DISSERTAÇÃO DE MESTRADO PROFISSIONAL

A atividade de Inteligência de Estado brasileira está em xeque com a promulgação da Emenda Constitucional n. 115/2022? Uma avaliação de riscos e impactos e proposta de uma agenda de soluções

Márcio da Mota Ribeiro

Orientador: Prof. Dr. Rafael Rabelo Nunes, UnB

Coorientador: Prof. Dr. William Ferreira Giozza, FT/UnB

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

A atividade de Inteligência de Estado brasileira está em xeque com a promulgação da Emenda Constitucional n. 115/2022? Uma avaliação de riscos e impactos e proposta de uma agenda de soluções

Is the Brazilian State Intelligence in jeopardy with the enactment of constitutional amendment number 115/2022? An assessment of risks and impacts and a proposed solution agenda

Márcio da Mota Ribeiro

Orientador: Prof. Dr. Rafael Rabelo Nunes, UnB

Coorientador: Prof. Dr. William Ferreira Giozza, FT/UnB

PUBLICAÇÃO: PPEE.MP.039

BRASÍLIA-DF

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

A atividade de Inteligência de Estado brasileira está em xeque com a promulgação da Emenda Constitucional n. 115/2022? Uma avaliação de riscos e impactos e proposta de uma agenda de soluções

Márcio da Mota Ribeiro

Orientador: Prof. Dr. Rafael Rabelo Nunes, UnB

Coorientador: Prof. Dr. William Ferreira Giozza, FT/UnB

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Rafael Rabelo Nunes, Ph.D, UnB _____
Orientador/Presidente

Prof. José dos Santos Carvalho Filho, Ph.D, IDP _____
Examinador externo

Prof. Fabiana Freitas Mendes, Ph.D, FT/UnB _____
Examinador interno

Prof. Georges Daniel Amvame Nze, Ph.D, FT/UnB _____
Examinador suplente

FICHA CATALOGRÁFICA

RIBEIRO, MÁRCIO DA MOTA
A atividade de Inteligência de Estado brasileira está em xeque com a promulgação da Emenda Constitucional n. 115/2022? Uma avaliação de riscos e impactos e proposta de uma agenda de soluções [Distrito Federal] 2023.
xvi, 62 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Inteligência de Estado	2. *Big data analytics*
3. Fatores de risco	4. Engenharia de privacidade
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

RIBEIRO, M. M. (2023). *A atividade de Inteligência de Estado brasileira está em xeque com a promulgação da Emenda Constitucional n. 115/2022? Uma avaliação de riscos e impactos e proposta de uma agenda de soluções*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 62 p.

CESSÃO DE DIREITOS

AUTOR: Márcio da Mota Ribeiro
TÍTULO: A atividade de Inteligência de Estado brasileira está em xeque com a promulgação da Emenda Constitucional n. 115/2022? Uma avaliação de riscos e impactos e proposta de uma agenda de soluções.
GRAU: Mestre em Engenharia Elétrica ANO: 2023

Márcio da Mota Ribeiro
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Aos meus pais, José e Ermelinda, que sempre me incentivaram a estudar e a melhorar de vida por meio dos estudos; e à minha esposa, Alinne, que me apoiou, desde o início, na ideia de ingressar neste programa de mestrado profissional.

AGRADECIMENTOS

À Agência Brasileira de Inteligência (ABIN), por meio da Escola de Inteligência (Esint), e à Universidade de Brasília (UnB) por terem me proporcionado esta oportunidade de cursar o Mestrado Profissional na linha de pesquisa em Segurança Cibernética, com área de interesse em Lei Geral de Proteção de Dados Pessoais e em Inteligência de fontes abertas (*open source Intelligence* - Osint).

Aos meus professores orientadores, Doutores Rafael Rabelo Nunes e William Ferreira Giozza, pelos seus valiosos ensinamentos, e ao professor Doutor Alexandre Veronese pela sua colaboração com a minha pesquisa.

Especialmente, à minha família por me apoiarem em tudo que me proponho a desenvolver.

E a Deus, sempre.

RESUMO

Embora a Lei Geral de Proteção de Dados Pessoais (LGPD) estabeleça que suas disposições não são aplicáveis ao tratamento de dados pessoais realizados para fins exclusivos de segurança do Estado, as normas definidoras dos direitos e garantias fundamentais possuem aplicação imediata, razão pela qual o direito fundamental à proteção dos dados pessoais e a LGPD incidem na atividade de Inteligência de Estado e, em particular, nas aplicações de análise de grande volume de dados (*big data analytics*) utilizadas pelo serviço de Inteligência brasileiro para a produção da Inteligência de fontes abertas (*open source Intelligence* - Osint). Esta dissertação objetiva identificar os possíveis fatores de risco para a Inteligência de Estado decorrentes dessa incidência, analisar suas consequências e propor medidas para mitigá-los. O procedimento metodológico científico empregado foi a pesquisa aplicada, explicativa, bibliográfica e documental. Os principais resultados deste trabalho consistem na identificação dos possíveis fatores de risco, na sua análise e na proposição de medidas para mitigá-los, e na demonstração de que aquele direito fundamental pode ser limitado pela restrição constitucional do acesso a informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado. As principais contribuições desta dissertação são as sugestões para futuro anteprojeto de lei de proteção de dados pessoais para segurança do Estado e a proposta de como o órgão de Inteligência brasileiro poderia implementar a engenharia de privacidade no desenvolvimento de aplicações de *big data analytics* para produção da Osint.

Palavras-chave: Inteligência de Estado, *Big data analytics*, Fatores de risco, Engenharia de privacidade.

ABSTRACT

Although The General Personal Data Protection Law (LGPD) establishes that its provisions are not applicable to the processing of personal data carried out for exclusive purposes of State security, the rules that define fundamental rights and guarantees have immediate application, which is why the fundamental right to the protection of personal data and the LGPD affect the State Intelligence activity and, in particular, the analysis of big data (big data analytics) used by the Brazilian Intelligence service for the production of open source intelligence (Osint). This dissertation aims to identify the possible risk factors for State Intelligence arising from this fundamental right incidence, analyze their consequences and propose measures to mitigate them. The methodological scientific procedure used was applied, explanatory, bibliographical and documental research. The main results of this work consist in the identification of possible risk factors, in their analysis and proposition of measures to mitigate them, and in the demonstration that the fundamental right to the protection of personal data may be limited by the constitutional restriction on access to information, whose secrecy is essential to the security of society and of the State. The main contributions of this dissertation are suggestions for future draft law on the protection of personal data for State security and the proposal on how the Brazilian Intelligence Agency could implement privacy engineering in the development of big data analytics applications for the production of Osint.

Keywords: State Intelligence, Big data analytics, Risk factors, Privacy engineering.

SUMÁRIO

1 INTRODUÇÃO 1
1.1 PROBLEMA DE PESQUISA 3
1.2 HIPÓTESE 4
1.3 OBJETIVO GERAL 4
1.4 OBJETIVOS ESPECÍFICOS 4
1.5 PROCEDIMENTO METODOLÓGICO 5
1.6 PUBLICAÇÃO RESULTANTE DESTE TRABALHO 6
1.7 ESTRUTURA DA DISSERTAÇÃO 6

2 REVISÃO DA LITERATURA E DA LEGISLAÇÃO VIGENTE E SUA INTERPRETAÇÃO 7
2.1 RELAÇÃO ENTRE SEGURANÇA CIBERNÉTICA E PRIVACIDADE 7
2.2 INTELIGÊNCIA DE ESTADO BRASILEIRA 10
2.3 RECENTES DECISÕES DO STF SOBRE O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS 12
2.4 DEVIDO PROCESSO LEGAL, PRINCÍPIOS GERAIS DE PROTEÇÃO E DIREITOS DO TITULAR DOS DADOS PESSOAIS PREVISTOS NA LGPD 14
2.5 APLICAÇÕES DE BIG DATA ANALYTICS PARA PRODUÇÃO DA OSINT 15
2.6 OS SETE PRINCÍPIOS FUNDAMENTAIS DA ABORDAGEM PRIVACY BY DESIGN E A ENGENHARIA DE PRIVACIDADE 17
2.7 PRIVACY DESIGN STRATEGIES, TÁTICAS ASSOCIADAS, PRIVACY DESIGN PATTERNS E PRIVACY ENHANCING TECHNOLOGIES 18
2.8 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS 19

