

O EDPB elaborou ainda que, para manter a privacidade e a proteção adequada dos dados, os princípios de minimização de dados devem ser mantidos em mente e o armazenamento de informações pessoais deve ser limitado.[120] Os servidores usados em um sistema de rastreamento digital devem limitar-se a coletar o histórico de contatos ou os identificadores pseudônimos de infectados confirmados ou manter uma lista de identificadores pseudônimos de usuários infectados apenas pelo tempo necessário.[121] Além disso, os aplicativos de

rastreamento digital não podem coletar essas informações, a menos que o usuário seja diagnosticado por uma ação voluntária pelas autoridades médicas apropriadas e não tente identificar usuários potencialmente infectados.[122] As diretrizes do EDPB também se concentram no princípio da limitação de finalidades.[123] Para evitar o uso indevido potencial das informações coletadas pelo rastreamento digital, como o uso de dados de localização para fins de investigações ou publicidade comercial, as diretrizes da EDPB declaram que as finalidades devem ser restritas ao gerenciamento da pandemia e as finalidades não relacionadas devem ser excluídas do uso de dados de rastreamento digital.[124] O EDPB também observou que "[as] implementações para rastreamento de contatos podem seguir uma abordagem centralizada ou descentralizada" e que ambos são sistemas válidos com suas próprias vantagens e desvantagens, desde que o sistema escolhido tenha a segurança adequada[125].

O Comissário de Informação do Reino Unido também emitiu orientações em 17 de abril de 2020, diretamente em resposta ao anúncio da API pela Apple-Google.[126] Ele apoiou o conceito da plataforma Bluetooth e elogiou a proposta de "alinhar-se com os princípios de proteção de dados by design e by default."[127] Em uma declaração de lançamento, Apple e Google enfatizaram que "a adoção do usuário é a chave para o sucesso e que acreditam que a forte proteção à privacidade é a melhor maneira de incentivar o uso desses aplicativos."[128] A plataforma da API proibirá os desenvolvedores de aplicativos de usar o GPS de um dispositivo móvel para rastrear a localização dos usuários ou transmitir a identidade do usuário.[129] Além disso, quaisquer dados coletados sobre informações acerca da infecção devem ser usados apenas pelas autoridades de saúde pública. A Apple e o Google declararam que eles próprios não coletarão dados pessoais de usuários, nem mo-

netizarão os dados.[130] As empresas também enfatizaram que os identificadores anônimos a serem enviados via Bluetooth serão gerados aleatoriamente e quaisquer metadados que sejam transmitidos entre os dispositivos serão criptografados.[131] O Comissário aprovou essa abordagem, mas enfatizou a necessidade de promover as melhores práticas de proteção de dados e levantar possíveis preocupações com a privacidade. O Comissário incentivou, ainda, o uso sistemático de criptografia, a minimização de dados, a transparência e o controle do usuário.[132]

As orientações do Comissário do Reino Unido e da EDPB destacam várias estruturas de privacidade que servirão como foco para os desenvolvedores de aplicativos de rastreamento digital que tentam cumprir o GDPR.[133] Um tema geral é o conceito de minimização de dados e restrição e anonimização dos dados coletados de indivíduos, coletando apenas o necessário para realizar o rastreamento digital. O EDPB sugeriu que os aplicativos não deveriam exigir o rastreamento da localização de usuários individuais, e sim confiar apenas nos dados de proximidade.[134] O processamento desses dados de proximidade também deve estar de acordo com uma das bases legais do GDPR para o processamento de dados pessoais: consentimento, execução de um contrato, interesse legítimo, interesse vital, exigência legal ou interesse público.[135] Assim, o procedimento de consentimento do usuário do aplicativo deve atender ao padrão do GDPR.[136] Além disso, as Diretrizes de Pesquisa Científica da EDPB exploram as bases legais disponíveis para o processamento de dados pessoais para uso "primário" e "secundário."[137] Outras recomendações de privacidade incluem a limitação de finalidade dos dados coletados para uso durante a crise da COVID-19;[138] preocupações com segurança e hackers, que podem aumentar significativamente em um banco de dados centralizado;[139] problemas de com-

partilhamento e armazenamento de dados;[140] e transparência e notificação dada aos usuários pelas autoridades de saúde no controle dos dados do aplicativo.[141] Antes da introdução da plataforma API Apple-Google, o Parlamento Europeu exigiu que "fosse dada total transparência aos interesses comerciais (fora da UE) dos desenvolvedores desses aplicativos" e solicitou que fossem mostradas projeções claras sobre como os aplicativos de rastreamento de contatos levarão a "um número significativamente menor de pessoas infectadas."[142] O Parlamento Europeu também defendeu que os estados da UE sejam “totalmente transparentes sobre o funcionamento dos aplicativos de rastreamento de contatos, para que as pessoas possam verificar o protocolo subjacente de segurança e privacidade e verificar o próprio código para ver se o aplicativo funciona como as autoridades estão reivindicando (...)”[143]

