**PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ**
**ESCOLA DE DIREITO**
**PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD**

**JOÃO PAULO MACHADO PIRATELLI**

# *BIG DATA* E SISTEMA DE JUSTIÇA CRIMINAL NO ESTADO BRASILEIRO CONTEMPORÂNEO

**CURITIBA (PR)**
**2024**

**JOÃO PAULO MACHADO PIRATELLI**

# *BIG DATA* E SISTEMA DE JUSTIÇA CRIMINAL NO ESTADO BRASILEIRO CONTEMPORÂNEO

Dissertação apresentada ao Programa de Pós-Graduação em Direito, na área de concentração de Direito Socioambiental e Sustentabilidade e na linha de pesquisa em Estado, Sociedades, Povos e Meio Ambiente, da Escola de Direito da Pontifícia Universidade Católica do Paraná, como requisito parcial à obtenção do título de Mestre em Direito.

Orientadora: Prof.ª Dr.ª Cinthia Obladen de Almendra Freitas

**CURITIBA (PR)**
**2024**

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central
- CRB /

Piratelli, João Paulo Machado

*Big Data* e Sistema de Justiça Criminal no Estado Brasileiro Contemporâneo / João Paulo Machado Piratelli; orientadora: Cinthia Obladen de Almendra Freitas . – 2024.

118 f. ; 30 cm.

Dissertação (mestrado) - Pontifícia Universidade Católica do Paraná, Curitiba, 2024.

Bibliografia: p. 105-118.

1. Sociedades. 2. Novas Tecnologias. 3. Estado Contemporâneo. 4. Sistema de Justiça Criminal. 5. *Big Data*. I. Freitas, Cinthia Obladen de Almendra. II. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Direito. III. Título.

Dóris 3. ed. –

**JOÃO PAULO MACHADO PIRATELLI**

# *BIG DATA* E SISTEMA DE JUSTIÇA CRIMINAL NO ESTADO BRASILEIRO CONTEMPORÂNEO

Dissertação apresentada ao Programa de Pós-Graduação em Direito, na área de concentração de Direito Socioambiental e Sustentabilidade e na linha de pesquisa em Estado, Sociedades, Povos e Meio Ambiente, da Escola de Direito da Pontifícia Universidade Católica do Paraná, como requisito parcial à obtenção do título de Mestre em Direito.

**BANCA EXAMINADORA**

_____
Profa. Dra. Cinthia Obladen de Almendra Freitas (orientadora)

_____
Profa. Dra. Heline Sivini Ferreira (PPGD PUCPR)

_____
Prof. Dr. Jean Paul Barddal (PPGIa PUCPR)

_____
Profa. Dra. Danielle Jacon Ayres Pinto (PPGRI UFSC)

Curitiba (PR), 21 de março de 2024.

A todos que moram no meu coração, que sempre me apoiaram, incondicionalmente, não só em todos os projetos de trabalho e de estudo, mas em todos os momentos de minha vida**.**

# AGRADECIMENTOS

A Deus, por tudo.

À minha família e amigos, pela compreensão para comigo, pelas muitas horas de ausência, durante as quais foram necessários empenho e dedicação para a realização desta pesquisa e para a elaboração deste escrito acadêmico.

Um agradecimento especial à minha namorada Marcelle pelo carinho, dedicação e revisões contínuas.

Um agradecimento especial à minha mãe Nilza pelo incentivo e ternura.

À minha orientadora, Prof.ª Dr.ª Cinthia Obladen de Almendra Freitas, pela oportunidade, confiança, paciência, incentivo e ensinamento infinitos.

A todos os docentes e discentes do Programa de Pós-Graduação *Stricto Sensu* em Direito da Pontifícia Universidade Católica do Paraná, onde encontrei o ambiente e a infraestrutura ideais para desenvolver este trabalho.

Por fim, mas não menos importante, à Pontifícia Universidade Católica do Paraná, ao Ministério da Educação e ao Ministério da Justiça e da Segurança Pública que – por meio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior e do Programa de Cooperação Acadêmica em Segurança Pública e Ciências Forenses – financiaram esta pesquisa.

A todos vocês, a minha eterna gratidão.

“*Quid est veritas? Est vir qui adest*”.

Anagrama por Agostinho de Hipona
(354 d.C. – 430 d.C.)

# RESUMO

A dissertação de Mestrado, desenvolvida por meio de pesquisa que empregou o método hipotético-dedutivo, insere-se na Área de Concentração de “Direito Socioambiental e Sustentabilidade” e na linha de pesquisa de “Estado, Sociedades, Povos e Meio Ambiente”, da Escola de Direito, da Pontifícia Universidade Católica do Paraná. Tem, por objeto de estudo, o problema sintetizado por meio da seguinte pergunta: no atual contexto brasileiro, em que medida é juridicamente viável utilizar ferramentas de Computação Forense baseadas em Big Data no Sistema de Justiça Criminal? A hipótese de pesquisa é a de que o uso desse tipo de tecnologia no âmbito penal ainda não é possível no Brasil por inexistirem normas jurídicas que tratem especificamente sobre o tema. Estuda-se a formação e a evolução do Estado Contemporâneo, a sua relação com a vigilância e com o Panspectron no âmbito da Sociedade Informacional, e como ele – o Estado Contemporâneo – tem utilizado dados, pessoais ou não, para fins de espionagem e controle social e, também, no Sistema de Justiça Criminal. Na sequência discorre-se sobre a evolução histórica da Ciência da Computação ao mesmo tempo em que são apresentadas suas principais características, com destaque para o *Big Data* e para a Computação Forense. Para, então, apresentar os resultados das pesquisas anteriormente desenvolvidas na PUCPR e em conjunto com a Polícia Científica do Paraná no bojo dos projetos SiCReT e SiCReT II, assim como a relação desses estudos com o uso do *Big Data* no Sistema de Justiça Criminal. No contexto jurídico, discorre-se sobre o direito fundamental à proteção de dados pessoais e sobre os projetos de lei em trâmite que versam sobre a criação de uma Lei Geral de Proteção de Dados Pessoais em matéria penal, e como tudo isso se relaciona com a utilização do *Big Data* para fins penais. Concluiu-se que a hipótese de pesquisa é verdadeira, pois o uso do *Big Data* no atual Sistema de Justiça Criminal brasileiro não é juridicamente possível em razão da ausência de normas jurídicas específicas para isso, devendo prevalecer o direito fundamental à proteção de dados pessoais.



**Palavras-chave**: Sociedades. Novas Tecnologias. Estado Contemporâneo. Sistema de Justiça Criminal. *Big Data*.

# ABSTRACT

The master's thesis, developed through research that used the hypothetical-deductive method, falls within the Concentration Area of “Socio-environmental Law and Sustainability” and in the research line of “State, Societies, People and Environment”, of School of Law, Pontifical Catholic University of Paraná. The object of study is the problem summarized through the following question: in the current Brazilian context, to what extent is it legally viable to use Forensic Computing tools based on Big Data in the Criminal Justice System? The research hypothesis is that the use of this type of technology in the criminal sphere is not yet possible in Brazil as there are no legal standards that specifically address the topic. The formation and evolution of the Contemporary State is studied, its relationship with surveillance and Panspectron within the scope of the Information Society, and how it – the Contemporary State – has used data, personal or otherwise, for espionage and control purposes. social and also in the Criminal Justice System. Next, the historical evolution of Computer Science is discussed while its main characteristics are presented, with emphasis on Big Data and Forensic Computing. To then present the results of research previously developed at PUCPR and in conjunction with the Scientific Police of Paraná within the SiCReT and SiCReT II projects, as well as the relationship of these studies with the use of Big Data in the Criminal Justice System. In the legal context, it discusses the fundamental right to the protection of personal data and the bills in progress that deal with the creation of a General Law for the Protection of Personal Data in criminal matters, and how all this relates to the use of Big Data for criminal purposes. It was concluded that the research hypothesis is true, as the use of Big Data in the current Brazilian Criminal Justice System is not legally possible due to the absence of specific legal standards for this, and the fundamental right to the protection of personal data must prevail.



**Key-words:** Societies. New technologies. Contemporary State. Criminal Justice System. Big Data.

# LISTA DE ILUSTRAÇÕES

Figura 1 - Prisão baseada no panóptico 31
Figura 2 - Modelo de vigilância contemporânea 36
Figura 3 - Os cinco “Vs” do *Big Data* 57
Figura 4 - Do *Big Data* ao conhecimento 61
Figura 5 - Fluxograma do Direito Processual Penal 63
Figura 6 - Cruzamento de registros telefônicos entre arquivos 77

# LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| a. | ano |
| ABIN | Agência Brasileira de Inteligência |
| abr. | abril |
| a.C. | antes de Cristo |
| ago. | agosto |
| ampl. | ampliada |
| ANPD | Autoridade Nacional de Proteção de Dados |
| art(s). | artigo(s) |
| atual. | atualizado(a) |
| BA | Estado da Bahia |
| *BBC* | *British Broadcasting Corporation*; Corporação Britânica de Radiodifusão |
| *Big Techs* | *Big Technology Companies*; Grandes Companhias de Tecnologia |
| CAPES | Coordenadoria de Aperfeiçoamento de Pessoal de Nível Superior |
| CE | Estado do Ceará |
| CF | Constituição Federal |
| CFTV | Circuito Fechado de Televisão |
| CNJ | Conselho Nacional de Justiça |
| *COMPAS* | *Correctional Offender Management Profiling for Alternative Sanctions*; "Perfil de Gerenciamento de Infratores Correcionais para Sanções Alternativas |
| CPP | Código de Processo Penal |
| CRB | Conselho Regional de Biblioteconomia |
| dez. | dezembro |
| DF | Distrito Federal |
| DIMOS | Dispositivos Móveis e Sêniores |
| DJe | Diário da Justiça eletrônico |
| DL | Decreto-Lei |
| Dr. | Doutor |
| Dr.ª | Doutora |
| EC | Emenda Constitucional |
| ed. | edição |
| EJJL | Espaço Jurídico Journal of Law |
| EMERJ | Escola da Magistratura do Estado do Rio de Janeiro |
| ES | Estado do Espírito Santo |
| ESG | Escola Superior de Guerra |
| ESPIN | Estado de Emergência em Saúde Pública de Importância Nacional |
| ESPMU | Escola Superior do Ministério Público da União |
| *et al.* | *et alii*; e outros |
| *etc.* | *et cetera*; e outras coisas |
| EUA | Estados Unidos da América |
| f. | folha(s) |
| FADUSP | Faculdade de Direito da Universidade de São Paulo |
| fev. | fevereiro |
| FFLC | Faculdade de Filosofia, Letras e Ciências Humanas |
| FDV | Faculdade de Direito de Viçosa |
| GEN | Grupo Editorial Nacional |
| *GPS* | *Global Positioning System*; Sistema de Posicionamento Global |

| | |
|---|---|
| *HC* | *Habeas Corpus* |
| *HTML* | *Hyper Text Markup Language*; Linguagem de Marcação de Hipertexto |
| *HTTP* | *Hyper Text Transfer Protocol*; Protocolo de Transferência de Hipertexto |
| *IBM* | *International Business Machine Corporation*; |
| IDP | Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa |
| IEA | Instituto de Estudos Avançados |
| IF | Instituto de Física |
| IHGB | Instituto Histórico e Geográfico Brasileiro |
| il. | ilustrado |
| IME | Inferência para a Melhor Explicação |
| IME | Instituto de Matemática e Estatística |
| inc(s). | inciso(s) |
| *IoT* | *Internet of Things* |
| IVR | Inteligência, Vigilância e Reconhecimento |
| j. | julgado em |
| jan. | janeiro |
| jul. | julho |
| jun. | junho |
| L. | Lei |
| LGPD | Lei Geral de Proteção de Dados |
| *LLC* | *Limited Liability Company*; sociedade de responsabilidade limitada |
| LTC | Livros Técnicos e Científicos |
| mai. | maio |
| mar. | março |
| Me. | Mestre |
| MEC | Ministério da Educação |
| MG | Estado de Minas Gerais |
| MJSP | Ministério da Justiça e da Segurança Pública |
| Min. | Ministro(a) |
| *MIT* | *Massachusetts Institute of Technology*; Instituto de Tecnologia de Massachusetts |
| n. | número |
| *NASA* | *National Aeronautics and Space Agency*; Agência Nacional Espacial e Aeronáutica |
| *NIST* | *National Institute of Standards and Technology* |
| *NoSQL* | *Not Only Structured Query Language*; Não Apenas Linguagem de Consulta Estruturada |
| nov. | novembro |
| *Nov.* | *November*; novembro |
| *NSA* | *National Security Agency*; Agência de Segurança Nacional |
| *NY* | *State of New York*; Estado de Nova York |
| *NYC* | *New York City*; Cidade de Nova York |
| out. | outubro |
| p. | página(s) |
| par. | parágrafo |
| PCCh | Partido Comunista Chinês |
| PCP | Polícia Científica do Paraná |
| *PeeJ* | *Perverted Justice*; Justiça Pervertida |
| PL. | Projeto de Lei |
| PLN | Processamento de Linguagem Natural |

| | |
|---|---|
| PPGD | Programa de Pós-Graduação *Stricto Sensu* em Direito |
| PPGIa | Programa de Pós-Graduação em Informática |
| PPGRI | Programa de Pós-Graduação em Relações Internacionais |
| PR | Estado do Paraná |
| *PredPol* | *Predictive Policing*; Policiamento Preditivo |
| PROCAD | Programa de Cooperação Acadêmica |
| Prof. | Professor |
| Prof.ª | Professora |
| PUC | Pontifícia Universidade Católica |
| RDP | Revista de Direito Público |
| Rel. | Relator(a) |
| rev. | revisto(a) |
| RJ | Estado do Rio de Janeiro |
| RPC | República Popular da China |
| RS | Estado do Rio Grande do Sul |
| RT | Revista dos Tribunais |
| RUNA | Repositório Universitário da Ânima |
| s/p. | sem página |
| SC | Estado de Santa Catarina |
| SERPRO | Serviço Federal de Processamento de Dados |
| set. | setembro |
| SIBI | Sistema Integrado de Bibliotecas |
| SiCReT | Sistema de Cruzamento de Registros Telefônicos |
| SISNAD | Sistema Nacional de Políticas Públicas sobre Drogas |
| SP | Estado de São Paulo |
| SPCF | Segurança Pública e Ciências Forenses |
| ss. | seguintes |
| STF | Supremo Tribunal Federal |
| STJ | Superior Tribunal de Justiça |
| t. | tomo |
| TCC | Trabalho de Conclusão de Curso |
| *TEC* | *Institute for Technology, Entrepreneurship and Culture*; Instituto de Tecnologia, Empreendedorismo e Cultura |
| TIC | Tecnologias da Informação e Comunicação |
| tir. | tiragem |
| UCLA | Universidade da Califórnia em Los Angeles |
| UERJ | Universidade Estadual do Rio de Janeiro |
| UFCE | Universidade Federal do Ceará |
| UFGRS | Universidade Federal do Rio Grande do Sul |
| UFJF | Universidade Federal de Juiz de Fora |
| UFSC | Universidade Federal de Santa Catarina |
| UnB | Universidade de Brasília |
| UNISUL | Universidade do Sul Catarinense |
| UNOESC | Universidade do Oeste de Santa Catarina |
| *URL* | *Uniform Resource Locator*; Localizador-Padrão de Recursos |
| *USA* | *United States of America*; Estados Unidos da América |
| USP | Universidade de São Paulo |
| v. | volume |
| *VR* | *Virtual Reality*; Realidade Virtual |

# SUMÁRIO

**1 INTRODUÇÃO** 15

**2 A UTILIZAÇÃO DE DADOS PELO ESTADO CONTEMPORÂNEO NO CONTEXTO DO PANSPECTRON** 19

2.1 ESTADO, DADOS E INFORMAÇÃO 20

2.2 DA VIGILÂNCIA AO PANSPECTRON 29

2.3 A UTILIZAÇÃO DE DADOS PELO ESTADO CONTEMPORÂNEO 37

2.3.1 Espionagem: o caso Edward Snowden e a Agência de Segurança Nacional dos Estados Unidos da América 37

2.3.2 Controle social: o exemplo do crédito social chinês 40

2.3.3 Sistema de Justiça Criminal: as ferramentas computacionais *PredPol*, *HunchLab*, *COMPAS* e *Detecta* 42

2.4 ALGUMAS CONSIDERAÇÕES 45

**3 CIÊNCIA DA COMPUTAÇÃO, *BIG DATA* E COMPUTAÇÃO FORENSE** 46

3.1 CIÊNCIA DA COMPUTAÇÃO: HISTÓRICO E ASPECTOS BASILARES 47

3.2 CONCEITO E CARACTERÍSTICAS DO *BIG DATA* 55

3.3 COMPUTAÇÃO FORENSE: A CIÊNCIA DA COMPUTAÇÃO NO SISTEMA DE JUSTIÇA CRIMINAL 61

3.4 ALGUMAS CONSIDERAÇÕES 73

**4 REFLEXÕES JURÍDICAS ACERCA DA UTILIZAÇÃO DO *BIG DATA* PELO SISTEMA DE JUSTIÇA CRIMINAL BRASILEIRO** 75

4.1 OS PROJETOS DE PESQUISA “SiCReT” E “SiCReT II” E A POSSIBILIDADE DE CRIAÇÃO DO *BIG DATA* PARA FINS PENAIS 75

4.2 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS NO BRASIL 81

4.3 A (IN)VIABILIDADE JURÍDICA DO USO DE *BIG DATA* PELO SISTEMA DE JUSTIÇA CRIMINAL BRASILEIRO 89

4.4 ALGUMAS CONSIDERAÇÕES 100

**5 CONCLUSÃO** 102

**REFERÊNCIAS** 106

# 1 INTRODUÇÃO

A Sociedade Informacional é uma realidade contemporânea. A vida humana mergulhou nos meios digitais, sendo inimaginável conceber as relações sociais sem serem permeadas pelo uso da tecnologia.

A vigilância, consectário natural desse modo de vida atual, imerso na tecnologia, ganhou proporções jamais vistas. Praticamente todos os aspectos da realidade já são capturados por dispositivos tecnológicos e registrados por meio de dados (pessoais ou não). Portanto, a Sociedade Informacional concretiza o Panspectron, termo que nomeia o estado de vigilância sobre tudo e sobre todos, e de todas as formas possíveis, seja de modo voluntário ou não.

Nesse contexto, também o Estado Contemporâneo foi atingido pela mediação da cultura tecnológica nas sociedades humanas e se modificou. A própria utilização de dados extraídos desse manancial da tecnologia para a elaboração de Políticas Públicas nas mais diversas áreas já é algo comum. Não seria diferente no âmbito da Justiça e, particularmente, no da Justiça Criminal, haja vista que muitos são os crimes cometidos nos meios digitais, e outros delitos dependem, necessariamente, dos meios digitais, para serem praticados.

A importância da Computação Forense, nesse cenário, é inegável. A apreensão de dispositivos móveis, o monitoramento das comunicações interpessoais e a análise de dados extraídos das mais avançadas tecnologias tendem, mais e mais, à indispensabilidade do emprego da tecnologia para o esclarecimento do *iter criminis* e para a solução de casos penais.

A pesquisa desenvolvida no presente trabalho tem demonstrado a possibilidade do aperfeiçoamento das ferramentas computacionais, para tornar mais eficiente o Sistema de Justiça Criminal, até mesmo com a possível utilização de ferramentas baseadas em *Big Data* — “Dados Grandes”, na expressão literal vertida livremente para o português.

Ocorre que a propagação de tecnologias baseadas em *Big Data* é algo recente. Os custos e a *expertise* que esse tipo de ferramenta exige são elevados. Por outro lado, as possibilidades do *Big Data* são diversas. Se já é possível prever que tipo de produto uma pessoa comprará numa loja *online*, por que seria diferente prever o possível cometimento de um crime por alguém?

Longe de ser uma ficção científica, o conhecimento preditivo oferecido pela Ciência da Computação, se bem utilizado pelos órgãos estatais de Segurança Pública, pode reduzir drasticamente o número de crimes. Por outro lado, a descoberta do conhecimento baseada em técnicas de Mineração de Dados (*Data Mining*) aplicadas em *Big Data* pode auxiliar a descoberta de grupos criminosos até então desconhecidos.

É natural que a sociedade, como um todo, queira reduzir os índices de criminalidade e, com isso, deseje a adoção de ferramentas, como aquelas que se utilizem da tecnologia do *Big Data*. Contudo, por envolver a mitigação de direitos e garantias constitucionais, a adoção de tecnologias inovadoras pelo Sistema de Justiça Criminal deve ser devidamente regulamentada pelo Direito.

Com base nessas circunstâncias, desenvolveu-se o presente trabalho, tendo-se buscado resolver o problema sintetizado na seguinte pergunta: no atual contexto brasileiro, em que medida é juridicamente viável utilizar ferramentas de Computação Forense baseadas em *Big Data* no Sistema de Justiça Criminal?

A hipótese de pesquisa é a de que a utilização, no Sistema de Justiça Criminal, de ferramentas de Computação Forense baseadas em *Big Data* é possível, mas desde que seja observada a eficácia contida do direito fundamental à proteção de dados pessoais, razão pela qual é indispensável a existência de lei em sentido estrito que verse especificamente sobre a utilização de dados pessoais no âmbito penal, inclusive com menção expressa ao *Big Data,* sendo necessário, ainda, a edição de atos normativos infralegais aptos a evitar arbitrariedades pelo Estado, e a garantir todos os direitos e garantias constitucionais de quem é submetido ao crivo do Sistema de Justiça Criminal, seja na persecução penal, seja na Segurança Pública.

A pesquisa foi desenvolvida a partir da referida hipótese e utilizou o método hipotético-dedutivo, apoiado em técnicas de pesquisa bibliográfica, legislativa, documental e jurisprudencial. Para tanto, adotaram-se as premissas de que a utilização de *Big Data* para fins penais deve observar os direitos e garantias fundamentais de todas as pessoas, em especial, de quem é submetido ao Sistema de Justiça Criminal; que o Estado Democrático de Direito tem o dever de transparência e de prestação de contas para com seus cidadãos; e que o direito fundamental à proteção de dados pessoais deve ser interpretado em favor

do indivíduo, assim como ocorre com a presunção de inocência no âmbito penal.

O Capítulo 1 possui perspectiva sociológica e histórica e versa sobre e evolução do Estado até a contemporaneidade, nele discorrendo-se sobre a utilização das novas tecnologias baseadas em dados para o desempenho de funções públicas.

O Capítulo 2 sintetiza os principais conceitos e características que, dentro da Ciência da Computação, circundam o *Big Data*, destacando-se elementos próprios da Computação Forense, e analisa como tudo isso se relaciona com o Sistema de Justiça Criminal. O pano de fundo desse capítulo possui matriz técnico-científica, visto que se desenvolve a partir de termos próprios da área computacional. O objetivo é elucidar caracteres-chave da Ciência da Computação e, com isso, facilitar a compreensão do tema aí discutido por parte dos estudiosos do Direito.

O Capítulo 3 discorre sobre os projetos de pesquisa desenvolvidos na área da Computação Forense por meio da parceria acadêmica firmada entre a Polícia Científica do Paraná (PCP) e a Pontifícia Universidade Católica do Paraná (PUCPR), coordenados pela Profa. Dra. Cinthia Obladen de Almendra Freitas, visando o aperfeiçoamento de ferramentas computacionais utilizadas em perícias criminais. Inclusive, o recorte de pesquisa – focado, especificamente, em *Big Data* para fins penais – decorre justamente dos trabalhos que têm sido desenvolvidas no bojo dessa parceria acadêmica.

Demonstrou-se como o uso da análise de dados é indispensável para a solução de casos penais na atualidade. Do mesmo modo, restou evidenciado que é possível criar ferramentas computacionais baseadas em *Big Data*, para auxiliar o Sistema de Justiça Criminal, tanto nas áreas de Segurança Pública, quanto nas de persecução penal.

O último capítulo também versou sobre o direito fundamental à proteção de dados pessoais e sobre como ele está inserido no atual ordenamento jurídico. Discorreu-se sobre sua natureza jurídica de norma constitucional de eficácia contida e sobre como as leis gerais de proteção de dados podem regulamentar, de modo adequado, esse microssistema jurídico, utilizando-se, para isso, do estudo sobre as duas propostas legislativas que atualmente existem sobre a Lei Geral de Proteção de Dados (LGPD) Penal.

Por fim, concluiu-se que o atual ordenamento jurídico brasileiro não permite a utilização de ferramentas computacionais baseadas em *Big Data* dentro do Sistema de Justiça Criminal, seja na Segurança Pública, seja na persecução penal. Isso, porque o direito fundamental à proteção de dados pessoais é norma constitucional de eficácia contida, devendo prevalecer em benefício do réu ou do investigado no caso criminal, haja vista o postulado da presunção de inocência.

Eventual mitigação do direito fundamental à proteção de dados pessoais só pode ocorrer por meio de lei em sentido estrito e, posteriormente, por meio de exaustiva regulamentação infralegal do tema. Devem prevalecer a transparência, a adequação, a finalidade e o *accountability* no tratamento de dados pessoais. Ademais, no âmbito penal, isso é mais delicado, visto que, em última análise, o que está em jogo é a possibilidade de prisão de uma pessoa.

O trabalho se enquadra na Área de Concentração de Direito Socioambiental e Sustentabilidade do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná, por tratar do Sistema de Justiça Criminal brasileiro no âmbito da Sociedade Informacional, o que contribui para a Linha de Pesquisa “Estado, Sociedades, Povos e Meio Ambiente”, em razão da análise de aspectos tecnológicos aplicados ao Direito, com destaque para a utilização de ferramentas computacionais baseadas em *Big Data* e que se destinam ao aperfeiçoamento da Segurança Pública e a persecução penal no Brasil, ao mesmo tempo que os direitos e garantias fundamentais da pessoa humana são protegidos.

Por fim, cumpre mencionar que a presente dissertação de Mestrado em Direito é resultado do projeto de pesquisa coordenado pela Profa. Dra. Cinthia Obladen de Almendra Freitas, cujo nome é “SiCReT II - Forense Digital e Inteligência Artificial aplicadas aos Laudos Periciais de Dispositivos Móveis”, e que conta com o apoio técnico-científico da Polícia Científica do Estado do Paraná, e com financiamento do Programa de Cooperação Acadêmica em Segurança Pública e Ciências Forenses (PROCAD/SPCF) da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

# 2 A UTILIZAÇÃO DE DADOS PELO ESTADO CONTEMPORÂNEO NO CONTEXTO DO PANSPECTRON

O objetivo deste primeiro capítulo, intitulado “A utilização de dados pelo Estado Contemporâneo no contexto do Panspectron”, é demonstrar em que medida a tecnologia baseada em dados tem influenciado a atuação do Estado Contemporâneo.

Para alcançar tal objetivo, procede-se ao seguinte *iter* analítico. É descrita, inicialmente, a formação histórica do modelo ocidental de Estado, fazendo-se, aqui e ali, abordagens pontuais sobre a utilização de dados pela máquina estatal.

Posteriormente, discorre-se sobre o caráter pervasivo da tecnologia da informação na sociedade atual e sobre como essa sua característica deu origem ao Panspectron, sendo o foco de tal análise a atuação estatal, mas não se podendo deixar de mencionar, também, ainda que brevemente, o envolvimento de agentes privados nesse âmbito, haja vista a complexidade da temática desenvolvida.

Por fim, apresentam-se exemplos da utilização de dados por parte do Estado, em três diferentes frentes de atuação, quais sejam elas: na Espionagem; no Controle Social e, por fim, mas não menos importante, no Sistema de Justiça Criminal.

Em que pese o objetivo principal desta dissertação de Mestrado seja o estudo, em profundidade, da relação entre *Big Data* e Sistema de Justiça Criminal, justifica-se a abordagem do tema do Estado, como um todo, em razão de ser este um fenômeno multifacetário e complexo e, portanto, não restrito ao nicho criminal.

Desse modo, a compreensão global do que vem a ser o Estado e do que ele é capaz de fazer com o uso da tecnologia baseada em dados permite que as reflexões jurídicas acerca do *Big Data* também considerem esse contexto mais amplo e não estejam restritas aos interesses exclusivos daqueles que atuam no Sistema de Justiça Criminal. Afinal, como será visto adiante, a atuação estatal só é legítima, quando respeitados os direitos e as garantias fundamentais, com destaque para a dignidade da pessoa humana e para o bem comum.

## 2.1 ESTADO, DADOS E INFORMAÇÃO

A compreensão sobre o que é o Estado Contemporâneo obriga a que se remonte às suas fontes e a que se proceda ao refazimento das etapas de sua construção histórica. Etimologicamente falando, a palavra “Estado” decorre do vocábulo latino “*status*” (RAVIZZA, 1918, p. 128), o qual, por sua vez, remete à posição social que determinado indivíduo ocupa no meio em que vive (MICHAELIS, 2023).

No contexto nacional, cumpre mencionar que a tradição jurídico-política do Brasil é decorrente do pensamento político europeu e das tradições romano-germânicas (MARTINS, 2019), podendo-se falar, também, na existência, inclusive, da influência política e econômica da hegemonia estadunidense, sobretudo durante o século XX (AGOSTINHO; NEUMANN, 2020).

A adoção da palavra “Estado” no contexto da Ciência Política surgiu na Europa, com os conselheiros políticos dos monarcas medievais, que visavam a ensinar a seus respectivos consulentes como estes deveriam governar seus reinos, sem perderem o *status* de rei ou de príncipe (SKINNER, 2009, p. 327).[1]

Salienta-se que, no período medieval, vigorava o pensamento político da origem divina do direito dos reis — daí, direito divino dos reis —, cuja essência é o reconhecimento da legitimidade dos monarcas como sendo os representantes de Deus,[2] que foram por Ele escolhidos, para governarem as pessoas na Terra (SKINNER, 2009, p. 330).

A tradição do direito divino dos reis começou a ser criticada durante a transição do Período Medieval para o Período Iluminista na Europa (SKINNER, 2009, p. 332). Passou-se a questionar a legitimidade divina dos monarcas, em razão dos privilégios que eles detinham perante as pessoas comuns (PAES, 2020, p. 131).

Além disso, os cidadãos começaram a se agrupar e a questionar determinadas tradições, passando a reivindicar para si determinados direitos,

---

[1] O livro mais conhecido desse período é o “O príncipe”, publicado, originalmente, em 1514 e de autoria de Nicolau Maquiavel (1469-1527) (SKINNER, 2009, p. 327).

[2] Deus aqui é o professado pela fé dos cristãos, com destaque para a Igreja Católica Apostólica Romana, que deteve considerável hegemonia na Europa, durante o Período Medieval (HOFFMANN, 2020).

como o de se autogovernarem segundo suas próprias deliberações.

Com isso, construiu-se o pensamento político de que o Estado e o monarca não eram mais um só ente; mas, figuras distintas. Logo, o Estado passou a não corresponder mais ao *status* do rei; mas, a equiparar-se ao conjunto de súditos que formam a sociedade, a qual, por sua vez, está sob a autoridade real.

Desse modo, a soberania, que era do rei, em decorrência da vontade divina, foi transferida para o corpo social, ou seja, para o povo (SKINNER, 2009, p. 332). Em síntese, a soberania passou a ser fundamentada no povo e não mais, na vontade de Deus. Com isso, formou-se o entendimento de que o monarca servia ao Estado e não mais, aos seus próprios interesses, como outrora, durante o absolutismo político, braço político do Antigo Regime.

Tal mudança de paradigma político foi uma das principais causas do fim do modelo absolutista de governo (ASSIS, 2016, p. 49). Diante desse novo cenário, ou os reis europeus mudavam a ordem política interna, com a progressiva limitação aos poderes absolutistas dos monarcas, como ocorreu na Inglaterra da Revolução Gloriosa, com a Declaração de Direitos (em inglês, "*Bill of Rights*"), de 1689 (RAMOS, 2022, p. 23), aprovada pelo Parlamento britânico, como condição para a coroação da Rainha Maria II Stuart (1662-1694) e do marido, o Príncipe Guilherme III de Orange (1650-1702); ou eram depostos, como aconteceria um século mais tarde, na França, durante a Revolução Francesa, que começou em 1789 e que levou ao guilhotinamento, em 1793, do rei Luís XVI de Bourbon (1754-1793) (RAMOS, 2022, p. 27).

Nos casos ocorridos para além do continente europeu, as Colônias do Novo Mundo, isto é, as Colônias situadas nas Américas, seguiram o mesmo caminho e romperam com suas Metrópoles europeias, passando a adotar, como paradigma, o modelo republicano da Antiguidade Greco-Romana (PEREIRA, 2013, p. 42-49). Foi o caso da república fundada com a Independência dos Estados Unidos da América (EUA), em 1776, e de diversas outras repúblicas que surgiram na América Latina, com o fim das Colônias espanholas e as lutas respectivas por sua independência (MÄDER, 2008).