3 IDENTIFICAÇÃO E ANÁLISE DOS FATORES DE RISCO 21
3.1 FATORES DE RISCO OPERACIONAL 21
3.2 FATORES DE RISCO DE IMAGEM OU À REPUTAÇÃO 22
3.3 FATOR DE RISCO LEGAL 24
3.3.1 OBSERVÂNCIA DO DEVIDO PROCESSO LEGAL 24
3.3.2 OBSERVÂNCIA DOS PRINCÍPIOS GERAIS DE PROTEÇÃO 25
3.3.3 OBSERVÂNCIA DOS DIREITOS DOS TITULARES DOS DADOS PESSOAIS 28
3.4 FATORES DE RISCO FINANCEIRO OU ORÇAMENTÁRIO 29
3.5 RESUMO DOS FATORES DE RISCO IDENTIFICADOS 30
3.6 SUGESTÕES PARA FUTURO ANTEPROJETO DE LEI 34

4 PROPOSTA DE COMO A ABIN PODERIA IMPLEMENTAR A ENGENHARIA DE PRIVACIDADE . 36
4.1 MEDIDAS ADMINISTRATIVAS PARA IMPLEMENTAR OS PRINCÍPIOS FUNDAMENTAIS DA ABORDAGEM PRIVACY BY DESIGN 37
4.2 MEDIDAS TÉCNICAS PARA IMPLEMENTAR AS PRIVACY DESIGN STRATEGIES 42

5 CONCLUSÃO 50

REFERÊNCIAS BIBLIOGRÁFICAS 53

LISTA DE FIGURAS

2.1 As 5 categorias e as 21 KAs previstas no CyBOK 8
2.2 Relação entre riscos de segurança cibernética e riscos de privacidade 9
2.3 Ciclo de vida do sistema 19

LISTA DE TABELAS

2.1 Os 4 KAs da categoria Aspectos Humanos, Organizacionais e Regulatórios. 9

3.1 Resumo dos fatores de risco, das suas origens, das suas possíveis consequências e das medidas de mitigação propostas. 31

4.1 Correlação entre as medidas administrativas, os princípios e direitos previstos na LGPD e os fatores de risco..... 39

4.2 Correlação das *privacy design strategies* e das suas táticas com os princípios e direitos previstos na LGPD e com os fatores de risco. 43

4.3 Possíveis medidas técnicas para implementar as *privacy design strategies* na cadeia de valor de *big data analytics* e sua correlação com os fatores de risco..... 47

LISTA DE SIGLAS

Abin	Agência Brasileira de Inteligência
ADI	Ação Direta de Inconstitucionalidade
ADPF	Arguição de Descumprimento de Preceito Fundamental
AEPD	*Agencia Española de Protección de Datos* (Agência Espanhola de Proteção de Dados)
ANPD	Autoridade Nacional de Proteção de Dados
BND	*Bundesnachrichtendienst* (Serviço Federal de Inteligência)
BOK	*Body of Knowledge* (Corpo de Conhecimento)
Cepesc	Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações
CIA	*Central Intelligence Agency* (Agência Central de Inteligência)
CGU	Controladoria-Geral da União
CyBOK	*The Cyber Security Body of Knowledge* (Corpo de Conhecimentos de Segurança Cibernética)
DPIA	*Data Protection Impact Assessment* (avaliação do impacto sobre a proteção de dados)
EDPB	*European Data Protection Board* (Conselho Europeu de Proteção de Dados)
EDPS	*European Data Protection Supervisor* (Supervisor Europeu de Proteção de Dados)
Enint	Estratégia Nacional de Inteligência
Enisa	*European Union Agency for Cybersecurity* (Agência da União Europeia para Segurança Cibernética)
EPRS	*European Parliamentary Research Service* (Serviço de Estudos do Parlamento Europeu)
Europol	*European Union Agency for Law Enforcement Cooperation* (Agência da União Europeia para a Cooperação Policial)
Fisa	*Foreign Intelligence Surveillance Act* (Lei de Vigilância de Inteligência Estrangeira)
FRF-1	Primeiro fator de risco financeiro ou orçamentário
FRF-2	Segundo fator de risco financeiro ou orçamentário
FRF-3	Terceiro fator de risco financeiro ou orçamentário
FRI-1	Primeiro fator de risco de imagem ou à reputação
FRI-2	Segundo fator de risco de imagem ou à reputação
FRI-3	Terceiro fator de risco de imagem ou à reputação
FRL-1	Primeiro fator de risco legal
FRL-2	Segundo fator de risco legal
FRO-1	Primeiro fator de risco operacional
FRO-2	Segundo fator de risco operacional
FRO-3	Terceiro fator de risco operacional
GB	Reino Unido
GDPR	*General Data Protection Regulation* (Regulamento Geral de Proteção de Dados)
GPA	*Global Privacy Assembly* (Assembleia Global de Privacidade)

LISTA DE SIGLAS

IBGE	Instituto Brasileiro de Geografia e Estatística
ICO	*Information Commissioner's Office* (Gabinete do Comissário de Informação)
IEC	*International Electrotechnical Commission* (Comissão Eletrotécnica Internacional)
ISO	*International Organization for Standardization* (Organização Internacional para Padronização)
KA	*Knowledge Area* (área de conhecimento)
KAs	*Knowledge Areas* (áreas de conhecimento)
LGPD	Lei Geral de Proteção de Dados Pessoais
MI5	*Military Intelligence, Section 5* (Inteligência Militar, Seção 5)
MI6	*Military Intelligence, Section 6* (Inteligência Militar, Seção 6)
MP	Ministério do Planejamento, Orçamento e Gestão
MPV	Medida Provisória
NCSC	*National Cyber Security Centre* (Centro Nacional de Segurança Cibernética)
NDPA	*Norwegian Data Protection Authority* (Autoridade Norueguesa de Proteção de Dados)
Nist	*National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia)
NSA	*National Security Agency* (Agência de Segurança Nacional)
OECD	*The Organisation for Economic Co-operation and Development* (Organização para Cooperação e Desenvolvimento Econômico)
Osint	*Open source Intelligence* (Inteligência de fontes abertas)
PNI	Política Nacional de Inteligência
RGPD	Regulamento Geral de Proteção de Dados
RIPD	Relatório de impacto à proteção de dados pessoais
Sisbin	Sistema Brasileiro de Inteligência
STF	Supremo Tribunal Federal
UE	União Europeia
UNB	Universidade de Brasilia
WP29	*Article 29 Data Protection Working Party* (Grupo de Trabalho de Proteção de Dados do Artigo 29)

1 INTRODUÇÃO

Estima-se que oitenta a noventa por cento dos dados tratados pelos serviços de Inteligência sejam oriundos de fontes públicas ou abertas [1]. As plataformas online de redes sociais produzem diariamente uma enorme quantidade de dados de fontes abertas de interesse da atividade de Inteligência [2]. Por isso, no contexto de grandes volumes de dados (*big data*), a Inteligência precisa utilizar aplicações de análise de grande volume de dados (*big data analytics*) para a produção da Inteligência de fontes abertas (*open source Intelligence* - Osint).

A propósito, Osint é o produto da análise de informações disponíveis em fontes abertas e um importante método de coleta de dados e informações, haja vista que, quando combinada com alta tecnologia, é capaz de contribuir para uma parcela significativa das necessidades dos serviços de Inteligência, sendo considerada a técnica de coleta de Inteligência menos intrusiva [3].

Por conta da relevância dos dados disponíveis em fontes abertas para a atividade de Inteligência de Estado, os serviços de Inteligência, inclusive a Agência Brasileira de Inteligência (Abin), têm intensificado o uso de inteligência artificial e de técnicas de *big data analytics*, o que tem ensejado oportunidades para a atividade de Inteligência produzir conhecimentos diferenciados, capazes de promover resultados mais efetivos, por meio da utilização de aplicações para análise de vínculos, entendimento de contextos e localização de pessoas e de lugares [4].