COMPARANDO O GDPR E A LGPD NO CONTEXTO DO COVID-19

Os problemas de proteção de dados da UE em relação ao rastreamento de contatos provavelmente aparecerão no Brasil quando o seu sistema baseado no GDPR, a LGPD, entrar em vigor no futuro.[144] As autoridades de saúde brasileiras que esperam usar um sistema centralizado ou a plataforma Apple-Google Bluetooth descentralizada para criar aplicativos de rastreamento de contato provavelmente deverão cumprir o novo quadro jurídico da LGPD para o uso de dados pessoais processados ou relacionados a cidadãos brasileiros.[145] As diferenças entre o GDPR e a LGPD resultarão potencialmente em diferentes restrições às ferramentas de vigilância pandêmica, dependendo da implementação final da LGPD. Embora as duas estruturas sejam semelhantes, a falta de orientação interpretativa do governo brasileiro para a LGPD representa um desafio para determinar como os aplicativos de rastrea-

mento digital podem ser forçados a operar. Na ausência de orientação oficial sobre como interpretar a LGPD, identificar e analisar as diferenças em relação ao GDPR pode prever o impacto potencial dessas diferenças.

Uma distinção significativa é a expansão na LGPD das bases legais do GDPR para processamento de dados. Nos dois regimes de proteção de dados, deve haver uma base legal para que os dados sejam processados sem que medidas sejam tomadas contra os agentes de tratamento. Como explicado anteriormente, o GDPR lista várias bases ou justificativas para o processamento de dados, uma das quais uma entidade deve afirmar para processar dados pessoais. As diretrizes da EDPB e da Comissão Europeia favorecem a busca de uma base legal para o processamento de informações de rastreamento de contatos digitais nos artigos 6(1)c e e do GDPR, combinados com os artigos 9(2)g e i.[146] O GDPR declara que o processamento é permitido quando "necessário para o cumprimento de uma obrigação legal a que o controlador está sujeito" ou quando "necessário para a execução de uma tarefa realizada no interesse público ou no exercício da autoridade oficial investida no controlador." Outras disposições do GDPR proíbem o processamento de categorias especiais de dados pessoais, incluindo dados de saúde, prevendo várias exceções. Uma dessas exceções abrange "razões de interesse público substancial" e outra fala diretamente em saúde pública (art. 9 da LGPD). Sob essa exceção, o processamento de dados pessoais de saúde é permitido quando é proporcional ao fim almejado e respeita os direitos do titular dos dados.

A LGPD expande a lista do GDPR para dez bases possíveis diferentes, que são, em princípio, semelhantes ao GDPR. A LGPD acrescenta duas bases relacionadas à saúde, com o Artigo 7, VII, permitindo o processamento de dados pessoais " para a proteção da vida ou da incolumidade física do titular

ou de terceiro" e o Artigo 7, VIII, permitindo o processamento de dados pessoais "para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária." Além disso, os pesquisadores recebem direitos explícitos para processar dados pessoais por meio do artigo 7, IV, desde que garantam, sempre que possível, o anonimato dos dados pessoais. Essas amplas bases legais podem facilitar a coleta e o rastreamento de dados de saúde no Brasil, especialmente em tempos de crise. É provável que uma lógica global de pandemia permita a coleta de dados pelas autoridades de saúde por meio de aplicativos de rastreamento de contatos no escopo da LGPD.

Uma adição importante aos direitos de privacidade dos usuários sob a LGPD é o direito adicional dos titulares de dados de acessar "informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados" (art. 18, VII da LGPD). Esse direito mais amplo de saber o que está sendo feito com os dados adquiridos a partir do rastreamento digital pode, se efetivado, obrigar os desenvolvedores de aplicativos de rastreamento de contato e as autoridades de saúde a aumentar a transparência a pedido dos titulares dos dados.