Nesse cenário, o caso do Brasil é *sui generis*. Com as conquistas napoleônicas tomando boa parte do território da Europa durante o início do

século XIX, o então príncipe regente português Dom João (1767-1826) — futuro Dom João VI de Portugal, a partir de sua Aclamação, em 1818, em solo brasileiro, aliás — resolveu, em 1807, transferir, para o Brasil, a sede do governo de sua mãe, a Rainha Maria I de Portugal (1734-1816), aqui aportando em janeiro de 1808, tendo, em 1815, elevado o Brasil a Reino Unido de Portugal, Brasil e Algarves (GUIMARÃES, 2016). Em 1822, o Brasil tornou-se independente e passou a chamar-se Império do Brasil, tendo a sua primeira Constituição outorgada em 25 de março de 1824 (LENZA, 2023, p. 70-75).

Acerca desse texto constitucional, há debates acadêmicos sobre o modelo de governo adotado, se absolutista ou não, tendo em vista a existência do Poder Moderador, o qual, privativo do Imperador, era exercido para a "manutenção da Independência, equilíbrio, e harmonia dos mais Poderes Políticos" (BRASIL, 1824, p. 1), quais fossem esses demais Poderes: o Poder Legislativo, o Poder Executivo e o Poder Judicial (BRASIL, 1824).

Em que pesem esses debates e a cronologia histórica brevemente apresentados acima, demonstrou-se que o texto constitucional brasileiro de 1824 também seguiu a mesma tendência da política europeia da época, isto é, aquela de delimitar os poderes do monarca e de aumentar a independência do povo nas suas deliberações políticas, assim como ocorrera na Inglaterra, em 1689, conforme já mencionado.

Posteriormente, como é sabido, o Imperador Dom Pedro II (1825-1891) foi deposto, e a família imperial do Brasil, exilada, ambos por obra do Exército brasileiro em 1889, ocasião em que se proclamou a República dos Estados Unidos do Brasil, fortemente inspirada em ideias positivistas e no modelo estadunidense de Estado (LIMA FILHO, 2004).

Portanto, em resumo, o modelo político ocidental reconhece que soberania do Estado advém do povo e que o seu líder político é uma pessoa destinada a servir ao povo, seja como presidente (no modelo republicano), seja como rei ou imperador (no modelo monárquico). Tal imperativo também está positivado na atual Constituição brasileira, no parágrafo único do seu artigo (art.) 1º, que afirma que todo o poder emana do povo (BRASIL, 1988).

Nesse contexto, surge a ideia de Estado Democrático, visto que a etimologia, agora, da palavra "democracia" é o vocábulo grego "*dēmokratía*", em

que “*dēmos*” significa “povo”, e “*kratía*”, governo (SANTOS, 2019, p. 150-151).

Por sua vez, a ideia de Estado de Direito decorre do conceito anglo-saxônico de “*Rule of Law*”, ou de “Império da Lei”, em que tanto governantes, quanto governados devem igual obediência às leis do Estado, o que lhes garante mútua segurança jurídica e legitimidade política (SANTOS, 2018, p. 14 e 27). Por isso, no Brasil, vigora o Estado Democrático de Direito, conforme positivado no *caput* do art. 1º da Constituição da República Federativa do Brasil de 1988 (BRASIL, 1988).

O modelo brasileiro de Estado detém o monopólio do uso legítimo da força, o que guarda consonância com o pensamento do sociólogo Max Weber (1864-1920) (2011, p. 57).

Isso significa que somente os agentes estatais, quando investidos do estrito exercício da função pública, estão juridicamente autorizados a utilizar a força. Exemplo disso é o uso de violência pelas Forças Armadas, em caso de guerra; ou, então, em caso de prisão de criminosos e de insubordinados por parte das polícias, sejam estas judiciárias ou militares.

Salienta-se que o uso da força é sempre a exceção. Não pode o Estado exercê-la indiscriminadamente, sendo passível de punição o agente estatal que exorbite os limites legais de sua atuação, inclusive, no âmbito de guerra declarada, haja vista a existência das normas do Direito Internacional Humanitário (HUSEK, 2022).

Por sua vez, o uso da força por particulares, em regra, configura crime, a exemplo dos crimes de lesão corporal e de exercício arbitrário das próprias razões, entre outros.[3]

Por outro lado, o ordenamento jurídico brasileiro prevê algumas exceções no que tange ao uso da força por particulares e a autoriza, como no caso do desforço imediato, da legítima defesa e da prisão cidadã.[4]

Como visto, o Estado deve servir ao povo que o institui, sendo este o seu soberano. Desse modo, não há como imaginar o ente estatal agindo contra

---

[3] *Vide*, acerca dos crimes de lesão corporal e de exercício arbitrário das próprias razões, o disposto nos artigos 129 e 345 do Código Penal (BRASIL, 1940).

[4] *Vide*, a respeito do desforço imediato, da legítima defesa e da prisão cidadã, respectivamente, os artigos 1.210, § 1º, do Código Civil (BRASIL, 2002); 23, inciso II, do Código Penal (BRASIL, 1940), e, finalmente, 301 do Código de Processo Penal (BRASIL, 1941).

o próprio povo,[5] sendo as políticas públicas e o dever de proteção exemplos de suas principais obrigações, enquanto deveres do Estado.

Tanto é assim, que o conceito de soberania, no âmbito da política externa, determina, dentre outras coisas, que o Estado proteja e guarde seu território, suas fronteiras e seus cidadãos de qualquer ingerência externa (LIZIERO, 2013, p. 20-23).

A Segurança Nacional é uma das facetas externas da soberania e, por isso, tem viés mais político do que meramente jurídico e está ligada à proteção contra ingerências de outros Estados soberanos (LIZIERO, 2013, p. 20-23). Já o Sistema de Justiça Criminal — uma faceta interna da soberania — é ligado ao desrespeito às leis penais e objetiva combater a criminalidade tanto de modo preventivo, por meio de políticas públicas de Segurança Pública, quanto de modo repressivo, por meio da persecução penal e da aplicação de penas e de medidas de segurança correspondentes à infração penal praticada (SAPORI, 2000).

Quando se trata de temas como o do Sistema de Justiça Criminal e o da Segurança Nacional, é comum pensar-se, num primeiro momento, no citado uso legítimo da força. Contudo, muito embora, no mundo atual, ainda estejam em curso conflitos armados, o uso da força tem, desde o advento da Guerra Fria (1947-1991), sido secundário na disputa pela hegemonia global (RODRIGUES, 2022, p. 37-43).

Isso assim o é, porque os grandes protagonistas desse contexto político de conflagração de forças aspirantes a hegemônicas têm sido a ameaça do uso da força,[6] o emprego de sistemas de inteligência e a adoção de políticas econômicas (RODRIGUES, 2022, p. 37-43).

Como o tema central deste trabalho gira em torno da Computação Forense, em especial, da utilização do *Big Data* no Sistema de Justiça Criminal, é importante ressaltar que, atualmente, o cerne da disputa pela hegemonia global é a informação (GHISLENI, 2015, p. 31).

Afinal, são os dados que geram a informação, e a informação é a base

---

[5] Muito embora seja isso que se espere, não há dúvida de que muitos Estados atacam seu próprio povo. Exemplo disso são os regimes ditatoriais, em que determinado grupo ou líder político apropria-se da máquina estatal e a utiliza segundo seus próprios interesses, mesmo que isso signifique ter de violar os direitos humanos de seus próprios cidadãos nacionais.

[6] Exemplo: ameaça do uso de bombas atômicas.

da tomada de decisões por líderes políticos, inclusive, sobre os rumos que a economia de um país deva tomar. Ademais, a produção de informação, seja esta falsa ou não, é fundamental nas atividades de inteligência.[7]

Desse modo, o uso de dados não poderia deixar de ser fundamental em questões envolvendo o tema do Sistema de Justiça Criminal.[8] Nesse contexto, não se pode esquecer que os dispositivos móveis estão cada vez mais presentes na rotina das pessoas.

O acesso aos dados de um celular, por exemplo, permite descobrir por onde determinada pessoa transitou, com quem ela falou e quais eram os assuntos de seu interesse. Não é à toa que, atualmente, as *Big Techs* — forma reduzida da expressão inglesa "*Big Technology Companies*", ou seja, as "Grandes Companhias de Tecnologia" na tradução para o português — sejam as empresas mais valiosas do mundo (FORBES, 2023).

Em síntese, quem tem o acesso a dados possui um conhecimento preditivo poderosíssimo, que permite saber as tendências de compra e de voto de cada pessoa. Por isso, são tão paradigmáticas situações como a disputa política entre a República Popular da China (RPC) e os Estados Unidos da América (EUA) envolvendo o aplicativo *TikTok* (THORBECK, 2022), assim como o é a controvérsia política envolvendo as empresas *Cambridge Analytica* e *Facebook* (*BBC* BRASIL, 2018).

No âmbito da persecução penal, o conhecimento preditivo também se mostra fundamental. Acerca desse ponto, menciona-se, a título ilustrativo, o filme de ficção científica denominado "*Minority Report* – A Nova Lei", cuja trama passa-se nos EUA, no imaginário ano de 2054 e no qual a tecnologia disponível é capaz de prever quando crimes serão cometidos. De posse dessa informação antecipada, é possível à polícia local prender o criminoso, antes mesmo de ele vir a praticar o delito, submetendo-o à respectiva punição (NUNES, 2022).

---

[7] A produção de informação falsa nas atividades de inteligência é denominada de "campanhas de desinformação" e tem o intuito de "causar danos, confundir ou induzir a erro" (COUTINHO, 2020, p. 107).

[8] Considerando a pesquisa desenvolvida, o presente trabalho tem abordado o uso de dados pelo Estado para fins penais e para fins de Segurança Nacional, com destaque para os primeiros desses fins, os de natureza penal. Todavia, é sabido que os dados também podem ser utilizados pelo Estado para fins outros, em diversas outras áreas, como na formação de políticas públicas das áreas de Saúde, de Educação, de Meio Ambiente *et cetera* (*etc*.).

Note-se que a essência do conhecimento preditivo é justamente, como diz o próprio nome, a capacidade de prever o que acontecerá no futuro. Muito embora o enredo do filme acima citado seja uma ficção baseada em capacidades paranormais de pessoas que funcionam como os oráculos do Mundo Antigo e que são tidas com poderes de videntes, a construção do conhecimento preditivo já é perfeitamente possível de ser realizada, no mundo hodierno, por meio de modelos criados a partir de dados capazes de demonstrar determinado comportamento individual ou social (*GOOGLE CLOUD*, 2023).

Atualmente, a humanidade vive estágio de desenvolvimento dito da Sociedade da Informação (CASTELLS, 2003). Afinal, não mais se pode cogitar a existência de relações econômicas ou políticas que não dependam de algum tipo de informação, para virem a ser concretizadas.

Assim, a abertura de uma empresa costuma ser precedida de estudos de potencial de mercado. Do mesmo modo, campanhas eleitorais utilizam pesquisas de intenção de voto, para, por meio destas, direcionar sua abordagem e, com isso, maximizar o potencial de eleição dos candidatos contratantes desse tipo de pesquisa (FIRMINO; MURTA, 2019).

Dessa maneira, percebe-se que a produtividade e o poder passaram a ser dependentes diretos da geração, do processamento e da transmissão de informação (BOFF; FORTES; FREITAS, 2018, p. 9). Por isso, tecnicamente, prefira-se falar em Sociedade Informacional, em vez de em Sociedade da Informação (BOFF; FORTES; FREITAS, 2018).

A informação se tornou tão crucial atualmente, que até mesmo as Forças Armadas de muitos Estados soberanos — inclusive, da República Federativa do Brasil — possuem, em operação, departamentos destinados exclusivamente à denominada guerra cibernética, a qual consiste no quanto segue:

> Conjunto de ações ofensivas, exploratórias e defensivas, realizadas no espaço cibernético, visando [a] negar, explorar, corromper, degradar ou destruir capacidades [...] do adversário e [a] colaborar com a produção de conhecimento de inteligência e com a proteção das infraestruturas críticas de informação de interesse, no contexto de uma operação militar de nível operacional ou tático, coordenadas por um Comando Operacional ativado (BRASIL, 2018a, p. 181).

Tal postura militar visa a garantir a execução e a efetividade da

Segurança Nacional, ao criar mecanismos de defesa da infraestrutura de informática de um país. No caso de ataque ao inimigo, os militares que atuam na guerra cibernética costumam agir em, pelo menos, três frentes: (i) em primeiro lugar, no ataque direto à infraestrutura de informática do inimigo; (ii) depois, na obtenção de informações que possibilitem a construção de conhecimento preditivo, e, por fim, (iii) na inserção de informações falsas na base de dados inimiga, a fim de, assim atuando, vir a prejudicar a respectiva tomada de decisão.

Por sua vez, no âmbito do Sistema de Justiça Criminal, o uso de dados permite a construção de informação apta a ser utilizada na persecução penal. Para ilustrar isso, basta ter em mente o aparelho de telefonia móvel, ou celular. Nele, as pessoas concentram a guarda de praticamente tudo, vez que, é justamente no celular que elas mantêm armazenados agenda, fotos, lembretes, conversas, dados bancários, entre outros.

Uma análise pericial que venha a ser realizada nesse conjunto de dados armazenados em um tal dispositivo móvel, como um aparelho de telefonia móvel, permitirá conhecer muita coisa sobre quem é e como se comporta o possuidor do celular analisado, bem como sobre suas condutas pretéritas.

Logo, ao contrário de quando se trata de Segurança Nacional, a qual se pauta no conhecimento preditivo[9], quando se fala em matéria penal, o que ganha relevância são as ações pretéritas, ou seja, aquilo que foi feito no passado.

Nesse sentido, o conhecimento preditivo torna-se secundário na persecução penal, mas ele não é, por isso, menos importante, haja vista que ele ainda pode ser utilizado nos estudos comportamentais de criminosos e, com isso, pode otimizar a tomada de decisões na construção de políticas públicas de Segurança Pública (FIOROT, 2021, p. 17-31).

Todavia, é importante ter cautela no uso da análise preditiva nesses casos, pois há o risco de categorizar indivíduos de modo discriminatório e lombrosiano[10] (FIOROT, 2021, p. 26-28).

---

[9] Importante esclarecer que a análise preditiva não significa, necessariamente, prever o futuro. Ela pode, também, generalizar e prever dados que não tenham sido utilizados para treinar o modelo em que ela se baseia.

[10] Uma pessoa descrita como lombrosiana corresponde ao “indivíduo que apresenta traços físicos, típicos de criminoso nato, segundo teoria, não mais aceita, do criminologista italiano Cesare Lombroso (1835-1909)” (DICIONÁRIO AULETE, 2023b).

As normas jurídicas que regulamentam a persecução penal derivam do Direito Processual Penal, que consiste no “ramo do ordenamento jurídico pertencente ao Direito Público e que reúne o conjunto de normas jurídicas regentes da investigação e julgamento dos fatos preestabelecidos pela lei penal como delitos” (ABADE, 2014, p. 1). A persecução penal desdobra-se em duas fases: a da investigação criminal e a da persecução penal em juízo.

A fase da investigação criminal tem início já com a ocorrência do crime, momento em que passa a haver materialidade delitiva, isto é, passam a existir vestígios que permitem constatar que determinado delito foi praticado. Em regra, a persecução penal investigatória visa a apurar a autoria delitiva, bem como a colher todos os elementos de prova possíveis que venham a influenciar a materialidade do crime, vez que, a depender do que for descoberto, a tipificação penal do fato delitivo também pode ser modificada.

A fase investigatória é comum a todas as infrações penais, distinguindo-se a persecução penal realizada em juízo, a qual pode seguir diferentes procedimentos, de acordo com o rito processual que haja sido adotado e que pode ter sido o rito sumaríssimo, o rito sumário, ou, ainda, o rito ordinário (BRASIL, 1941), além dos ritos especiais, a exemplo do previsto na Lei de Drogas, isto é, na Lei n. 11.343, de 23 de agosto de 2006 (BRASIL, 2006).

No âmbito do rito ordinário — que vem a ser, dentre todos os ritos do Direito Processual Penal, o procedimento mais completo de um processo criminal e do qual derivam todos os demais ritos processuais nesta seara —, a persecução penal realizada em juízo tem início com o recebimento da denúncia, momento em que o juízo competente analisa sumariamente tanto a acusação, quanto os elementos de prova apresentados pelo Ministério Público e conclui existirem indícios suficientes de materialidade e de autoria delitivas em desfavor do acusado, transformando-o em réu (BRASIL, 1941).

Após o recebimento da denúncia,[11] o réu é, então, citado, para que, devidamente cientificado da acusação que pesa contra si, apresente sua

[11] É possível que o juiz rejeite a denúncia, quando ele entenda que inexistam indícios mínimos de materialidade e/ou de autoria delitivas, ou quando considere penalmente atípico o fato. Caso isso ocorra, abre-se a possibilidade de recurso ao Ministério Público e, no caso de improcedência recursal ou mesmo de ausência de recurso ministerial, o caso é encerrado.

resposta à acusação, momento em que, se quiser, poderá alegar hipóteses de absolvição sumária e poderá, outrossim, vir a indicar as provas que pretenda produzir na ulterior fase de instrução processual (BRASIL, 1941).

O juízo analisará a resposta à acusação e, uma vez concluindo não ser o caso de absolvição sumária, ele determinará o prosseguimento do feito à instrução, delimitando as provas que serão produzidas em juízo e designando a audiência de instrução e julgamento (BRASIL, 1941).

Finalizada a fase de instrução, dá-se início à fase de diligências complementares, momento em que as partes podem pedir a realização de diligências, para, assim, complementar as provas que tenham sido produzidas até então (BRASIL, 1941).

Superada essa outra fase, o juízo sentencia o processo, condenando ou absolvendo o réu, abrindo-se, imediatamente depois disso, a fase recursal do processo criminal, até que sobrevenha a sua conclusão, com o trânsito em julgado da decisão (BRASIL, 1941).

A persecução penal, como um todo, tem, como finalidade, “a reconstituição do fato criminoso, apurando, assim, a culpabilidade ou a inocência do acusado” (SUPERIOR TRIBUNAL DE JUSTIÇA, 2008, p. 1). Desse modo, é fundamental a obtenção dos elementos de prova, para o Ministério Público ou oferecer denúncia ou arquivar uma investigação (persecução penal investigatória), bem como é crucial para o juiz ou condenar ou absolver o réu (persecução penal em juízo).

Assim, a análise de dados extraídos a partir de dispositivos móveis é capaz de auxiliar no Processo Penal como um todo e, em alguns casos, pode ser, até mesmo, indispensável para o resultado do processo.

## 2.2 DA VIGILÂNCIA AO PANSPECTRON

A vigilância é inerente a qualquer governo, seja ele autoritário ou democrático. É difícil imaginar governantes desassistidos na área de Inteligência, Vigilância e Reconhecimento (IVR). A espionagem, longe de ser algo caricato dos tempos da Guerra Fria, existe desde muito antes disso, pois remonta ao povo persa da Antiguidade (ARAÚJO; FARIAS, 2005, p. 87).

Mas a vigilância não diz respeito apenas a atividades de inteligência direcionadas à área da Segurança Nacional. Ela também abrange, dentre outras, as atividades de monitoramento da criminalidade no âmbito do Sistema de Justiça Criminal, com destaque para a área da Segurança Pública.

A vigilância e o policiamento são fundamentais para a manutenção da paz social. Entretanto, a vigilância vai além dessas duas áreas (de Segurança Nacional e de Segurança Pública): ela também se mostra fundamental em outros nichos de atuação do Estado, tal como na Saúde Pública. Basta lembrar da vigilância epidemiológica exercida pelo Estado brasileiro durante todo o período pandêmico do coronavírus (BRASIL, 2022).

Além disso, também não é possível falar de vigilância, sem levar em consideração o panóptico, inicialmente desenhado por Jeremy Bentham (1748-1832), para otimizar a vigilância nas prisões. O panóptico consistia, em síntese, em um projeto arquitetônico segundo o qual a prisão era construída em formato circular, em cujo perímetro externo do círculo situavam-se as celas dos prisioneiros e, em cujo centro do círculo, era instalada uma torre de vigilância: desta, os carcereiros conseguiam vigiar, de modo otimizado, todas as celas da prisão, ao passo que os prisioneiros não tinham como saber em que momento os carcereiros olhavam para as celas deles, os encarcerados. Tal estrutura arquitetônica causava em quem estava dentro das celas uma constante sensação de vigilância (FOUCAULT, 1987, p. 46-51).

O efeito psicológico dessa percepção de eterna vigilância diminuía o potencial de rebelião, assim como reduzia o número de agentes penitenciários necessários para vigiarem os encarcerados na prisão. A Figura 1 ilustra, exatamente, essa situação.

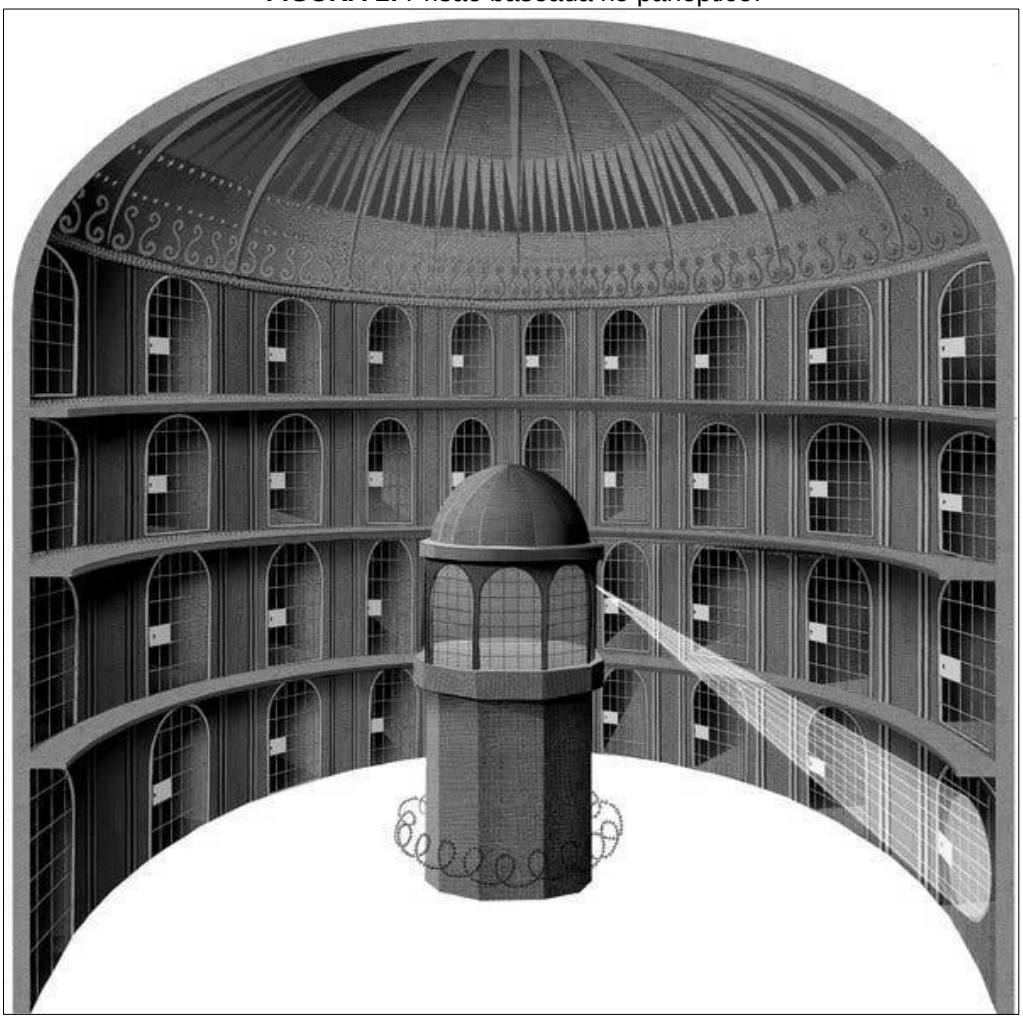
Muito embora, não se tenha conhecimento, ao menos não, no Brasil, da construção de uma prisão nesses moldes arquitetônicos do panóptico, o que se mostra relevante aqui não é exatamente haver-se concretizado tal arquitetura prisional no País, por meio da construção de um prédio prisional no modelo do panóptico; antes, importa o efeito psicológico causado pelo projeto arquitetônico baseado no modelo do panóptico.

Afinal, a constante sensação de estar sendo vigiado é uma realidade indubitável atualmente. A vigilância não é, ademais, algo exclusivo do Estado.

Basta entrar em um estabelecimento comercial, que é possível constatar-se, quase de imediato, a existência de, ao menos, uma câmera de segurança instalada voltada geralmente para a porta e para o caixa (CANDIOTTO; COUTO NETO, 2019, p. 89).

Do mesmo modo, a facilidade de gravar uma cena qualquer, com um celular ou com um relógio inteligente, torna qualquer um passível de sofrer monitoramento por quem quer que seja.

**FIGURA 1:** Prisão baseada no panóptico.



FONTE: SIMPSON, 2013, p. 1.

Desse modo, o ideal do espírito de vigilância permanente, exaustiva, onipresente do panóptico impregnou-se na vida das pessoas, em um caminho sem volta. Não foi preciso construir uma prisão minuciosamente arquitetada para isso. A vigilância e o controle do Estado potencializaram-se com o acesso à informação e com o caráter pervasivo da tecnologia. Tal conjuntura resulta em

uma nova versão do panóptico de Bentham, em que o exercício do poder passa a ser invisível, ou seja, passa a ser praticamente imperceptível (BOFF; FORTES; FREITAS, 2018, p. 9-10).

Surge, então, o Estado Informacional na sociedade de vigilância, cujo poder estrutural passa a modelar "o comportamento humano pela manipulação do mundo material", baseada na informação (BOFF; FORTES; FREITAS, 2018, p. 19-20).[12]

Com isso, a tecnologia passou a dificultar, cada vez mais, o exercício da autodeterminação informativa, visto que o desenvolvimento tecnológico tornou cada vez mais difícil eliminar seus próprios rastros digitais (RODOTÀ, 2008, p. 112-113).

Desse modo, o exercício do direito ao livre desenvolvimento da personalidade nesse cenário tem sido cada vez mais prejudicado, haja vista que o panóptico induz à adoção de condicionantes do comportamento humano (RODOTÀ, 2008, p. 116-117).

A sociedade da vigilância tem materializado novas formas de manifestação do panóptico de Jeremy Bentham e do poder disciplinar de Michel Foucault (1926-1984), dando origem ao Panspectron, um poder invisível que, por meio da tecnologia, exerce vigilância constante e recíproca sobre tudo e todos, a partir de qualquer lugar do Planeta (BOFF; FORTES; FREITAS, 2018, p. 24-25).

Com isso, os "indivíduos são submetidos a padrões de comportamento e postura e, até mesmo, a modelos de pensamento" (BOFF; FORTES; FREITAS, 2018, p. 25).

Nesse sentido e de acordo com Bauman e com Lyon (2013, p. 58-59), a modernidade reinventou o poder disciplinar e o panóptico, ensejando ampla cooperação dos dominados e vítimas dos instrumentos de vigilância, numa espécie de "servidão voluntária".

Em outras palavras, o exercício do poder na Sociedade da Vigilância é

---

[12] Note-se que a classificação da sociedade atual não é estanque. Denominá-la como Sociedade da Informação (ou Sociedade Informacional) ou, então, como Sociedade da Vigilância não significa que se esteja falando de fenômenos distintos, mas, apenas, de um único fenômeno, a partir de diferentes perspectivas, as quais, não raras vezes, se sobrepõem.

sutil e dotado de uma falsa espontaneidade. As pessoas são categorizadas de acordo com suas preferências e induzidas a fazer escolhas pré-estabelecidas, causando-lhes falsa sensação de liberdade.

Tal situação é muito comum em *sites* de comércio eletrônico baseados em perfil de consumo, mas nada impede que isso seja ou já esteja sendo indevidamente usado por entidades estatais (BAUMAN; LYON, 2013, p. 73-74).

Além disso, ainda de acordo com Bauman e com Lyon (2013, p. 61), "os subordinados estão tão preparados para o papel de autovigilantes, que se tornam redundantes em relação às torres de vigilância do esquema de Bentham e Foucault", até porque a sensação panóptica da sociedade da vigilância baseia-se na figura abstrata do "outro".

Isto é, o comportamento humano passa a ser moldado na intensificação do medo do que o "outro" vá pensar, mesmo não sendo possível individualizar esse "outro" e mesmo que o "outro" possa nem se importar com a vida alheia (BAUMAN; LYON, 2013, p. 98).

O uso de dispositivos móveis como *notebooks*, *smartphones*, *smartwatches*, *tablets*, entre outros, tem gerado rastros digitais quase infinitos. Esses rastros digitais são constituídos por dados que ficam armazenados em diversos locais, seja na memória interna do próprio aparelho usado para produzir tais rastros; seja em nuvem computacional; seja em algum servidor espalhado mundo afora, o que indiscutivelmente torna vulnerável a privacidade individual.

A simples utilização de um cartão de crédito em determinado estabelecimento comercial permite que a operadora do cartão trace o perfil de consumo do usuário, para, depois, vender esse perfil a um anunciante de produtos compatíveis com aquele perfil e, por isso, potencialmente consumíveis por aquele usuário.

A utilização de aplicativos de *Global Positioning System (GPS*) em celulares e em centrais multimídias de veículos automotores permite traçar um perfil de risco do motorista, o qual, se revendido a companhias seguradoras de automóveis, será decisivo para determinar a precificação do seguro.

Compras de medicamentos e de produtos de higiene pessoal em farmácias e drogarias são capazes de dizer a agências de publicidade se uma mulher que lá esteve está grávida, mesmo que ela sequer tenha compartilhado

tal fato com seus familiares.

Tudo isso é resultado da definição de perfil dos usuários, a partir do tratamento automatizado de seus dados pessoais, que, por sua vez, são obtidos por intermédio dos rastros digitais produzidos por seus dispositivos móveis e demais *gadgets* empregados em atividades rotineiras (TEIXEIRA; GUERREIRO, 2022, p. 15).

Saliente-se que, no âmbito econômico, o consumo é, atualmente, baseado em dados, em categorizações de perfis e em discriminações estatísticas, sendo que a capacidade de tal conjunto de dados de espelhar a realidade do consumidor depende, cada vez mais diretamente, de uma escala exponencial de vigilância na sociedade (BAUMAN; LYON, 2013, p. 113). Quanto maior a vigilância, mais completo será o conjunto de dados, e mais minucioso, o perfil de consumo do indivíduo.

Por sua vez, a vigilância, como núcleo da sociedade moderna, também se sustenta no prazer que as pessoas em geral têm de serem observadas e no desejo, mesmo que inconsciente, que elas nutrem de tentarem influenciar o comportamento alheio (BAUMAN; LYON, 2013, p. 114).

Desse modo, verifica-se que a autoexposição é um dos elementos fundantes da sociedade de vigilância, tratando-se de um verdadeiro *voyeurismo*-exibicionismo digital (HAN, 2017, p. 108).

Acerca disso, ressalte-se que a “cooperação não apenas voluntária, mas entusiástica, dos manipulados é o principal recurso empregado pelos sinópticos dos mercados de consumo” (BAUMAN; LYON, 2013, p. 125).

As pessoas se desnudam “livremente” perante o panóptico digital, porque são “livres” e assim se colocam, porque “querem” colocar-se (HAN, 2017, p. 115).

Tal conjuntura revela nada mais do que a coisificação do ser humano, por meio da sua própria transformação em dados, em informação (BAUMAN; LYON, 2013, p. 126).

É, nesse contexto de coisificação humana — eis que o ser humano passa a ser o criador de uma plêiade de dados a seu próprio respeito, reduzindo-se praticamente a estes —, que o Panspectron se manifesta. Ele é resultado de práticas de vigilância difusa por parte de instituições estatais e de entes privados,

resultando no monitoramento constante e impositivo do indivíduo, sem que ele saiba que é vigiado (BEZERRA; LOPES, 2018, p. 630).

A Figura 2 ilustra o modelo de vigilância contemporâneo, ao mostrar a dinâmica do Panspectron e ao demonstrar o seu caráter onipresente, multifacetado e interdependente da vigilância tecnológica no dia a dia do indivíduo.

A exaustiva vigilância ilustrada na Figura 2 é o que alimenta o Panspectron, tornando-o um elemento poderoso na sociedade atual, visto que é pautado, essencialmente, no conhecimento preditivo.

Se, em um primeiro momento, os dados geravam informação apta a ser comercializada, agora essa informação serve de base para a construção do conhecimento preditivo, desenhando perfis comportamentais de modo automatizado e segundo parâmetros previamente estabelecidos.