Por outro lado, as aplicações de *big data analytics* trazem consigo vários desafios de privacidade e de proteção de dados, haja vista que a facilidade de acesso aos dados pessoais disponíveis em bancos de dados informatizados, somada à velocidade com que esses dados são acessados, transmitidos e combinados, potencializa as possibilidades de afetação de direitos fundamentais das pessoas naturais, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social [5].

Nesse contexto, é preciso garantir um equilíbrio adequado entre a disponibilidade e a segurança durante todo o tratamento realizado nos dados obtidos por meio de aplicações de *big data analytics* [6]. Para minimizar o risco das violações de dados decorrentes da utilização de tecnologias intrusivas, enfatizou-se a criação de legislações de proteção de dados, para preservar a segurança da informação e defender a privacidade [7]. No Brasil, foi criada a Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), que fornece fundamento legal para o tratamento de dados pessoais, segurança jurídica para controladores e operadores e bases claras para a proteção e garantia do direito fundamental à proteção de dados, reduzindo riscos à privacidade em todo o ciclo de vida do dado pessoal, que vai desde a coleta até o seu descarte, englobando diversas fases que devem ser desenvolvidas em conformidade com essa norma [8].

De acordo com a LGPD [9], controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; e agentes de tratamento são o controlador e o operador.

A LGPD regulamenta o tratamento de dados pessoais e objetiva proteger os direitos fundamentais de

liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Segundo o art. 5º, inciso V, dessa lei, tratamento é qualquer operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, modificação, comunicação, transferência e difusão [9]. Os dados pessoais são, em princípio, as informações tratadas previamente, ou não, de caráter personalíssimo caracterizadas pela identificabilidade e pela possibilidade de determinação do seu titular. Além deles, cabe indicar a classificação jurídica dos dados sensíveis, que são caracterizados pela possibilidade de serem utilizados de modo discriminatório, afetando diretamente a pessoa humana. Exemplos são os dados genéticos e biométricos, bem como aqueles dados que versam sobre a saúde da pessoa, sua origem racial e étnica, suas convicções políticas, ideológicas, religiosas, além de sua orientação sexual [10].

A personalidade de um indivíduo pode ser gravemente violada com a divulgação não autorizada de informações armazenadas a seu respeito [11]. Isso porque os dados pessoais traduzem aspectos únicos e revelam comportamentos e preferências, permitindo até mesmo formar um perfil psicológico e uma imagem detalhada da pessoa, inclusive na esfera da intimidade [12]. Por isso, a LGPD representa um grande avanço do ordenamento jurídico brasileiro no que diz respeito à proteção dos direitos e liberdades fundamentais relacionados com a privacidade dos titulares de dados pessoais.

Trata-se de uma lei geral nacional, de observância obrigatória tanto por particulares quanto pela União, pelos Estados, pelo Distrito Federal e pelos Municípios. Essa norma é aplicável a qualquer operação de tratamento de dados pessoais realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio (físico ou digital), do país no qual os agentes de tratamento estão sediados, ou do país em que estejam localizados os dados pessoais dos titulares protegidos [9]. Por outro lado, a própria LGPD relaciona, nos incisos I a IV do *caput* do art. 4º, uma série de hipóteses nas quais o tratamento de dados pessoais não se submete a essa lei. Essas exceções à aplicabilidade da LGPD são justificadas por um direito fundamental (liberdade de informação, no caso da finalidade jornalística, por exemplo) ou por um interesse público relevante (segurança pública e defesa nacional) e não comprometem a integridade da lei caso exista legislação específica sobre proteção de dados pessoais que compreenda os princípios da LGPD [11].

Há que se mencionar especificamente o conteúdo do art. 4º, inciso III, da LGPD, que excepciona a aplicabilidade dessa lei para o tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais. Apesar dessa exceção, o art. 4º, § 1º, da LGPD determina que o tratamento de dados pessoais, nessas hipóteses, será regido por legislação específica que preverá medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD [9]. Essas exceções objetivam garantir o interesse público de combater infrações penais, crime organizado, fraude digital, ou até mesmo terrorismo [13]. Esse ponto é muito importante para a presente dissertação, uma vez que justifica que tais operações de tratamento de dados pessoais, ainda que feito nessas hipóteses, se submetem à LGPD, em alguma medida.

O tratamento de dados pessoais realizado pela Abin no exercício da atividade de Inteligência de Estado possui finalidade exclusiva de segurança do Estado e se enquadra na exceção prevista no inciso III, alínea "c", do art. 4º da LGPD. Isso fica claro, porque esse órgão de Inteligência possui as competências legais

de “planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade” e de “avaliar as ameaças, internas e externas, à ordem constitucional” [14]. Uma interpretação literal do art. 4º, *caput*, inciso III, alínea “c”, e § 1º, da LGPD poderia levar a concluir que, até a entrada em vigor da legislação específica, aquela lei geral seria integralmente inaplicável às operações de tratamento de dados pessoais realizadas pela Abin no exercício da atividade de Inteligência, com finalidade exclusiva de segurança do Estado.

Ocorre que, durante a vacância ou *vacatio legis* da LGPD, período compreendido entre a data da publicação de uma lei e o início de sua vigência, o Supremo Tribunal Federal (STF) proferiu decisões reconhecendo que a proteção de dados pessoais é um direito fundamental autônomo, implícito na Constituição Federal e decorrente da garantia da inviolabilidade da intimidade e da vida privada e do princípio da dignidade da pessoa humana [15], [16]. Além disso, a Emenda Constitucional nº. 115, de 10 de fevereiro de 2022, incluiu no texto constitucional a proteção de dados pessoais entre os direitos e garantias fundamentais, com a seguinte redação: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” [17]. Por fim, o STF decidiu, em 15 de setembro de 2022, que o compartilhamento de informações pessoais em atividades de Inteligência observará o disposto em legislação específica e os parâmetros fixados no julgamento da Ação Direta de Inconstitucionalidade (ADI) nº 6.529, dentre os quais destaca-se a “observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal” [18], [19].

Consequentemente, pelo fato de as normas definidoras dos direitos e garantias fundamentais terem aplicação imediata [20], o direito fundamental à proteção dos dados pessoais e, por conseguinte, os princípios gerais de proteção e os direitos do titular previstos na LGPD devem ser observados pela Abin, no que forem compatíveis com o exercício da atividade de Inteligência de Estado, inclusive em relação à utilização de aplicações de *big data analytics* para produção da Osint, mesmo diante da exceção prevista expressamente na LGPD e da ausência da legislação específica mencionada no art. 4º, § 1º, dessa lei.

A propósito, a norma de direito fundamental, por ter aplicabilidade direta, possui presunção de ser sempre também de eficácia plena, ou seja, de não ser completamente dependente de uma prévia regulamentação legal para gerar, desde logo, seus principais efeitos. Essa é a razão jurídica pela qual eventual ausência de lei infraconstitucional não pode servir de obstáculo absoluto à aplicação da norma de direito fundamental e da extração de efeitos úteis, cuja extensão dependerá do direito em causa e de seus limites fáticos e jurídicos, principalmente em relação à dedução de posições subjetivas [21].

1.1 PROBLEMA DE PESQUISA

A problemática a ser tratada nesta dissertação é a aplicabilidade do direito fundamental à proteção dos dados pessoais e de alguns dispositivos da LGPD na atividade de Inteligência da Abin e nas aplicações de *big data analytics* utilizadas pelo serviço de Inteligência brasileiro para a produção da Osint e as consequências dessa incidência. Isso será exposto e analisado, mesmo diante da exceção prevista expressamente na LGPD e da ausência de uma legislação específica que normalize o tratamento de dados pessoais realizado para fins exclusivos de segurança do Estado.

Por conseguinte, este trabalho procura responder à seguinte pergunta: *quais fatores de risco para a Abin podem decorrer da incidência do direito fundamental e da LGPD na atividade de Inteligência de Estado e nas aplicações de "big data analytics"utilizadas por esse órgão para a produção da Osint*?

1.2 HIPÓTESE

Como resposta do problema de pesquisa, este trabalho formula a hipótese de que se o direito fundamental à proteção dos dados pessoais – pelo acima exposto – e a LGPD incidem na atividade de Inteligência da Abin, inclusive nas aplicações de *big data analytics* utilizadas por esse órgão para a produção da Osint, então poderão decorrer para o serviço de Inteligência brasileiro fatores de risco com potencial de impactar o cumprimento de sua missão institucional.