O artigo 5 da LGPD inclui uma definição semelhante de "dados pessoais" à definição do GDPR e ambos oferecem proteções adicionais de privacidade de dados a dados pessoais sensíveis, como dados pessoais de saúde. O artigo 11 da LGPD inclui o consentimento explícito do usuário como uma situação em que uma entidade pode processar legalmente dados pessoais sensíveis, mas também contém cláusulas semelhantes às do artigo 9(2) do GDPR. Os Artigos 11(2) b, c, e, f da LGPD refletem a base para o processamento de dados fornecidos nos Artigos 7(3), (4), (7) e (8) do GDPR para questões de ordem pública, entidades de pesquisa, proteção da vida

ou segurança física e proteção da saúde. O artigo 12 da LGPD observa especificamente que "dados anonimizados não serão considerados dados pessoais", desde que o processo de anonimização ao qual os dados foram submetidos não tenha sido revertido ou não possa ser revertido simplesmente aplicando "esforços razoáveis". Essa linguagem deixa a porta aberta em um contexto de sistema descentralizado, como a plataforma Apple-Google, para um possível argumento de que os dados coletados via Bluetooth envolvendo identificadores anônimos e nenhum banco de dados central não se enquadram em "dados pessoais".

Como a LGPD ainda não entrou em vigor, naturalmente haverá perguntas sobre a eficácia do novo esquema abrangente de proteção de dados do Brasil. Tais questões são destacadas pelas questões levantadas sobre a eficácia do esquema de aplicação da LGPD. A primeira questão levantada em comparação ao GDPR é a falta de impacto das multas que podem ser cobradas sob a LGPD. O GDPR prevê multas de até 2% da receita global de um infrator no ano anterior (art. 83). Por outro lado, a LGPD só pode ensejar multas de até 2% da receita de um infrator no Brasil, até um total de cinquenta milhões de reais por infração. Isso pode ser uma diferença substancial em grandes empresas multinacionais que exercem maior influência na coleta de dados.[147]

Além disso, também houve preocupações acerca da autoridade incumbida da implementação da lei, a ANDP. Embora as Agências de Proteção de Dados (DPA, sigla em inglês) criadas pelo GDPR tenham a intenção de ser agências independentes, a ANDP está sob controle do poder executivo.[148] Isso pode afetar negativamente a independência dos mecanismos de implementação do Brasil e abrir a LGPD para um uso indevido. Sem uma aplicação adequada, as proteções de privacidade fornecidas pela LGPD são incertas.[149] O grande número

de informações pessoais sensíveis sobre dados de saúde e localização que podem ser obtidas com a liberação de dados de rastreamento de contatos pode ser apropriado por atores hostis, seja no governo brasileiro ou por terceiros, sem o cumprimento rigoroso das leis de proteção de dados e privacidade.

Os requisitos de notificação de violação da LGPD também são muito mais incertos em comparação com os do GDPR. O GDPR exige que os controladores de dados relatem violações dentro de 72 horas após seu conhecimento da violação, ou quando praticável.[150] Em comparação, os requisitos de violação da LGPD não são fixados no texto da lei, exigindo apenas que os incidentes de segurança sejam endereçados à ANPD brasileira "em um período de tempo razoável", cabendo à ANPD emitir orientações futuras (art. 48 da LGPD).

CONCLUSÃO

Este capítulo se concentra em um dos aspectos mais discutidos da tecnologia de vigilância COVID-19: um sistema de rastreamento de proximidade baseado em dispositivos móveis para auxiliar na prevenção da propagação da COVID-19. A recente parceria da Apple e do Google permitirá o armazenamento de dados Bluetooth de telefones iOS e Android - um empreendimento histórico que operacionalizará aplicativos de rastreamento digital em todo o mundo. Sob a plataforma API da Apple e do Google, os usuários de um aplicativo de rastreamento digital durante a pandemia de COVID-19 podem compartilhar voluntariamente se e quando testarem positivo para o vírus. A plataforma da API depende de um modelo descentralizado e nenhum dado de localização geográfica pode ser coletado por nenhum aplicativo criado na plataforma. A Apple e o Google afirmam que o sistema é protetor de privacidade, pois os dados são descentralizados e criptografados e o armazenamento dos dados é temporário. [151]