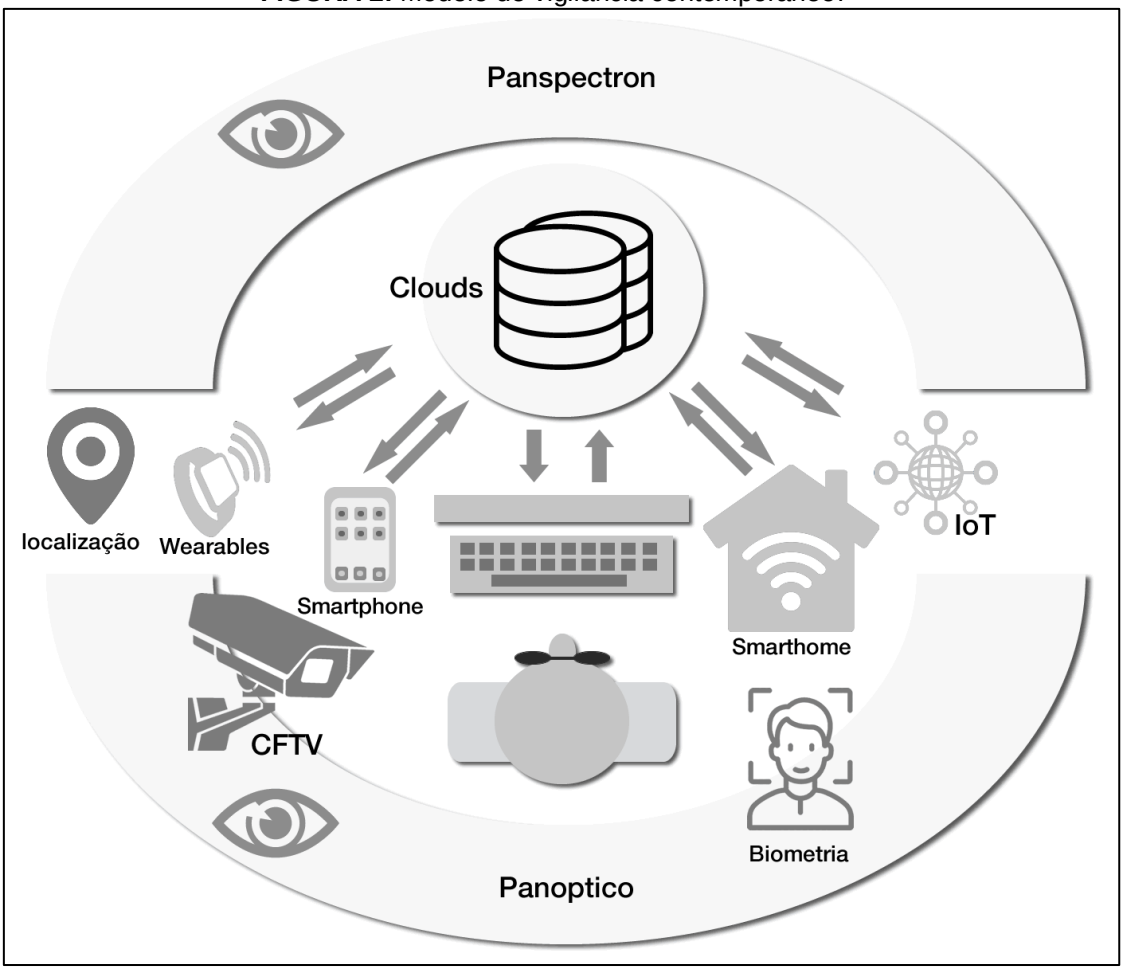
Além disso, esse tipo de conhecimento preditivo, capaz de reunir informações a ponto de padronizar certos tipos de comportamento parametrizado dos indivíduos, é capaz não só de categorizar perfis individuais deles, mas, em casos extremos, é capaz, ainda, de produzir discriminação desses indivíduos ou de grupos deles. Versão do panóptico em um estágio mais avançado, ou seja, espécie de panóptico digital, o Panspectron, além de penetrar em todas as esferas da vida dos indivíduos, vigia-os e ainda os categoriza, podendo, até mesmo, discriminá-los.

A vigilância tecnológica tornou-se um modo efetivo de controle social "pós-pan-óptico", semelhante ao controle social exercido pelo fictício Grande Irmão orwelliano,[13] vez que, além de humano, o indivíduo passou a ser um *hiperlink* (BAUMAN; LYON, 2013, p. 16-17), pois é, ao mesmo tempo, vigia e vigiado, criador e consumidor de conteúdos digitais. Em última análise, a vigilância resulta em categorização social, podendo ser utilizada para fins tanto lícitos, quanto ilícitos (BAUMAN; LYON, 2013, p. 18).

---

[13] O "Grande Irmão" (no original, em inglês, "Big Brother") é um personagem ficcional do livro "1984", publicado originalmente em 1949, de autoria do escritor britânico nascido na Índia, Eric Arthur Blair, mais conhecido pelo pseudônimo de George Orwell. A história aí contada passa-se em uma sociedade distópica, na qual o "Grande Irmão", soberano de um Estado totalitário, tem o poder de saber tudo de todos, o tempo todo. Desde então, ele tem sido o ícone da vigilância estatal.

**FIGURA 2:** Modelo de vigilância contemporâneo.[14]




FONTE: Adaptado de CARIBE (2019, p. 85).

Todavia, um dos grandes problemas dessa transformação dos seres humanos em *hiperlinks*, sujeitos a um efetivo controle pós-pan-óptico, a tal ponto capaz de torná-los produtos da vigilância e reduzidos à categorização social,

[14] Acerca dos itens ilustrados na Figura 2, explica-se que "*clouds*", palavra traduzida para o português como "nuvens", são nuvens computacionais, nas quais são armazenados e processados os dados, que, tratados, servirão para gerar informação e, por conseguinte, valor. "*Wearables*", por sua vez, são um termo traduzido em português como "vestíveis", o que efetivamente corresponde ao fato de se tratar de dispositivos móveis vestíveis, ou seja, que podem ser trazidos junto ao corpo, como os "relógios inteligentes" ("*smartwatches*") e como os óculos de realidade virtual (em inglês, referidos como "*Virtual Reality Eyes*", ou simplesmente, como "*VRs*"). CFTV é a sigla de "Circuito Fechado de Televisão" e faz referência aos sistemas de câmeras de segurança. A "*smart home*" ("casa inteligente", em português) e a "*Internet of Things*" (cuja abreviação é "*IoT*", ou "internet das coisas", em português) dizem respeito ao uso expressivo da tecnologia em objetos que inicialmente não foram pensados para que gerassem dados ou se conectassem à internet. Exemplo da "*IoT*" é o monitoramento do consumo de uma torneira, por meio de um sensor na saída de água, ou mesmo do interior de uma geladeira, por meio de uma câmera conectada à Internet.

reside no fato de os cidadãos estarem cada vez mais expostos e, portanto, mais e mais vulneráveis a controles descabidos por parte de agentes estatais responsáveis por exercerem aquela vigilância (MONTARGIL, 2008, p. 23-24).

Em síntese, se, antes, a análise de dados era capaz de prever comportamentos, atualmente, isto é, no contexto do Panspectron, tal análise de dados não apenas monitora os comportamentos, como os induz, prejudicando a liberdade e a privacidade das pessoas.

## 2.3 A UTILIZAÇÃO DE DADOS PELO ESTADO CONTEMPORÂNEO

Uma vez apresentada a formação do Estado Contemporâneo ocidental, bem como uma vez apresentadas as características do Panspectron, passa-se, agora, a discorrer sobre a atuação estatal baseada em dados em três nichos, quais sejam eles: o da Espionagem, o do Controle Social e o do Sistema de Justiça Criminal. Em cada uma dessas três áreas em que se verifica a atuação estatal, no sentido da utilização de dados pelo Estado Contemporâneo ocidental, será apresentado e, a seguir, examinado, um exemplo concreto desse tipo de atuação, a fim de tornar mais clara a compreensão das possibilidades computacionais, sobretudo para todos aqueles que, não sendo especialistas nessa área do conhecimento, não a dominem. Por fim, cumpre mencionar que, muito embora o presente trabalho foque em *Big Data*, não é possível afirmar que os exemplos de *softwares* apresentados a seguir são baseados nesse tipo de tecnologia, uma vez que não foi possível acessar os pormenores dessas ferramentas computacionais.

### 2.3.1 Espionagem: o caso Edward Snowden e a Agência de Segurança Nacional dos Estados Unidos da América

No ano de 2013, Edward Joseph Snowden revelou ao mundo um esquema de vigilância global perpetrado pelos EUA, por meio da *National Security Agency* (*NSA*), a Agência de Segurança Nacional daquele país.

Em síntese, Edward Snowden trabalhava como analista de dados da

*NSA*, desempenhando funções de espionagem doméstica e, também, de espionagem estrangeira, em benefício do governo estadunidense e, por discordar de tal prática, tomou a iniciativa de divulgar a jornalistas esse tipo de atuação estatal (FALK, 2017, p. 23).

Segundo Snowden, a *NSA* possui uma infraestrutura computacional e de pessoal capaz de coletar, armazenar, monitorar e analisar todas as comunicações de todos os indivíduos e organizações do mundo inteiro, sejam essas comunicações eletrônicas ou mesmo telefônicas (FALK, 2017, p. 33).

As divulgações das reportagens baseadas nos relatos e no material fornecido por Snowden causaram indignação ao redor do Planeta, tendo, inclusive, gerado mal-estares e constrangimentos no âmbito das Relações Internacionais.

Todavia, a postura estadunidense não surpreende. Como já mencionado neste trabalho, a inteligência e a espionagem existem desde muito tempo, tendo-se alterado somente os meios pelos quais elas são praticadas.

Desse modo, ao considerar que atualmente se vive na Sociedade Informacional, não causa espanto pensar em espionagem que venha sendo praticada por meios computacionais. Pelo contrário, esse tipo de prática é até esperado, visto que a informação obtida dessa forma também tem valor estratégico.

A importância da informação no contexto das Relações Internacionais guarda relação, assim, com o denominado "*Smart Power*" do inglês (ou "Poder Inteligente", em tradução livre para o português).

Não obstante, antes que se pense em algo simplista, como ocorre com a expressão "Poder Inteligente", muito popular na área da tecnologia e decorrente do uso de algum artifício tecnológico de última geração que torne um "aparelho" qualquer (ou "*gadget*") em um dispositivo capaz de fazer seu usuário conseguir interagir, em tempo real, com outras pessoas, a exemplo do adjetivo "inteligente" aposto aos nomes com que foram batizados o "telefone inteligente" ("*smartphone*") e o "relógio inteligente" ("*smartwatch*"), é importante esclarecer que a expressão "*Smart Power*" não se reduz a esse âmbito da tecnologia interativa, muito embora também não exclua essa possibilidade.

O *Smart Power* de que aqui se trata é aquele cujo conceito combina as

características (i) do *Hard Power* e (ii) do *Soft Power*, características estas que consistem, respectivamente, (i) no uso coercitivo do poder militar e econômico e (ii) na difusão não coercitiva de valores culturais e de políticas de um determinado Estado, no âmbito das Relações Internacionais (PINTO, 2016).

Deste modo, o *Smart Power* de um Estado baseia-se na estratégia relacional e contextual entre o seu *Hard Power* e o seu *Soft Power* e tem, como fim último, a obtenção de resultados pragmáticos e efetivos para cada decisão tomada no cenário internacional.

Segundo Pinto (2016, p. 156), o *Smart Power* consistiria, assim, na:

> "[C]apacidade de repensar a maneira de utilizar recursos de poder que o Estado já possui, através de estratégias que sejam capazes de distinguir cenários, recursos, objetivos e demandas, o que pode ser identificado como uma capacidade de inteligência contextual do Estado".

Logo, a adoção do *Smart Power* por um Estado soberano consiste na possibilidade de gerar ganhos mútuos para todos os envolvidos na tomada de decisão em âmbito internacional. Não se trata, portanto, de uma postura de soma zero; mas, de uma conduta diplomática que seja capaz de compor diversos interesses em prol de um resultado pragmático e efetivo, mesmo que os benefícios entre os atores envolvidos sejam diferentes, mas desde que essas diferenças ainda assim tornem as tratativas internacionais atraentes para quem delas participa (PINTO, 2016).

Verifica-se, portanto, que o *Smart Power* consiste na adoção, no âmbito das Relações Internacionais, de uma postura inteligente de um Estado soberano, a fim de que ele possa, de modo eficiente e otimizado, obter resultados pragmáticos na esfera internacional, de acordo com as possibilidades de cada circunstância que se apresente.

Trata-se, pois, da adoção de condutas mistas no desenvolvimento da Política Externa de determinado país, o que logicamente guarda relação com o uso de técnicas computacionais empregadas para a produção da informação, além de guardar relação com outras frentes de atuação estatal, como no caso da guerra cibernética.

Acerca da relação entre *Smart Power* e informação, explica Xavier (2022, p. 78):

> “[N]a atual conjuntura internacional, ter *smart power* depende de controlar o ciclo da informação; isso exige do ator internacional mais do que tecnologia para se apropriar das informações, depende da reflexão para planejar e executar as ações a serem tomadas, isto é, saber identificar as informações necessárias, reunir informações relevantes na imensidão de informações existentes no sistema internacional, triar e organizar a informação possuída, produzir informação estratégica, disponibilizar de forma seletiva as informações de seu interesse, atingir os destinatários corretos, com linguagem acessível, e proteger o que é sensível. Estar inserido na sociedade da informação vai além de ser transparente, é preciso saber coletar, disponibilizar e negar informação em um processo relacional que depende da capacidade informacional.”

Com isso, verifica-se que o Estado Contemporâneo passou, na Sociedade Informacional, a preocupar-se com o desempenho de suas funções em torno da informação, exigindo-se dele conhecimento computacional e estratégias de atuação baseada em *Smart Power*, visto que, do contrário, ele estará vulnerável a interações internacionais em detrimento de seus próprios interesses nacionais.

### 2.3.2 Controle social: o exemplo do crédito social chinês

O crédito social (expressão comumente referida, em inglês, como sendo “*social credit*”) da República Popular da China, ou *social credit* chinês, pode ser citado como exemplo já clássico da materialização do controle social do Estado Contemporâneo da China, no contexto atual do Panspectron, baseado em ferramentas de vigilância usadas pela Administração Pública chinesa, com o propósito de categorizar os habitantes do território nacional chinês, por meio do emprego de técnicas chamadas, em inglês, de *profiling* — e traduzidas, para o português, como de perfilamento, ou perfilagem.

Logo, o *profiling* consiste na adoção de técnicas computacionais que objetivam constatar aquilo que, a partir do tratamento de dados, torna-se relevante em determinado contexto (BOFF; FORTES; FREITAS, 2018, p. 161). Isto é, busca-se traçar perfis de comportamentos, sejam estes individuais ou coletivos, a fim de, por meio de tais condutas previamente categorizadas, averiguar tendências e intenções. Trata-se, pois, de uma faceta do conhecimento preditivo, visto que o *profiling* utiliza o conhecimento obtido a partir

de dados coletados no passado, para, a partir deles, prever cenários futuros.

Ocorre que, ao longo dos últimos anos, o mais do que centenário Partido Comunista Chinês (PCCh), fundado em 1921, vem desenvolvendo e aplicando nos moradores da China uma tecnologia de *profiling* baseada no monitoramento contínuo de pessoas e empresas com o intuito de atribuir-lhes pontuações de acordo com seu comportamento social (BRAUN, 2021). Segundo autoridades chinesas, esse sistema visa a construir relações de confiança entre seus cidadãos e o Estado.

Trata-se, portanto, da construção de relações sociais e estatais baseadas em reputação, o que nitidamente se traduz em ações estatais discriminatórias e danosas para com seus cidadãos, pois condutas eventualmente praticadas por estes, como atrasar o pagamento de uma fatura de cartão de crédito, parar um veículo automotor na faixa de pedestre ou fumar em lugar proibido são capazes de influenciar negativamente a pontuação do crédito social (ou *social credit*) chinês.

Por outro lado, um cidadão ou uma sociedade empresária respeitarem as determinações do Estado chinês aumenta a sua respectiva pontuação ("*score*", em inglês), de indivíduo ou de empresa perante o Estado chinês, o que pode vir a dar ensejo a um ambiente propício que facilite não só a perpetuação das pessoas que estejam no poder, como também a violação estatal da liberdade individual ou da livre iniciativa empresarial.

Em casos extremos, um cidadão adulto com baixa pontuação pode ter seus filhos impedidos de frequentarem determinadas escolas, pois será dada preferência de matrícula para os filhos de quem tiver uma pontuação (ou crédito) social maior frente ao Estado (BRAUN, 2021).

Esse exemplo do crédito social chinês demonstra que, na Sociedade Informacional, existe uma assimetria de conhecimento entre o Estado e seus concidadãos, em razão de o avanço das Tecnologias da Informação e Comunicação (TICs) permitir ao Estado conhecer cada vez mais do indivíduo, enquanto o contrário não ocorre.

Esse contexto faz, inclusive, com o que o indivíduo sequer possa escolher sobre o que será conhecido sobre ele (BOFF; FORTES; FREITAS, 2018, p. 26). Trata-se de verdadeira coação não violenta, onipresente e

descentralizada (BOFF; FORTES; FREITAS, 2018, p. 27).

### 2.3.3 Sistema de Justiça Criminal: as ferramentas computacionais *PredPol, HunchLab, COMPAS* e *Detecta*

A utilização de dados pelo Estado no âmbito penal já é uma realidade. Ferramentas computacionais baseadas em *profiling* e em conhecimento preditivo já estão presentes em diversos Sistemas de Justiça Criminal, inclusive, no do Brasil. É o caso dos *softwares PredPol*, *HunchLab*, *COMPAS* e *Detecta*, os quais têm auxiliado o Estado na área de Segurança Pública, bem como na tomada de decisões por juízes no âmbito da persecução penal.

Contudo, nem sempre os resultados são bons, vez que a adoção desse tipo de tecnologia pode resultar em graves violações de direitos, como a discriminação racial, como será visto adiante.

Um exemplo da utilização de conhecimento preditivo decorre do monitoramento de crimes ocorridos em determinada localidade, durante determinado intervalo de tempo, o que auxilia as autoridades de Segurança Pública a desenharem estratégias aptas a diminuir o índice de criminalidade.

Em outras palavras, é perfeitamente possível recorrer à análise de dados, para, por intermédio dela, lograr obter informações que sejam aptas a desenhar padrões comportamentais, os quais servirão de base para a construção de conhecimento preditivo, o que, por sua vez, poderá ser utilizado por autoridades públicas para implementar mecanismos capazes de prevenir a criminalidade (ARRUDA; RESENDE; FERNANDES, 2022).

Acerca disso, menciona-se o policiamento ostensivo praticado em áreas comerciais, durante o período das compras de Natal (G1, 2022). O final de ano é época em que os trabalhadores recebem o décimo terceiro salário e na qual, não raras vezes, utilizam-no, para fazerem compras de Natal. Sabendo disso, criminosos planejam suas ações em áreas comerciais durante esse período natalino, haja vista a maior circulação de dinheiro nessa região, o que, por conseguinte, aumenta o índice de crimes contra o patrimônio.

Diante desses fatos, as autoridades de Segurança Pública têm-se

adiantado e oferecido policiamento ostensivo aos comerciantes durante o período natalino, o que vem reduzindo a criminalidade de modo preventivo e vem garantindo a livre e segura circulação de riquezas (GOVERNO DO ESTADO DO PARANÁ, 2022). Trata-se, portanto, de um exemplo de policiamento preditivo, isto é, do policiamento baseado em conhecimento preditivo.

O *PredPol* é uma ferramenta baseada em técnicas computacionais direcionadas ao policiamento preditivo. No ano de 2008, o Departamento de Polícia de Los Angeles (em inglês, *Los Angeles Police Department*) e a Universidade da Califórnia em Los Angeles (*University of California in Los Angeles*, *UCLA*) criaram o *software PredPol*, o qual tem sido capaz de prever, com considerável precisão, a ocorrência de crimes (FIOROT, 2021, p. 17).

No ano de 2013, a utilização do *PredPol* atingiu uma "redução média de 7,4% no volume de crimes em função do tempo de patrulha e uma redução de 12% no número de crimes contra a propriedade em comparação ao [do] ano anterior" (FIOROT, 2021, p. 18).

Segundo a empresa que desenvolveu e comercializa o *PredPol*:

> "[E]le consiste na prática de identificar os horários e os locais onde crimes específicos têm maior probabilidade de ocorrer, então patrulhando essas áreas, para evitar que esses crimes ocorram"[15] (*PredPol*, 2023, p. 1) [em tradução livre].

Ainda acerca do *PredPol*, Freitas e Barddal (2019, p. 112) discorrem:

> "O sistema é baseado em um algoritmo preditivo que demonstrou repetidamente a capacidade de prever mais do que o dobro da quantidade de crimes em operações de campo, quando comparado com especialistas criminais utilizando aplicações comerciais já existentes. Além disso, o mesmo *site* aponta que o *PredPol* também aplica métodos matemáticos, para prever a violência armada. O sistema tem um desempenho melhor, quando comparado ao método tradicional de geração do *hot-spot mapping* ["mapeamento dos pontos quentes", na tradução para o português], pois obtém informações do *Big Data*, combinando comportamentos pessoais e dados sobre as vizinhanças. Além disso, o sistema consegue orientar melhor os esforços policiais para reduzir a criminalidade."

---

[15] No original, em inglês: "*it is the practice of identifying the times and locations where specific crimes are most likely to occur, then patrolling those areas to prevent those crimes from occurring*" (*PredPol*, 2023, p. 1).

Outro sistema computacional utilizado para fins de Segurança Pública preditiva é o *HunchLab*, presente em cidades como Nova Iorque e Miami, localizadas respectivamente nos Estados de Nova Iorque e da Flórida, nos EUA.

Referido *software*, qual seja, o *HunchLab*, “não apenas mapeia locais mais suscetíveis à criminalidade, mas também examina o porquê de determinadas áreas apresentarem maior risco, estando muitas dessas causas associadas ao ambiente ou à demografia de uma área” (FIOROT, 2021, p. 18). Com isso, o *HunchLab* indica a probabilidade de um determinado crime ocorrer em diversos lugares, durante determinado período (CHEETHAM, 2019).

No Brasil, o conhecimento preditivo também vem sendo utilizado no Sistema de Justiça Criminal. Em 2014, o estado mais populoso da Federação, o Estado de São Paulo, adquiriu o *software Detecta* da empresa *Microsoft Corporation* e passou a utilizá-lo no monitoramento da criminalidade por meio da análise das imagens, tendo sido capaz de, até o ano de 2018, efetuar a prisão de quase nove mil e quinhentas pessoas em flagrante delito, a interceptação de mais de cinco mil e quinhentos veículos automotores suspeitos e a apreensão de mais de quinhentas armas ilegais de fogo (FIOROT, 2021, p. 20). Além disso, o Brasil já vem implementando, com sucesso, câmeras de reconhecimento facial, as quais têm sido fundamentais para a prisão de foragidos (G1, 2023).

Por sua vez, no âmbito da atividade típica do Poder Judiciário, os EUA também desenvolveram o *software* chamado, em inglês, de *Correctional Offender Management Profiling for Alternative Sanctions* (em português, “Perfil de Gerenciamento de Infratores Correcionais para Sanções Alternativas”, em tradução livre), mais conhecido pela sigla *COMPAS*, que era destinado a auxiliar juízes em decisões sobre a prisão ou sobre a soltura de infratores, com base na probabilidade de reincidência (FREITAS; BARDDAL, 2019, p. 121).

Todavia, com o passar do tempo, notou-se que o *COMPAS* era mais severo com pessoas negras, uma vez que elas apresentavam duas vezes mais chances de reincidência penal em comparação com as pessoas brancas, demonstrando que a programação do *software* era enviesada com posicionamentos racistas (FREITAS; BARDDAL, 2019, p. 121).

Acerca do enviesamento do *COMPAS*, esclarecem Freitas e Barddal (2019, p. 121) que, após uma auditoria, verificou-se que:

> “A cor da pele não foi utilizada como característica (*feature*) pelo modelo preditivo, mas o sistema ainda foi considerado tendencioso, principalmente, porque considerava informações sobre onde o réu residia, o que está correlacionado indiretamente com a cor de pele nos EUA”.

Optou-se, então, por descontinuar o uso desse instrumental computacional (FIOROT, 2021, p. 30-31).

## 2.4 ALGUMAS CONSIDERAÇÕES

Diante do exposto neste primeiro capítulo, verifica-se que a Sociedade Informacional tem influenciado, de modo bastante significativo, a atuação do Estado Contemporâneo, por meio do tratamento de dados. Não mais é possível imaginar o ente estatal atuando, sem levar em conta o tratamento de dados, para a obtenção de informação e de conhecimento sobre o cidadão e o ambiente público. O aspecto pervasivo e onipresente da Computação é uma realidade irreversível, visto que, atualmente, vive-se em meio ao Panspectron.

O Estado passou a depender da informação de uma forma antes inimaginável. Para efetuar planejamentos e concretizar ações, a Administração Pública depende de dados. A Política Externa de um país está vulnerável à vigilância e à espionagem estrangeira cada vez mais potencializadas pelas tecnologias computacionais. O Sistema de Justiça Criminal, tanto nas áreas de Segurança Pública, quanto nas áreas de persecução penal, necessita de ferramentas capazes de direcionar e otimizar recursos, para combater e punir a criminalidade, inclusive, aquela cometida por meios computacionais.

Todavia, as ferramentas de Computação não são infalíveis, visto que são criadas por seres humanos. É possível que ocorram práticas discriminatórias com o enviesamento de aplicações, como ocorreu no caso do sistema COMPAS, o que, paradoxalmente, traz mais insegurança jurídica, ao mesmo tempo em que se busca aumentar a eficiência do Sistema de Justiça.

# 3 CIÊNCIA DA COMPUTAÇÃO, *BIG DATA* E COMPUTAÇÃO FORENSE

O intuito perseguido neste segundo capítulo, intitulado “Ciência da Computação, *Big Data* e Computação Forense”, é verificar se é tecnicamente possível que o Estado Contemporâneo utilize ferramentas computacionais baseadas em *Big Data* no âmbito do Sistema de Justiça Criminal.

Muito embora, no capítulo anterior, tenham sido trazidos exemplos concretos da utilização de ferramentas computacionais no âmbito do Sistema de Justiça Criminal, é necessário aprofundar aspectos técnicos da Ciência da Computação, para que, só então, seja possível passar adiante, para estudar como funciona o *Big Data*.

Para tanto, no presente capítulo, apresenta-se o retrospecto histórico e se apresentam, também, alguns dos aspectos basilares da Ciência da Computação, a fim de que o leitor — sobretudo, o leitor não familiarizado com essa área específica do conhecimento — possa entrar em contato com noções básicas sobre o funcionamento das tecnologias computacionais, ainda mais quando se tem em vista que o presente trabalho acadêmico foi desenvolvido dentro de um Programa de Pós-Graduação *Stricto Sensu* em Direito (PPGD), área do conhecimento em que, em princípio, não são estudados, em profundidade, aspectos relacionados à tecnologia e à computação, não se esperando, pois, que o leitor seja dotado de conhecimento especializado em Ciência da Computação.

Após essa apresentação, conceitua-se o que é o *Big Data* e se descrevem as suas características distintivas, haja vista a produção massiva de dados decorrente do fenômeno do Panspectron no bojo da Sociedade Informacional.

Por fim, são abordados elementos do Processo Penal brasileiro e como ele se desenvolve desde a prática de um delito até a solução do respectivo caso penal. Nesse contexto, são descritas características da perícia envolvendo Computação Forense, bem como é analisada a relação desse cenário com a teoria da prova e a cadeia de custódia.

Desse modo, objetiva-se correlacionar o surgimento da Computação

com seu caráter pervasivo na sociedade atual, a fim de que seja possível demonstrar se o *Big Data* pode auxiliar o Sistema de Justiça Criminal, seja no âmbito da Segurança Pública, seja no âmbito da persecução penal.

## 3.1 CIÊNCIA DA COMPUTAÇÃO: HISTÓRICO E ASPECTOS BASILARES

A Ciência da Computação, como diz o próprio nome, relaciona-se ao ato de computar, isto é, ao ato de calcular (DICIONÁRIO AULETE, 2023a). Portanto, inicialmente, a Computação nada mais era do que um desdobramento da Ciência Matemática, direcionada à execução de cálculos complexos.

Com o tempo, a Computação evoluiu para se tornar um ramo autônomo, da grande área das Ciências Exatas, a Ciência da Computação, cuja essência é a interdisciplinaridade, com destaque para sua intersecção com as áreas da Física e da Química e, recentemente, até mesmo, com a Linguística, em razão do desenvolvimento da subárea do Processamento de Linguagem Natural.[16]

Partindo do pressuposto de que a Matemática seja, em si mesma, uma forma de linguagem, a Ciência da Computação consiste na área do conhecimento em que a linguagem matemática é não só transmitida e compreendida por uma máquina, como, ainda, pode ser submetida a tratamento de dados, de uma forma antes impensável.

Nesse sentido, Brookshear (2013, p. 2) afirma que a "Ciência da Computação é a disciplina que busca construir uma base científica para tópicos, como projeto e programação de computadores, processamento de informação, soluções algorítmicas de problemas e o próprio processo algorítmico".

O algoritmo é, portanto, a essência e um dos fundamentos da Ciência da Computação, pois condensa "um conjunto de passos que define como uma tarefa é realizada" (BROOKSHEAR, 2013, p. 2-4).

Desse modo, é possível afirmar que um programa (o *software*) é a representação de um algoritmo, o qual é codificado em uma linguagem capaz de

---

[16] O Processamento de Linguagem Natural (PLN) diz respeito à capacidade de máquinas compreenderem a linguagem falada por humanos (*IBM*, 2023).

ser compreendida por uma máquina (o *hardware*), sendo tal tarefa de codificação denominada de programação (BROOKSHEAR, 2013, p. 2).

A execução de cálculos é tão inerente à Computação, que, durante o século XX, havia os chamados “computadores humanos”, os quais eram, em sua maioria, mulheres dedicadas a efetuar, manualmente, cálculos complexos em áreas de grande importância (IEA/USP, 2017), como os laboratórios estadunidenses destinados a subsidiar decisões durante a Segunda Guerra Mundial, bem como a própria *National Aeronautics and Space Agency* (*NASA*) durante a Guerra Fria. Todavia, a importância do cálculo e, portanto, da Computação é bem mais antiga do que isso.

Desse modo, a Ciência da Computação não se limita a estudar computadores, constituindo-se em área muito mais abrangente do conhecimento e consistindo, em síntese, no “estudo de problemas, [na] resolução de problemas e [de] soluções que surgem do processo de resolução de problemas” (MILLER; RANUM; COLLEGE, 2019, p. 1).

O cientista da Computação tem seu trabalho voltado para o estudo de problemas, em busca de encontrar-lhes soluções com base em algoritmos. Estes, por sua vez, podem ser definidos como processos finitos, segmentados em etapas passo a passo, e que, se devidamente seguidos, solucionarão o problema posto sob análise (MILLER; RANUM; COLLEGE, 2019). Desse modo, o cientista da Computação aplica seus estudos e trabalhos da construção de algoritmos capazes de solucionar os mais diversos problemas (MILLER; RANUM; COLLEGE, 2019).

A história dos computadores é milenar e está intrinsicamente ligada às necessidades matemáticas ao longo da história humana. Fedeli, Polloni e Peres (2013, p. 1-2) cogitam do início da História da Ciência da Computação aproximadamente no ano de 2.000 antes de Cristo (a.C.), com a criação do ábaco, espécie de calculadora baseada no arranjo de pequenas esferas conhecidas como contas e utilizadas pelos povos orientais para diversas atividades, especialmente, para o comércio — inclusive podendo o ábaco, conforme apontam os citados autores, ter sido o primeiro *hardware* da História.

A partir dos anos de 1960, o desenvolvimento da Ciência, como um todo, foi fortemente impulsionado pelas duas Grandes Guerras do século XX e,

também, pela corrida nuclear e aeroespacial da Guerra Fria, resultou na evolução das linguagens de programação e na construção de *hardwares* cada vez mais sofisticados e eficientes (FEDELI; POLLONI; PERES, 2013, p. 1-2).

Contudo, muito embora o estado da arte da Ciência da Computação esteja atualmente num estágio significativamente avançado, ainda assim existem problemas que não são possíveis de serem solucionados, razão pela qual se pode afirmar que a Ciência da Computação estuda as soluções algorítmicas para determinados problemas, bem como a impossibilidade de soluções de outros tipos de problemas (MILLER; RANUM; COLLEGE, 2019).