1.3 OBJETIVO GERAL

Este trabalho objetiva identificar os possíveis fatores de risco decorrentes da incidência do direito fundamental à proteção de dados pessoais e de alguns dispositivos da LGPD na atividade de Inteligência da Abin, inclusive nas aplicações de *big data analytics* utilizadas pelo serviço de Inteligência brasileiro para a produção da Osint, analisar as consequências dos fatores de risco identificados e propor medidas para mitigá-los.

Cumpre esclarecer que este trabalho não tratará dos fatores de risco para os demais órgãos integrantes do Sistema Brasileiro de Inteligência (Sisbin), considerando que a maioria deles não se enquadra plenamente na exceção prevista no art. 4º, *caput*, inciso III, alínea "c", da LGPD. Com efeito, esses órgãos possuem unidades de Inteligência de atuação eminentemente administrativa, como a Controladoria-Geral da União e as agências reguladoras, que desenvolvem atividade de Inteligência como um instrumento de gestão [22] e, por isso, geralmente não tratam dados pessoais para fins exclusivos de segurança do Estado.

1.4 OBJETIVOS ESPECÍFICOS

Com o objetivo geral proposto, os objetivos específicos foram definidos e cumpridos, quais sejam:

a) demonstrar que o direito fundamental à proteção de dados pessoais pode ser limitado pela restrição constitucional do acesso a informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

b) apresentar sugestões para futuro anteprojeto de lei de proteção de dados pessoais para segurança do Estado; e

c) apresentar proposta de como a Abin poderia implementar a engenharia de privacidade no desenvolvimento de aplicações de *big data analytics* para produção da Osint, ainda na fase de concepção dessas

aplicações, com o intuito de compatibilizar o uso dessa técnica analítica pelo órgão de Inteligência brasileiro com o direito fundamental à proteção de dados pessoais.

1.5 PROCEDIMENTO METODOLÓGICO

O procedimento metodológico empregado nesta dissertação foi a realização de pesquisa de natureza aplicada, com propósitos explicativos e com utilização de procedimentos técnicos bibliográficos e documentais. A pesquisa de natureza aplicada objetiva adquirir conhecimentos científicos já assentados – explicações racionais sobre os fenômenos – para, depois, aplicá-los em situações específicas, sempre em consonância com o conhecimento científico sedimentado nos resultados oferecidos pelos estudos explicativos [23]. Já a pesquisa explicativa é a mais complexa e completa, por analisar os dados e buscar suas causas e explicações, ou seja, os fatores determinantes desses dados [24]. O procedimento técnico bibliográfico permite ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente [23] e consiste no estudo de artigos, teses, livros e outras publicações usualmente disponibilizadas por editoras e indexadas, sendo um passo fundamental e prévio para qualquer trabalho científico [24]. Por sua vez, o procedimento técnico documental abrange a pesquisa em uma variedade de documentos, elaborados com finalidades diversas, sendo bastante amplo o conceito de documento, que pode ser qualquer objeto capaz de comprovar algum fato ou acontecimento [23].

O delineamento ou planejamento da pesquisa bibliográfica realizada para a elaboração deste trabalho seguiu as etapas propostas por [23]. Inicialmente, procedeu-se à escolha do tema, a partir do conhecimento do autor na área de estudo; em seguida, realizou-se levantamento bibliográfico preliminar, para subsidiar a formulação do problema, de maneira clara, precisa e suficientemente delimitada. Na sequência, foi elaborado o plano provisório da pesquisa, que definiu a estrutura lógica do trabalho e um conjunto de seções ordenadas em itens. Na etapa seguinte foram identificadas e localizadas as fontes bibliográficas capazes de fornecer as respostas adequadas à solução do problema proposto, tendo sido consultados artigos científicos disponíveis nas bases de dados Google Acadêmico e Portal de Periódicos da CAPES e livros físicos e eletrônicos (*e-books*). A busca nessas bases foi realizada combinando as seguintes palavras-chave ou descritores essenciais para o desenvolvimento deste trabalho: "direito fundamental à proteção dos dados pessoais", "*big data*", "atividade de Inteligência", "lei geral de proteção de dados", "*data privacy*", "*privacy by design*", "*privacy-enhancing technologies*", "*big data analytics*", "*data protection*", "*open source Intelligence*", "*privacy engineering*", "relatório de impacto à proteção dos dados pessoais" e "*privacy design strategies*". Após a obtenção do material de interesse para a pesquisa, procedeu-se à sua leitura; à tomada de apontamentos; ao fichamento; à construção lógica do trabalho, que consiste na organização das ideias com o intuito de atender aos objetivos da pesquisa; e, finalmente, à redação da dissertação.

Já a pesquisa documental foi realizada na Internet, para localizar legislação sobre proteção de dados pessoais e sobre atividade de Inteligência, recentes decisões do STF acerca do direito fundamental à proteção de dados pessoais, informações referentes à estrutura e às peculiaridades da Abin e estudos de agências governamentais brasileiras e de outros países sobre os temas tratados neste trabalho.

Os possíveis fatores de risco decorrentes da aplicação do direito fundamental à proteção de dados

pessoais e da LGPD na atividade de Inteligência de Estado e nas aplicações de *big data analytics* utilizadas pela Abin para a produção da Osint foram identificados e analisados por meio de análise documental e comparativa, levando-se em consideraçao recentes decisões do STF sobre esse direito fundamental, da legislação brasileira interpretada, do direito comparado, de estudos de agências governamentais brasileiras e de outros países e de artigos científicos sobre o assunto.

Cumpre ressaltar que este trabalho não versa sobre as operações de tratamento de dados pessoais que não estejam relacionadas com o exercício da atividade de Inteligência de Estado. O objetivo desta dissertação também não visa mapear e avaliar todos os riscos possíveis, mesmo que não conhecidos. Para delimitar e sistematizar os fatores de risco identificados, utilizou-se a tipologia prevista no art. 18 da Instrução Normativa Conjunta MP/CGU (Ministério do Planejamento, Orçamento e Gestão e Controladoria-Geral da União) nº 1, de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Essa norma classifica os riscos em:

> a) riscos operacionais: eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;
>
> b) riscos de imagem/reputação do órgão: eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional;
>
> c) riscos legais: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade; e
>
> d) riscos financeiros/orçamentários: eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações [25].

Os dados foram coletados no período de 1º de fevereiro de 2021 a 30 de março de 2023.

1.6 PUBLICAÇÃO RESULTANTE DESTE TRABALHO

Publicação de [26], artigo científico intitulado "Inteligência de Estado, aplicações de *big data analytics* e o direito fundamental à proteção de dados pessoais", nos anais do V Congresso de Gestão de Operações e Projetos em Organizações Públicas, realizado no período de 29 a 31 de agosto de 2022, na Universidade de Brasília, em Brasília/DF.

1.7 ESTRUTURA DA DISSERTAÇÃO

O restante desta dissertação está organizado da seguinte maneira: o Capítulo 2 apresenta uma revisão da literatura, da legislação e da sua intepretação; o Capítulo 3 identifica os fatores de risco, analisa as suas consequências e propõe medidas para mitigá-los, e, ainda, apresenta sugestões para futuro anteprojeto de lei de proteção de dados pessoais para segurança do Estado; e o Capítulo 4 propõe como a Abin poderia implementar a engenharia de privacidade no desenvolvimento de aplicações de *big data analytics* para produção da Osint, ainda na fase de sua concepção. Finalmente, o Capítulo 5 apresenta as conclusões deste trabalho.

2 REVISÃO DA LITERATURA E DA LEGISLAÇÃO VIGENTE E SUA INTERPRETAÇÃO

Nas Seções seguintes é apresentado o referencial teórico necessário para o entendimento dos assuntos abordados neste trabalho.