Conforme discutido acima, os EUA não possuem uma lei federal de privacidade abrangente equivalente ao GDPR. No entanto, a API Apple-Google e os aplicativos de rastreamento digital suportados pela API ainda podem suscitar preocupações de privacidade nos níveis federal e estadual.[152] No nível federal, a coleta de qualquer informação de saúde corre o risco de acionar a Lei de Portabilidade e Responsabilidade do Seguro de Saúde (HIPAA, sigla em inglês) se os desenvolvedores de aplicativos fizerem parceria com as "entidades abrangidas" do HIPPA para desenvolver ou gerenciar seus aplicativos.[153] No nível estadual, há uma colcha de retalhos de leis de privacidade e segurança de dados que os desenvolvedores de aplicativos devem navegar. Por exemplo, a legislação da California, Consumer Privacy, que garante proteções abrangentes à privacidade do consumidor quanto a informações pessoais, inclui direitos de acesso, eliminação e exclusão da venda dessas informações.[154] A aplicação da Quarta Emenda da Constituição dos EUA ainda não foi verificada, e dependerá da coleta de dados relacionados à COVID-19 pelo governo sem ordem judicial e se os tribunais interpretarão a exigência da coleta de dados como uma busca e apreensão irrazoável.

Embora a proeminente plataforma Apple-Google API tenha capturado atenção internacional, várias outras ferramentas de vigilância de pandemia foram introduzidas para combater a propagação do vírus em diferentes comunidades em todo o mundo. Até a data desta publicação, as reportagens da mídia anunciaram que o Brasil desenvolveu ferramentas para ajudar a agregar a riqueza de dados públicos e privados relacionados à resposta do COVID-19 do governo em uma única fonte.[155] Com a assistência de empresas de tecnologia como Apple, Experian e outras - bem como universidades, governo nacional, governos locais e organizações internacionais - o "Radar COVID-19" do Brasil visa monitorar e prever a propa-

gação da pandemia e outras informações, como dados sobre suprimentos médicos e disponibilidade hospitalar.[156] Lançado em abril, o Radar fornece dados e estatísticas sobre o COVID-19, incluindo informações sobre casos confirmados, casos notificados e mortes em estados e municípios.[157] A plataforma serve como um hub centralizado para essas informações, agregando dados de fontes públicas e privadas para fornecer ao governo, pesquisadores e indivíduos brasileiros um banco de dados maior para usar.[158] O "Radar COVID-19" coleta dados anonimizados sobre os cidadãos, incluindo "sintomas e monitoramento geolocalizado" diariamente.[159] Tais práticas levam a perguntas sobre as implicações de privacidade que podem surgir no caso de vazamentos ou acesso indevido ao servidor central.

Seja centralizado e coletando dados de geolocalização, como o "Radar COVID-19" proposto, ou descentralizado e usando rastreamento de proximidade via Bluetooth, como os aplicativos potenciais da plataforma API, qualquer tipo de coleta de dados poderá questionada quando a LGPD entrar em vigor. No entanto, existem preocupações sobre a eficácia do esquema de proteção de dados proposto no Brasil para proteger os cidadãos de possíveis desvios e abusos no tratamento de dados pessoais que possam resultar dos programas de vigilância COVID-19. Questões como a força do esquema de imposição da LGPD, a independência da Autoridade Nacional de Proteção de Dados do Brasil e a incerteza dos requisitos de notificação de violação, provavelmente, desempenharão um papel na interação entre desenvolvedores de aplicativos de rastreamento de contatos, plataformas que suportam os novos sistemas de aplicativos e nova estrutura de proteção de dados brasileira.

Diante dessas incertezas, as conclusões a seguir podem ajudar a orientar os responsáveis por garantir a proteção de

dados. Primeiro, embora as orientações da UE sejam informativas, a LGPD varia de forma significativa em relação ao GDPR. As bases legais adicionais, um direito à informação abrangente e outras disposições podem criar uma estrutura mais branda no Brasil. Segundo, tanto se o Brasil escolher seguir a proposta centralizada do "Radar COVID-19" como se direcionar seus esforços para um aplicativo que usa uma abordagem descentralizada de rastreamento de contatos da API, a conversa sobre a coleta, uso e armazenamento de dados de geolocalização certamente será controversa. Além disso, o nível de anonimato necessário para evitar que os dados se enquadram na categoria "dados pessoais" é um tópico propício para interpretação nos tribunais brasileiros e por meio de orientação executiva semelhante à emitida na UE. Terceiro, é provável que surjam problemas de transparência e notificação do usuário, pois os usuários individuais exercem seus direitos, sob a LGPD, de saber exatamente como os dados coletados nos programas de vigilância sobre COVID-19 estão sendo armazenados e usados. Essa questão pode ser acentuada pelo eventual "fim" da pandemia, quando os titulares dos dados certamente reavaliam a quantidade de informações que estão confortáveis compartilhando fora do contexto de uma crise. Finalmente, devem ser feitas tentativas para minimizar os dados processados por essas ferramentas. Os programas de vigilância sobre COVID-19 devem se limitar à coleta de dados necessários para combater o vírus e permitir o acesso apenas a funcionários da saúde pública que desejem usar os dados como uma ferramenta de saúde pública. Navegar na legalidade de tais tecnologias sob a LGPD, independentemente de usarem um sistema centralizado ou descentralizado de coleta de dados, continuará sendo difícil. Devido à sua própria natureza de coleta de informações, essas ferramentas essenciais de rastreamento de contatos correm o risco de violar a priva-