Em outras palavras, “a Ciência da Computação é o estudo de problemas que são e que não são computáveis, o estudo da existência e da inexistência de algoritmos” (MILLER; RANUM; COLLEGE, 2019, p. 1). Esse estudo ambivalente sobre problemas solucionáveis e sobre problemas não solucionáveis permite o desenvolvimento contínuo da Computação como Ciência, no seio da qual as mais diversas ferramentas têm sido criadas ao longo do tempo, com destaque para o já mencionado grande salto tecnológico do século XX, essencialmente impulsionado — como também já citado — pelas duas Guerras Mundiais e pelo período do Pós-Segunda Guerra Mundial chamado de Guerra Fria.

A programação é indispensável à Ciência da Computação, eis que consiste na codificação de um algoritmo em uma linguagem de programação (ou seja, em uma notação) capaz de ser compreendida e executada por um computador (MILLER; RANUM; COLLEGE, 2019). Entretanto, por ter como pressuposto uma solução algorítmica, a Ciência da Computação vai além da programação, visto que, sem uma solução abstrata para um determinado problema, não é possível programar um computador, para solucioná-lo (MILLER; RANUM; COLLEGE, 2019).

Nesse sentido, é possível afirmar que “algoritmos descrevem a solução para um problema em termos de dados necessários para representar a instância do problema e o conjunto de etapas necessárias para produzir o resultado pretendido” (MILLER; RANUM; COLLEGE, 2019, p. 1). Por sua vez, as “linguagens de programação devem fornecer uma maneira notacional de representar tanto o processo, como os dados”, fornecendo, com isso, “construções de controle e tipos de dados” (MILLER; RANUM; COLLEGE, 2019,

p. 1).

Durante o desenvolvimento da Computação, a utilização de representações binárias foi um marco revolucionário e, portanto, uma mudança paradigmática importante no âmbito da Ciência da Computação, porque a adoção de binários permitiu a construção de linguagens de programação em baixo nível, caracterizadas, em suma, por representações numéricas de 0 (zero) e 1 (um) (UFRGSb, 2023).

As sequências de números binários – 0 (zero) e 1 (um) – passaram a constituir os denominados tipos de dados, os quais, por sua vez, possibilitam a sua interpretação e, com isso, dão sentido perante o problema a ser solucionado (MILLER; RANUM; COLLEGE, 2019). Com isso, “os tipos de dados internos de baixo nível (às vezes chamados de tipos de dados primitivos) fornecem os blocos de construção para o desenvolvimento de algoritmos” (MILLER; RANUM; COLLEGE, 2019, p. 1).

Desse modo, a base da Computação é o algoritmo direcionado à solução de problemas, por meio de abstrações. Nesse sentido, abstrai-se determinado problema em etapas, as quais devem ser aptas a serem executadas pelo computador, o qual, por sua vez, deve ter sido programado mediante a codificação de uma linguagem que seja capaz de ser compreendida por essa máquina, isto é, efetua-se, em última análise, a programação do computador por meio de uma linguagem de programação que, em seus fundamentos, baseia-se em sequências binárias.

Contudo, atualmente, as linguagens de programação não são mais em baixo nível, isto é, em binários de 0 (zero) e 1 (um). Entretanto, isso não elimina a existência da lógica binária, haja vista que o que evoluiu ao longo do tempo foram os modos como códigos binários passaram a ser descritos e manipulados por cientistas da Computação. Em outras palavras, a Computação parte da linguagem de baixo nível (binários 0 e 1) até alcançar linguagens de programação de alto nível, como, por exemplo, as linguagens C, C++, Java e *Python*. Isto é, existem diversas camadas sobrepostas da linguagem de baixo nível até a linguagem de alto nível. O que se altera nessa sobreposição é a interface por meio da qual o código de programação é escrito pelo cientista, tornando menos complexa a tarefa de programar.

Afinal, seria um tanto quanto ilógico imaginar um cientista da Computação desenvolvendo, por exemplo, um sistema administrativo para uma empresa a partir de uma linguagem binária 0 (zero) e 1 (um), visto que o que se faz, na prática, é aproveitar bibliotecas já existentes de linguagens de programação (C, C++, Java, *Python* etc.), para construir soluções para os mais diversos problemas. Ou seja, utiliza-se a combinação de algoritmos já criados para determinadas tarefas, para construir soluções aptas a resolverem problemas mais complexos.

Desse modo, uma vez compreendido o modo básico por meio do qual se opera um computador atualmente, é possível definir os dois conceitos básicos que circundam essa área do conhecimento: *Hardware* e *Software*. O *Hardware* diz respeito ao aspecto físico da Computação, isto é, à própria máquina, o computador em si. Já o *Software* é o aspecto lógico, por meio do qual são criados programas executados pelo *Hardware* (ZOTELLI, 2023). É da combinação entre *Hardware* e *Software* que surge tudo o que se conhece atualmente na Computação. E é seguindo esse raciocínio de acumulação de conhecimento que a história do computador se desenvolve.

Como dito, a base do computador é o cálculo, cuja aplicação básica em tarefas cotidianas como o comércio fez surgir, entre os povos orientais, o ábaco há cerca de 4.000 anos (isto é, em 2.000 a. C.), o qual é considerado o primeiro *hardware* da História (IVEY, 2023).

Até os séculos XVII e XIX, não se tem muito conhecimento a respeito de outros dispositivos computacionais para além do ábaco. Muito embora não se desconsidere que outros computadores possam ter existido nesse meio-tempo, a mudança mais significativa, desde então, foi a criação de calculadoras mecânicas baseadas em engrenagens para a realização de cálculos, com destaque para a “Pascalina” de Blaise Pascal (1623-1662), e para o “Contador Escalonado” de Gottfried Leibniz (1646-1716) (séculos XVII a XIX) (IVEY, 2023).

Posteriormente, em 1837, Charles Babbage (1791-1871) criou a Máquina Analítica, que consistia em um computador mecânico capaz de efetuar diversos tipos de cálculo, a partir de cartões perfurados. Durante o período de transição do século XIX para o século XX, foram criadas por Hermann Hollerith (1860-1929) as Máquinas de Tabulação, que eram capazes de processar e de

analisar dados, por meio de cartões perfurados. As Máquinas de Tabulação foram um dos primeiros computadores a serem utilizados em ampla escala, vez que foram fundamentais para a realização de censos populacionais por parte do governo dos EUA, no período referido (IVEY, 2023).

Nas décadas de 1930 e de 1940, foram desenvolvidos os primeiros computadores eletrônicos, baseados em tubos de vácuo, com destaque para o *Electronic Numerical Integrator and Computer* (*ENIAC*). Computadores como o ENIAC já eram capazes de serem programados e de efetuarem diversas tarefas de forma mais rápida, além de terem alterado o paradigma da Computação mecânica para o da Computação eletrônica (IVEY, 2023).

Em 1947, cientistas da empresa *Bell Telephone Labs* inventaram o transistor, um dispositivo semicondutor que substituiu os tubos de vácuo nos computadores, fazendo com que estes diminuíssem significativamente de tamanho e se tornassem mais confiáveis. A revolução do transistor na Computação foi de tal magnitude, que fez com que os seus criadores — John Bardeen (1908-1991), William Bradford Shockley (1910-1989), e Walter Houser Brattain (1902-1987) — fossem agraciados com o Prêmio Nobel de Física de 1956 (IVEY, 2023).

Em 1958, Jack S. Kilby (1923-2005) e Robert Noyce (1927-1990) inventaram o *microchip*, suporte material de diminuta dimensão, dotado de rigidez e de propriedade semicondutora, capaz de criar um circuito integrado entre vários transistores e outros componentes elétricos. A criação do *microchip* permitiu que fossem criados computadores e eletrônicos cada vez menores (IVEY, 2023).

Além disso, em 1965, Gordon Moore (1929-2023), um dos fundadores da empresa *Integrated Electronics* (*INTEL*) *Corporation*,[17] teorizou a Lei de Moore, segundo a qual “o número de transistores em um *chip* dobraria aproximadamente a cada dois anos, com um aumento mínimo no custo” (KELLEHER, 2022). Em outras palavras, a capacidade de processamento dos computadores dobraria a cada dois anos, sem interferir, de modo significativo, no preço de comercialização para o consumidor final.

---

[17] A *Integrated Electronics* (*INTEL*) *Corporation* e a *Advanced Micro Devices Incorporated* (*AMD*, *Inc*.) são duas das maiores empresas de processadores do mundo (TARASOV, 2022).

Esse rápido crescimento tecnológico fez com que, a partir das décadas de 1970 e de 1980, os computadores pessoais começassem a ser largamente comercializados, com destaque para os modelos *IBM-PC* e o *Apple*-II (IVEY, 2023). A partir de então, surgiu uma nova era para a Computação, vez que os computadores começaram a ficar mais e mais acessíveis e cada vez mais populares, seja para pessoas comuns, seja para empresas.

Na década de 1990, a Internet, tal como a concebemos hoje, de relativamente fácil acesso universal, foi finalmente criada pelo cientista britânico da Computação Timothy John Berners-Lee, mais conhecido, simplesmente, por Tim Lee, responsável pela invenção da rede mundial de computadores (*World Wide Web*),[18] pelo Protocolo de Transferência de Hipertexto (em inglês, *Hyper Text Transfer Protocol*, ou *HTTP*), pelo *Hyper Text Markup Language* (*HTML*) e pelo Localizador Padrão de Recursos (*Uniform Resource Locator*, *URL*), o que permitiu a simplificação da troca de informações e, também, contribuiu para a popularização dos computadores (IVEY, 2023).

A partir dos anos 2.000, com o aperfeiçoamento das tecnologias sem fio (ou *wireless*, em inglês), começaram a surgir os dispositivos móveis com significativa capacidade computacional. Desde então, eletrônicos tais como *smartphones, tablets* e *notebooks* têm sido cada vez mais comuns, haja vista a capacidade da indústria de produzi-los em larga escala e a preço acessível, do mesmo modo que tem ocorrido com o acesso à Internet (IVEY, 2023).

Além disso, o aperfeiçoamento da infraestrutura da Internet permitiu a comercialização de serviços de computação em nuvem. Tal comercialização permite contratar determinada capacidade computacional ao mesmo tempo escalável e adquirida sob demanda, sem ser necessário ter de obter um *hardware* específico para esse tipo de tecnologia, reduzindo-se, destarte, os custos e tornando-a mais popular (IVEY, 2023).

Em 2007, a empresa canadense *D-Wave Systems, Incorporated (Inc.),* apresentou ao público o primeiro computador quântico do mundo, batizado de “Orion” (GUIMARÃES, 2019). A Computação Quântica é o novo divisor de águas na área da Computação, rompendo com conceitos e funcionamentos da

[18] A sigla “www” que precede os sítios eletrônicos faz referência, justamente, à *World Wide Web*.

Computação Clássica.

A Computação Quântica abandona o processamento de *bits* binários e recorre, em benefício próprio, a fenômenos da Física Quântica, operando por meio da superposição e do emaranhamento quânticos, o que dá origem aos "*qubits"* — redução, em inglês, de "bits quânticos" ("*quantum bits*").

Acerca da superposição quântica, explica-se:

> "*Qubits* podem representar inúmeras combinações possíveis de 1 e 0 ao mesmo tempo. Essa capacidade de estar simultaneamente em vários estados é chamada de superposição. Para colocar *qubits* em superposição, pesquisadores os manipulam usando lasers de precisão ou raios de micro-ondas. Graças a esse fenômeno contraintuitivo, um computador quântico com vários *qubits* em superposição pode processar um vasto número de possíveis resultados simultaneamente. O resultado final de um cálculo emerge apenas quando os *qubits* são medidos, o que imediatamente faz com que seu estado quântico 'colapse' para 1 ou 0" (*MIT TECHNOLOGY REVIEW*, 2020, p. 1).

Por sua vez, o emaranhamento quântico pode ser assim descrito:

> "Os pesquisadores podem gerar pares de *qubits* 'emaranhados', o que significa que os dois membros de um par existem em um único estado quântico. Alterar o estado de um dos *qubits* instantaneamente altera o estado do outro de maneira previsível. Isso acontece, mesmo se eles forem separados por longas distâncias. [...] Em um computador convencional, dobrar o número de *bits* dobra sua capacidade de processamento. Porém, graças ao entrelaçamento, a adição de *qubits* extras a uma máquina quântica produz um aumento exponencial em sua capacidade de processamento de números" (*MIT TECHNOLOGY REVIEW,* 2020, p. 1).

Entretanto, em que pese o aspecto revolucionário da Computação Quântica, ela está ainda em estágio inicial. Possivelmente, terá aplicações em nichos específicos, como no das indústrias aeroespacial e farmacêutica, além de no da pesquisa científica, entre outros. Neste momento, inexistem perspectivas de que, no curto prazo, a Computação Quântica substitua a Computação Clássica a um nível amplamente popular e comercializável.

Nesse sentido, uma vez apresentados os aspectos basilares da Ciência da Computação, passa-se a discorrer, agora, sobre o *Big Data*, haja vista que, como visto no capítulo anterior, na sociedade atual, é indispensável a utilização de dados, sendo o *Big Data* o tipo de tecnologia computacional capaz de lidar com esse imenso quantitativo de dados.

## 3.2 CONCEITO E CARACTERÍSTICAS DO *BIG DATA*

Inicialmente, para compreender o *Big Data*, é necessário discorrer sobre o que sejam dados, informação e conhecimento.

Segundo Dale e Lewis (2010, p. 39), dados são “valores básicos ou fatos, ao passo que informação é o dado que foi organizado e/ou processado de modo que ele seja útil na solução de algum tipo de problema.”

Já Fedeli, Polloni e Peres (2013, p. 10) afirmam ser dado o “elemento identificado em sua forma bruta que por si só não conduz a uma compreensão de um fato ou uma situação”.

Rousse (2023a) explica que, na sua forma bruta, dados não costumam ser úteis; mas, desde que organizados de forma relacional, eles se transformam em informação e, em razão disso, passam a ser úteis para os usuários.

Dados, em síntese, são conjuntos de números, de palavras e de símbolos que não têm significado e que necessitam passar por um processamento ou estar em determinado contexto, para, só então, poderem ser considerados informação (*CAMBRIDGE INTERNATIONAL*, 2015, p. 6).

Nas palavras de Boff, Fortes e Freitas (2018, p. 179):

> “[A] informação é tratada como elemento de valor que permite aos diversos programas computacionais processarem dados brutos e gerarem informação, a qual, por sua vez, pode ser continuamente processada em conjunto com novos dados ou informações, a ponto de se estabelecer um ciclo a partir de, para, sobre e com a informação.”

Por sua vez, conhecimento consiste em informação aplicada a uma finalidade prática (*CAMBRIDGE INTERNATIONAL*, 2015, p. 6). Isto é, conhecimento é a informação empregada na tomada de decisão em determinado contexto (BOFF; FORTES; FREITAS, 2018, p. 180-181).

Quanto ao *Big Data*, seu nome pode levar à crença de tratar-se simplesmente de uma grande quantidade de dados. Tal assertiva não é, contudo, correta.

Acerca do tema, Boff, Fortes e Freitas (2018, p. 218-219) ensinam:

> "*Big Data* é muito mais do que um grande volume de dados. *Big Data* inclui o poder de tratamento e [de] análise de dados semiestruturados e não estruturados provenientes de diversas fontes, formatos, estruturas, origens e tipos. Consequentemente, *Big Data* permite revelar tanto as formalidades quanto as restrições dos bancos de dados relacionais, de modo a ampliar as análises interativas e exploratórias sobre os dados, sejam estes quaisquer conjuntos de dados capturados e armazenados. O importante é que o *Big Data* tem características que permitem preservar a fidedignidade dos dados, ou seja, a autenticidades dos dados."

Para Oliveira (2022, p. 44-46), conceituar o *Big Data* como sendo mera imensidão de dados acabaria por reduzi-lo a um "mar de dados", ou melhor, a um "Lago de Dados", na expressão, em inglês, "*Data Lake*", a qual corresponde a uma enorme quantidade de dados a partir dos quais não se podem produzir informação nem conhecimento.

Afinal, além de grande, para ser considerado um *Big Data*, o conjunto de dados deve ser passível de produzir informação e conhecimento, com o estabelecimento de correlações e de tendências, a partir de técnicas computacionais avançadas e de alto nível de processamento, o que não seria possível diante de uma simples análise humana, nem mesmo diante da Computação clássica.

Além disso, segundo Oliveira (2022, p. 43-44), o *Big Data* é mais do que um simples banco de dados, porquanto, a partir dele, pode-se produzir conhecimento altamente refinado, ao:

> "(i) tratar dados em contextos específicos; (ii) criar e moldar tendências mesmo em relações dotadas de complexidade e dinamismo; (iii) compilar e organizar tendências de um determinado conjunto de pessoas ou coisas; e (iv) segmentar e classificar dados referentes a questões financeiras, preferências, e metadados em geral".

Floridi (2012, p. 1-3) considera um desafio epistemológico a expressão "*Big Data*", haja vista que é comum relacioná-la simplesmente com uma grande quantidade de dados que as ferramentas tradicionais da Computação ainda não são capazes de analisar, necessitando, para tanto, de soluções próprias.

Diante disso, por se tratar de fenômeno complexo na Sociedade Informacional, com características diversas, as quais impossibilitam uma conceituação estanque e definitiva, buscaram-se, na literatura, traços distintivos capazes de permitirem delimitar o que pode, ou não, ser considerado *Big Data*.

Apuraram-se, então, as características comuns ao *Big Data*, as quais podem ser sintetizadas nos chamados “cinco Vs”: (i) volume; (ii) velocidade; (iii) variedade; (iv) veracidade e (v) valor (ROUSE, 2023a).

Iniciando pelo volume e pela velocidade: aquele atine ao elevado tamanho do conjunto de dados do *Big Data*; ao passo que este diz respeito a enormes quantidades de dados continuarem a ser produzidas independentemente de já existir elevadíssimo número de dados (ROUSE, 2023a).

Saliente-se que não é possível se falar em *Big Data* sem considerar o volume de dados. Isso, porque o *Big Data* é um nicho específico da Ciência da Computação que decorre, justamente, da necessidade de ferramentas específicas para superar a dificuldade da análise de grandes volumes de dados, a exemplo das ferramentas baseadas em computação paralela e distribuída.

Por seu turno, a variedade caracteriza o aspecto não uniforme dos dados, podendo constituir-se, por exemplo, em um conglomerado de arquivos de mídia, em um vastíssimo compêndio de documentos formados por textos ou, ainda, em um conjunto gigantesco de expressões numéricas ou, mesmo, de expressões linguísticas esparsas (ROUSE, 2023a).

Já a veracidade consiste na qualidade e na integridade dos dados, ou seja, diz respeito à fidedignidade dos dados em relação ao que eles representam frente à adequação à finalidade para a qual foram concebidos.

Por fim, o valor dos dados atine à capacidade que eles têm de produzir informação e conhecimento úteis, seja para, com estes, subsidiar a tomada de decisões, seja para, a partir destes, elaborar predições (ROUSE, 2023a).

Podem-se representar os cinco “Vs” do *Big Data* conforme a Figura 3.

**FIGURA 3:** Os cinco “Vs” do *Big Data.*


FONTE: Adaptado de PONTOTEL, 2023.

Note-se que a imagem representa exatamente aquilo que foi descrito acima, bem como justifica, também com exatidão, o porquê de o *Big Data* ter tanto valor. Isso assim o é, porque o volume de dados é crescente e extremamente veloz; apresenta significativa variedade e passa a ter valor, na medida em que vai sendo averiguada a veracidade tanto das informações, quanto do conhecimento extraídos dos dados analisados.

Autores como Kitchin (2014) entendem que o *Big Data* possua sete características próprias, a saber: (i) volume; (ii) exaustividade; (iii) resolução e indexicalidade; (iv) relacionalidade; (v) velocidade; (vi) variedade e, por fim, (vii) flexibilidade e escalabilidade.[19]

Começando, novamente, pela característica do volume, tem-se que o *Big Data* é resultado do crescimento exponencial de dados pelo avanço e pela popularização da economia, o que tem exigido soluções aptas para extrair desse volume informação e conhecimento úteis (KITCHIN, 2014, p. 101-103).

Quanto à exaustividade, o *Big Data* permite análise exaustiva de todos os dados em estudo, o que contrasta, fortemente, com as tradicionais soluções da Computação clássica, visto limitarem-se estas a extrair informação e conhecimento tão somente de amostras de dados (os chamados "pequenos dados"; em inglês, "*small data*"); ou seja, sem retirar informação e conhecimento do conjunto completo de dados (KITCHIN, 2014, p. 104-105).

Já a resolução e a indexicalidade significam que o *Big Data* permite a devida indexação e a perfeita individualização dos dados, promovendo uma sua análise de modo altamente refinado, de maneira que cada dado seja analisado de forma individual e não, por atacado — isto é, e não, em lotes ou em conjuntos de amostras. Tal característica faculta a extração de informação e de conhecimento cada vez mais assertivos (KITCHIN, 2014, p. 106).

Ressalta-se que, para além de um simples filtro destinado a individualizar dados, as ferramentas computacionais baseadas em *Big Data* permitem a identificação de padrões capazes de generalizar e resumir o conjunto de dados analisados.

---

[19] Tradução livre de *"*(i) *volume;* (ii) *exhaustivity;* (iii) *resolution and indexicality*; (iv) *relationality;* (v) *velocity;* (vi) *variety* e (vii) *flexibility and scalability"* (KITCHIN, 2014, p. 101-111).

Quanto à relacionalidade, o *Big Data* é capaz de extrair informação e conhecimento a partir de *insights* antes impensados. Ou seja, a análise global de grandes quantidades de dados permite que sejam visualizados padrões e comportamentos populacionais que eram invisíveis em soluções de *small data* (KITCHIN, 2014, p. 107-108).

A velocidade, por sua vez, é um aspecto intrinsicamente ligado ao volume, pois algumas tecnologias *Big Data* já são capazes de gerar e de analisar dados de modo contínuo e, em alguns casos, em tempo real, produzindo, assim, não só farta informação — em quantidade —, como de qualidade, dentro um curto espaço de tempo (KITCHIN, 2014, p. 109).

No que diz respeito à variedade, eis aqui o caráter de grandiosidade do *Big Data*, que faz com que os dados que o componham sejam variados. Ou seja, o *Big Data* é um conjunto de dados estruturados, de dados não estruturados, de dados semiestruturados, bem como é formado por dados numéricos, por imagens, por áudios, por vídeos, por textos *etc*. (KITCHIN, 2014, p. 109-110).

Em relação à flexibilidade e à escalabilidade, tem-se que a velocidade e a variedade dos dados dentro do *Big Data* exigem que este seja flexível e escalável, pois, sem isso, praticamente não é possível analisá-los em tempo real. Portanto, soluções computacionais flexíveis e escaláveis são fundamentais para o *Big Data* (KITCHIN, 2014, p. 111).

Desse modo, considerando aquilo que Ciuriak (2018, p. 1) denomina de “dataficação”, onipresente no cotidiano das pessoas, haja vista que tudo o que é feito é, de certo modo, monitorado e transformado em dados — o que converge para o Panspectron descrito anteriormente —, não resta outra conclusão senão a de que o *Big Data* é uma realidade cada vez mais comum nos diversos nichos da sociedade atual.

Nas palavras de Boff, Fortes e Freitas (2018, p. 213-214):

> “Na sociedade contemporânea e informacional, a variedade de dispositivos gera uma pluralidade de dados em formatos, origens, fontes, estruturas, entre outros aspectos. Há que se mencionar a variedade de sensores e de dispositivos inteligentes. Não se pode deixar de lado as tecnologias colaborativas e das redes sociais. [...] Portanto, os sistemas computacionais estão sendo mais exigidos para tratar, armazenar, indexar e recuperar dados, visto que os sistemas tradicionais de processamento de dados tendem a colapsar.”

Foram apresentados, até aqui, os conceitos de dados, de informação, de conhecimento e de *Big Data*. Todavia, ainda falta abordar a descrição de como se dá a descoberta do conhecimento a partir do *Big Data*.

Para entender seu funcionamento, deve-se imaginar uma mina de metal precioso, como o ouro.

O garimpeiro (ou minerador) elege, para ser explorada, uma parcela do solo e, utilizando técnicas específicas, dá início às escavações do solo.

Depois de muito trabalho, encontra uma pepita de ouro, que nada mais é do que aquilo à procura do que ele sempre esteve e aquilo que, de fato, tem valor.

Em suma, nessa breve descrição do trabalho de mineração de metal precioso em uma mina aurífera, verifica-se ter havido a mineração de parcela do solo e ter sido descoberto o valioso e cobiçado ouro.

O *Big Data* segue a mesma lógica. Contudo, a parcela do solo a ser minerado é o próprio *Big Data*.

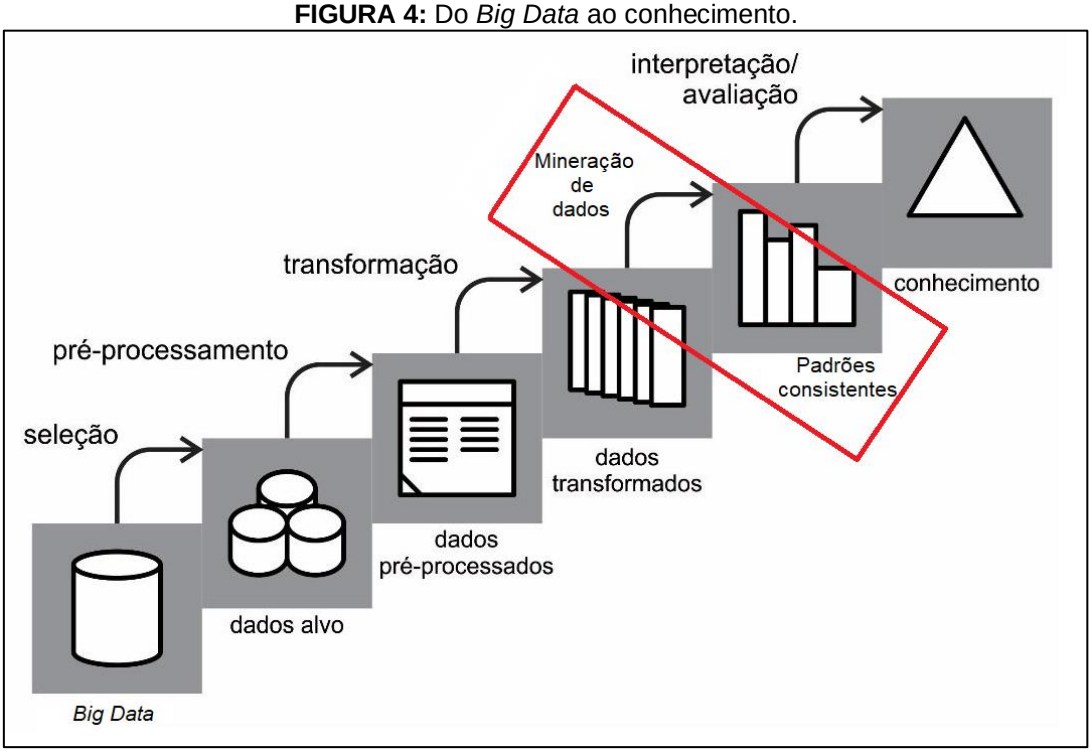
As técnicas de escavação de dados correspondem às técnicas computacionais de *Data Mining,* expressão em inglês cuja tradução para o português é “Mineração de Dados”.

O ouro é equivalente ao conhecimento obtido a partir da análise computacional do *Big Data*, pois é o conhecimento que tem valor ao ser utilizado para a tomada de decisões em determinado contexto.

Entretanto, do ponto de vista da Ciência da Computação, a Mineração de Dados deve ser compreendida como a “descoberta de padrões consistentes” a partir da aplicação de diversas técnicas computacionais de pré-processamento, de extração e de exploração de dados (BOFF; FORTES; FREITAS, 2018, p. 191).

Desse modo, a Figura 4 demonstra como ocorre a descoberta do conhecimento produzido a partir do *Big Data*, com destaque para a etapa da Mineração de Dados.

**FIGURA 4:** Do *Big Data* ao conhecimento.




FONTE: Adaptado de CARVALHO; TSUNODA, 2018.

Diante do exposto, verifica-se que a Mineração de Dados[20] consiste na descoberta de padrões consistentes em *Big Data*, sendo que a análise e a interpretação desses padrões são destinadas à solução de problemas, de acordo com seus respectivos contextos, o que, em última análise, resulta na construção de conhecimento apto à tomada de decisões, gerando, com isso, valor.

## 3.3 COMPUTAÇÃO FORENSE: A CIÊNCIA DA COMPUTAÇÃO NO SISTEMA DE JUSTIÇA CRIMINAL

Antes de se falar sobre Computação Forense propriamente dita, é preciso entender o contexto jurídico no qual esse ramo das Ciências da Computação se desenvolve. No ordenamento jurídico brasileiro, tal desenvolvimento se dá no âmbito do Direito Processual Penal. Segundo Abade (2014, p. 1), o “Direito Processual Penal é o ramo do ordenamento jurídico

[20] É importante ressaltar que a Mineração de Dados não é algo exclusivo do *Big Data*, pois também é possível minerar dados a partir de pequenas amostras. Contudo, não é possível imaginar *Big Data* sem ferramentas de Mineração de Dados.

pertencente ao Direito Público que reúne o conjunto de normas jurídicas regentes da investigação e julgamento dos fatos preestabelecidos pela lei penal como delitos.”

De acordo com Marques (2023, p. 20), o Direito Processual Penal “é o conjunto de princípios e normas que regulam a aplicação jurisdicional do Direito Penal, bem como as atividades persecutórias da Polícia Judiciária, e a estruturação dos órgãos da função jurisdicional e respectivos auxiliares”. Portanto, do ponto de vista estritamente jurídico, o processo é a instrumentalização juridicamente instituída por meio da qual o Estado exerce o poder jurisdicional (AVENA, 2023, p. 1).

Nucci (2023, p. 32) afirma que o Processo Penal “é o corpo de normas jurídicas cuja finalidade é regular a persecução penal do Estado, através de seus órgãos constituídos, para que se possa aplicar a norma penal, realizando-se a pretensão punitiva no caso concreto”. No entendimento de Bonfim (2019, p. 54), o Processo Penal constitui-se a partir de dois traços distintivos. O primeiro destes é a característica de “instrumento que determina como será exercido o poder do Estado de averiguar a verdade e impor uma sanção”. Por sua vez, o segundo aspecto diz respeito a:

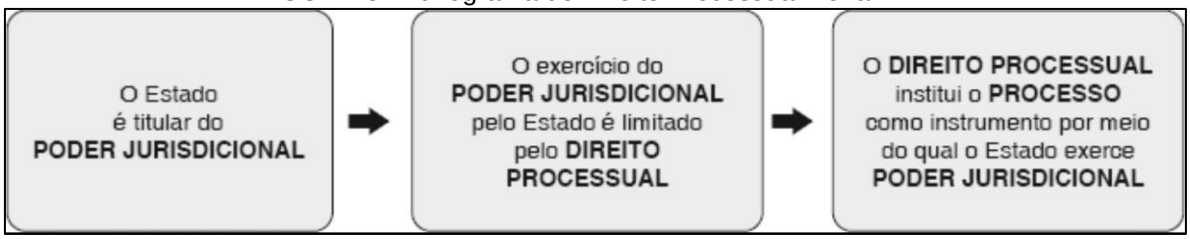
> “Uma garantia para o réu — e para a sociedade em geral — de que apenas haverá punição, caso, após concedida oportunidade plena de defesa, reste demonstrada a sua culpa. É possível ver o processo, portanto, também como um instrumento de proteção ao réu, que só poderá ter restrita sua liberdade, caso haja fundados motivos para tanto” (BONFIM, 2019, p. 54).

Desse modo, pode-se dizer que o Processo Penal diz respeito ao poder-dever de punir do Estado (*jus puniendi*) diante da prática de infrações penais, segundo normas e princípios jurídicos pré-estabelecidos, razão pela qual Avena (2023, p. 1) discorre que:

> “[...] Se uma pessoa realizar determinada conduta descrita em um tipo penal incriminador, a consequência desta prática será o surgimento para o Estado do poder-dever de aplicar-lhe a sanção correspondente. Essa aplicação não poderá ocorrer à revelia dos direitos e garantias fundamentais do indivíduo, sendo necessária a existência de um instrumento que, voltado à busca da verdade real, possibilite ao imputado contrapor-se à pretensão estatal” (AVENA, 2023, p. 1).

Nesse sentido, o fluxograma mostrado na Figura 5 sintetiza, de forma didática, o exercício do poder jurisdicional do Estado, por meio da instrumentalização processual como um todo, o que logicamente influencia a subárea jurídica do Direito Processual Penal, observadas as nuances que foram descritas anteriormente.