2.1 RELAÇÃO ENTRE SEGURANÇA CIBERNÉTICA E PRIVACIDADE

Embora haja uma série de iniciativas para estabelecer estruturas de habilidades, áreas-chave e diretrizes curriculares para a segurança cibernética, ainda não há um consenso sobre o que pesquisadores, educadores e profissionais entendem como conhecimento fundamental estabelecido nesse campo. Uma dessas iniciativas é o Corpo de Conhecimento de Segurança Cibernética (*The Cyber Security Body of Knowledge* – CyBOK), projeto financiado pelo Programa Nacional de Segurança Cibernética no Reino Unido (*National Cyber Security Programme in the UK*) e que visa codificar o conhecimento fundamental e geralmente reconhecido sobre segurança cibernética, para que possam ser desenvolvidos, com base no CyBOK, programas educacionais em segurança cibernética que vão desde o ensino secundário e de graduação até programas de pós-graduação e desenvolvimento profissional contínuos [27].

O CyBOK é utilizado pelo Centro Nacional de Segurança Cibernética do Reino Unido (*National Cyber Security Centre* - NCSC) como base de sua certificação de programas de graduação e pós-graduação em segurança cibernética no Reino Unido, viabilizando a criação de um cenário educacional em que tanto amplos cursos gerais de segurança cibernética quanto programas especializados nessa área atendam às necessidades de alunos e empregadores [28].

Um Corpo de Conhecimento (*Body of Knowledge* - BOK) se refere à totalidade dos fatos, crenças atuais ou entendimentos, conceitos e práticas de um domínio acadêmico ou profissional e geralmente é dividido em áreas de conhecimento (*Knowledges Areas* - KAs) e subáreas ou tópicos (denominados unidades de conhecimento em alguns currículos) [29]. Atualmente o CyBOK é dividido em 21 KAs de alto nível, agrupadas em cinco categorias amplas, conforme Figura 2.1. As categorias pretendem captar o conhecimento relacionado à segurança cibernética no projeto de *hardware* e *software*, ou em diversas outras áreas, como o Direito [27].

Além disso, o CyBOK reconhece que há crescente preocupação quanto à privacidade e à potencial utilização abusiva dos dados pessoais, razão pela qual sustenta que os projetistas devem considerar as implicações de segurança e privacidade desde a concepção e ao longo de todo ciclo de vida de sistemas e infraestruturas conectados em larga escala [27]. De fato, as organizações responsáveis pelo gerenciamento de dados pessoais não podem escapar da obrigação de implementar requisitos compatíveis com as leis e regulamentos de privacidade [30].

Segundo Barret [31], privacidade e segurança cibernética possuem uma forte conexão, uma vez que

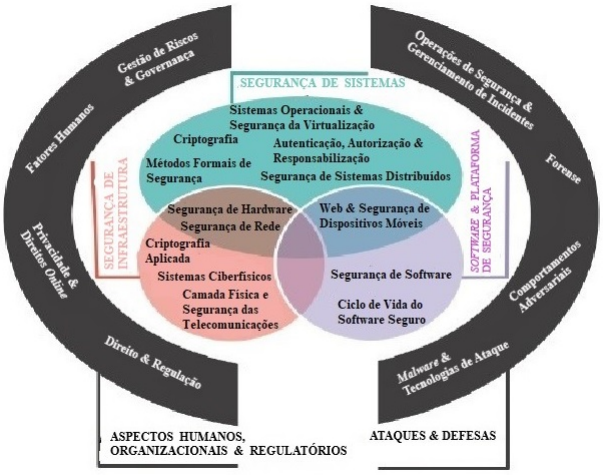

Figura 2.1: As 5 categorias e as 21 KAs previstas no CyBOK

Fonte: Adaptado de Cybok.org [27]

as atividades de segurança cibernética de uma organização também podem criar riscos à privacidade e às liberdades civis quando dados pessoais são usados, coletados, processados, armazenados ou divulgados. Isso pode ocorrer, por exemplo, quando resultarem dessas atividades a coleta ou retenção excessiva de dados pessoais. Por esse motivo, para mitigar as implicações de privacidade, referido autor recomenda que as organizações considerem em seu programa de segurança cibernética a incorporação de princípios de privacidade como: minimização de dados na coleta, divulgação e retenção de material contendo dados pessoais relacionado ao incidente de segurança cibernética; transparência para certas atividades de segurança cibernética; consentimento individual e reparação por impactos adversos decorrentes do uso de dados pessoais em atividades de segurança cibernética; qualidade, integridade e segurança dos dados; e prestação de contas e auditoria.

De acordo com o *National Institute of Standards and Technology* (Nist) [32], o gerenciamento do risco de segurança cibernética contribui para o gerenciamento do risco de privacidade, mas isso não é suficiente, haja vista que os riscos de privacidade também podem surgir de fontes não relacionadas aos incidentes de segurança cibernética. Por esse motivo, esse instituto considera os eventos de privacidade como sendo problemas potenciais que podem afetar os titulares dos dados pessoais e que são decorrentes de operações de sistema, produtos ou serviços contendo dados pessoais, seja em formato digital ou não digital, desde a coleta desses dados até o seu descarte. A relação entre riscos de segurança cibernética e riscos de privacidade é apresentada na Figura 2.2.

Nesse sentido, Stallings [33] explica que reconhecer os limites e sobreposições entre privacidade e segurança é fundamental para determinar quando os modelos de risco de segurança existentes e as orientações focadas em segurança podem ser aplicados para endereçar questões de privacidade, e quando há lacunas que precisam ser preenchidas a fim de alcançar uma abordagem de engenharia de privacidade.

A presente dissertação de mestrado profissional segue a linha de pesquisa Segurança e Inteligência Cibernética (área de concentração: segurança cibernética) e aborda algumas das áreas de interesse previstas em [34], edital de seleção de candidatos às vagas do Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE) da Universidade de Brasília (UnB) para turma específica do curso de Mestrado

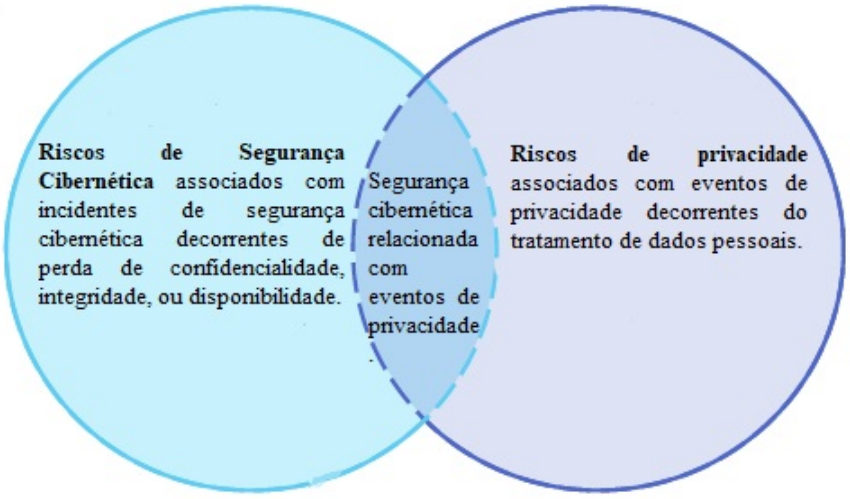

Figura 2.2: Relação entre riscos de segurança cibernética e riscos de privacidade

Fonte: Adaptado do Nist [32]

Profissional em Engenharia Elétrica, área de concentração em Segurança Cibernética, ingresso no segundo semestre letivo de 2020, em conformidade com termo de execução descentralizada celebrado entre a UnB e a Abin em 2019.

Além de adotar a referida linha de pesquisa, este trabalho compreende as seguintes áreas de interesse previstas em [34]: análise de grande volume de dados; Inteligência Artificial aplicada à análise de dados; Osint; análise de risco; LGPD e suas implicações na área cibernética; e privacidade dos dados.

Em relação ao CyBOK, esta dissertação pode ser enquadrada na categoria "Aspectos Humanos, Organizacionais e Regulatórios", por abordar os KAs "Gerenciamento de Riscos e Governança"; "Direito e Regulação"; "Fatores Humanos"; e "Privacidade e Direitos *Online*". Um resumo dessa categoria e de seus KAs respectivos é apresentada na Tabela 2.1.

Tabela 2.1: Os 4 KAs da categoria Aspectos Humanos, Organizacionais e Regulatórios.