cidade constitucional dos indivíduos em nome de uma causa maior. Assim, no contexto de uma pandemia internacional e de rastreamento de contatos, as proteções de privacidade oferecidas pela estrutura LGPD se tornarão mais cruciais do que nunca.

O GDPR e a LGPD são os primeiros de seu tipo. Eles fornecem um modelo potencial para proteção de dados e devem ser analisados por outras jurisdições comprometidas em adotar abordagens abrangentes de proteção à privacidade das informações. No entanto, ao mesmo tempo, é importante reconhecer as limitações do GDPR e da LGPD. Devido à complexidade dos direitos implicados pelas ferramentas de rastreamento de dados sobre COVID-19 e aplicativos de rastreamento digital, as leis de proteção de dados discutidas acima, em última análise, podem ser insuficientes para salvaguardar totalmente as liberdades e garantias fundamentais.

NOTAS

1. Tradução por Ester Borges.

2. Menezes, F. Z. (2020). Brazilian Location Platform In Loco Arrives in the United States, *Latin Am. Bus. Stories*, https://bit.ly/2BXbscV.

3. Menezes, op. cit. (explicando que "todas as informações coletadas pela In Loco são agrupadas, gerando insights que ajudam as empresas a entender melhor seus consumidores" e afirmando que a tecnologia é "30 vezes mais precisa que o GPS e permite que a plataforma identifique a localização de smartphones mesmo dentro de casa").

4. Mari, A. (2020). Brazil Introduces Surveillance Tech to Slow the Spread of Coronavirus: Hundreds of Thousands of Smartphones are Being Tracked to Support Lockdown Measures, *Brazil Tech*. https://zd.net/3gVPztf (afirmando que "a cidade está rastreando pelo menos 700.000 smartphones para identificar onde as regras de bloqueio estão sendo seguidas").

5. Mari, A., op. cit.

6. Mari, A., op. cit.

7. Klosek, J. et al. (2020). Contact Tracing Apps in the UK, EU and US: Privacy Implications, *JDSUPRA*. https://bit.ly/32d6fs7 ("[T]he United States does not have a broadly applicable federal privacy law that applies to all personal data across industry sectors").

8. *id*. ("CCPA grants expansive consumer privacy protections through new data privacy rights").

9. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018); Freiwald, S.; Smith, S.W. (2018). The Carpenter Chronicle: A Near-Perfect Surveillance, 132 *Harv. L. Rev*. 205, 208 ("The first federal legislation to deal with tracking devices was the Electronic Communications Privacy Act of 1986 (ECPA), a wide-ranging and complex statute.").

10. Carpenter v. United States (2018), 138 S. Ct. 2206, 2211. ("whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements").

11. *id*. at 2216 (observando que o Tribunal havia anteriormente rejeitado a aplicação da Quarta Emenda a uma coleção de registros porque os documentos eram "registros comerciais" do banco).

12. *id*. at 2220 ("Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection. The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.").

13. Taylor, D. B. (2020). How the Coronavirus Pandemic Unfolded: A Timeline, *NY Times*. https://nyti.ms/2Dvo1JF (declarando que o coronavírus apareceu pela primeira vez em um mercado chinês de frutos do mar e aves).

14.Taylor, D. B., op.cit. (declarando que o coronavírus matou mais de 346.000 e infectou mais de cinco milhões de pacientes em questão de meses).

15.Taylor, D. B., op.cit. (observando que a doença se espalhou para pelo menos 117 países).