**FIGURA 5:** Fluxograma do Direito Processual Penal.




FONTE: AVENA, 2023, p. 1.

Uma vez examinados os caracteres gerais do Direito Processual Penal brasileiro, faz-se necessário discorrer, agora, sobre o que ocorre entre a prática delitiva e a conclusão do exercício do poder jurisdicional por parte do Estado.

É justamente nesse hiato que se desenvolve a atividade estatal da investigação criminal, cujo desiderato último é o de reconstituir a verdade dos fatos do caso concreto sob análise, para que o Estado-Juiz possa apreciá-los e, com isso, aplicar-lhes as normas jurídicas correspondentes ao caso *sub judice*.

Portanto, insta mencionar que a origem moderna da investigação criminal remonta à década de 1.750, na Inglaterra, tendo em vista o crescimento urbano decorrente da Revolução Industrial, o que acabou por aumentar a criminalidade e ensejou a necessidade de se apurarem delitos, como furtos e roubos, os quais começaram a ser cada vez mais comuns nesses agrupamentos de pessoas (MENDRONI, 2013, p. 5).

Gloeckner e Lopes Júnior (2014, p. 90-91) definem a investigação como sendo “o conjunto de atividades realizadas concatenadamente por órgãos do Estado, [...] que pretende averiguar a autoria e as circunstâncias de um fato aparentemente delitivo, com o fim de justificar o exercício da ação penal ou o arquivamento (não processo)”.

Segundo Pereira (2022, p. 109), a investigação criminal consiste na “pesquisa ou [na] indagação que se faz, interrogando, buscando e examinando. É a ação dirigida a vestígios, ao que se deixou inscrito no rasto, na pegada”.

Nesse sentido, Lopes Júnior (2014, p. 549) afirma que “o Processo Penal é um instrumento de retrospecção, de reconstrução aproximada de um determinado fato histórico. [...] Nesse contexto, as provas são os meios através dos quais se fará essa reconstrução do fato passado (crime)”.

Logo, a investigação criminal pauta-se no senso permanente de descoberta, que é típico do Processo Penal, pois a investigação não se limita à fase de inquérito, isto é, não se restringe à fase anterior à ação penal, mas se vincula ao processo como um todo.

Desse modo, a investigação é indispensável à instrução probatória e ao convencimento do juízo, até mesmo na fase recursal (PEREIRA, 2022, p. 192).

A indispensabilidade da investigação criminal explica-se, porque ela “não é apenas uma questão de meios técnicos, é também uma questão de controles intersubjetivos do conhecimento, o que, em última análise, é uma questão de poder, de exercício do poder punitivo pela investigação durante o Processo Penal” (PEREIRA, 2022, p. 535).

Portanto, considerando-se que a investigação criminal é, também, um modo de exercício do poder estatal e considerando-se, ainda, que o resultado da investigação é destinado, no âmbito penal, à reconstituição dos fatos delitivos, torna-se imprescindível analisar como se utiliza o resultado investigatório em um processo criminal.

Afinal, conforme já mencionado anteriormente, o Processo Penal é, também, um instrumento de garantia fundamental para o indivíduo que a ele é submetido: o réu.

Desse modo, verifica-se ganhar importância a Teoria da Prova no processo, haja vista que, para além de reconstituir fatos delitivos, a investigação criminal busca, processualmente, levantar elementos de prova que sejam juridicamente aptos a serem utilizados em um processo criminal.

Conclui-se, com isso, que a investigação se destina a provar algo para o Estado-juiz.

A prova tem, como objeto, os fatos da vida real que repercutem no Processo Penal e que, em razão disso, devem ser de conhecimento do órgão julgador, para o desfecho do caso criminal (AVENA, 2023, p. 437).

Acerca do tema, Oliveira (2015, p. 327) sustenta que:

> "[A] prova judiciária tem um objetivo claramente definido: a reconstrução dos fatos investigados no processo, buscando a maior coincidência possível com a realidade histórica, isto é, com a verdade dos fatos, tal como efetivamente ocorridos no espaço e no tempo."

Renato Brasileiro de Lima (2014, p. 553) afirma, por sua vez, que:

> "A palavra prova pode ser vista como conclusão que se extrai da análise dos elementos de prova constantes do processo: é o resultado da prova (*proof*, em inglês), obtido não apenas pelo somatório dos elementos de prova, como também por meio de uma atividade intelectual do magistrado, que permite estabelecer se a afirmação ou negação do fato é verdadeira, ou não".

Portanto, a prova decorre da inferência que se faz sobre os elementos de prova constantes do processo, segundo uma determinada hipótese e com base no conhecimento de mundo pretérito — *background* — de quem faz essa análise (DALLAGNOL, 2015, p. 24-25). A hipótese, dentro de um processo criminal, diz respeito à ocorrência, ou não, de um crime e ao envolvimento, ou não, do réu nesse crime.

Desse modo, pode-se dizer que a prova é a o resultado da intelecção feita a partir dos elementos de prova, isto é, é o resultado da intelecção realizada a partir das evidências. O elemento de prova (ou evidência) "nada mais é do que uma hipótese em que se confia, a ponto de colocá-la como base para uma inferência a outra hipótese" (DALLAGNOL, 2015, p. 23).

Assim sendo, a inferência que se faz a partir dos elementos de prova constitui os argumentos que consubstanciam a própria prova, razão pela qual esse método de análise do caso penal é denominado de "Inferência para a Melhor Explicação" (IME). Isto é: "uma dada hipótese é (provavelmente) verdadeira, pelo fato de que ela é aquela que melhor explica a evidência", ou seja, o conjunto de elementos de prova (DALLAGNOL, 2015, p. 77).

Com isso, verifica-se a importância do caminho percorrido pela investigação, a qual levanta as evidências que servem de substrato para a prova inferida dentro de um processo criminal.

Desse modo, é indubitável que, para um Processo Penal que respeite direitos e garantias fundamentais, a produção dos elementos de prova deve seguir um caminho auditável e acessível a todos os atores do processo.

Tamanha é a importância disso, que a própria legislação processual reconhece que determinados fatos dizem respeito a questões complexas e que, por isso, precisam ser estudados com o auxílio de um especialista. É nesse contexto que surgem as figuras do perito e da cadeia de custódia.

A perícia, no âmbito penal brasileiro, está regulamentada pelos artigos 158 a 184 do Código de Processo Penal (CPP), estando topograficamente inserida no Título VII do referido diploma legal, vez que diz respeito a um dos modos de se produzirem provas no Processo Penal (BRASIL, 1941).

Por sua vez, na área computacional, a perícia é denominada de "Computação Forense" e tem, como sinônimos, as expressões: perícia digital, forense computacional, forense digital, *computer forensics, digital forensics*, entre outros (VECCHIA, 2020, p. 95).

No contexto dos dispositivos móveis, as características da Computação Forense e da cadeia de custódia também podem ser aplicadas, haja vista que esses equipamentos podem ser considerados pequenos computadores de bolso, uma vez que são capazes de executar, com mobilidade, todas as tarefas de um computador comum (UFRGS, 2023a).

Nesse sentido, o *National Institute of Standards and Technology* (*NIST*) dos EUA fornece a definição para dispositivo móvel:

> "Um dispositivo móvel (...) é um dispositivo de Computação portátil que: (i) possui um formato pequeno, de modo que pode ser facilmente transportado por um único indivíduo; (ii) foi projetado para operar sem conexão física (por exemplo, transmitir ou receber informações sem fio); (iii) possui armazenamento de dados local, não removível ou removível; e (iv) utiliza uma fonte de energia independente. Os dispositivos móveis também podem incluir capacidades de comunicação de voz, sensores integrados que permitem aos dispositivos capturar informações e/ou recursos integrados para sincronizar dados locais com locais remotos. Os exemplos incluem smartphones, tablets e leitores eletrônicos" (NIST, 2015, p. 1).[21]

[21] No original, em inglês: "*A mobile device, for the purpose of this document is a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers*" (NIST, 2015, p. 1).

Já a *State Library of Kansas* (2023, p. 1) considera dispositivo móvel todo dispositivo eletrônico de Computação portátil, podendo ser de vários tamanhos e modelos, bem como podendo utilizar diversos tipos de sistemas operacionais e aplicações.

Por sua vez, o *Cambridge Dictionary* considera dispositivo móvel todo e qualquer equipamento eletrônico que seja dotado de capacidade computacional e que possa ser utilizado em diversos lugares (*CAMBRIDGE DICTIONARY*, 2023, p. 1).

Com isso, pode-se afirmar que *tablets*, *notebooks* e *smartphones* são exemplos de dispositivos móveis.

Acerca das características dos dispositivos móveis, a Universidade Federal do Rio Grande do Sul (UFRGS) (2023a, p. 1) discorre que:

> "Os dispositivos móveis apresentam características físicas, como: um tipo de computador portátil, tamanho de tela pequeno, fina espessura e manuseio dos recursos através do toque na tela (*touchscreen*). Além disso, mostram-se com propriedades na sua funcionalidade quanto a mobilidade e flexibilidade nos processos de comunicação. Tais características são colocadas em prática através da conectividade, que é uma realidade presente e disponível para os dispositivos móveis. Assim, tornam-se competentes para ampliar as possibilidades de comunicação entre os envolvidos."

Portanto, o que condensa as características de um dispositivo móvel é justamente congregar funções computacionais com mobilidade, tanto que todos eles utilizam sistemas operacionais e aplicações específicas para o desempenho de determinadas tarefas, bem como dispõem de acesso à Internet e utilizam uma fonte de energia independente, como baterias (UFRGS, 2023a).

Desse modo, conclui-se que a Computação Forense é aplicável aos dispositivos móveis, sendo que o seu objetivo principal é:

> "Determinar a dinâmica, a materialidade e a autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnicos-científicos, conferindo-lhes validade probatória em juízo" (ELEUTÉRIO; MACHADO, 2010, p. 16-17).

Note-se que tal conceituação guarda profunda consonância com o que foi dito anteriormente sobre o fato de as investigações objetivarem o levantamento de evidências destinadas a provarem algo.

Ocorre que, independentemente, do modo pelo qual a prova seja produzida, o ordenamento jurídico em vigor determina o respeito à cadeia de custódia, a qual consiste na preservação e na documentação de cada um dos passos que o elemento de prova percorre, desde a sua constatação até o seu uso dentro de um processo criminal.

Com isso, permite-se que todos os envolvidos no processo criminal tenham conhecimento do caminho percorrido pelo elemento de prova, podendo averiguar eventual inconsistência procedimental ou, até mesmo, algo que possa tornar o elemento de prova ilícito e, portanto, imprestável para fins processuais.[22]

Segundo Avena (2023, p. 509), a cadeia de custódia tem a finalidade de preservar "todas as etapas da cadeia probatória, de modo a possibilitar, em cada uma delas, o rastreamento das [etapas] que lhe antecederam e a verificação da legalidade e da licitude dos procedimentos adotados".

O desrespeito ou violação à cadeia de custódia é tecnicamente denominado de "quebra da cadeia de custódia" e é considerado um vício processual capaz de invalidar um processo criminal (AVENA, 2023, p. 509).

Por sua vez, o artigo 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" (BRASIL, 1941, p. 1).

O artigo 158-B do CPP enumera cada uma das dez etapas da cadeia de custódia, conforme a seguir, em blocos, elencadas (BRASIL, 1941, p. 1). A seguir, o primeiro bloco no qual são tratadas as etapas de 1 (um) a 6 (seis):

> **Código de Processo Penal Brasileiro (DL. n. 3.689/1941)**
> "**Art. 158-B.** [...]:
> I - reconhecimento: ato de distinguir um elemento como de potencial interesse para a produção da prova pericial;
> II - isolamento: ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime;
> III - fixação: descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de

[22] Não se descarta, todavia, o entendimento jurídico acerca da possibilidade de se utilizarem provas ilícitas em benefício do réu, o que guarda relação com as teorias de garantismo penal (REIS, 2013, p. 4-5).

> exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento;
> IV - coleta: ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza;
> V - acondicionamento: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento;
> VI - transporte: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;
> [...].”

Note-se que os seis primeiros passos da cadeia de custódia dizem respeito ao processo de descoberta do delito. Nesse estágio, o que se procura fazer é preservar as evidências, evitando toda e qualquer interferência que possa, por algum motivo, torná-las juridicamente inválidas ou até mesmo inúteis para a reconstrução da verdade dos fatos.

Seguindo, os incisos (incs.) VII e VIII do artigo 158-B do CPP (BRASIL, 1941, p. 1), referente a outras duas etapas da cadeia de custódia, dizem o seguinte:

> **Código de Processo Penal Brasileiro (DL. n. 3.689/1941)**
> “**Art. 158-B.** [...]:
> [...].;
> VII - recebimento: ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu;
> VIII - processamento: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito;
> [...].”

Nessa fase, a cadeia de custódia já permite a internalização, no caso penal, das evidências, submetendo-as à apreciação dos investigadores, dos peritos e dos demais atores da persecução penal.

Por fim, os incisos IX e X do art. 158-B do CPP (BRASIL, 1941, p. 1) constituem as últimas etapas da cadeia de custódia e demonstram a preocupação do Direito em permitir a auditagem dos elementos de prova, até

que estes se tornem dispensáveis pelo Poder Judiciário. A intenção disso é garantir o pleno respeito aos direitos e às garantias fundamentais daquele que esteja sob o crivo do Estado-juiz. Veja-se:

> **Código de Processo Penal Brasileiro (DL. n. 3.689/1941)**
> "**Art. 158-B.** [...]:
> [...].;
> IX - armazenamento: procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado, com vinculação ao número do laudo correspondente;
> X - descarte: procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial." (BRASIL, 1941, p. 1).

Isto posto, passa-se a discorrer, agora, sobre a perícia por meio da aplicação de métodos e técnicas de Computação Forense e sobre como ela se relaciona com os elementos da cadeia de custódia.

A perícia digital pode ser compreendida como exame técnico efetuado por um perito especialista que analisa dados armazenados em mídias no formato digital e, em determinados casos, características próprias do *hardware* sob estudo (VECCHIA, 2020, p. 95).

Vecchia (2020, p. 95) afirma que "a perícia digital (ou Computação Forense) utiliza um conjunto de técnicas e procedimentos com embasamento científico para coletar, analisar e apresentar as evidências encontradas."

Além disso, referido autor destaca que o objetivo da Computação Forense é "buscar informações relativas a eventos passados em uma investigação" e, a partir disso, "reconstruir as ações executadas nos diversos equipamentos e mídias de armazenamento" que estejam sendo averiguados (VECCHIA, 2020, p. 95).

Acerca do tema, é importante mencionar o potencial uso dos equipamentos computacionais como (i) ferramenta de apoio para a prática de delitos; ou, então, como (ii) meio para o cometimento de crimes (ELEUTÉRIO; MACHADO, 2010, p. 17).

A compreensão dessa dualidade da prática delitiva perpassa a conceituação de crime cibernético, que nada mais é do que delito cometido pelo aproveitamento das facilidades proporcionadas pelas tecnologias computacionais e pelo acesso à informação, com destaque para a Internet

(VECCHIA, 2020, p. 52).

No primeiro caso, o computador é só uma ferramenta auxiliar à prática do crime, o qual pode ser cometido sem equipamentos computacionais. Trata-se, pois, de crime classificado como “crime cibernético impróprio ou aberto”, a exemplo do estelionato e da ameaça (VECCHIA, 2020, p. 53).

No segundo caso, o computador é elemento central do delito, a exemplo do que ocorre com o crime de invasão de dispositivo informático (ELEUTÉRIO; MACHADO, 2010, p. 17-18). Nessa hipótese, fala-se de “crime cibernético próprio” ou de “crime exclusivamente cibernético”, pois a ausência do elemento computacional inviabiliza a prática delitiva (VECCHIA, 2020, p. 53).

Por sua vez, no entendimento de Eleutério e Machado (2010, p. 20-21),[23] os exames de Computação Forense podem ser classificados em: (i) exames e procedimentos em locais de crime de informática; (ii) exames em dispositivos de armazenamento computacional; (iii) exames em aparelhos de telefone celular; (iv) exames em *sites* da Internet e (v) exames em mensagens eletrônicas.

Os exames e procedimentos em locais de crime de informática dizem respeito a “mapeamento, identificação e correta preservação dos equipamentos computacionais, a fim de permitir melhor seleção do material a ser apreendido, para serem examinados posteriormente em laboratório” (ELEUTÉRIO; MACHADO, 2010, p. 20).

Os exames em dispositivos de armazenamento computacional consistem na análise de arquivos, de sistemas e de programas instalados em dispositivos de armazenamento digital de dados. Esse tipo de exame utiliza técnicas de recuperação de arquivos apagados, de quebra de senhas e de virtualização e é dividido em quatro fases: preservação, extração, análise e formalização (ELEUTÉRIO; MACHADO, 2010, p. 20).

Os exames em aparelhos de telefone celular consistem na extração dos dados neles contidos, com o intuito de formalizar as informações armazenadas

---

[23] A classificação de exames de Computação Forense citada no parágrafo acima baseia-se na obra de Eleutério & Machado (2010). Todavia, cumpre ressaltar que a classificação de exames de Computação Forense varia de autor para autor. Decidiu-se utilizar os ensinamentos de Eleutério e Machado (2010) em razão de sua didática e pelo fato de este trabalho acadêmico ter-se desenvolvido na área do Direito e não, na da Computação, o que facilita a compreensão por parte das pessoas que não são familiarizadas com esta área do conhecimento.

em sua memória, tais como a lista de contatos, o histórico de ligações, o elenco de imagens *etc*. (ELEUTÉRIO; MACHADO, 2010, p. 20).

Os exames em *sites* da Internet visam a extrair cópias e a verificar o conteúdo de determinados *sites*, bem como a averiguar os seus responsáveis (ELEUTÉRIO; MACHADO, 2010, p. 20). Os exames em mensagens eletrônicas analisam as suas respectivas propriedades, tais como os interlocutores, o local de origem, a data, a hora *etc*. (ELEUTÉRIO; MACHADO, 2010, p. 20).

No que diz respeito à cadeia de custódia aplicada às provas relacionadas à área da Computação Forense, Vecchia (2020, p. 96 e 100-101) faz significativos apontamentos para a sua preservação, ao enumerar as seguintes seis condições que devem ser garantidas durante a coleta, a análise e a preservação das provas digitais por meio da Computação Forense: (i) garantia de integridade, ao impedir que nenhuma evidência possa ser alterada ou destruída; (ii) respeito total às normas jurídicas e às formalidades relacionadas à cadeia de custódia; (iii) adoção das condutas minimamente necessárias para o exame pericial, em especial, quando o objeto analisado ainda esteja em funcionamento, pois assim são evitados eventuais incidentes; (iv) adoção de conduta ética, para que informações irrelevantes para o caso sob investigação não sejam divulgadas; (v) adoção de procedimentos que possam ser futuramente auditáveis, e (vi) documentação de todo o processo pericial, para que seja possível auditá-lo futuramente.

Com base no que se discorreu até aqui, é possível verificar convergência com quatro princípios que também norteiam o trabalho com evidências digitais, a saber:

> “a) ações realizadas por investigadores/peritos não devem alterar dados contidos em dispositivos digitais ou em mídias de armazenamento, que podem posteriormente ser solicitados perante o Juiz;
> b) indivíduos que acessam dados originais devem ser competentes para fazê-lo e devem ter a capacidade de explicar suas ações, visto que tais procedimentos são questionáveis pelas partes ou em juízo;
> c) uma cadeia de custódia deve ser estabelecida, bem como o registro de todos os procedimentos realizados deve ser mantido, de maneira que se possa garantir a replicação dos resultados por um terceiro independente, sendo que toda a documentação deve ser criada e preservada, documentando-se cada passo investigativo/pericial;
> d) a pessoa encarregada da investigação tem a responsabilidade geral de assegurar os procedimentos já mencionados e de assegurar, ainda, se os mesmos serão ou foram seguidos de conformidade com os métodos científicos e as leis vigentes (DECARLI, 2015, p. 9).”

Assim sendo, verifica-se que a lógica investigatória e processual que circunda a Computação Forense é muito similar àquela que trata de delitos que não envolvem elementos computacionais. Isso, porque, como visto ao longo deste trabalho, a função inerente ao Direito Processual Penal é reconstruir fatos — em tese — delitivos para a apreciação pelo Estado-juiz, resultando em absolvições ou em condenações correspondentes às infrações penais cometidas, e sempre respeitando os direitos e as garantias fundamentais.

## 3.4 ALGUMAS CONSIDERAÇÕES

O *Big Data* é o novo paradigma da Ciência da Computação e o fundamento contemporâneo da Sociedade Informacional. A produção massiva e contínua de dados por dispositivos móveis consubstancia a Computação pervasiva e a vigilância constante. Os rastros digitais são capazes de definir o que é cada ser humano. Por sua vez, o avanço computacional aliado ao Panspectron torna possível a modelagem comportamental das pessoas.

Longe de ser uma história de ficção científica, o *Big Data* oferece a oportunidade de tratamento de dados para a obtenção de conhecimento antes inalcançável. E, considerando que o aperfeiçoamento dos equipamentos e das técnicas computacionais tem sido constante ao longo dos últimos anos, a dependência digital também é indubitável. Portanto, não há como negar a importância do *Big Data*, também, no âmbito do Sistema de Justiça Criminal, seja para reconstruir fatos na persecução penal, seja para prever delitos na área da Segurança Pública (Preditiva).

O desenvolvimento tecnológico permitiu o cometimento de novas modalidades de delitos. Nesse contexto, os crimes cibernéticos, sejam eles próprios ou impróprios, demandam um ferramental apto a solucioná-los, haja vista que as técnicas de Computação Forense tradicionais já não são suficientes para tratar tais delitos.

Por fim, em que pesem as inovações tecnológicas, a essência do Processo Penal e da Teoria da Prova permanece. O respeito à cadeia de custódia e a proibição de provas ilícitas em detrimento do réu também

permanecem. O que mudou foi a compreensão dos novos meios para o cometimento de um crime. Por outro lado, todo o resto permanece o mesmo. Resta saber se o ordenamento jurídico atual possui mecanismos capazes de comportar as inovações trazidas pelo *Big Data*, notadamente no âmbito do Sistema de Justiça Criminal, tanto nas áreas de Segurança Pública, quanto na própria persecução penal.

# 4 REFLEXÕES JURÍDICAS ACERCA DA UTILIZAÇÃO DO *BIG DATA* PELO SISTEMA DE JUSTIÇA CRIMINAL BRASILEIRO

O escopo deste capítulo é avaliar a viabilidade jurídica do uso de um ferramental forense baseado em *Big Data*, de acordo com o atual ordenamento jurídico brasileiro. Daí, intitular-se o capítulo “Reflexões jurídicas acerca da utilização do *Big Data* pelo Sistema de Justiça Criminal brasileiro”.

Inicialmente, a fim de que seja explicado como seria possível formar-se um *Big Data* para fins penais, são descritos os resultados das pesquisas científicas desenvolvidas entre o Instituto de Criminalística da Polícia Científica do Paraná e a Pontifícia Universidade Católica do Paraná, no âmbito da Computação Forense.

Após essa descrição, discorre-se sobre o direito fundamental à proteção de dados pessoais e se discorre, ainda, sobre em que medida esse direito relaciona-se com o tratamento de dados pelo Sistema de Justiça Criminal. Também são feitos breves comentários acerca das propostas legislativas em tramitação na Câmara dos Deputados que visem a regulamentar o tema.

Por fim, procede-se a uma análise jurídica acerca da viabilidade, ou não, do uso de *Big Data* para fins penais, distinguindo-se o seu uso na área de Segurança Pública daquele adotado no âmbito da persecução penal.

## 4.1 OS PROJETOS DE PESQUISA “SICRET” E “SICRET II” E A POSSIBILIDADE DE CRIAÇÃO DE UM *BIG DATA* PARA FINS PENAIS

O projeto de pesquisa denominado “SiCReT”, realizado no ano de 2015, consiste em uma parceria acadêmica de fins científicos, no âmbito da Ciência da Computação, entre o Instituto de Criminalística da Polícia Científica do Paraná e a PUCPR, ambos situados na capital paranaense, Curitiba.

O projeto foi batizado com o acrônimo resultante das letras iniciais das

palavras que formam o nome da ferramenta computacional concebida especificamente para tal projeto, qual seja esse acrônimo, SiCReT, palavra formada a partir dos segmentos, aqui grifados, da expressão “Sistema de Cruzamento de Registros Telefônicos”.

Além disso, a fonética de “SiCReT” — com a sílaba tônica em “si” — constitui uma paronomásia, ou seja, um trocadilho, vez que corresponde à mesma fonética da palavra inglesa “*secret*”, cuja tradução livre é “segredo”.

Muito embora referido jogo linguístico pareça, em um primeiro momento, trivial e, até mesmo, algo de somenos importância, ele confere um significado que sintetiza todo o trabalho científico desenvolvido no projeto de pesquisa SiCReT. Isso, porque a ferramenta computacional que aí foi criada permitiu a descoberta de um conhecimento que, até então, encontrava-se “em segredo”.

Em outras palavras, o projeto SiCReT foi capaz de, a partir de uma ferramenta de Computação Forense de cruzamento de registros telefônicos, permitir o acesso a um conhecimento que, até então, permanecia desconhecido dos próprios órgãos de investigação criminal do Estado do Paraná.

Em síntese, o objetivo do SiCReT foi a criação de uma ferramenta computacional capaz de efetuar o cruzamento de registros telefônicos, com base em laudos de perícia criminal de dispositivos móveis do Instituto de Criminalística do Paraná (DECARLI, 2015, p. 19).

Tal ferramenta foi criada, portanto, para verificar se era verdadeira a hipótese de que é “possível recuperar os registros telefônicos e representar o cruzamento de dados existente entre os laudos periciais de dispositivos móveis, utilizando técnicas de recuperação de informações” (DECARLI, 2015, p. 19).

Nas palavras de Decarli (2015, p. 53):

> *“*O Sistema de Cruzamento de Registros Telefônicos (SiCReT) surgiu da necessidade de as Seções de Informática Forense utilizarem um procedimento computacional capaz de realizar o cruzamento de informações contidas nos laudos periciais de dispositivos móveis*.”*

Ainda segundo Decarli (2015, p. 54):

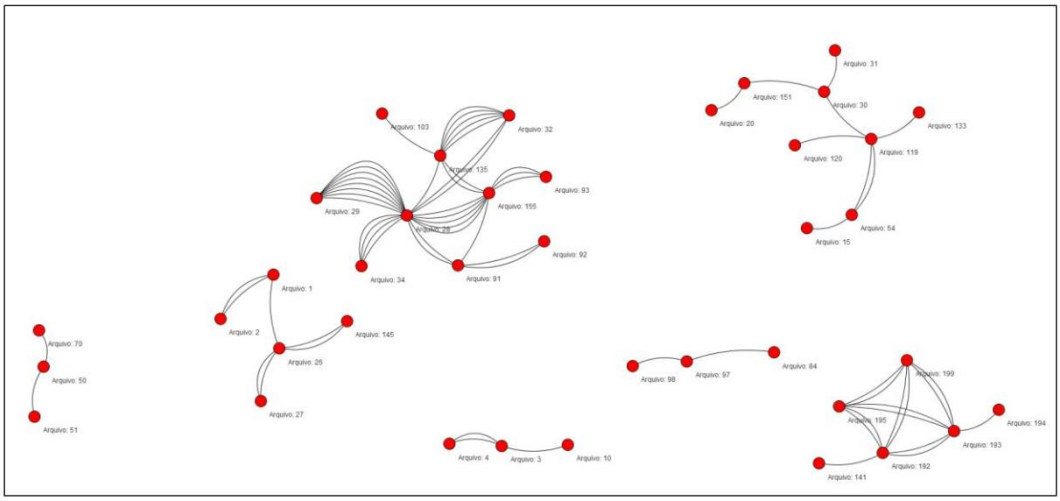
> “[O] SiCReT pode ser definido como uma ferramenta computacional capaz de realizar o processo de recuperação, detecção e visualização de cruzamentos existentes entre termos de interesse de um determinado conjunto de laudos periciais de dispositivos móveis.”

A ferramenta SiCReT foi aplicada em uma base de dados formada por duzentos laudos de perícia criminal de dispositivos móveis que integravam o arquivo do Instituto de Criminalística do Paraná, cujo acesso foi possibilitado por meio da citada parceria acadêmica e científica firmada com a PUCPR (DECARLI, 2015, p. 64).

Os laudos estudados têm origem em perícias criminais que tanto foram baseadas em Computação Forense, quanto foram realizadas em investigações distintas, isto é, sem qualquer tipo de vínculo entre si. Contudo, com a aplicação da ferramenta SiCReT, foi possível confirmar — como verdadeira — a hipótese de que é “possível recuperar os registros telefônicos e representar o cruzamento de dados existente entre os laudos periciais de dispositivos móveis, utilizando técnicas de recuperação de informações” (DECARLI, 2015, p. 19). Isso, porque foram constatadas intersecções entre laudos distintos, com uma precisão de 91% (DECARLI, 2015, p. 73).

Logo, referida ferramenta computacional foi capaz de descobrir relações entre diferentes investigações criminais. Tal descoberta pode ser representada por meio de grafos, ou seja, por meio de representações gráficas de conjunto de dados e de suas relações entre si. No caso específico, o conhecimento descoberto apontou para sete intersecções entre diferentes casos criminais, o que, até o uso do SiCReT, permanecia “em segredo”. Na Figura 6, é possível visualizar os grafos dessa descoberta:

**FIGURA 6**: Cruzamento de registros telefônicos entre arquivos.




FONTE: Adaptado de DECARLI, 2015, p. 68.

Acerca dos resultados obtidos com o SiCReT, afirma Decarli (2015, p. 74):

> "O cruzamento entre esses laudos é de grande interesse, por representar novas evidências forenses, fluxo de informações e cruzamentos de dados que, até então, estavam ocultos nas Sessões (*sic*) de Informática Forense. Esses resultados apresentados nunca puderam ser alcançados ou, mesmo, visualizados antes da existência do SiCReT; dessa forma, foi gerado um conhecimento que ninguém havia observado até então."

Por fim, Decarli (2015, p. 76) sugere a utilização do ferramental forense em questão para a criação de um *Big Data*[24] a nível nacional:

> "Aplicar o SiCReT em um *Big Data*: ou seja, em uma estrutura centralizada entre todos os laudos periciais do país, proporcionando o processamento em grandes volumes de dados a verificação de laudos em tempo real. Quando o SiCReT for aplicado utilizando essa tecnologia, no momento em que o laudo pericial estiver sendo elaborado pelos peritos, as informações armazenadas nas Seções de Informática Forense do País podem ser consideradas no cruzamento de dados."

Seguindo o interesse de aperfeiçoamento do ferramental criado com o SiCReT, surge uma nova versão desse projeto de pesquisa: o SiCReT II.[25] Nessa nova etapa da pesquisa — ainda em andamento —, busca-se o aperfeiçoamento do ferramental forense, para que, por meio deste, possam ser analisados não só registros telefônicos, mas, também, mensagens de texto extraídas de dispositivos móveis, como *smartphones*, haja vista a massiva utilização, para a prática de crimes, de aplicativos de mensagens de texto (ALVES *et al.*, 2023), a exemplo, entre outros, do *WhatsApp* e do *Telegram*.

No âmbito do SiCReT II, Alves *et al.* (2023) desenvolveram um estudo de Computação Forense semelhante ao que havia sido feito, anteriormente, no SiCReT. Todavia, o objeto de análise consistiu em mensagens de texto, e não,

---

[24] Foi essa sugestão que embasou o recorte de pesquisa desta dissertação, focada na utilização de ferramentas baseadas em *Big Data* para fins penais.

[25] Importa observar que o tratamento de dados pessoais dentro dos projetos SiCReT e II destina-se a fins exclusivamente acadêmicos, o que encontra permissivo legal no art. 4º, inc. II, alínea "b", da LGPD (2018). O SiCReT é do ano de 2015 e, portanto, anterior à LGPD de 2018. O SiCReT II é um projeto ainda em andamento.

registros telefônicos, como ocorrera na primeira fase do projeto. Para tanto, utilizaram-se ferramentas computacionais destinadas a detectar palavras-chave e expressões comumente ligadas a atividades criminosas (ALVES *et al.*, 2023).

Como o estudo teve foco nos delitos de aliciamento sexual de menores[26] e de tráfico de drogas,[27] foram concebidos modelos computacionais treinados, isto é, aptos a detectar termos ligados à prática de tais ilícitos, inclusive com mecanismos capazes de decifrar eventuais conversas codificadas, visto que, muitas vezes, criminosos usam códigos e gírias, para se comunicarem, no intuito de, assim, dificultarem os trabalhos de investigação (ALVES *et al.*, 2023).