Categoria: Aspectos Humanos, Organizacionais e Regulatórios	
KAs	**Descrição**
1. Gerenciamento de riscos e Governança	Sistemas de gerenciamento de segurança e controles de segurança organizacional, incluindo padrões, melhores práticas, e abordagens para avaliação e mitigação de riscos.
2. Direito e regulação	Requisitos estatutários e regulamentares internacionais e nacionais, obrigações de conformidade e segurança ética, incluindo proteção de dados e desenvolvimento de doutrinas sobre guerra cibernética.
3. Fatores humanos	Segurança utilizável, fatores sociais e comportamentais que afetam a segurança, a cultura de segurança e a conscientização também como o impacto dos controles de segurança no comportamento do usuário

4. Privacidade e direitos *on-line*	Técnicas para proteger informações pessoais, incluindo comunicações, aplicativos e inferências de bancos de dados e processamento de dados. Também inclui outros sistemas de suporte a direitos *on-line.*

Fonte: Adaptado de Cybok.org [27] .

Com efeito, esta dissertação abrange todas as quatro KAs descritas na Tabela 2.1, haja vista que, a partir da análise da LGPD e do direito fundamental à proteção de dados pessoais (KA "Direito e Regulação"), foram identificados os possíveis fatores de risco decorrentes da aplicação desse direito fundamental e dessa lei na atividade de Inteligência da Abin e nas aplicações de *big data analytics* utilizadas pelo serviço de Inteligência brasileiro para a produção da Osint, analisadas suas consequências e sugeridas medidas para mitiga-los (KAs "Gerenciamento de Riscos e Governança" e "Privacidade e Direitos *Online*"); foram apresentadas sugestões para futuro anteprojeto de lei de proteção de dados pessoais para segurança do Estado (KA "Direito e Regulação"); e foi apresentada proposta de como a Abin poderia implementar a engenharia de privacidade no desenvolvimento dessas aplicações, ainda em sua fase de concepção, incluindo a adoção de medidas administrativas ou organizacionais que abrangem a KA "Fatores Humanos", a exemplo do compromisso claro da organização quanto à proteção dos dados pessoais, promovido desde os mais altos níveis da Administração; do desenvolvimento de uma cultura de comprometimento e melhoria contínua em relação à privacidade envolvendo todos os trabalhadores; e da definição e atribuição de responsabilidades para que cada membro da organização esteja ciente de suas tarefas para preservar a privacidade.

2.2 INTELIGÊNCIA DE ESTADO BRASILEIRA

A Inteligência de Estado brasileira foi estruturada pela Lei nº 9.883/1999, que criou a Abin e o Sisbin, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional. Consoante Lei nº 9.883/1999, poderão ingressar no Sisbin os órgãos e as entidades da Administração Pública Federal que, direta ou indiretamente, possam produzir conhecimentos de interesse da atividade de Inteligência. Órgãos das demais unidades da Federação também poderão fazer parte desse sistema, mediante ajustes específicos e convênios, ouvido o órgão de controle externo da atividade de Inteligência [14], que é a Comissão Mista de Controle das Atividades de Inteligência, comissão permanente do Congresso Nacional [35]. Atualmente, o Sisbin é composto por quarenta e oito órgãos públicos federais para o compartilhamento de informações e conhecimentos de Inteligência [36].

A atividade de Inteligência de Estado é uma política pública consubstanciada no Decreto nº 8.793, de 29 de junho de 2016, que fixou a Política Nacional de Inteligência (PNI), com previsão legal no art. 5º da Lei nº 9.883/1999, segundo o qual "a execução da Política Nacional de Inteligência, fixada pelo Presidente da República, será levada a efeito pela ABIN, sob a supervisão da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo" [14]. A PNI define atividade de Inteligência como

> o exercício permanente de ações especializadas, voltadas para a produção e difusão de conhecimentos, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planeja-

mento, a execução, o acompanhamento e a avaliação das políticas de Estado [37].

De maneira sintética, a Estratégia Nacional de Inteligência (Enint), aprovada pelo Decreto de 15 de dezembro de 2017, atribuiu à Atividade de Inteligência a competência de acompanhar o ambiente interno e externo, com o propósito de identificar oportunidades e possíveis ameaças e riscos aos interesses do Estado e à sociedade brasileira [4].

A Abin ocupa a posição de órgão central do Sisbin e possui as competências legais de avaliar as ameaças, internas e externas, à ordem constitucional, de planejar e de executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade, bem como de obter e analisar dados para produção de conhecimentos sobre esses assuntos. Essas competências são exercidas com o intuito de assessorar o Presidente da República [14]. Logo, o tratamento de dados pessoais realizado pela Abin, no exercício da atividade de Inteligência, possui finalidade exclusiva de segurança do Estado. Por força da aplicação imediata dos direitos e garantias individuais, o direito fundamental à proteção de dados pessoais e a LGPD incidem sobre esse tratamento, mesmo diante da exceção prevista no art. 4º, inciso III, alínea "c", dessa lei, como já explicado.

A Abin possui em sua estrutura o Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (Cepesc), departamento de tecnologia que desenvolve programas e ferramentas com a finalidade de garantir o sigilo e a transmissão segura das informações e das comunicações governamentais, por meio da criação e utilização da criptografia de Estado, que consiste em algoritmos desenvolvidos no Brasil por órgão governamental para garantir a privacidade dos dados transmitidos [38].

Dentre as competências regimentais do Cepesc, destacam-se: realizar pesquisas em tecnologia da informação e comunicação, inteligência cibernética, criptologia e segurança cibernética, de informações, de comunicações e de dados; desenvolver soluções de tecnologia da informação e de comunicações, para uso no âmbito da Abin, do Sistema Brasileiro de Inteligência e da administração pública federal; planejar e executar a gestão da infraestrutura e dos serviços de tecnologia da informação e comunicações; conduzir a seleção, a aquisição e a implementação de soluções de terceiros de tecnologia da informação e de comunicações, para uso no âmbito da Abin, do Sistema Brasileiro de Inteligência e da administração pública federal; planejar e executar atividades de inteligência em matéria cibernética, de tecnologia e de segurança da informação e das comunicações; e promover a cooperação em inteligência cibernética com instituições nacionais e estrangeiras [39].

Para exercer adequadamente suas competências regimentais, o Cepesc conta com agentes públicos qualificados que seriam capazes de desenvolver para a Abin aplicações de *big data analytics* para produção da Osint. Recentemente, os servidores do Cepesc desenvolveram a *libharpia*, biblioteca criptográfica com suporte a algoritmos pós-quânticos que foi implementada em urnas eletrônicas utilizadas nas eleições brasileiras de 2022 [40]. A criptografia pós-quântica permite criptografar dados sensíveis, incluindo dados pessoais, para protegê-los contra um ataque criptoanalítico promovido por meio de um computador quântico [41].

2.3 RECENTES DECISÕES DO STF SOBRE O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

A LGPD foi publicada no Diário Oficial da União de 15 de agosto de 2018. Porém, a maioria dos seus dispositivos entrou em vigor em 18 de setembro de 2020. Cabe ressaltar, inclusive, que somente em 1º de agosto de 2021 tiveram vigência os artigos que tratam das sanções que podem ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), entidade responsável por zelar, implementar e fiscalizar o cumprimento dessa lei geral em todo o território nacional. A ANPD tem se corporificado paulatinamente. A mais recente mudança foi a edição da Lei nº 14.460, de 25 de outubro de 2022, por meio da qual lhe foi atribuída a categoria de autarquia de natureza especial [42], como uma forma de reforçar sua autonomia.

Em 2020, durante a *vacatio legis* da LGPD, o STF proferiu três acórdãos relacionados com tratamentos e proteção de dados pessoais. No primeiro acórdão, referente ao julgamento do Referendo na Medida Cautelar na ADI nº 6.387 [15], o STF se manifestou pela primeira vez sobre o direito fundamental à proteção de dados pessoais e a sua tutela constitucional [43], reconhecendo a existência desse direito fundamental autônomo que possui âmbito de proteção distinto ao do direito à privacidade [44]. O argumento central é que o bem jurídico sob a proteção de dados pessoais é mais amplo do que a privacidade, na medida em que engloba vários componentes da dignidade da pessoa humana, tais como a integridade física e moral, a igualdade, as liberdades em geral, além da personalidade da pessoa e a própria privacidade [45]. Com esse acórdão, o STF aderiu ao entendimento predominante na literatura jurídica brasileira de que a Constituição Federal consagrou um direito fundamental à proteção de dados pessoais implicitamente positivado, vinculado diretamente à proteção da personalidade e obtido por meio da leitura harmônica e sistemática do texto constitucional [44].