16. Meaker, M. (2020). Coronavirus Contact Tracing and the Right to Privacy in a Pandemic, World Pol. Rev. https://bit.ly/2DxOhpO

17. Meaker, M., op. cit.

18. Woodhams, S. (2020) COVID-19 Digital Rights Tracker, *Top10VPN*. https://bit.ly/3fqozi1 (listando as respostas dos países ao coronavírus e os protocolos e procedimentos que estão sendo adotados); Meaker, M., op. cit.

19. Woodhams, op. cit..

20. Woodhams, op. cit..

21. Huang, Y. et al., (2020) How Digital Contact Tracing Slowed Covid-19 in East Asia, *Harv. Bus. Rev.* https://bit.ly/3frN690

22. Recommendations on Privacy and Data Protection in the Fight Against COVID-19 (2020), *Access Now*, https://bit.ly/2OpdCUY

23. *Id.*

24. *Id.*

25. *Id.*

26. *Id.*

27. *Id.* (Explicando que o governo usa o monitoramento de redes móveis para impor a quarentena para pessoas recém chegadas ao país ou pessoas em risco).

28. *Id.*

29. Woodhams, op. cit..

30. Evans, J. (2020). Test and Trace with Apple and Google, *TechCrunch*. https://tcrn.ch/2CsTu1Q

31. Zastrow, M. (2020). Coronavirus Contact-Tracing Apps: Can They Slow the Spread of COVID-19?, *Nature*. https://go.nature.com/32f60ws

32. Zastrow, M. (2020). Coronavirus Contact-Tracing Apps: Can They Slow the Spread of COVID-19?, *Nature*. https://go.nature.com/32f60ws

33. Gurman et al. (2020). Apple, Google's COVID-19 Tracing Tool is One Big Step Closer to Being Put to Use, *Fortune*. https://bit.ly/3907j40

34. Criddle, C.; Kelion, L (2020). Coronavirus Contact-tracing: World Split Between Two Types of App, *BBC* https://bbc.in/3099EFs

35. Ingram, D.; W, Jacob (2020). Behind the global efforts to make a privacy-first coronavirus tracking app, *NBC News*. https://nbcnews.to/2CtB6Ws

36. Lemos, R. (2020). Centralized Contact Tracing Raises Concerns Among Privacy-Conscious Citizens, *Dark Reading*. https://bit.ly/2WfqVMe

37. Ingram & Ward, op.cit.; Woodhams, op. cit.; Srivastava, M. (2020). How India is using its contact tracing app Aarogya Setu to Prevent COVID-19's Spread, *KrAsia*, https://bit.ly/3flvxbb.

38. Albergotti, R.; Harwell, D. Apple and Google Are Building a Virus-Tracking System. Health Officials Say It Will Be Practically Useless, *Wash. Post*. https://wapo.st/3frDoWi

39. Albergotti, R.; Harwell, D., op. cit.

40. Albergotti, R.; Harwell, D., op. cit.

41. Albergotti, R.; Harwell, D., op. cit.

42. *Private Automated Contact Tracing*, Mass. Inst. Tech. https://bit.ly/3fq2fbB

43. *Covid Watch*, Stanford Univ. https://covid-watch.org

44. Zastrow, M. (2020). Coronavirus Contact-Tracing Apps: Can They Slow the Spread of COVID-19?, *Nature*. https://go.nature.com/32f60ws

45. Zastrow, M. (2020). Coronavirus Contact-Tracing Apps: Can They Slow the Spread of COVID-19?, *Nature*. https://go.nature.com/32f60ws

46. Lomas, N. (2020). Europe's PEPP-PT Covid-19 Contacts Tracing Standard Push Could Be Squaring Up for a Fight with Apple and Google, *TechCrunch*. https://tcrn.ch/2On1NyY

47. Eur. Parl. Doc. (COM P9_TA (2020)0054) Seção 52. https://bit.ly/2DEnTL6

48. Eur. Parl. Doc. (COM P9_TA (2020)0054) Seção 52. https://bit.ly/2DEnTL6

49. Zastrow, M. (2020). Coronavirus Contact-Tracing Apps: Can They Slow the Spread of COVID-19?, *Nature*. https://go.nature.com/32f60ws

50. Zastrow, M. (2020). Coronavirus Contact-Tracing Apps: Can They Slow the Spread of COVID-19?, *Nature*. https://go.nature.com/32f60ws

51. Serge Vaudenay, Centralized or Decentralized? The Contact Tracing Dilemma, *Cryptology ePrint Archive* (6 de maio de 2020), p. 29. https://eprint.iacr.org/2020/531.pdf.