As mensagens de texto utilizadas para detectar a possível prática do crime de aliciamento sexual de menores de idade são escritas em língua inglesa e foram obtidas a partir do projeto *Perverted Justice (PeeJ*), o qual consiste em uma "iniciativa *online* que expõe indivíduos ligados ao aliciamento e abuso sexual de crianças e adolescentes. Adultos voluntários fingem ser crianças ou adolescentes e mantêm conversas *online*, com o objetivo de identificar possíveis 'predadores'" (ALVES *et al.*, 2023, p. 2)[28] [tradução livre].

Por sua vez, as mensagens de texto utilizadas para os estudos ligados à prática do crime de tráfico de drogas são escritas em língua portuguesa; foram obtidas a partir da parceria acadêmica firmada com a Polícia Científica do Estado do Paraná e têm origem em conversas mantidas em aplicativos de mensagens de texto para *smartphones*, como o *WhatsApp* (ALVES *et al.*, 2023, p. 1).

O estudo de Alves *et al.* (2023) concluiu que a utilização de ferramentas de Computação Forense modeladas para a detecção de palavras isoladas e de expressões (conjunto de palavras) de interesse criminal em mensagens de texto pode ser de grande valia para os peritos criminais.

Todavia, ainda há limitações técnicas que precisam ser aperfeiçoadas, a fim de que os resultados obtidos possam ser mais precisos, haja vista que a utilização de linguagem cifrada e de gírias pelos criminosos dificulta esse tipo de

---

[26] O crime de aliciamento de crianças e de adolescentes está penalmente tipificado no art. 241-D do Estatuto da Criança e do Adolescente, mais conhecido como ECA (BRASIL, 1990).

[27] O crime de tráfico de drogas está penalmente tipificado no art. 33 da Lei n. 11.343/2006 (BRASIL, 2006), mais conhecida como Lei de Drogas.

[28] No original, em inglês, "*PeeJ is an online initiative that exposes individuals involved in grooming and sexually abusing children or teens. Adult volunteers pose as children/teens in online conversations to identify potential predators"* (ALVES *et al*., 2023, p. 2).

trabalho (ALVES *et al.*, 2023).

Desse modo, diante do que se apresentou, até aqui, no bojo deste trabalho, verificam-se duas situações práticas: (i) a atividade criminosa acompanha o desenvolvimento tecnológico, vez que o SiCReT analisou registros telefônicos e vez que o SiCReT II avançou para a análise de mensagens de texto extraídas de dispositivos móveis, em ambos os casos havendo sucesso no ferramental forense utilizado; e (ii) há uma tendência de expansão da Computação Forense para o estudo de dados cada vez mais volumosos, variados e com significativa velocidade de crescimento.

Além disso, é preciso ter em vista que:

> "[Na] área de Computação Forense, as atividades de exame pericial e elaboração de laudos exigem que nada seja desprezado, sendo essencial a consideração de toda e qualquer informação disponível, a fim de coletar o que for necessário para a elaboração de laudos de perícia criminal" (DECARLI, 2015, p. 53).

Portanto, considerando-se que a apreensão de dispositivos móveis tende a ser algo cada vez mais frequente em investigações criminais e considerando-se, ainda, que tais aparelhos produzem uma infinidade de dados variados,[29] verifica-se que as circunstâncias caminham para a possibilidade, cada vez mais concreta, de se utilizarem técnicas de Computação Forense baseadas em *Big Data*.

Desse modo, faz-se necessário discorrer sobre a (in)viabilidade jurídica do uso de *Big Data* pelo Sistema de Justiça Criminal brasileiro, com destaque para as áreas da persecução penal e da Segurança Pública.

Antes, porém, cumpre tratar do direito fundamental à proteção de dados pessoais no contexto brasileiro, vez que esse direito constitucionalmente assegurado serve de paradigma para toda a normatização jurídica do tema tratado nesta Dissertação.

---

[29] Exemplos: registros telefônicos, mensagens de texto, localização baseada em *GPS*, redes sociais, perfis de consumo *etc*.

## 4.2 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

O direito fundamental à proteção de dados pessoais está positivado no art. 5º, inc. LXXIX, da Constituição da República Federativa do Brasil de 1988 (BRASIL, 1988), por força do disposto na Emenda Constitucional (EC) n. 115, de 10 de fevereiro de 2022 (BRASIL, 2022).

Até o advento dessa Emenda à Constituição, prevalecia o entendimento de que tal direito à proteção de dados pessoais era implícito ao texto constitucional, sendo, até então, considerado, portanto, como um desdobramento do direito fundamental à privacidade — o qual, por sua vez, encontra-se positivado no mesmo art. 5º, porém nos incisos X e XII, a saber:

> **Constituição da República Federativa do Brasil de 1988 (CF/1988)**
> "**Art. 5º.** [...].
> [...];
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à 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;
> [...] (BRASIL, 1988, p. 1)."

Da leitura dos supracitados dispositivos constitucionais, depreendem-se, por conseguinte, as facetas nas quais se desdobra o bem jurídico da privacidade, garantindo-se, por meio de sua proteção, a incolumidade da intimidade, da vida privada, da imagem, da honra e do sigilo das comunicações.

Nesse contexto, a proteção de dados pessoais surge como resultado hermenêutico, isto é, emerge como resultante da interpretação da norma constitucional, cujo sentido projeta-se para além da literalidade do texto positivado. Isso, porque dados podem gerar informação e conhecimento capazes de atingir, de várias formas, a privacidade de determinada pessoa.

Antes mesmo de entrar em vigor a LGPD Cível (Lei n. 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais) (BRASIL, 2018b), o Supremo Tribunal Federal (STF) manifestou-se sobre o caráter implícito do

direito fundamental à proteção de dados pessoais,[30] entendido como desdobramento de outros direitos fundamentais já expressos no texto constitucional.

O caso julgado pela Suprema Corte brasileira dizia respeito ao compartilhamento, com o Poder Público, para fins estatísticos, de dados telefônicos relativos ao período pandêmico do covid-19, colhidos durante o ano tão somente de 2020.

Na ocasião, o STF fundamentou sua decisão no seguinte argumento:

> "Na medida em que relacionados à identificação — efetiva ou potencial — de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados" (SUPREMO TRIBUNAL FEDERAL, 2020, p. 1).

O entendimento jurisprudencial de que a proteção de dados pessoais é uma consequência da privacidade também encontra respaldo nos livros jurídicos sobre o tema, vez que a doutrina costuma referenciar o "direito de ser deixado só", como o início jurídico da proteção de dados (DONEDA, 2021, p. 30).

Tal início da tutela jurídica do direito fundamental à proteção de dados pessoais remontaria, assim, ao século XIX, nos EUA, quando Warren e Brandeis (1890) publicaram, na *Harvard Law Review*, artigo acadêmico de sua autoria, no qual debateram, do ponto de vista doutrinário, sobre o conceito do que hoje se entende, em sentido lato, por proteção de dados e o fizeram a partir da análise de como o desenvolvimento da imprensa e da fotografia vinha atingindo a privacidade das pessoas, devendo ser-lhes resguardado — a elas — o direito de serem deixadas sós (WARREN; BRANDEIS, 1890).

Em que pese o entendimento de que a proteção de dados seja um desdobramento da privacidade e da intimidade, parte da doutrina jurídica no Brasil já afirmava que a Constituição Federal de 1988 (BRASIL, 1988), antes

---

[30] Acerca dos estudos da jurisprudência do STF sobre a proteção de dados pessoais como direito fundamental implícito, recomenda-se a leitura da dissertação de Mestrado de Ribeiro (2023).

mesmo de qualquer normatização específica acerca da proteção de dados pessoais, tutelava somente as comunicações e não, os dados em si, em entendimento doutrinário atribuído, em especial, à letra do art. 5º, inc. XII, do texto constitucional (DONEDA, 2011, p. 105).

Nesse sentido, Souza e Acha (2022, p. 680) contextualizam a necessidade de haver normas específicas para a proteção de dados pessoais:

> "Percorreu-se um caminho longo desde a proteção à privacidade, em sua forma ampla, até atualmente poder-se falar em direito fundamental à proteção de dados. Contudo, com a atual sociedade da informação, em que tudo é computadorizado, transmitido e divulgado na rede mundial de computadores em tempo real, via Internet, fez-se necessário uma maior e mais eficaz proteção da privacidade dos usuários dos meios digitais. Sabe-se que, atualmente, praticamente tudo gira em torno da Internet, desde comunicações mais simples com pessoas do convívio diário e familiares, até transferências bancárias, negócios jurídicos, comércio e trabalho. Para essas integrações serem possíveis, os usuários disponibilizam seus dados diariamente em vários cadastros, ou até mesmo em aplicativos, *WhatsApp*, dentre outros. Nesse cenário, o direito à intimidade e à privacidade das pessoas ficou fortemente ameaçado, tendo muitas delas sofrido com divulgações e até mesmo com o uso ilícito de seus dados pessoais."

Antes da EC n. 115/2022, Sarlet (2020, p. 213) concluiu:

> "Venha — ou não — a ocorrer a inserção de um direito à proteção de dados pessoais no texto da CF, a condição de direito fundamental autônomo não depende, em si, de tal expediente, porquanto sobejamente demonstrado que se trata de um direito implicitamente positivado".

Por outro lado, Scheuermann (2023, p. 271) afirma que, somente com a EC n. 115/2022, a proteção de dados pessoais foi transformada num direito autônomo, retirando-se "das sombras da intimidade e privacidade".

Com essa nova perspectiva constitucional, a proteção de dados foi fortalecida, tornando-se uma "barreira normativa contra todas as tendências que, cada vez mais, pretendem transformar o indivíduo em mero objeto de obtenção de informação" (MENKE, 2019, p. 230).

Segundo Doneda (2021, p. 177), a transição da privacidade para a proteção de dados pessoais, como direito autônomo, é resultado da necessidade de proteção do indivíduo perante tecnologias baseadas na informação. Em síntese, a proteção de dados pressupõe privacidade, mas "modifica seus

elementos, aprofunda seus postulados e toca nos pontos centrais dos interesses em questão" (DONEDA, 2021, p. 178).

Jalil e Burlamaqui (2022, p. 14) afirmam que:

> "(...) o reconhecimento da proteção de dados como direito fundamental, vem conferir, um moderno e contemporâneo sentido à proteção da pessoa humana e da dignidade, da autonomia e das esferas de liberdade que lhes são inerentes. Significa dar efetividade ao sujeito de direito que busca desenvolver livremente a sua personalidade, sem que suas informações sejam utilizadas de forma indevidas ou ilegítimas de forma a comprometer ou tolher o exercício de sua liberdade e de ter controle sobre seus próprios dados."

Na seara infraconstitucional, em 2018, foi promulgada a Lei n. 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais de natureza cível, ou LGPD Cível (BRASIL, 2018b), a qual somente entrou em vigor, de modo integral, em agosto de 2021. Desde então, esse conjunto normativo tem norteado o tratamento de dados no Brasil.

Entretanto, ainda não existe uma lei geral de proteção de dados de natureza penal, isto é, uma LGPD Penal[31]. Esse hiato normativo entre a proteção de dados pessoais e a seara penal será tratado, com a devida atenção, no próximo tópico desta dissertação.

O foco do presente tópico é discorrer sobre a natureza jurídica do direito fundamental à proteção de dados, em especial, sobre a sua aplicabilidade no meio social, para que, posteriormente, seja estudada a sua concretização no âmbito do Sistema de Justiça Criminal.

Como visto, o direito fundamental à proteção de dados pessoais era, inicialmente, entendido como mero desdobramento do direito fundamental à privacidade. Posteriormente, foi reconhecido como direito autônomo pela LGPD Cível. Mais recentemente, em 2022, a EC n. 115/2022 elevou-o ao patamar de direito fundamental expresso.

Os direitos fundamentais têm, como características, a historicidade, a universalidade, a limitabilidade, a concorrência, a irrenunciabilidade, a inalienabilidade, e a imprescritibilidade (LENZA, 2023, p. 1.122).

---

[31] Muito embora ainda não exista uma LGPD Penal, já existem dois projetos de lei em andamento, os quais serão tratados com maior profundidade mais a frente.

A historicidade dos direitos fundamentais decorre do fato de eles serem um “produto da fusão de várias fontes, desde tradições arraigadas nas diversas civilizações, até a conjugação dos pensamentos filosófico-jurídicos, das ideias surgidas com o cristianismo e com o direito natural” (MORAES, 2021, p. 1).

A universalidade significa que os direitos fundamentais são aplicados a todas as pessoas, as quais não podem a eles renunciar (irrenunciabilidade), mas, tão somente, não os exercer (LENZA, 2023, p. 1122).

Por sua vez, os direitos fundamentais também são concorrentes e cumulativos entre si, haja vista que podem ser aplicados, de modo simultâneo, em um mesmo caso concreto, por meio de técnicas de ponderação hermenêutica (LENZA, 2023, p. 1.122).

Já os caracteres de sua inalienabilidade e de sua imprescritibilidade (LENZA, 2023, p. 1122) decorrem justamente do senso de permanência dos direitos fundamentais, o que tem a ver com a sua historicidade, vez que não são submetidos aos aspectos negativos do decurso do tempo, bem como não possuem valor patrimonial.

Por sua vez, as garantias fundamentais não podem ser confundidas como direitos fundamentais, vez que “os direitos são bens e vantagens prescritos na norma constitucional, enquanto as garantias são os instrumentos através dos quais se assegura o exercício dos aludidos direitos (preventivamente) ou prontamente os repara, caso violados” (LENZA, 2023, p. 1.121).

Em síntese, direitos e garantias fundamentais são normas constitucionais, cuja eficácia pode ser classificada em (i) plena; (ii) contida; e (iii) limitada.

As normas constitucionais de eficácia plena (i) “têm aplicabilidade imediata e, portanto, independem de legislação posterior para sua plena execução” (TAVARES, 2023, p. 80).

Por sua vez, as normas constitucionais de eficácia contida (ii) “têm igualmente aplicabilidade imediata, irrestrita, comparando-se, nesse ponto, às normas de eficácia plena, mas delas se distanciando, por admitirem a redução de seu alcance (constitucional) pela atividade do legislador infraconstitucional” (TAVARES, 2023, p. 80).

Já as normas constitucionais de eficácia limitada (iii) “dependem de

regulamentação futura, na qual o legislador infraconstitucional vai dar eficácia à vontade do constituinte" (TAVARES, 2023, p. 80).

Diante disso, considerando-se o que, até aqui, foi mencionado, verifica-se que: a proteção de dados pessoais, no Brasil, tem natureza constitucional de direito fundamental; esse direito fundamental foi regulamento no âmbito cível com a LGPD de 2018, e, até o momento, inexiste uma LGPD de natureza penal.

Nesse contexto, é importante avaliar qual tipo de eficácia possui a norma constitucional do direito fundamental à proteção de dados pessoais. Isso, porque a conclusão que será obtida a partir dessa aferição demonstrará o quanto a ausência de uma LGPD Penal influencia ou, até mesmo, impede o tratamento de dados pessoais dentro do Sistema de Justiça Criminal brasileiro.

A proteção de dados pessoais deve ser entendida como uma norma constitucional de cunho individual, haja vista que, a depender da tecnologia utilizada, o tratamento de dados pode definir o perfil de um indivíduo de uma maneira extremamente precisa, o que pode, até mesmo, prejudicar o livre desenvolvimento da sua personalidade e a sua autodeterminação informativa, em todos os aspectos da sua vida.

Portanto, a partir desse raciocínio, seguindo a lógica de que os direitos individuais são uma maneira que o cidadão tem de se defender do abuso de poder político e econômico, conclui-se que o direito fundamental à proteção de dados tem natureza amplamente negativa,[32] uma vez que isso não é restrito às relações perante o Estado, mas também abrange as relações entre particulares, como fruto da eficácia tanto horizontal, quanto vertical dos direitos fundamentais.

Salienta-se que a eficácia horizontal dos direitos fundamentais consiste na aplicabilidade destes às relações privadas, mesmo que estas se realizem sem a participação do Estado. Ou seja, os direitos fundamentais fazem-se presentes nas relações jurídicas mantidas entre particulares situados em um mesmo plano horizontal (LENZA, 2023, p. 1.126).

Por sua vez, a eficácia vertical dos direitos fundamentais pode ser

---

[32] O caráter negativo e individual dos direitos fundamentais decorre da sua perspectiva histórica e diz respeito ao surgimento de normas de proteção do indivíduo perante o Estado, ou seja, normas que impunham à abstenção estatal diante das pessoas, razão pela qual essa característica é predominante nos direitos fundamentais de primeira dimensão (LENZA, 2023, p. 1.118) como, por exemplo, o direito de ir e vir.

entendida como a aplicabilidade dos direitos fundamentais às relações jurídicas estabelecidas entre indivíduos e o Estado (LENZA, 2023, p. 1.126). Nesse caso, utiliza-se o termo vertical, eis que o Estado estaria em um plano superior em relação ao indivíduo. Todavia, o termo “superior” não significa que o Estado paire acima do indivíduo, nem que seja melhor do que o indivíduo; significa, apenas, que o ente estatal goza de prerrogativas necessárias ao exercício de suas funções públicas destinadas ao bem comum.[33]

Portanto, verifica-se que o direito fundamental à proteção de dados pessoais: (i) tem natureza individual; (ii) consubstancia um mecanismo de defesa dos indivíduos tanto nas relações particulares-particulares, quanto naquelas particulares-Estado; e (iii) tem eficácia contida, podendo ser parcialmente limitado por meio de leis gerais de proteção de dados.

Ressalte-se que a EC n. 115/2022 trouxe as seguintes alterações:

> **EC 115/2002**
> “**Art. 1º.** O *caput* do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:
> ‘Art. 5º. [...]:
> [...];
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.’
> **Art. 2º.** O *caput* do art. 21 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXVI:
> ‘Art. 21. [...].
> [...].
> XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei (NR)’.
> **Art. 3º.** O *caput* do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX:
> ‘Art. 22. [...].
> [...];
> XXX - proteção e tratamento de dados pessoais” (BRASIL, 2022, p. 1).

A leitura sistemática dessas alterações constitucionais evidencia que a proteção de dados pessoais deve, necessariamente, ser regulamentada com base na legislação, o que demonstra sua natureza de norma constitucional de eficácia contida.

---

[33] Um exemplo para se compreender a verticalidade da relação Estado-indivíduo é o regime jurídico de Direito Administrativo, cujos princípios basilares são a supremacia do interesse público e a indisponibilidade do interesse público (DI PIETRO, 2023, p. 103).

Além disso, deve-se levar em consideração o caráter pervasivo da tecnologia no atual Panspectron, razão pela qual a exposição dos dados pessoais é uma constante imperativa no cotidiano das pessoas.

Argumentar a favor da natureza não contida dessa norma constitucional ocasionaria, aos menos, dois problemas incompatíveis com o Estado Democrático de Direito.

Primeiro, na hipótese de o direito fundamental à proteção de dados pessoais ser uma norma constitucional de eficácia limitada, a ausência de legislação regulamentadora impediria seu exercício, colocando os cidadãos em uma situação de plena insegurança jurídica face a todo e qualquer tratamento de dados, seja pelo Estado, seja por agentes privados.

Por outro lado, na hipótese de o direito fundamental à proteção de dados pessoais ser considerado uma norma constitucional de eficácia plena, não seria viável a criação de um arcabouço normativo infraconstitucional, para regular o tema; vez que a eficácia irradiante[34] desse tipo de direito demandaria o sopesamento de princípios em cada caso concreto, gerando insegurança diante da falta de uniformidade jurídica sobre o tema.

Portanto, a adoção da tese sobre a eficácia contida permite — e mais do que isso, exige — que a contenção do direito fundamental à proteção de dados só possa ocorrer por meio de lei em sentido estrito, na qual venham a ser criados mecanismos específicos para que cada cidadão não só tenha pleno conhecimento sobre o que é feito com seus dados, bem como disponha, ainda, de instrumentos jurídicos de tutela efetiva do seu direito à proteção de dados.

Com base nisso, o tópico seguinte tratará sobre a eficácia contida do direito fundamental à proteção de dados perante as normas jurídicas que circundam o Sistema de Justiça Criminal brasileiro, para, então, discorrer-se sobre a viabilidade jurídica de um *Big Data* para fins penais.

---

[34] O aspecto irradiante dos direitos fundamentais significa que sua eficácia transpassa todas as facetas do Estado e das relações privadas, exigindo a sua observância por todos os envolvidos em toda e qualquer relação jurídica (LENZA, 2023, p. 1.126).

## 4.3 A (IN)VIABILIDADE JURÍDICA DO USO DE *BIG DATA* PELO SISTEMA DE JUSTIÇA CRIMINAL BRASILEIRO

A vigilância é uma constante na Sociedade Informacional, justamente por transpassar todas as facetas da vida humana. O caráter pervasivo da tecnologia impregna-se no cotidiano de todos, quer o indivíduo queira isso ou não (GREENFIELD, 2006, p. 9-14).

Como visto, o direito fundamental à proteção de dados pessoais no Brasil é norma constitucional de eficácia contida, com aplicação imediata em todo o ordenamento jurídico, podendo, porém, ser parcialmente restringida pela legislação.

Desse modo, em circunstâncias específicas, as leis gerais de proteção de dados, sejam estas de natureza cível ou de natureza penal, materializam referido direito fundamental, esclarecendo sua amplitude e seus limites de aplicação; o que torna as relações jurídicas mais claras e transparentes e, portanto, mais seguras juridicamente.

Também, como visto anteriormente, só no ano de 2022, a Emenda Constitucional n. 115/2022 elevou a proteção de dados pessoais à categoria de direito fundamental (TEIXEIRA; GUERREIRO, 2022, p. 12), ao positivá-lo no art. 5º, inc. LXXIX, da Constituição Federal de 1988 (BRASIL, 1988).

Na seara infraconstitucional, somente com o Regulamento Geral de Proteção de Dados da União Europeia de 2016, a legislação brasileira passou, de modo mais específico, a tratar da proteção de dados pessoais (TEIXEIRA; GUERREIRO, 2022, p. 12), vez que, logo em seguida, no ano de 2018, foi editada, no Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), de natureza cível (BRASIL, 2018b).

O fim último da LGPD Cível é “a proteção do indivíduo, em sua autodeterminação informacional, em sua esfera privada, representada por informações que lhe dizem respeito como sujeito, em suas liberdades e no livre desenvolvimento de sua personalidade” (OLIVEIRA, 2022, p. 93).

Entretanto, muito embora tenham sido criadas normas jurídicas para proteger dados pessoais, esses mecanismos, em alguns casos, não são aplicados. Como mencionado, a LGPD em questão é de natureza cível, razão

pela qual ela não se aplica aos casos em que o tratamento de dados pessoais é realizado para fins exclusivos de Segurança Pública, de Defesa Nacional, de Segurança do Estado e de persecução penal; ou seja, a LGPD não se aplica às atividades de investigação e de repressão de infrações penais, conforme dispõe o seu art. 4º, inc. III (BRASIL, 2018b).

Tal contexto normativo causa preocupação, visto que é fundamental que:

> "Sob a ótica de se combater o terrorismo, tráfico de drogas, dentre outros crimes graves, o Estado não estabeleça uma vigilância constante de seus cidadãos, com a coleta massiva e irrestrita de dados pessoais e, somente na hipótese do cometimento de algum ilícito, haja a avaliação da real necessidade dos dados coletados" (TEIXEIRA; GUERREIRO, 2022, p. 15).

Acerca da coleta massiva e irrestrita de dados pessoais para fins penais, cita-se o caso do assassinato da vereadora do Rio de Janeiro (RJ) Marielle Franco e do motorista Anderson Gomes, ocorrido em 2018 (GONÇALVES *et al.*, 2018).

Durante as investigações, a pedido do Ministério Público, o Juízo da 4ª Vara Criminal da Comarca do Rio de Janeiro (RJ) decretou a quebra de sigilo dos dados de localização e de pesquisa das pessoas que transitavam no local, no momento do crime.

A empresa *Google Limited Liability Company (LLC)*, destinatária da ordem judicial, recorreu da decisão afirmando, em síntese, que a medida era desproporcional e que "o ordenamento jurídico brasileiro não admite quebras de sigilo e interceptações genéricas, sem a individualização das pessoas afetadas" (SUPERIOR TRIBUNAL DE JUSTIÇA, 2020, p. 1).

Em que pesem os argumentos da *Google*, o Superior Tribunal de Justiça (STJ), em 2020, julgou improcedente o recurso dessa empresa e a obrigou ao fornecimento dos dados em questão (SUPERIOR TRIBUNAL DE JUSTIÇA, 2020).[35]

Sem entrar nas circunstâncias fáticas e na repercussão do trágico

---

[35] Conforme afirmado pela própria assessoria de imprensa do STJ, o número dos autos não é divulgado, por se tratar de caso com segredo de justiça (SUPERIOR TRIBUNAL DE JUSTIÇA, 2020).

assassinato de Marielle Franco e de Anderson Gomes, fato é que a referida investigação demonstra que a ausência de regulamentação sobre o tratamento de dados para fins penais gera discussões jurídicas que poderiam ser evitadas, causando insegurança jurídica para todos os envolvidos no processo criminal.

Portanto, é indispensável que sejam criadas normas jurídicas de proteção de dados pessoais para além do âmbito cível. Nesse contexto, atualmente, há duas propostas legislativas destinadas à criação de uma LGPD Penal, a qual ainda inexiste no Brasil.

No ano de 2020, foi criado o Anteprojeto da LGPD Penal por uma comissão de juristas a pedido da Câmara dos Deputados (ENCCLA, 2021, p. 2). Já no ano de 2022, o então deputado federal Coronel Armando, do Partido Liberal de Santa Catarina, apresentou o Projeto de Lei (PL) n. 1.515/2022 (CÂMARA DOS DEPUTADOS, 2022).[36]

O Anteprojeto da LGPD Penal (ESMPU, 2021)[37] foi finalizado em 2020 e é fruto do trabalho de uma comissão de juristas instituída por Ato da Presidência da Câmara dos Deputados no dia 26 de novembro de 2019. O presidente dessa comissão foi o então, e hoje aposentado, ministro do Superior Tribunal de Justiça (STJ), Néfi Cordeiro.

Segundo a exposição de motivos do Anteprojeto, seu objetivo é equilibrar "a proteção do titular [dos dados pessoais] contra [o] mau uso e abusos como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações" (ESMPU, 2021, p. 1). Há, nesse contexto, uma dualidade que precisa ser equilibrada pela legislação: de um lado a eficiência investigatória e, do outro, a proteção de dados pessoais (ESMPU, 2021).

De acordo com o Anteprojeto, a transparência é o fundamento da

---

[36] A pesquisa desenvolvida encontrou a página de tramitação do PL. 1.515/2022 junto ao site da Câmara dos Deputados. Entretanto, essa página não foi encontrada em relação ao Anteprojeto da LGPD Penal. Apenas foram encontradas notícias diversas em *sites* especializados em temas jurídicos e políticos, razão pela qual se optou pela utilização da íntegra do documento do Anteprojeto, tal qual disponibilizada no *site* da Escola Superior do Ministério Público da União (ESMPU).

[37] Em nenhum dos *sites* oficiais do Poder Legislativo da União, foi encontrada a íntegra do Anteprojeto da LGPD Penal. Diante disso, optou-se por utilizar, como fonte, publicação disponível — novamente — no *site* oficial da ESMPU, por se tratar de instituição de ensino pública vinculada a um dos principais atores da persecução penal brasileira, o Ministério Público Federal.

proteção de dados, devendo-se garantir aos titulares o acesso e a retificação de seus dados pessoais. Além disso, o tratamento automatizado de dados deve ser regulado, para que, sempre que necessário, sejam fornecidas explicações acerca do tratamento realizado, inclusive, com a disponibilização dos registros, os quais deverão ser passíveis de serem auditados a qualquer tempo, nas chamadas trilhas de auditoria.[38] Também devem ser tomadas medidas que evitem a discriminação de grupos ou de indivíduos, determinando-se, ainda, a adoção dos conceitos de *privacy by design* e de *privacy by default* nas ferramentas computacionais utilizadas (ESMPU, 2021, p. 3-4).

Simonette (2021, p. 2) explica que o *privacy by design* determina que: "[d]esde o início de qualquer projeto envolvendo dados pessoais, é necessário considerar a segurança e privacidade dos dados, antecipando problemas e reduzindo o risco de furto e vazamento de dados". Acerca do *privacy by default*, sua adoção é assim explicada por referido autor:

> "(...) significa que as configurações mais seguras são aplicadas por padrão, assim que o produto ou serviço é lançado ao público. Ou seja, as pessoas não precisam escolher as configurações de privacidade e proteção, pois essas configurações são pré-configuradas, considerando a privacidade. Todas as informações pessoais fornecidas são coletadas apenas para a entrega do serviço ou produto. Mesmo com *Privacy by Design* e *Privacy by Default*, todos os dados necessários devem ser informados às pessoas, bem como a finalidade de cada um deles" (SIMONETTE, 2021, p. 2).

Em síntese, o Anteprojeto de LGPD Penal enumera diversos requisitos para o tratamento de dados pessoais para fins penais, mas determina regulamentação infralegal sob a supervisão e o monitoramento do Conselho Nacional de Justiça (CNJ), inclusive, para a posterior determinação da adoção de certos padrões técnicos mínimos, ainda a serem elaborados. Ou seja, em última análise, os detalhes que circundam o tratamento de dados pessoais, no âmbito penal, ainda dependeriam de atos normativos específicos e supervenientes, mesmo que o Anteprojeto fosse aprovado como lei.

A escolha do CNJ para essa tarefa é justificada pela Comissão de

---

[38] "A trilha de auditoria realiza o registro das atividades, eventos e ações que uma pessoa ou sistema fez ao lidar com dados. Ela auxilia a gestão a detectar se houve criações, alterações ou exclusão de registros. Além disso, ajuda a monitorar atividades automatizadas" (DOCUSIGN, 2022, p. 1).

Juristas do Anteprojeto, nos termos seguintes:

> "[A] indicação do CNJ, como órgão supervisor, é importante, na medida em que: (i) evita o dispêndio de novos gastos com a criação de um órgão específico; (ii) aproveita a *expertise* dos setores, dos Conselheiros e dos servidores do CNJ, que já vêm expedindo atos normativos importantes sobre a proteção de dados no âmbito brasileiro (v.g. Recomendação CNJ n. 73, de 20/08/2020, e Portaria CNJ n. 63/2019); e (iii) permite a formulação de políticas públicas uniformes para todo território nacional, a partir de uma composição plural e independente, com membros de instituições diversas, à luz do art. 103-B, da Constituição Federal (v.g. Poder Judiciário estadual, federal e trabalhista, Ministério Público estadual e federal, Ordem dos Advogados do Brasil, Câmara dos Deputados e Senado Federal)."

Por sua vez, o PL. 1.515/2022 (CÂMARA DOS DEPUTADOS, 2022) é muito semelhante ao Anteprojeto de LGPD Penal (ESMPU, 2021), mas há, entre ambos, diferenças em alguns pontos relevantes. O Anteprojeto versa apenas sobre o tratamento de dados pessoais para fins de Segurança Pública e de persecução penal, excluindo de seu bojo as áreas de Defesa Nacional e de Segurança do Estado (ESMPU, 2021).

Já o PL. 1.515/2022 abrange, expressamente, o tratamento de dados pessoais para fins exclusivos de Segurança do Estado, de Defesa Nacional, de Segurança Pública e de atividades de investigação e repressão de infrações penais. Além disso, o PL. 1.515/2022 prevê que cabe à Autoridade Nacional de Proteção de Dados Pessoais a responsabilidade de supervisionar, fiscalizar e regulamentar o tratamento de dados nessas áreas de atuação estatal (CÂMARA DOS DEPUTADOS, 2022).

O deputado federal Coronel Armando, do Partido Liberal de Santa Catarina, justifica a proposição do PL. 1.515/2022, nos seguintes termos:

> "Busca-se, portanto, harmonizar, de um lado, os deveres do Estado no exercício das atividades de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais; e, de outro, a observância das garantias processuais e as prerrogativas fundamentais dos cidadãos brasileiros no que tange ao tratamento de dados pessoais para tais fins. Nesse sentido, tendo em vista a pretensão de introduzir normas gerais, este projeto pretende complementar o sistema legislativo de tratamento de dados pessoais, com ênfase nos fins de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais, abordando de forma abrangente as responsabilidades dos órgãos incumbidos dessas atividades, sem fragmentar sua interpretação ou endereçá-la a instrumentos posteriores" (PL. 1515/2022, p. 33).