Nesse julgamento, o Plenário do STF referendou medida cautelar para suspender a eficácia da Medida Provisória (MPV) nº 954/2020. Essa MPV previa a obrigatoriedade de as empresas de telecomunicações prestadoras de serviço telefônico fixo comutado e de serviço móvel pessoal compartilharem com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), em meio eletrônico, os nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas, para auxiliar a produção estatística oficial durante a pandemia decorrente da Covid-19. O STF reconheceu que o tratamento dos dados das pessoas naturais, incluída a operação de compartilhamento, deve observar as garantias constitucionais da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). O texto da MPV nº 954/2020 violaria esses direitos [15]. O ponto nodal é visualizar que, antes do advento da LGPD, o STF reconheceu direitos como a autodeterminação informativa, positivado no art. 2º, II, dessa Lei, além de indicar que essa proteção decorre dos direitos da personalidade.

No segundo acórdão, proferido no julgamento da Medida Cautelar na ADI nº 6.529, o STF reafirmou que a proteção de dados pessoais é um direito fundamental autônomo na ordem constitucional brasileira, especialmente como projeção alargada do direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas [16]. Ressalte-se que os direitos fundamentais se caracterizam pelo atributo da abertura ou inexauribilidade, que consiste na possibilidade de reconhecimento de outros direitos fundamentais, diante do advento de novas preocupações específicas [45]. Ademais, a condição de direito fundamental autônomo não dependeria da inserção do direito à proteção de dados pessoais no texto da Constituição Fe-

deral, por se tratar de um direito implicitamente positivado [5]. Nesse julgamento, a questão controvertida era o fato de a Lei nº 9.883/1999 determinar que os órgãos componentes do Sisbin fornecerão à Abin, nos termos e condições a serem aprovados mediante ato presidencial, dados e conhecimentos específicos relacionados à defesa das instituições e dos interesses nacionais, ao passo em que o Decreto nº 10.445, de 30 de julho de 2020, estabeleceu que esse compartilhamento ocorrerá sempre que solicitado pela Abin.

O STF deferiu parcialmente a medida cautelar e conferiu uma interpretação conforme a Constituição Federal ao parágrafo único do art. 4º da Lei nº 9.883/1999, para atribuir validade ao texto legal e dar integral cumprimento ao § 3º do art. 1º do Decreto nº 10.445/2020: o compartilhamento de dados do Sisbin para a Abin somente deve ocorrer quando os dados a serem fornecidos estiverem vinculados ao interesse público objetivamente comprovado e com motivação específica, em procedimento formalmente instaurado, afastada qualquer possibilidade de atendimento de interesses pessoais ou privados, além de ser vedado o compartilhamento de dados sujeitos à cláusula de reserva de jurisdição. Nesse último caso, esses dados somente podem ter seu sigilo retirado mediante autorização prévia do Poder Judiciário, a exemplo do segredo dos dados e das comunicações telefônicas, por expressa previsão constitucional [16]. Em 11 de outubro de 2021, o STF confirmou, por unanimidade, a medida cautelar deferida parcialmente Medida Cautelar na ADI nº 6.529 [46].

No terceiro acórdão, referente ao julgamento da Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 722, o Plenário do STF deferiu medida cautelar para suspender, por desvio de finalidade, toda e qualquer atividade de Inteligência do Ministério da Justiça e Segurança Pública relacionada com a produção e compartilhamento de dossiê sigiloso contendo informações sobre a vida pessoal, as escolhas pessoais e políticas de cidadãos, servidores públicos federais, estaduais e municipais identificados como integrantes de movimento político antifascista e de professores universitários [47].

Cumpre ressaltar que, em 10 de fevereiro de 2022 foi promulgada a Emenda Constitucional nº 115/2022, que inseriu a proteção de dados pessoais entre os direitos e garantias fundamentais previstos no art. 5º da Constituição Federal [17]. Dessa maneira, as decisões do STF que reconheceram essa proteção como um direito fundamental autônomo foram chanceladas e legitimadas pelo Congresso Nacional. Essa Emenda Constitucional atribuiu regime jurídico-constitucional pleno a esse direito fundamental em sentido material e formal, de modo que as normas relativas ao direito à proteção de dados passaram a vincular diretamente todos os atores públicos e, com as devidas ressalvas, os atores privados, por força da aplicabilidade imediata dos direitos fundamentais [21].

Além disso, em 15 de setembro de 2022, o STF reiterou que o compartilhamento de informações pessoais em atividades de inteligência observará o disposto em legislação específica e os parâmetros fixados no julgamento da ADI nº 6.529, dentre os quais destaca-se a "observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal" [18], [19].

Os julgados do STF apresentados nesta Seção são relevantes para demonstrar que a interpretação da Suprema Corte é no sentido de que o direito fundamental à proteção dos dados pessoais e, por conseguinte, os princípios gerais de proteção e os direitos do titular previstos na LGPD devem ser observados pela atividade de Inteligência de Estado, no que forem compatíveis com o exercício dessa atividade, mesmo diante da exceção prevista expressamente na LGPD em relação ao tratamento de dados pessoais realizado

com finalidade exclusiva de segurança do Estado e da ausência da legislação específica mencionada no art. 4º, § 1º, dessa lei. Esses julgados servem também para identificar os possíveis fatores de risco decorrentes da aplicação dessas normas na atividade de Inteligência da Abin e para prever medidas para mitigá-los.

2.4 DEVIDO PROCESSO LEGAL, PRINCÍPIOS GERAIS DE PROTEÇÃO E DIREITOS DO TITULAR DOS DADOS PESSOAIS PREVISTOS NA LGPD

A LGPD estabelece que o tratamento de dados pessoais com finalidade de segurança do Estado será regido por legislação específica, "que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei" [9].

O devido processo legal, previsto no art. 5º, inciso LIV, da Constituição Federal, exige a demonstração da existência de interesse público prevalente e do "nexo causal sólido para se invadir a privacidade de uma pessoa, uma vez que os direitos humanos, como os de personalidade, fundamentam a própria legitimidade do Estado de Direito, cuja autoridade serve ao bem comum" [48].

O art. 6ª da LGPD relaciona dez princípios gerais de proteção:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas [9].

De acordo com Ruaro e Sarlet [10], a transparência é elemento central da LGPD e todos os procedimentos envolvendo dados pessoais, sobretudo os dados sensíveis, devem ser compatíveis com a finalidade da coleta e minimizados em uma política de uso racional.

Os direitos dos titulares dos dados pessoais estão previstos nos arts. 17 e 18 da LGPD, destacando-se os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos dessa lei; e o direito de obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição, a confirmação da existência de tratamento; o acesso aos dados; a correção de dados incompletos, inexatos ou desatualizados; a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD; portabilidade dos dados, de acordo com regulamentação da ANPD; a eliminação dos dados pessoais tratados com o consentimento do titular; a informação das entidades públicas e privadas com as quais o controlador compartilhou os dados; a informação sobre a possibilidade de não fornecer consentimento e as consequências da negativa; e a revogação do consentimento [9].

A apresentação do devido processo legal, dos princípios gerais de proteção e dos direitos do titular dos dados pessoais previstos na LGPD é relevante para a identificação dos fatores de risco legal e da metodologia adequada para implementar os sete princípios fundamentais da abordagem *privacy by design* e as oito *privacy design strategies* no desenvolvimento de aplicações de *big data analytics* para produção da Osint, ainda na fase de concepção desses *softwares*.

2.5 APLICAÇÕES DE BIG DATA ANALYTICS PARA PRODUÇÃO DA OSINT

No contexto da atividade de Inteligência, verifica-se que muitas das ameaças tradicionais encontram correspondente no espaço cibernético, a exemplo da espionagem, do terrorismo, do ativismo extremista, da guerra e das atividades criminais, afetando a esfera econômica e a segurança nacional [49]. As redes sociais têm sido cada vez mais utilizadas como meio de mobilização social, por influenciarem significativamente o comportamento humano, podendo ser utilizadas inclusive para incentivar radicalizações de quaisquer gêneros [4]. Além disso, criminosos internacionais e grupos terroristas operam em todo o mundo e utilizam as mais recentes tecnologias para cometer ilícitos e para se comunicar por meio de sites publicamente disponíveis, mídias sociais e fóruns na *darknet*, compartilhando propaganda, reivindicando crédito por ataques e incitando crimes [50].