52. Albergotti, R.; Harwell, D., op. cit.

53. Criddle & Kelion, op. cit.

54. Lomas, op. cit.

55. Criddle & Kelion, op. cit.

56. Lomas, op. cit. (enfatizando que o núcleo dos PEPP-PT é "'privacy-preserving' claim rests on the use of system architectures that do not require location data to be collected").

57. Zastrow, op. cit.

58. Ratnam, G. (2020). Apple, Google Release Template for COVID-19 Contact Tracing Apps, *RollCall.com.* https://bit.ly/2Wf7xyZ.

59. Ratnam, G., ibid.

60. Ratnam, G., ibid.

61. Ratnam, G., ibid.

62. Zastrow, op. cit..

63. Zastrow, ibid.

64. Zastrow, ibid.

65. Zastrow, ibid.

66. Gurman et al., op. cit..

67. Ratnam, op. cit..

68. Ratnam, ibid.

69. Gurman et al., op. cit..

70. Gurman et al., ibid.

71. Ratnam, op. cit..

72. Ratnam, op. cit..

73. Nellis, S; Paresh, D. (2020). Apple, Google ban use of location tracking in contact tracing apps, *Reuters*. https://reut.rs/3fsl7p3

74. Nellis & Paresh, ibid.

75. Gurman et al., op. cit..

76. *Id.*

77. Ratnam, op. cit..

78. Ollstein, A.M.; Ravindranath, M. (2020). Getting it Right: States Struggle with Contact Training Push, *Politico*. https://politi.co/2OlizhF

79. *Id.*

80. Albergotti & Harwell, op. cit.. 37.

81. Morrow, A. (2020). France to Test Controversial Covid-19 Tracking App During Lockdown Exit, *RFI*. https://bit.ly/2AZdGIe

82. Smith, C. (2020). Switzerland is the First to Use Apple-Google Coronavirus Contact Tracing Technology, *BGR*. https://bit.ly/32qN3az

83. *Id.*

84. Zastrow, op. cit..

85. *Id.*

86. Wolford, B. What is GDPR, The EU's New Data Protection Law? *GDPR.EU*. https://bit.ly/3i5RKLk.

87. Conselho da Europa, Convenção Europeia para a Proteção dos Direitos Humanos e Liberdades Fundamentais, conforme emendada pelos Protocolos Nos. 11 e 14. (4 de novembro de 1950).

88. Diretiva 95/46/ CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa ao tratamento de dados pessoais e à livre circulação de dados (Diretiva Europeia de Proteção de Dados), JO 1995 (L 281).

89. Wolford, op. cit..

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

94. 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).

95. Wolford, op. cit..

96. GDPR, par. 8–9.

97. *Id.* at 39–47.

98. *Id.* at 9.

99. Wolford, op. cit..

100. Wolford, ibid.

101. Paes, A.T. (2017). Privacy and Data Protection in Brazil, 5 *JL & Cyber Warfare* 225, 230 (apresentando um cronograma da legislação brasileira em torno da proteção de dados a partir de 2015).

102. Rustad, M.L.; Koenig, T.H. (2019). Towards A Global Data Privacy Standard, 71 *Fla. L. Rev.* 365, 446–47.

103. McGruer, J. (2020) Emerging Privacy Legislation in the International Landscape: Strategy and Analysis for Compliance, 15 Wash. JL Tech. & Arts 120, 155-56 (Explicando que a LGPD regula "the processing of personal data in Brazil, processing in connection with providing goods or services to individuals in Brazil, and personal data collected in Brazil").

104. Paes, op. cit.., p. 226-27. (descrevendo o Artigo 5 da Constituição brasileira).

105. *Id.*

106. Erickson, A. (2019) Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD, 44 Brook. J. Int'l L. 859, 872.

107. Paes, op. cit.. 228-29. (comparing the Civil Code with the Consumer Defense Code).

108. *Id*. at 229 "In essence, this law addresses principles, users' rights, data storage, and limited access to personal data.".

109. *Id*. at 883.

110. *Id*. no artigo 7.

111. Erickson, op. cit., no 882 (afirmando que a "falta de proscrição e ausência de textos explicativos" pode causar confusão e incerteza para as organizações brasileiras que procuram cumprir).

112. Erickson, ibid., no 884 (observando que a linguagem vaga da LGPD "deixa muito espaço" para a ANPD criar diretrizes adicionais sobre a notificação de violação).