A partir da leitura dessas duas propostas de LGPD Penal, verifica-se que elas influenciam, de maneira direta, o modo como o Sistema de Justiça Criminal atinge o indivíduo. Todavia, nenhum desses dois projetos legislativos trata especificamente sobre o uso de *Big Data.*

Do ponto de vista computacional, referidas propostas legislativas fazem menções genéricas a “bancos de dados”, mas não, a bancos de dados de *Big Data*, fenômeno que vai muito além de um “grande banco de dados”, em razão das suas características distintivas próprias, conforme já abordadas no Capítulo 2 desta Dissertação.

Salienta-se que, muito embora a LGPD Cível também não verse, de forma específica, sobre *Big Data*, as suas normas jurídicas para o tratamento de dados são suficientes, para regular esse nicho específico da Ciência da Computação.

A adoção de normas genéricas no âmbito cível decorre do fato de existirem inúmeras formas de se construir e de se trabalhar em cima de um *Big Data* e, principalmente, do fato de a livre iniciativa praticar tudo aquilo que a lei não proíbe. Na seara cível, não cabe ao Poder Público engessar a dinâmica das relações privadas, mas, apenas, atuar de modo a garantir a sua segurança jurídica.

Ademais, mesmo que a LGPD Cível regule o tratamento de dados pelo Poder Público, ela não o faz dentro do Sistema de Justiça Criminal, mas, tão somente, em nichos relacionados à formação de políticas públicas e à adoção de boas práticas governamentais (BRASIL, 2018b). Em síntese, o tratamento de dados pelo Estado, nessas circunstâncias, destina-se a concretizar e a ampliar direitos e garantias fundamentais.

Todavia, do ponto de vista da LGPD Penal, a adoção de critérios genéricos de normatização do *Big Data*, como ocorre com a LGPD Cível, tende a não ser suficiente, visto que a utilização de *Big Data* para fins penais destina-se a restringir direitos e garantias fundamentais.[39]

---

[39] Um exemplo de restrição de direitos e garantias fundamentais pelo Sistema de Justiça Criminal é a quebra de sigilo de dados telefônicos, bancários ou fiscais. As normas jurídicas que tratam desse tipo de quebra de sigilo são destinadas a casos concretos, tratados individualmente. Por exemplo: quebra de sigilo fiscal e bancário de uma pessoa física individualizada que respondia inquérito policial sobre lavagem de dinheiro decorrente de sonegação fiscal.

No âmbito da Segurança Pública, o caráter pervasivo da vigilância objetiva inibir comportamentos criminosos. Já no contexto da persecução penal, seja esta na fase investigatória, seja ela já na fase judicial, o que está em jogo, em última análise, é a liberdade de ir e vir do cidadão, devido à possibilidade concreta de sua prisão.

Além do mais, por se tratar de típica função de Estado, a concretização do Sistema de Justiça Criminal rege-se pelas normas de Direito Público, segundo as quais só é lícito ao Estado agir de acordo com as determinações legais (DI PIETRO, 2017).

Em outras palavras, se ao particular é possível fazer tudo aquilo que a lei não proíbe, ao Estado só é lícito agir de acordo com os imperativos legais, sendo que a restrição de direitos e garantias exige uma legalidade qualificada, ou seja, lei em sentido estrito, não sendo suficientes, por exemplo, normas infralegais.

Desse modo, a construção de um *Big Data* para fins penais exige regulamentação específica, não podendo o Estado utilizar esse tipo de tecnologia computacional sem expressa regulamentação legal.

As normas jurídicas vigentes que regem o Direito Processual Penal e as regras de Computação Forense no Brasil não tratam expressamente da obtenção de elementos de prova a partir de ferramentas baseadas em *Big Data,* razão pela qual ainda não é possível a utilização desse tipo de tecnologia no âmbito da persecução penal. Por outro lado, a utilização do *Big Data* na área da Segurança Pública já é juridicamente possível, mas desde que devidamente regulada por normas infralegais.

De acordo com a Constituição (BRASIL, 1988), a Segurança Pública é formada e concretizada por diversas polícias, com destaque para as Polícias Militares e as Polícias Civis dos Estados, sendo aquelas na qualidade de polícia ostensiva e repressiva, e estas na qualidade de polícia judiciária[40].

As Polícias Militares são reguladas pela Lei n. 14.751, de 12 de

[40] Não se descartam os demais tipos de polícias, como as polícias rodoviárias, a Polícia Federal e as polícias penais. Contudo, justifica-se o foco nas polícias militares e nas polícias civis, em razão do que foi tratado nos projetos SiCReT e SiCReT II (item 4.1), e dos exemplos apresentados no item 2.3.3.

dezembro de 2023, denominada de Lei Orgânica Nacional das Polícias Militares e dos Corpos de Bombeiros Militares dos Estados, do Distrito Federal e dos Territórios (BRASIL, 2023b). Acerca do caráter preventivo e do uso de dados por parte das Polícias Militares, destacam-se, da referida lei, os seguintes dispositivos:

> **L. 14.751/2023**
> "**Art. 4º.** São diretrizes a serem observadas pelas polícias militares e pelos corpos de bombeiros militares dos Estados, do Distrito Federal e dos Territórios, além de outras previstas na legislação e em regulamentos, no âmbito de suas atribuições constitucionais e legais: [...];
> IX - cooperação e compartilhamento recíproco das experiências entre os órgãos de segurança pública, mediante instrumentos próprios, na forma da lei;
> X - utilização recíproca de sistema integrado de informações e acesso a dados cadastrais, observados os credenciamentos e os sigilos legais, nos limites de suas atribuições [...];
> XII - instituição de base de dados on-line e unificada por Estado da Federação, em conformidade com graus de sigilo estabelecidos pelo Ministério da Justiça e Segurança Pública, com compartilhamento recíproco dos dados entre os órgãos e instituições integrantes do Susp, por meio de cadastro prévio de servidor de cargo efetivo;
> XIII - utilização dos meios tecnológicos disponíveis e atualização das metodologias de trabalho para a constante melhoria dos processos de prevenção [...];
> XVII - gestão da proteção e compartilhamento de seus bancos de dados e demais sistemas de informação [...];
> XX - edição de atos administrativos normativos no âmbito de suas atribuições constitucionais e legais."

Além disso, dispõe o artigo 5º da Lei n. 14.751/2023:

> **L. 14.751/2023**
> "**Art. 5º.** Compete às polícias militares dos Estados, do Distrito Federal e dos Territórios, nos termos de suas atribuições constitucionais e legais, respeitado o pacto federativo: [...]
> XV - ter acesso, na apuração das infrações penais militares praticadas pelos seus membros, aos bancos de dados existentes nos órgãos de segurança pública relativos à identificação civil e criminal e a armas, veículos e objetos, observado o disposto no inciso X do *caput* do art. 5º da Constituição Federal, no âmbito de suas atribuições constitucionais e legais, bem como ter acesso a outros bancos de dados mediante convênio ou outro instrumento de cooperação [...];
> XXII - administrar as tecnologias da instituição, tais como sistemas, comunicações, aplicações, aplicativos, bancos de dados, *sites* na Internet, rede lógica e segurança da informação, entre outros recursos de suporte [...]."

Por sua vez, as Polícias Judiciárias são reguladas pela Lei n. 14.735, de 23 de novembro de 2023, a Lei Orgânica Nacional das Polícias Civis (BRASIL, 2023a), da qual se destacam os seguintes dispositivos acerca do tratamento de

dados:

> **L. 14.735/2023**
> "**Art. 5º.** São diretrizes a serem observadas pela polícia civil, além de outras previstas em legislação ou regulamentos:
> [...];
> VI - cooperação e compartilhamento das experiências entre os órgãos de segurança pública, mediante instrumentos próprios, na forma da lei;
> VII - integração ao sistema de segurança pública com instituição de mecanismos de governança;
> VIII - gestão da proteção e compartilhamento de seus bancos de dados e demais sistemas de informação;
> [...];
> X - utilização dos meios tecnológicos disponíveis e atualização e melhorias permanentes das metodologias de trabalho, para aprimoramento nos processos de investigação;
> [...];
> XIII - cooperação com a sociedade e com os órgãos do sistema de segurança pública e de justiça criminal;
> [...];
> XXI - edição de atos administrativos normativos no âmbito de suas atribuições constitucionais e legais."

Além disso, o art. 6º da Lei n. 14.735/2023 dispõe:

> **L. 14.735/2023**
> **Art. 6º.** Compete à polícia civil, ressalvadas a competência da União e as infrações penais militares, executar privativamente as funções de polícia judiciária civil e de apuração de infrações penais, a serem materializadas em inquérito policial ou em outro procedimento de investigação, e, especificamente:
> [...];
> V - garantir a adequada coleta, a preservação e a integridade da cadeia de custódia de dados, informações e materiais que constituam insumos, indícios ou provas;
> [...];
> VIII - organizar e realizar tratamento de dados e pesquisas jurídicas, técnicas e científicas relacionadas às funções de investigação criminal e de apuração das infrações penais, além de outras que sejam relevantes para o exercício de suas atribuições legais;
> IX - estimular o processo de integração dos bancos de dados existentes no âmbito do poder público e dele participar, preservando as informações sujeitas a sigilo legal, classificadas na forma do art. 23 da Lei .nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), ou que interessarem à apuração criminal;
> [...];
> XIII - atuar de forma cooperada com outros órgãos de segurança pública, nos limites de suas competências constitucionais e legais;
> [...];
> XXIII - administrar privativamente as tecnologias da instituição, tais como sistemas, aplicações, aplicativos, bancos de dados, sítios na rede mundial de computadores, rede lógica, segurança da informação, entre outros recursos de suporte;
> [...]".

Acerca do disposto nos incisos VIII e IX do art. 6º da Lei n. 14.735/2023,

cumpre salientar que o que está autorizado é apenas a possibilidade de criação de um *Big Data* por parte das polícias judiciárias para fins de persecução penal. Entretanto, do ponto de vista constitucional, essa autorização é genérica e carece de legislação específica no âmbito da proteção de dados pessoais, o que somente é possível por parte uma lei geral de proteção de dados de natureza penal.

Em outras palavras, a lei orgânica das polícias civis somente autoriza que, sob a perspectiva estatal, elas criem um *Big Data* para fins de persecução penal. Contudo, é incompleta a regulamentação dessa matéria, vez que trata apenas da postura estatal em relação ao cidadão, não prevendo como este poderá agir contra eventuais abusos e arbitrariedades por parte do Estado.

Nesse contexto, transcreve-se a crítica feita por Freitas *et al.* (2023, p. 116), haja vista que, ao que parece, não existe uma genuína preocupação em solucionar o problema da ausência normativa da Computação Forense baseada no tratamento de dados pessoais, mas, tão somente, demonstrar que algo será feito, mesmo sem se saber quando:

> "Não fosse apenas essa particularidade e apesar da necessidade, cada vez mais premente, da capacitação e difusão de conhecimentos e das técnicas da Computação Forense, o que se pode observar no Judiciário brasileiro é uma preocupação muito mais direcionada à criação de estratégias nacionais de segurança cibernética que pouco ou quase nada se debruçam acerca dos aspectos da Computação e da Forense Digital, apresentando-se muito mais como cartas de intenções que fazem menção, quando muito, a alguns princípios de Segurança da Informação ou de Cibersegurança, mas sem se preocupar com questões técnico-informáticas."

Além do mais, como já mencionado, o direito fundamental à proteção de dados pessoais é norma constitucional de eficácia contida, prevalecendo sempre em benefício do indivíduo. Afinal, dentro de um Sistema de Justiça Criminal, o postulado da "dúvida em favor do réu" é uma máxima inegociável, por concretizar o direito fundamental à presunção de inocência, conforme dispõe o art. 5º, inc. LVII, da Constituição da República Federativa do Brasil de 1988 (BRASIL, 1988).

Portanto, verifica-se que os citados dispositivos legais dão abertura legislativa somente para o tratamento de dados pessoais destinados a auxiliar o desempenho das funções públicas estatais no âmbito da Segurança Pública. Nesse contexto, conclui-se como parcialmente regulamentada, ao menos do

ponto de vista legal, a eficácia contida da norma constitucional do direito fundamental à proteção de dados pessoais, na referida seara estatal.

O caráter genérico dessas leis policiais impõe o detalhamento regulatório de natureza infralegal, sendo, por exemplo, incompatível com a Constituição (BRASIL, 1988) o disposto no artigo 15, §3º, da Lei 14.735/2023 (BRASIL, 2023a), a saber: “Fica garantido, mediante requisição fundamentada, o livre acesso das polícias civis aos bancos de dados de unidades técnico-científicas não integradas à instituição”.

Isso, porque a requisição é um imperativo ao seu destinatário, de modo que o seu não atendimento pode configurar até mesmo crime de desobediência.[41] Nesse caso, só haverá constitucionalidade na requisição se ela se basear em ato normativo regulamentador, mesmo que de natureza infralegal. Desse modo, torna-se legítima a recusa no atendimento de uma requisição se ausente a referida regulamentação.

Portanto, só é juridicamente legítimo utilizar o *Big Data* para fins de Segurança Pública quando existem atos normativos regulamentando sua utilização de forma transparente, permitindo aos cidadãos o pleno conhecimento acerca de como seus dados são tratados.[42]

Em suma, deve ser aplicada a mesma lógica de *accountability* (BUTA; TEIXEIRA; SCHURGELIES, 2018) que circunda a cadeia de custódia no Processo Penal,[43] isto é: o constante dever de prestação de contas do Estado em relação aos seus cidadãos. Além disso, também deve ser garantida a paridade de armas no Processo Penal, evitando-se eventual assimetria informacional acerca dos elementos de prova em detrimento da defesa (MASSENA, 2023).

Diante disso, considerando-se que o direito fundamental à proteção de

---

[41] O crime de desobediência está penalmente tipificado no artigo 330 do Código Penal (BRASIL, 1940).

[42] Salgado e Saito (2020) também se posicionam sobre o dever de transparência no tratamento de dados pessoais, com destaque para o dever do Estado de fazê-lo.

[43] Aqui, o termo “*accountability*” é utilizado no sentido de o Estado ter o dever de sempre prestar contas (BUTA; TEIXEIRA; SCHURGELIES, 2018) acerca de tudo que é feito durante o tratamento de dados de seus cidadãos. A correlação feita com a cadeia de custódia no âmbito da perícia forense diz respeito ao postulado de que tudo que é feito dentro de um sistema democrático deve ser transparente, acessível, rastreável e auditável por toda e qualquer pessoa.

dados pessoais consiste em uma norma constitucional de eficácia contida, conclui-se que o atual ordenamento jurídico brasileiro não autoriza o uso de ferramentas de Computação Forense baseadas em *Big Data* na persecução penal, haja vista a ausência de uma LGPD Penal que trate especificamente desse tema na persecução penal, devendo-se priorizar os direitos e garantias individuais, visto que, nesse contexto, a prisão do indivíduo é uma possibilidade concreta.

Por sua vez, no âmbito da Segurança Pública, verifica-se que a mesma conclusão se faz presente, haja vista que também existe um hiato normativo acerca da matéria; muito embora, nesse caso, a regulamentação possa se dar por meio de normas infralegais, conforme explanado.

## 4.4 ALGUMAS CONSIDERAÇÕES

Verificou-se já existirem, em curso, no âmbito da Computação Forense, pesquisas científicas e acadêmicas capazes de criar ferramentas computacionais baseadas em *Big Data*.

A possibilidade de utilização desse tipo de tecnologia necessita observar duas limitações: os imperativos do direito fundamental à proteção de dados pessoais, bem como a legislação vigente acerca do tema.

Todavia, não há, atualmente, uma lei em sentido estrito que regulamente o uso específico do *Big Data* para fins de Segurança Pública ou de persecução penal. Em vez disso, o que existe são permissivos legais para operacionalizar ferramentas computacionais baseadas em *Big Data*, no âmbito da Segurança Pública. Contudo, em que pese isso, não há regulamentação infralegal específica, razão pela qual o uso dessa tecnologia para tal fim não é legítimo.

Por sua vez, no âmbito da persecução penal, inexiste sequer lei em sentido estrito para o tratamento de dados pessoais, mesmo com o risco de prisão sendo concreto para quem está submetido aos órgãos persecutórios. O que existe são duas propostas legislativas para a criação de uma lei geral de proteção de dados em matéria penal. Entretanto, o estudo de tais projetos de lei evidencia que nenhum deles regulamenta a matéria de modo satisfatório.

As propostas de LGPD Penal limitam-se a traçar diretrizes genéricas

para o tratamento de dados pessoais, delegando a sua regulamentação específica para autoridades determinadas, seja o CNJ, seja a ANPD.

Desse modo, conclui-se que o uso de *Big Data* para fins penais, seja na área da Segurança Pública, seja na da persecução penal, é juridicamente inviável, não podendo, portanto, ser utilizado para tal fim, sem que exista exaustiva regulamentação a respeito.

# 5 CONCLUSÃO

A Sociedade Informacional e o Panspectron têm influenciado a atuação do Estado Contemporâneo por meio do tratamento de dados (pessoais ou não). Isso é resultado da tecnologia computacional, de natureza pervasiva e onipresente, o que torna os dados o cerne da vida humana e, também, da própria máquina estatal.

Em síntese, os dados consistem num fenômeno exponencial, cuja análise exige ferramentas cada vez mais sofisticadas, como o *Big Data.* Desse modo, como toda a vida humana transpassa, necessariamente, pela produção de dados, não poderia ser diferente no âmbito criminal, vez que diversos delitos são cometidos e até mesmo dependem de computadores; basta lembrar dos crimes cibernéticos próprios e impróprios. Nesse contexto, o *Big Data* passa a ganhar relevância, também, no âmbito do Sistema de Justiça Criminal.

No Brasil, o Sistema de Justiça Criminal baseado em *Big Data* pode ser classificado a partir de 02 (dois) pontos de vista: (i) prevenção da ocorrência de delitos e, por isso, denomina-se "*Big Data* para fins de Segurança Pública Preditiva"; e (ii) solução de crimes já cometidos, razão pela qual se denomina "*Big Data* para fins de persecução penal".

Em que pese isso, os direitos e garantias fundamentais das pessoas submetidas a um processo criminal permanecem, razão pela qual normas processuais relativas à Teoria da Prova e à cadeia de custódia continuam inalteradas.

Todavia, no atual ordenamento jurídico brasileiro, inexistem normas que regulamentem, no âmbito penal, a utilização de ferramentas computacionais sofisticadas, a exemplo daquelas baseadas em *Big Data*. Entretanto, mesmo assim, diversas são as Secretarias de Estado de Segurança Pública que têm utilizado *softwares* de análise preditiva e, até mesmo, de reconhecimento facial, para combater a criminalidade.

Contudo, muito embora as leis orgânicas das polícias militares e civis deem abertura legislativa para o tratamento de dados pessoais na área da Segurança Pública, é imprescindível que haja regulamentação infralegal para que se possa recorrer à utilização desses dados, inclusive, sob a forma de *Big*

*Data,* haja vista o inegociável dever de *accountability* do Estado perante os seus cidadãos.

Por sua vez, no âmbito da persecução penal, dados extraídos de dispositivos móveis já têm sido utilizados em estudos acadêmicos capazes de criar ferramentas de Computação Forense baseadas em *Big Data*. Isso, porque a Sociedade Informacional e a prática de crimes cibernéticos já têm exigido das polícias científicas uma postura apta a solucionar os novos imbróglios causados pelo Panspectron. Afinal, à medida em que a tecnologia se desenvolve, a criminalidade também avança.

Portanto, não há dúvida de que essa intersecção entre o Sistema de Justiça Criminal e o Panspectron exija ferramentas igualmente avançadas, como a Computação Forense baseada em *Big Data*, seja no âmbito da persecução penal, seja na área da Segurança Pública.

A questão é saber como conciliar todo esse contexto com o respeito aos direitos e garantias fundamentais dos cidadãos. Isto é, no atual contexto brasileiro, em que medida é juridicamente viável utilizar ferramentas de Computação Forense baseadas em *Big Data* no Sistema de Justiça Criminal?

O presente trabalhou foi guiado por essa pergunta, sendo que a pesquisa desenvolvida validou a hipótese de que a utilização, no Sistema de Justiça Criminal, de ferramentas de Computação Forense baseadas em *Big Data* é possível, mas desde que seja observada a eficácia contida do direito fundamental à proteção de dados pessoais, razão pela qual é indispensável a existência de lei em sentido estrito que verse especificamente sobre a utilização de *Big Data* no âmbito penal, sendo necessário, ainda, a edição de atos normativos infralegais aptos a evitar arbitrariedades pelo Estado, e a garantir todos os direitos e garantias constitucionais de quem é submetido ao crivo do Sistema de Justiça Criminal, seja na persecução penal, seja na Segurança Pública.

Os projetos de pesquisa SiCReT e SiCReT II contribuíram com esta dissertação ao terem demonstrado que é necessário e, também, possível construir e utilizar ferramentas computacionais baseadas em *Big Data* para serem utilizadas no combate à criminalidade.

Todavia, o uso de tecnologias avançadas, por si só, não resolve os

desafios do Sistema de Justiça Criminal. A eficiência da Segurança Pública e da persecução penal dependem, também, do respeito aos direitos e garantias fundamentais do indivíduo, razão pela qual são apresentadas as seguintes conclusões acerca do uso do *Big Data* no atual Sistema de Justiça Criminal brasileiro.

Primeiramente, (i) o direito fundamental à proteção de dados pessoais tem aplicação imediata, por se tratar de norma constitucional de eficácia contida destinada à proteção do indivíduo face ao abuso de poder, seja perante o Estado, seja perante agentes privados, como as empresas de tecnologia.

Em segundo lugar, (ii) as leis voltadas à proteção de dados pessoais possuem caráter regulamentador e esclarecem as possibilidades e os limites da utilização de dados pessoais, tendo sempre, como norte, o direito fundamental à proteção de dados.

Na sequência, em terceiro lugar, (iii) o uso, pelo Estado, de ferramentas baseadas em *Big Data* no âmbito criminal deve-se desdobrar em duas circunstâncias: (a) *Big Data* para fins de persecução penal; e (b) *Big Data* para fins de Segurança Pública.

Justifica-se essa terceira conclusão pela diferença de finalidade aí constatada, já que, enquanto a persecução penal destina-se à solução de um crime já cometido (função de polícia judiciária), a Segurança Pública tem, como objetivo, prevenir a ocorrência de delitos (função de polícia ostensiva e repressiva).

Posteriormente, em quarto lugar, (iv) está a inexistência de uma LGPD no âmbito penal, o que impede a utilização de ferramentas computacionais baseadas em *Big Data* no contexto da persecução penal.

Ademais, no que concerne à inexistência de uma LGPD no âmbito penal e à vedação, para fins de persecução penal, do recurso a ferramentas computacionais cuja base seja o *Big Data*, sabe-se serem insuficientes, para tal fim, as normas processuais genéricas, como as da cadeia de custódia, haja vista que a complexidade desse tipo específico de tecnologia exige a existência de uma legislação especial, transparente e capaz de garantir a sua compreensão por todos os atores da persecução penal — mesmo que isso se dê com auxílio pericial, garantindo-se, assim, o amplo direito de defesa do indivíduo submetido

à persecução penal do Estado, haja vista a possibilidade concreta da sua prisão.

Finalmente, em quinto e último lugar, (v) a inexistência de uma LGPD em âmbito penal não impede a utilização de *Big Data* no contexto da Segurança Pública, vez que a liberdade do indivíduo não é diretamente ameaçada pela prisão, como ocorre na persecução penal; bem como pelo fato de as leis orgânicas das polícias militares e civis darem abertura legislativa para esse tipo de atuação estatal.

Contudo, ainda assim, no que tange à quinta conclusão, é indispensável a regulamentação jurídica desse tipo de ferramenta, haja vista, por exemplo, a necessidade de anonimização de dados e da utilização de mecanismos antidiscriminatórios. Justifica-se, pois, essa última conclusão, por se tratar de uma tecnologia invasiva, por monitorar comportamentos individuais e populacionais.

Além do mais, ainda no que se atine à quinta e última conclusão, deve-se considerar a hipótese de utilização de dados pessoais obtidos a partir de casos penais específicos, o que torna indispensável que, além da regulamentação específica, haja autorização judicial expressa, para que, por exemplo, os dados extraídos de um celular apreendido em um inquérito policial sejam utilizados para alimentar um *Big Data* destinado à Segurança Pública.

Nesse último caso, o juízo criminal deverá garantir a anonimização dos dados, antes de estes deixarem o respectivo processo, vez que, caso contrário, o risco do uso indevido de tais dados é potencializado, além do impedimento decorrente da aplicação imediata do direito fundamental à proteção de dados pessoais.

Diante do exposto, verifica-se que o *Big Data* é apenas mais uma das ferramentas que podem ser utilizadas contra criminosos, não podendo ser visto como uma solução de forma isolada.

As conclusões apresentadas auxiliam no entendimento das circunstâncias e dos problemas jurídicos que orbitam a utilização de ferramentas de Computação Forense baseadas em *Big Data*, razão pela qual se espera que o presente trabalho possa contribuir de modo positivo numa futura regulamentação jurídica do tema.

## REFERÊNCIAS


ABADE, Denise Neves. **Processo Penal.** 1.ed. Barueri/Rio de Janeiro: GEN/Método, 2014, 512p. (Série Carreiras Federais).

AGOSTINHO, Emanuel Furlan de Bona. **A influência da hegemonia norte-americana no Brasil durante a Guerra Fria – Golpe de 1964.** Orientador: Prof. Dr. Ricardo Neumann. 2020, 19 f. Trabalho de Conclusão de Curso (Licenciatura em História). Instituto Ânima Sociesc de Inovação, Pesquisa e Cultura, UNISUL. Tubarão, 2020. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/16208. Acesso em: 15 set. 2023.

ARAÚJO, Raimundo Teixeira de; FARIAS, Regina Marques Braga. História Secreta dos Serviços de Inteligência: origens, evolução e institucionalização. **Revista Brasileira de Inteligência.** Brasília: Escola de Inteligência/ABIN, v. 1, n. 1, p. 85-89, 1º dez. 2005. Disponível em: https://rbi.enap.gov.br/index.php/RBI/article/view/19/11. Acesso em: 7 fev. 2024.

ARRUDA, Ana Julia Pozzi; RESENDE, Ana Paula Bougleux Andrade; FERNANDES, Fernando Andrade. Sistemas de Policiamento Preditivo e Afetação de Direitos Humanos à luz da Criminologia Crítica. **RDP.** Brasília: IDP, v. 18, n. 100, 2022. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5978. Acesso em: 7 fev. 2024.

ASSIS, Luiz Gustavo Bambini de. O absolutismo e sua influência na formação do Estado brasileiro. **Revista dos Tribunais.** São Paulo: *Thomson Reuters*/RT, a. 2016, v. 969, p. 49-71, jul. 2016 [texto eletrônico *online*]. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_bibliotec a/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.969.03.PDF. Acesso em: 7 fev. 2024.

AULETE, Caldas (1826-1878). Computar. **Aulete digital:** Dicionário Contemporâneo de Língua Portuguesa [*e-book*]. Rio de Janeiro: *Lexikon*, 2023a, s/p. [texto eletrônico *online*]. Disponível em: https://www.aulete.com.br/computar. Acesso em: 7 fev. 2024.

AULETE, Caldas (1826-1878). Lombrosiano. **Aulete digital:** Dicionário Contemporâneo de Língua Portuguesa [*e-book*]. Rio de Janeiro: *Lexikon*, 2023b, s/p. [texto eletrônico *online*]. Disponível em: https://www.aulete.com.br/lombrosiano. Acesso em: 7 fev. 2024.

AVENA, Norberto. **Processo Penal.** 15.ed., rev. e atual. Barueri/Rio de Janeiro: GEN/Método, 2023, 3.068p.

BADARÓ, Caio Massena. A propósito da cadeia de custódia das provas digitais no Processo Penal: breves notas sobre lógica da desconfiança, assimetria informacional e direito de defesa. **Boletim IBCCRIM**, São Paulo, v. 31, n. 368, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/506. Acesso em: 19 jan. 2024.

BAUMAN, Zygmunt (1925-2017); LYON, David. **Vigilância líquida:** diálogos com David Lyon. (Tradução) Carlos Alberto Medeiros. 1.ed. Rio de Janeiro: Zahar, 2013, 160p.

*BBC* BRASIL. “O escândalo que fez o Facebook perder *US*$ 35 bilhões em horas”. São Paulo: ***BBC* Brasil**, 20 mar. 2018, s/p. [texto eletrônico *online*]. Disponível em: https://www.bbc.com/portuguese/internacional-43466255. Acesso em: 7 fev. 2024.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: *Lumen Juris*, 2018, 251p.

BONFIM, Edilson Mougenot. **Curso de Processo Penal.** 13.ed. São Paulo: Saraiva*Jur*, 2019, 1.132p.

BRASIL. Câmara dos Deputados. Projetos de Lei e outras proposições. **PL 1515/2022:** inteiro teor. Brasília: 7 jun. 2022, s/p. [texto eletrônico *online*]. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300. Acesso em: 7 fev. 2024.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **Glossário de termos e expressões para uso no Exército**. 5.ed. Brasília: 2018a, 405p. [texto eletrônico *online*]. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/1/1148/1/Gloss%C3%A1rio%20EB%202018.pdf. Acesso em: 7 fev. 2024.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Constituição da República Federativa do Brasil de 1988.** Brasília: 2024, s/p. [texto eletrônico *online* compilado]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 7 fev. 2024.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Constituição Política do Império do Brasil de 25 de março de 1824.** Rio de Janeiro: Presidência da República, 1824. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao24.htm. Acesso em: 7 fev. 2024.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto-Lei n. 2.848, de 7 de dezembro de 1940.** Código Penal. Rio de Janeiro: 1940, s/p. [texto eletrônico *online* compilado]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 7 fev. 2024.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto-Lei n. 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Rio de Janeiro: 1941, s/p. [texto eletrônico *online* compilado]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm. Acesso em: 7 fev. 2024.

BRASIL. **Guia de vigilância epidemiológica:** Emergência de Saúde Pública de Importância Nacional pela Doença pelo Coronavírus 2019. Brasília: Ministério da Saúde, 2022, s/p. [texto eletrônico *online*]. Disponível em: https://www.gov.br/saude/pt-br/coronavirus/publicacoes-tecnicas/guias-e-planos/guia-de-vigilancia-epidemiologica-covid-19/@@download/file. Acesso em: 7 fev. 2024.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei n. 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Brasília: 2024, s/p. [texto eletrônico *online* compilado]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 7 fev. 2024.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei n. 11.343, de 23 de agosto de 2006.** Institui o SISNAD; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. Brasília: 2024, s/p. [texto eletrônico *online* compilado]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm#view. Acesso em: 7 fev. 2024.

BRASIL. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. **Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: 2018b, s/p. [texto eletrônico *online* compilado]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 7 fev. 2024.

BRASIL. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. **Lei n. 14.735, de 23 de novembro de 2023.** Institui a Lei Orgânica Nacional das Polícias Civis, dispõe sobre suas normas gerais de funcionamento e dá outras providências. Brasília: 2023a, s/p. [texto eletrônico *online* compilado]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14735.htm. Acesso em: 9 fev. 2024.

BRASIL. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. **Lei n. 14.751, de 12 de dezembro de 2023.** Institui a Lei Orgânica Nacional das Polícias Militares e dos Corpos de Bombeiros Militares dos Estados, do Distrito Federal e dos Territórios, nos termos do inciso XXI do caput do art. 22 da Constituição Federal, altera a Lei nº 13.675, de 11 de junho de 2018, e revoga dispositivos do Decreto-Lei nº 667, de 2 de julho de 1969. Brasília: 2023b, s/p. [texto eletrônico *online* compilado]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14751.htm. Acesso em: 7 fev. 2024.

BRASIL. Supremo Tribunal Federal (STF). Medida Cautelar na Ação Direta de Inconstitucionalidade n. 6.387 – Distrito Federal, Plenário, Rel. Min. Rosa Weber. Brasília, DF, 7 de maio de 2020.

BRAUN, Julia. Na China, atos dos cidadãos valerão pontos e limitarão seus projetos. **Veja.** São Paulo: Abril, 15 nov. 2018, às 08h00min; atual. 15 nov. 2018, às 12h44min, s/p [texto eletrônico *online*]. Disponível em: https://veja.abril.com.br/mundo/na-china-atos-dos-cidadaos-valerao-pontos-e-limitarao-seus-projetos/. Acesso em: 7 fev. 2024.

BROOKSHEAR, J. Glenn. **Ciência da Computação.** Porto Alegre: *Bookman*, 2013 [E-book]. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582600313/. Acesso em: 7 fev. 2024.

*CAMBRIDGE DICTIONARY*. ***Datum*.** *Cambridge*, *UK: Cambridge University Press*. Disponível em: https://dictionary.cambridge.org/dictionary/english/datum. Acesso em: 12 fev. 2024.

*CAMBRIDGE DICTIONARY*. ***Mobile device*.** *Cambridge*, *UK: CUP*, 2023. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/mobile-device. Acesso em: 7 fev. 2024.

CAMBRIDGE INTERNATIONAL. ***Data, information and knowledge*.** *Cambridge*, *UK: CUP*, 2015. Disponível em: https://www.cambridgeinternational.org/images/285017-data-information-and-knowledge.pdf. Acesso em: 7 fev. 2024.

CANDIOTTO, César; COUTO NETO, Sílvio. O panoptismo eletrônico virtual e sua ameaça ao exercício da atitude crítica. **Cadernos de Ética e Filosofia Política**, São Paulo: FFLC/USP, v. 2, n. 35, p. 83-101, 2019 [texto eletrônico *online*]. Disponível em: https://www.revistas.usp.br/cefp/article/view/162507. Acesso em: 7 fev. 2024.

CARIBÉ, João Carlos Rebello. **Algoritmização das relações sociais em rede, produção de crenças e construção da realidade.** Orientador: Prof. Dr. Arthur Coelho Bezerra. 2019, 151 p. Dissertação (Mestrado em Ciência da Informação) . UFRJ. Rio de Janeiro, 2019. Disponível em: https://ridi.ibict.br/handle/123456789/1040. Acesso em: 7 fev. 2024.

CARVALHO, Marcelo Batista de; TSUNODA, Denise Fukumi. Análise de dados em artigos recuperados da *Web of Science* (*WoS*). **Encontros Bibli**, Florianópolis, v. 23, n. 1, p. 112-125, 2018. Disponível em: https://www.redalyc.org/journal/147/14762635010/html/. Acesso em: 30 jan. 2024.

CASTELLS, Manuel. **A galáxia da Internet.** Rio de Janeiro: Zahar, 2003.

CHEETHAM, Robert. *Why We Sold HunchLab*. ***Azavea Company*.** Philadelphia, 23 jan. 2019, s/p. [texto eletrônico *online*]. Disponível em: https://www.azavea.com/blog/2019/01/23/why-we-sold-hunchlab/. Acesso em: 7 fev. 2024.

CIURIAK, Dan. ***The Economics of Data:*** *Implications for the Data-Driven Economy*. Canadá, 13 fev. 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118022. Acesso em: 7 fev. 2024.

COUTINHO, Lilian. LGPD e Inteligência: os limites no tratamento de dados pessoais coletados em fontes abertas. **Revista Brasileira de Inteligência.** Brasília: Escola de Inteligência/ABIN, n. 15, p. 99-116, dez. 2020 [texto eletrônico *online*]. Disponível em: https://rbi.enap.gov.br/index.php/RBI/article/view/183. Acesso em: 7 fev. 2024.

DALE, Nell; LEWIS, John. **Ciência da Computação.** (Tradução e Revisão Técnica) Jorge Duarte Pires. 4.ed. Rio de Janeiro: LTC, 2010, 456p.

DALLAGNOL, Deltan Martinazzo. **As lógicas das provas no processo:** prova direta, indícios e presunções. 1.ed., 1.tir. Porto Alegre: Livraria do Advogado, 2015, 362p.

DOCUSIGN. **Trilha de auditoria**: saiba como funciona e suas vantagens. São Paulo, 27 out. 2022. Disponível em: https://www.docusign.com/pt-br/blog/trilha-auditoria. Acesso em: 6 fev. 2024.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental/*Protection of Personal Data as a Fundamental Right*. **Revista Espaço jurídico/Espaço Jurídico *Journal of Law*.** Joaçaba: UNOESC, v. 12, n. 2, p. 91-108, jul./dez. 2011 [texto eletrônico *online*]. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 14 fev. 2024.

ENCCLA. Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro. Nota Técnica LGPD Penal. *In*: CÂMARA DOS DEPUTADOS. **Portal**. Brasília, 2021. Disponível em: https//enccla.camara.gov.br/acoes/arquivos/resultados-enccla-2021/e2021a4-enccla-2021-nota-tecnica-lgpd-penal. Acesso em: 30 jan. 2024.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense.** São Paulo: *Novatec*, 2011, 200p. (Redes & Segurança).

ESMPU. Escola Superior do Ministério Público da União. **Especialistas discutem anteprojeto da LGPD Penal**. Brasília, 15 jan. 2021. Disponível em: https://escola.mpu.mp.br/a-escola/comunicacao/noticias/especialistas-discutem-anteprojeto-da-lgpd-penal. Acesso em: 5 fev. 2024.

FALK, Matheus. **A necessidade de proteção aos dados pessoais no Direito brasileiro**: tutela jurídica na era da Modernidade Líquida e da *Surveillance*. Orientador: Prof. Dr. Cesar Antonio Serbena. 2017. 192 p. Dissertação (Mestrado em Direito) - Faculdade de Direito da Universidade Federal do Paraná, Curitiba, 2017. Disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=6028729#. Acesso em: 29 jan. 2024.

FEDELI, Ricardo Daniel; POLLONI, Enrico Giulio Franco; PERES, Fernando Eduardo. **Introdução à Ciência da Computação.** São Paulo: *Cengage*, 2003, 238p.

FIOROT, Bruna Luchi. **A plausibilidade da utilização do *Big Data* para a predição de crimes no Brasil frente aos seus riscos e consequências**. Orientador: Prof. Me. Anderson Burke Gomes. 2021, 64 p. Monografia (Bacharelado em Direito) - FDV, Vitória, 2021. Disponível em: http://repositorio.fdv.br:8080/handle/fdv/1203. Acesso em: 7 fev. 2024.

FIRMINO, Leonardo Magalhães; MURTA, Felipe. Comunicação política no *Facebook* e previsão eleitoral: análise de *Big Data* da eleição presidencial brasileira de 2018 no Brasil. ***Lumina*.** Juiz de Fora: UFJF, v. 13, n. 3, p. 47-63, set./dez. 2019 [texto eletrônico *online*]. Disponível em: https://periodicos.ufjf.br/index.php/lumina/article/view/28589. Acesso em: 7 fev. 2023.

FLORIDI, Luciano. *Big Data and Their Epistemological Challenge.* ***Philosophy & Technology*:** *Special Issue – Evolution, Genetic Engineering and Human Enhancement. (Edition) Russel Powell, Guy Kahane, Julian Savulescu. New York City (NY), USA*: *Springer Nature*, V. 25, 8 *Nov*. 2012, p. 435-437 [texto eletrônico *online*]. (*Editor Letters Collection*). Disponível em: https://link.springer.com/article/10.1007/s13347-012-0093-4. Acesso em: 7 fev. 2024.

FORBES BRASIL. **O que difere as *Big Techs* de outras empresas de tecnologia?** São Paulo (SP): *Forbes* Brasil, 8 fev. 2023, s/p. [texto eletrônico *online*]. Disponível em: https://forbes.com.br/forbes-tech/2023/02/o-que-difere-as-big-techs-de-outras-empresas-de-tecnologia/. Acesso em: 7 fev. 2024.

FOUCAULT, Michel (1926-1984). **Vigiar e punir:** nascimento da prisão. (Tradução) Ligia Maria Pondé Vassalo. Petrópolis: Vozes, 1977, 277p., il.

FREITAS, Cinthia Obladen de Almendra; BARDDAL, Jean Paul. **Análise preditiva e decisões judiciais:** controvérsia ou realidade? Revista Democracia Digital e Governo Eletrônico, Florianópolis, v. 1, n. 18, p. 107-126, 2019.

FREITAS, Cinthia Obladen de Almendra; SILVA, Rui Miguel; SOUSA, Devilson da Rocha; PIRATELLI, João Paulo Machado. A cadeia de custódia de provas digitais sob a perspectiva da forense digital: considerações a partir de uma perspectiva tecno-científica. **Revista Síntese de Direito Penal e Processual Penal**, Porto Alegre: Síntese, v.23, n.141, ago/set, 2023. p. 101-123. ISSN 2179-1627.

G1 GLOBO. Portal de Notícias. Com a ajuda de câmeras de reconhecimento facial, 77 foragidos da polícia são presos no carnaval da Bahia. **Fantástico.** Salvador: Grupo Globo, 26 fev. 2023, às 23h59min, atual. há 11 meses, s/p [texto eletrônico *online*]. Disponível em: https://g1.globo.com/fantastico/noticia/2023/02/26/com-ajuda-de-cameras-de-reconhecimento-facial-77-foragidos-da-policia-sao-presos-no-carnaval-da-bahia.ghtml. Acesso em: 7 fev. 2024.

G1 GLOBO. Portal de Notícias. Com a chegada do Natal, policiamento é reforçado nos centros comerciais de Juiz de Fora. Juiz de Fora: 28 nov. 2022, s/p. [texto eletrônico *online*]. Disponível em: https://g1.globo.com/mg/zona-da-mata/noticia/2022/11/28/com-a-chegada-do-natal-policiamento-e-reforcado-nos-centros-comerciais-de-juiz-de-fora.ghtml. Acesso em: 7 fev. 2024.

GHISLENI, Eduardo Steffenello. **Vigilância na sociedade em rede**: a coleta de dados pessoais na Internet e suas implicações ao direito à privacidade. Santa Maria: 2015, 60p. Disponível em: https://repositorio.ufsm.br/handle/1/2821. Acesso em: 25 set. 2023.

GONÇALVES, João Ricardo; LEITÃO, Leslie; ARAÚJO, Marina; TEIXEIRA, Patrícia. Vereadora do PSOL, Marielle Franco é morta a tiros na Região Central do Rio. *In*: G1. **Rio de Janeiro**. Rio de Janeiro, 14 mar. 2018. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/vereadora-do-psol-marielle-franco-e-morta-a-tiros-no-centro-do-rio.ghtml. Acesso em: 14 jan. 2024.

*GOOGLE CLOUD*. **O que é análise preditiva?** São Paulo, 2023, s/p. [texto eletrônico *online*]. Disponível em: https://cloud.google.com/learn/what-is-predictive-analytics?hl=pt-br. Acesso em: 7 fev. 2024.

GOVERNO DO ESTADO DO PARANÁ. Agência Estadual de Notícias. Polícia Militar lança Operação Natal e reforça segurança em todo o Paraná. **Notícias.** Curitiba, 5 dez. 2022, s/p. [texto eletrônico *online*]. Disponível em: https://www.aen.pr.gov.br/Noticia/Policia-Militar-lanca-Operacao-Natal-e-reforca-seguranca-em-todo-o-Parana. Acesso em: 7 fev. 2024.

GREENFIELD, Adam. ***Everyware*****:** *The Dawning Age of Ubiquitous Computing*. *Berkeley* (*CA*), *USA*: *New Riders*, 2006.

GUIMARÃES, Lucia Maria Paschoal. A elevação do Brasil a Reino Unido e a historiografia luso-brasileira. **Revista do Instituto Histórico e Geográfico Brasileiro**, Rio de Janeiro, p. 47-58, 2016 [texto eletrônico *online*]. Disponível em: https://ihgb.org.br/revista-eletronica/artigos-470/item/108307-a-elevacao-do-brasil-a-reino-unido-e-a-historiografia-luso-brasileira.html. Acesso em: 7 fev. 2024.

GUIMARÃES, Paulo Henrique. O computador quântico já existe? Segunda parte. **Notícias.** Brasília (DF): SERPRO, 25 out. 2019, s/p. [texto eletrônico *online*]. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2019/computador-quantico-ja-existe. Acesso em: 7 fev. 2024.

HAN, Byung-Chul. **Sociedade da transparência.** Petrópolis (RJ): Vozes, 2017, 120p.

HOFFMANN, Mauro da Silva. O domínio ideológico da Igreja durante a Alta Idade Média Ocidental. **Revista Historiador.** Porto Alegre (RS), n. 1, 2020. Disponível em: https://revistahistoriador.com.br/index.php/principal/article/view/28. Acesso em: 7 fev. 2024.

HUSEK, Carlos Roberto. Conflitos armados específicos, casos e decisões específicas. **Enciclopédia Jurídica da Pontifícia Universidade Católica de São Paulo:** t. Direito Internacional. 1.ed. São Paulo (SP): PUCSP, 2022, s/p. [texto eletrônico *online*]. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/504/edicao-1/conflitos-armados-especificos,-casos-e-decisoes-especificas. Acesso em: 7 fev. 2024.

*INTERNATIONAL BUSINESS MACHINE CORPORATION*. *Customer Engineering* ***Manual of Instruction:*** *650 Data-Processing System*. *NYC (NY)*, *USA: IBM*,1956/1957, 213p. [texto eletrônico *online*]. Disponível em: http://bitsavers.informatik.uni-stuttgart.de/pdf/ibm/650/22-6284-1_650_CE_Manual_of_Instruction.pdf. Acesso em: 7 fev. 2024.

IBM. **O que é Processamento de Linguagem Natural?** São Paulo, 2023, s/p. [texto eletrônico *online*]. Disponível em: https://www.ibm.com/br-pt/topics/natural-language-processing. Acesso em: 7 fev. 2024.

INSTITUTO DE ESTUDOS AVANÇADOS. Observatório da Inovação. *In*: HIARBIX. *Quando mulheres negras eram computadores da NASA*. São Paulo: IEA/USP, 25 jul. 2017, s/p. [texto eletrônico *online*]. Disponível em: https://oic.nap.usp.br/news/quando-mulheres-negras-eram-os-computadores-da-nasa/. Acesso em: 7 fev. 2024.

IVEY, Alice. *History of computing: From Abacus to Quantum Computers.* ***News.*** *USA*: *Cointelegraph*, 13 jun. 2023, s/p. [texto eletrônico *online*]. Disponível em: https://cointelegraph.com/news/history-of-computing-from-abacus-to-quantum-computers. Acesso em: 7 fev. 2024.

JALIL, Simone Medeiros; BURLAMAQUI, Aquiles Medeiros Filgueira. *The importance of recognizing the protection of personal data as a fundamental right.* ***Research, Society and Development***, Vargem Grande Paulista, v. 11, n. 14, p. e223111432707, 2022.

Disponível em: https://rsdjournal.org/index.php/rsd/article/view/32707. Acesso em: 17 jan. 2024.

KELLEHER, Ann. Lei de Moore: Agora e no Futuro. INTEL. ***Opinion***. *USA*: 16 fev. 2022. Disponível em: https://www.intel.com.br/content/www/br/pt/newsroom/opinion/moore-law-now-and-in-the-future.html. Acesso em: 7 fev. 2024.

KITCHIN, Rob. ***The Data Revolution****: Big Data, Open Data, Data Infrastructures and their consequences*. *USA*: 2014.

LENZA, Pedro. **Direito Constitucional.** São Paulo: Saraiva*Jur*, 2023.

LIMA FILHO, Acacio Vaz de. O positivismo e a República. **Revista da Faculdade de Direito, Universidade de São Paulo**. São Paulo, v. 99, p. 3-33, 2004. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67617. Acesso em: 7 fev. 2024.

LIZIERO, Leonam Baesso da Silva. **O conceito de soberania no estado contemporâneo e suas implicações na dicotomia entre o direito interno e o direito internacional**. Orientador: Marco Aurélio Marrafon. 2013, 156 p. Dissertação (Mestrado em Direito) - UERJ, Rio de Janeiro, 2013. Disponível em: https://www.bdtd.uerj.br:8443/handle/1/9618. Acesso em: 7 fev. 2024.

LOPES JÚNIOR, Aury. **Direito Processual Penal**. 11.ed. São Paulo: Saraiva, 2014, 1.402p.

LOPES JÚNIOR, Aury; GLOECKNER, Ricardo Jacobsen. **Investigação preliminar no Processo Penal.** 6.ed. São Paulo: Saraiva, 2014, 552p.

MÄDER, Maria Elisa Noronha de Sá. Revoluções de Independência na América Hispânica: uma reflexão historiográfica. **Revista de História.** São Paulo: FFLC/USP, n. 159, 2008, p. 225-241 [texto eletrônico *online*]. Disponível em: https://www.revistas.usp.br/revhistoria/article/view/19094. Acesso em: 5 fev. 2024.

MARQUES, José Frederico (1912-1993). **Elementos de Direito Processual Penal**. Rio de Janeiro: Forense, 2023.

MARTINS, Ricardo Evandro Santos. História da tradição da civil law e a questão do direito processual brasileiro: um breve ensaio sobre a nossa proximidade com a common Law. **Revista Acadêmica Escola Superior do Ministério Público do Ceará**, Fortaleza, v. 11, n. 1, p. 195-211, 2019. Disponível em: https://revistaacademica.mpce.mp.br/revista/article/view/72. Acesso em: 7 fev. 2024.

MENDRONI, Marcelo Batlouni. **Curso de investigação criminal.** 3.ed., rev. e aum. São Paulo: GEN, 2013, 386p.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015, p. 205-

230.

MICHAELIS. *Status*. **Dicionário Brasileiro da Língua Portuguesa.** São Paulo: Melhoramentos, 2015, s/p. [texto eletrônico *online*]. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/status/. Acesso em: 7 fev. 2024.

*MICROSOFT AZURE*. O que são bancos de dados? Definições, tipos e exemplos de bancos de dados. São Paulo: ***Microsoft***, 2023, s/p. [texto eletrônico *online*]. Disponível em: https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-are-databases. Acesso em: 7 fev. 2024.

*MICROSOFT AZURE*. Dados não relacionais e *NoSQL*. **Centro de Arquitetura.** São Paulo: *Microsoft*, 2023, s/p. [texto eletrônico *online*]. Disponível em: https://learn.microsoft.com/pt-br/azure/architecture/data-guide/big-data/non-relational-data. Acesso em: 7 fev. 2024.

MILLER, Brad; RANUM, David; COLLEGE, Luther. **Resolução de Problemas com Algoritmos e Estruturas de Dados usando Python**. (Tradução) Andrew Toshiaki Nakayama Kurauchi; Carlos Eduardo Leão Elmadjian; Carlos Hitoshi Morimoto; José Coelho de Pina. São Paulo: IME/USP, 3 jan. 2024, s/p. [texto eletrônico *online*]. Disponível em: https://panda.ime.usp.br/panda/static/pythonds_pt/index.html. Acesso em: 7 fev. 2024.

*MICHIGAN INSTITUTE OF TECHNOLOGY*. **O que é um computador quântico?** *USA*, 2 ago. 2020, s/p. [texto eletrônico *online*]. Disponível em: https://mittechreview.com.br/o-que-e-um-computador-quantico/. Acesso em: 7 fev. 2024.

NUCCI, Guilherme de Souza. **Manual de Processo Penal:** volume único. 3.ed., rev. e atual. São Paulo: GEN/Forense, 2023, 728p.

NUNES, Nathan. Vinte anos depois, *Minority Report* continua assustadoramente parecido com a realidade. **Persona Jornalismo Cultural:** Cinema. Bauru: 2 ago. 2022, s/p. [texto eletrônico *online*]. Disponível em: https://personaunesp.com.br/?s=minority+report. Acesso em: 1º fev. 2024.

OLIVEIRA, Dânton Hilário Zanetti de. ***Big Data* e a Lei Geral de Proteção de Dados Pessoais:** diálogos necessários em prol da livre iniciativa. Rio de Janeiro: *Lumen Juris* Direito, 2022, 216p. (Informática e Direito Digital).

OLIVEIRA, Eugênio Pacelli de. **Curso de Processo Penal.** 19.ed., rev. e atual. São Paulo: Atlas, 2015.

*ORACLE BRASIL*. **O que é *Big Data*?** São Paulo: *Oracle* Brasil, 2023, s/p. [texto eletrônico *online*]. Disponível em: https://www.oracle.com/br/big-data/what-is-big-data/. Acesso em: 7 fev. 2024.

*ORACLE* BRASIL. O que é banco de dados? **Banco de Dados.** São Paulo: *Oracle* Brasil, 2023a, s/p. [texto eletrônico *online*]. Disponível em: https://www.oracle.com/br/database/what-is-database. Acesso em: 7 fev. 2024.

*ORACLE* BRASIL. O que é NoSQL? **Banco de Dados.** São Paulo: *Oracle* Brasil, 2023b, s/p. [texto eletrônico *online*]. Disponível em: https://www.oracle.com/br/database/nosql/what-is-nosql/. Acesso em: 7 fev. 2024.

PAES, Bruno Lincoln Ramalho. **O direito divino dos reis em Ricardo II, de William Shakespeare.** Orientadora: Prof.ª Dr.ª Mara Regina de Oliveira. 2020, 240 f. Dissertação (Mestrado em Filosofia e Teoria Geral do Direito) – FADUSP, São Paulo, 2020. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2139/tde-09052021-220542/pt-br.php. Acesso em: 7 fev. 2024.

PEREIRA, Antonio Kevan Brandão. **Teoria Democrática Contemporânea:** o conceito de poliarquia na obra de Robert Dahl. Orientador: Prof. Dr. Jawdat Abu-El-Haj. 2013. 107 f. Dissertação (Mestrado em Sociologia) – UFCE, Fortaleza, 2013. Disponível em: https://repositorio.ufc.br/handle/riufc/8685. Acesso em: 7 fev. 2024.

PEREIRA, Eliomar da Silva. **Teoria da Investigação Criminal.** Lisboa, Portugal: Almedina, 2022. E-book. ISBN 9786556275802. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556275802/. Acesso em: 7 fev. 2024.

PINTO, Danielle Jacon Ayres. ***Smart Power* como um novo paradigma de poder na esfera internacional**: uma análise do Brasil e sua inserção internacional nos governos de Fernando Henrique Cardoso e Luiz Inácio Lula da Silva. Orientador: Prof. Dr. Paulo Cesar Souza Manduca. 2016. 352 p. Tese (Doutorado em Ciência Política) - Universidade Estadual de Campinas, Campinas, 2016. Disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=3675869. Acesso em: 30 jan. 2024.

PONTOTEL. **Entenda o que é o *Big Data* e qual a importância dessa ferramenta para a gestão de pessoas.** São Paulo (SP): 23 maio 2023. Disponível em: https://www.pontotel.com.br/big-data/. Acesso em: 27 dez. 2023.

PREDPOL. ***Overview*.** Santa Cruz, 2023. Disponível em: https://www.predpol.com/about/. Acesso em: 28 out. 2023.

RAMOS, André de Carvalho. **Curso de Direitos Humanos.** 9.ed., rev. e ampl. São Paulo (SP): Saraiva*Jur*, 2022, 1.234p.

RAVIZZA, João (1885-1941). **Gramática Latina.** 9.ed. Niterói: Escolas Profissionais Salesianas, 1918, 560p. [texto eletrônico *online*]. Disponível em: https://latim.paginas.ufsc.br/files/2012/06/Gram%C3%A1tica-Latina.-Ravizza.pdf. Acesso em: 7 fev. 2024.

REIS, Juliana Duclerc Costa. **Provas ilícitas no Processo Penal brasileiro:** admissibilidade ou inadmissibilidade? Orientadora: Prof.ª Me. Mônica Cavalieri Fetzner Areal. Coorientadores: Prof.ª Me. Néli Luísa Cavalieri Fetzner; Prof. Me. Nélson Carlos Tavares Júnior. 2013, 21p. Especialização (Direito). EMERJ, Rio de Janeiro, 2013. Disponível em: https://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/1semestre2013/trabalhos_12013/JulianaDuclercCostaReis.pdf. Acesso em: 7 fev. 2024.

RIBEIRO, João Gabriel Silva. Entre o capitalismo de vigilância e a espionagem digital. ***Shifter*.** Lisboa, Portugal: *Shifter Generation*, 2021, s/p. [texto eletrônico *online*]. Disponível em: https://shifter.pt/2021/08/pegasus-capitalismo-de-vigilancia/?doing_wp_cron=1707093977.4074308872222900390625. Acesso em: 7 fev. 2024.

RIBEIRO, Márcio da Mota. **A atividade de inteligência de Estado brasileira está em xeque com a promulgação da Emenda n. 115/2022?** Uma avaliação de riscos e impactos e proposta de uma agenda de soluções. Orientador: Prof. Dr. Rafael Rabelo Nunes. Coorientador: Prof. Dr. William Ferreira Giozza. 62p. Dissertação (Mestrado em Engenharia Elétrica). Faculdade de Tecnologia da UnB. Brasília, 2023. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/05/Marcio-da-Mota-Ribeiro-1.pdf. Acesso em: 14 fev. 2024.

RODOTÀ, Stefano (1933-2017). **A vida na sociedade de vigilância:** a privacidade hoje. (Organização, Seleção e Apresentação) Maria Celina Bodin de Moraes. (Tradução) Danilo Doneda (1970-2022); Luciana Cabral Doneda. 1.ed. Rio de Janeiro: Renovar, 2008, 382p.

RODRIGUES, Clara Sanchez. **As bases da hegemonia americana no século XXI.** Orientador: Prof. Dr. Guilherme Sandoval Góes. 2022, 83 f. Dissertação (Mestrado em Segurança Internacional e Defesa). ESG, Rio de Janeiro, 2022. Disponível em: https://repositorio.esg.br/bitstream/123456789/1590/1/Clara%20Rodrigues%20-%20Dissertacao%20final.pdf. Acesso em: 7 fev. 2024.

ROUSE, Margaret. *Semi-Structured Data*. ***TechDictionary*.** *Canada*: *Techopedia*, 30 mai 2020, s/p. [texto eletrônico *online*]. Disponível em: https://www.techopedia.com/definition/28802/semi-structured-data. Acesso em: 7 fev. 2024.

ROUSE, Margaret. *Structured Data*. ***TechDictionary*.** *Canada*: *Techopedia*, 30 out. 2023c, s/p. [texto eletrônico *online*]. Disponível em: https://www.techopedia.com/definition/30363/structured-data. Acesso em: 7 fev. 2024.

ROUSE, Margaret. *Unstructured Data*. ***TechDictionary*.** *Canada*: *Techopedia*, 27 nov. 2023b. Disponível em: https://www.techopedia.com/definition/13865/unstructured-data. Acesso em: 7 fev. 2024.

ROUSE, Margaret. *What is Big Data?* ***TechDictionary*.** *Canada*: *Techopedia*, 23 nov. 2023a. Disponível em: https://www.techopedia.com/definition/27745/big-data. Acesso em: 7 fev. 2024.

SALGADO, Eneida Desiree; SAITO, Vitoria Hiromi. Privacidade e proteção de dados: por uma compreensão ampla do direito fundamental em face da sua multifuncionalidade. ***International Journal of Digital Law***, Belo Horizonte, ano 1, n. 3, p. 117-137, set./dez. 2020.

SANTOS, Gilberto Antonio Duarte. **O conceito de *rule of law* nas relações internacionais**: direitos humanos e restrições à liberdade de navegação nos oceanos. Orientador: Luiz Daniel Jatobá França. 2015, 139 p. Dissertação (Mestrado em Relações Internacionais) - UnB. Brasília, 2015. Disponível em:

http://repositorio.unb.br/bitstream/10482/19406/3/2015_GilbertoAntonioDuarteSantos.pdf. Acesso em: 7 fev. 2024.

SANTOS, Valmir Gonçalez dos. O desentendimento como característica inerente à democracia. **Revista Diaphonía.** Toledo, v. 5, n. 1, p. 149-159, 2019 [texto eletrônico *online*]. Disponível em: https://e-revista.unioeste.br/index.php/diaphonia/article/view/22782. Acesso em: 19 set. 2023.

SAPORI, Luís Flávio. Uma abordagem organizacional da justiça criminal na sociedade brasileira. **Atlas da Violência**, Brasília, p. 1-11, 12 jan. 2000 [texto eletrônico *online*]. Disponível em: https://www.ipea.gov.br/atlasviolencia/arquivos/artigos/2129-3765-anais-forum-cesec-ipea-263-273.pdf. Acesso em: 19 set. 2023.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Revista Brasileira de Direitos Fundamentais & Justiça**, Porto Alegre, v. 14, n. 42, p. 179–218, 2020. DOI: 10.30899/dfj.v14i42.875. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 19 fev. 2024.

SCHEUERMANN, Gabriela Felden. Dados pessoais como um direito fundamental autônomo a partir da Emenda Constitucional nº 115/2022. **Revista da Defensoria Pública do Estado do Rio Grande do Sul**, Porto Alegre, v. 2, n. 33, p. 253–274, 2023. Disponível em: https://revista.defensoria.rs.def.br/defensoria/article/view/600. Acesso em: 19 fev. 2024.

SIMPSOON, Adam. *Surveillance State.* ***The New York Times*****:** *Book Review*. *USA*, 18 jul. 2013, s/p. [texto eletrônico *online*]. Disponível em: https://www.nytimes.com/2013/07/21/books/review/the-panopticon-by-jenni-fagan.html. Acesso em: 7 fev. 2024.

SKINNER, Quentin. *A Genealogy of the Modern State*: *British Academy Lecture*. ***British Academy Scholarship Online*****:** *Proceedings of the British Academy*. London, v. 162, p. 324-370, 2009 [texto eletrônico *online*]. Disponível em: https://doi.org/10.5871/bacad/9780197264584.003.0011. Acesso em: 7 fev. 2024.

SOUZA, Nicolle Bêtta de; ACHA, Fernanda Rosa. A Proteção de Dados como direito fundamental: uma análise a partir da Emenda Constitucional 115/2022. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, Brasil, v. 8, n. 9, p. 666–684, 2022. Disponível em: https://periodicorease.pro.br/rease/article/view/6822. Acesso em: 19 fev. 2024.

*STATE LIBRARY OF KANSAS*. ***What is a mobile device?*** *USA*, 2023. Disponível em: https://kslib.info/1282/What-is-a-mobile-device. Acesso em: 7 fev. 2024.

SUPERIOR TRIBUNAL DE JUSTIÇA. *Habeas Corpus* 117763/SP (2008/0221469-7): inteiro teor de acórdão. Rel. Min. Jane Silva (Desembargadora Convocada do TJ/MG). DJ: 05/11/2008. **Superior Tribunal de Justiça**, 2008. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=200802214697. Acesso em: 7 fev. 2024.

TARASOV, Katie. *How AMD became a chip giant and leapfrogged Intel after years of playing catch-up. In: CONSUMER NEWS AND BUSINESS CHANNEL*. **CNBC U.S**.: *Tech*. Estados Unidos da América, 22 nov. 2022. Disponível em: https://www.cnbc.com/2022/11/22/how-amd-became-a-chip-giant-leapfrogged-intel-after-playing-catch-up.html. Acesso em: 28 jan. 2024.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria**. Lei Geral de Proteção de Dados Pessoais:** comentada artigo por artigo. São Paulo: Saraiva, 2022. E-book. ISBN 9786555599015. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 7 fev. 2024.

THORBECKE, Catherine. Entenda por que os laços entre TikTok e China comprometeram o app nos EUA. ***CNN Business***. São Paulo: *CNN* Brasil, 2 ago. 2022, s/p. [texto eletrônico *online*]. Disponível em: https://www.cnnbrasil.com.br/economia/entenda-por-que-os-lacos-entre-tiktok-e-china-estao-comprometendo-o-app-nos-eua/. Acesso em: 7 fev. 2024.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL. Módulo 1: o que é um dispositivo móvel? **DIMOS.** Porto Alegre, 2023a, s/p. [texto eletrônico *online*]. Disponível em: http://www.nuted.ufrgs.br/oa/dimos/modulo1.html. Acesso em: 7 fev. 2024.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL. Instituto de Física. **Linguagens de Programação e Linguagens de Máquina**. Porto Alegre (RS): 2023b. Disponível em: https://www.if.ufrgs.br/~betz/fis01226/aula1/textoa1.htm. Acesso em: 7 fev. 2024.

VECCHIA, Evandro Dalla. **Perícia digital:** da investigação à análise forense. 2.ed. Campinas: *Millenium*, 2019, 404p.

XAVIER, Vítor César Silva. **Transparência nos Estados democráticos**: estratégia do segrego nas políticas públicas de transparência do Brasil e dos EUA de 2013 a 2020. Orientador: Profa. Dra. Maria Helena de Castro Santos. 2022. 421 p. Tese (Doutorado em Relações Internacionais) - Universidade de Brasília, Brasília, 2022. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/73778/3/Tese_de_Doutorado_Vitor_Cesar.pdf . Acesso em: 17 jan. 2024.

WAZLAWICK, Raul Sidnei. **História da Computação.** São Paulo: GEN, 2016, 584p. [e-book].

WEBER, Max. **Ciência e Política**: Duas Vocações. São Paulo: *Cultrix*, 2011.

ZOTELLI, Pedro. *Hardware x Software.* **Sistemas de Informação.** São Paulo: ESPM, 2023, s/p. [texto eletrônico *online*]. Disponível em: https://sistemasdeinformacao.espm.edu.br/acontece-no-curso/noticias-da-area/hardware-vs-softaware/. Acesso em: 7 fev. 2024.