113. Conselho Europeu de Proteção de Dados, Diretrizes 04/2020 -, ,sobre o uso de dados de localização e ferramentas de rastreamento de contatos no contexto do surto de COVID-19. https://bit.ly/3freTa3

114. *Id.*

115. EP Statement.

116. Diretiva 2002/58 / CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (diretiva relativa à privacidade e às comunicações eletrónicas), JO 2002 (L 201).

117. Conselho Europeu de Proteção de Dados, Diretrizes 04/2020, sobre o uso de dados de localização e ferramentas de rastreamento de contatos no contexto do surto de COVID-19. https://bit.ly/2WbXf2w

118. *Id.*

119. *Id.*

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. Gabinete do Comissário da Informação (2020), ref. No. 2020/01, Apple and Google joint initiative on COVID-19 contact tracing technology. https://bit.ly/3j23FLi

127. *Id.*

128. Gurman et al., op. cit..

129. Ratnam, op. cit..

130. *Id.*

131. *Id.*

132. Gabinete do Comissário da Informação, op. cit..

133. Klosek et al., op. cit..

134. Conselho Europeu de Proteção de Dados, Diretrizes 04/2020, sobre o uso de dados de localização e ferramentas de rastreamento de contato no contexto do surto de COVID-19. https://bit.ly/3freTa3.

135. Hinely, M. (2018). *GDPR Fundamentals: Legal Basis For Processing*, KirkpatrickPrice Blog. https://bit.ly/3j2qZZp

136. Klosek et al., op. cit..

137. Conselho Europeu de Proteção de Dados, Diretrizes 03/2020, sobre o tratamento de dados referentes à saúde para fins de pesquisa científica no contexto do surto de Covid-19. https://bit.ly/2OlgcLR

138. *Id.*

139. EP Statement, op. cit..

140. Conselho Europeu de Proteção de Dados, Diretrizes 03/2020, sobre o tratamento de dados referentes à saúde para fins de pesquisa científica no contexto do surto de Covid-19. https://bit.ly/2OlgcLR

141. *Id.*

142. EP Statement, op. cit..

143. *Id.*

144. Brook, C. (2019). Breaking Down LGPD, Brazil's New Data Protection Law, *Digital Guardian Blog*. https://bit.ly/3067OFx.

145. Schreiber, M. (2020). Coronavírus: uso de dados de geolocalização contra pandemia em risco de privacidade? *BBC*. https://bbc.in/2CucCfJ

146. Scantambulo, E. et al. (2020). COVID-19 e Contact Tracing Apps: A Review Under the European Legal Framework, *arXiv*. https://bit.ly/2OoaGrM

147. Erickson, Ibid., 861-62.

148. *Id.*

149. *Id.* em 887.

150. *Id.* em 881.

151. Ng, A.& Shankland, S. (2020). Apple and Google's coronavirus tracking tool: How privacy fits in, *Cnet.* https://cnet.co/2DFd5fJ

152. Klosek et al., op. cit., p. 6.

153. *Id.*

154. Lei de Privacidade do Consumidor da Califórnia de 2018, AB 375 (CCPA).

155. Por exemplo, Edwards, N. (2020). Tech Giants Like Apple, Experian, And Google Fight Pandemic With Digital Tools, *Forbes*. https://bit.ly/2AVNRbT

156. Id.

157. Companies and organizations launch Covid Radar, a platform for action against the pandemic (2020). https://bit.ly/3fqXe2p; *Radar Covid-19 monitora*

dados do coronavírus no Brasil e no MT, Tribunal de Contas Mato Grosso. https://bit.ly/38U6Z6K

158. *Id*.; Edwards, N. op.cit..

159. Companies and Organizations Launch Covid Radar, A Platform for Action Against the Pandemic (2020). *EXPERIAN*. https://bit.ly/3j3vO5o

ESTE LIVRO FOI COMPOSTO COM AS FAMÍLIAS TIPOGRÁFICAS *DECIMA MONO* E *FF META*. PARA O MIOLO FOI UTILIZADO O PAPEL *OPALINA* 120G/M² E PARA A CAPA O PAPEL *DUO DESIGN* 300G/M². O PROJETO GRÁFICO É DE AUTORIA DO *ESTÚDIO CLARABOIA* E AS ILUSTRAÇÕES SÃO DA *PINGADO SOCIEDADE ILUSTRATIVA*. FORAM IMPRESSAS 250 CÓPIAS PELA GRÁFICA *CINELÂNDIA* EM NOVEMBRO DE 2020.