O enfrentamento moderno à criminalidade e ao terrorismo, em um período de globalização e de revolução na área da tecnologia da informação, exige uma reavaliação de cenários e de atores, devendo o Estado potencializar a atuação das suas instituições de Inteligência, para otimizar o processo de produção do conhecimento e acompanhar a celeridade e a instantaneidade dos modernos fluxos de informação [51]. Essa é a razão pela qual o domínio do ciberespaço pela Inteligência de Estado garante segurança para a sociedade e possibilita a identificação de oportunidades, isto é, a indicação de tendências e a antecipação de cenários estratégicos [49].

Tendo em vista que as técnicas sigilosas para buscar dados negados (dados sensíveis protegidos por seu detentor, para resguardá-los do acesso não autorizado) podem ser invasivas, com o potencial de violar direitos individuais, a atividade de Inteligência, em regra, somente recorre a esses meios após esgotados todos os outros procedimentos de obtenção de dados veiculados por fontes abertas ou fontes humanas [49]. Em outras palavras, a atividade de Inteligência prioriza a obtenção e análise de dados disponíveis em fontes

abertas, ou seja, a Inteligência de fontes abertas ou Osint.

Atualmente, a obtenção eficaz da Osint exige a utilização de tecnologia de última geração, em virtude do crescimento exponencial da produção e armazenamento de grandes volumes de dados nos meios digitais, fenômeno denominado *big data*. Do ponto de vista social e jurídico, o que é mais relevante em conjuntos de dados muito grandes é a possibilidade de utilizá-los para análises, ou seja, para descobrir correlações e fazer previsões, muitas vezes usando técnicas de inteligência artificial [52]. Para descobrir essas correlações, a atividade de Inteligência utiliza aplicações para análise de vínculos, entendimento de contextos, localização de pessoas e de lugares; inteligência artificial; e técnicas analíticas para grandes conjuntos de dados, denominadas *big data analytics* [4].

O termo *big data analytics* refere-se a todo o ciclo de vida do gerenciamento de grandes volumes de dados, incluindo sua coleta, organização e análise para descobrir padrões, inferir situações ou estados, prever e entender comportamentos [53]. Na camada de tratamento dos dados, algoritmos sofisticados estão sendo desenvolvidos para analisar uma grande quantidade de dados com o intuito de obter informações valiosas para a tomada de decisões precisas, detectando oportunidades sem precedentes para encontrar padrões significativos, presumir situações e prever e inferir comportamentos [54].

A obtenção e a análise dessa quantidade massiva de dados ensejam oportunidades para a atividade de Inteligência de Estado, seja ela brasileira ou adversa, haja vista que um dos objetivos dos órgãos de Inteligência é identificar oportunidades que possam surgir para o Estado, indicando-as às autoridades detentoras de poder decisório [37]. Essa realidade impõe à atividade de Inteligência a necessidade de aprimoramento contínuo de seus métodos e processos, sendo imprescindíveis a apropriação das técnicas e aplicações de *big data analytics* e um processo estruturado de produção de conhecimentos, para que a Inteligência cumpra com eficácia suas atribuições legais [55].

A descoberta de conhecimento em bases de dados, com a utilização de ferramentas de análise, como a mineração de dados e a elaboração de modelos preditivos, é diferencial essencial [8], notadamente para a Abin, a quem compete "planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República" [14].

Embora as ferramentas de *big data analytics* tenham melhorado a eficiência das atividades estatais e criado oportunidades significativas para os serviços intensivos em informação, seus benefícios são restringidos pelo risco elevado de o tratamento desses dados violarem a privacidade, devido à grande quantidade de informações pessoais contida no *big data* [56]. As crescentes interações no meio digital, em âmbito mundial, permite a formação de trilhas digitais, que vêm sendo exploradas intensamente pelas instituições para tomada de decisões, por meio da inteligência artificial e de conexões em rede de algoritmos, permitindo a criação de perfis a respeito dos interesses pessoais para toda espécie de finalidades possíveis [57], deixando a pessoa natural em evidente posição de vulnerabilidade, haja vista que parte de seus dados pessoais estão à disposição de terceiros sem que ela tenha domínio sobre isso, colocando em risco sua privacidade e intimidade e os seus dados pessoais [8]. A utilização de aplicações de *big data analytics* pode acarretar, dentre outros riscos, vigilância eletrônica em larga escala, criação de perfis, divulgação de dados pessoais [53], reutilização incompatível de dados, inferência e reidentificação de dados e tomada de decisão automatizada [58].

Logo, os benefícios da utilização de *big data* pelo poder público e os riscos à privacidade dela decor-

rentes devem ser analisados conjuntamente, sobretudo para avaliar as medidas que podem mitigar esses riscos, com o objetivo de identificar os modelos de proteção e de governança mais adequados, para maximizar os efeitos positivos do acesso a *big data* e para prevenir eventuais prejuízos que podem advir do uso das aplicações de *big data analytics* [59]. O direito fundamental à proteção de dados pessoais exige a observância dos critérios previstos na LGPD no que tange à inserção das medidas necessárias à garantia da segurança do tratamento de dados pessoais durante todo o ciclo de vida desses dados [8].

2.6 OS SETE PRINCÍPIOS FUNDAMENTAIS DA ABORDAGEM PRIVACY BY DESIGN E A ENGENHARIA DE PRIVACIDADE

Privacy by Design é uma abordagem de engenharia de sistemas destinada a garantir a proteção da privacidade nos estágios iniciais de um projeto e em todo o processo de engenharia de software [60]. Trata-se de um conceito holístico que se aplica à tecnologia da informação, às práticas de negócios, aos processos, ao projeto físico e à infraestrutura de rede [33].

Os sete princípios fundamentais da abordagem *privacy by design*, desenvolvidos por Ann Cavoukian [61], são apresentados a seguir, sendo que as suas definições constam na Seção 4.1:

1) proativo e não reativo;

2) privacidade como configuração padrão;

3) privacidade incorporada ao design;

4) funcionalidade total;

5) segurança de ponta a ponta;

6) visibilidade e transparência; e

7) respeito pela privacidade do usuário.

De acordo com [62], a abordagem *privacy by design* foi aceita internacionalmente na 32ª Conferência Internacional de Comissários de Proteção de Dados e Privacidade, realizada em Jerusalém, em 2010, com a adoção do documento *Resolution on Privacy by Design*. Essa resolução reconheceu a *privacy by design* como um componente essencial da proteção da privacidade e incentivou a adoção daqueles sete princípios fundamentais desenvolvidos por Ann Cavoukian como orientação para estabelecer a privacidade como o modo padrão de operação de uma organização [63].

A engenharia de privacidade é um processo sistemático com foco orientado a riscos cujo objetivo é traduzir, em termos práticos e operacionais, os princípios de *privacy by design* dentro do ciclo de vida dos sistemas de informação que tratam dados pessoais, como parte integrada do projeto do sistema, de modo que os requisitos de privacidade sejam definidos ainda na concepção dos *softwares* e que qualquer risco de privacidade identificado seja adequadamente gerenciado pelo sistema de forma proativa durante todo o ciclo de vida dos dados pessoais [62].

Além disso, a engenharia de privacidade objetiva apoiar a seleção, implantação e configuração de

medidas técnicas e organizacionais adequadas para satisfazer princípios específicos de proteção de dados [58] e abrange implementação, implantação e operação e gerenciamento contínuos de recursos e controles de privacidade nos sistemas [33].

2.7 PRIVACY DESIGN STRATEGIES, TÁTICAS ASSOCIADAS, PRIVACY DESIGN PATTERNS E PRIVACY ENHANCING TECHNOLOGIES

Inicialmente será feito um breve histórico da criação e da evolução da teoria das oito *privacy design strategies* e depois serão apresentados conceitos relevantes para o entendimento dessa teoria.

Hoepman [64] apresenta a teoria sobre *privacy design strategies*, derivadas da legislação europeia sobre proteção de dados pessoais, e fornece uma versão preliminar sobre os possíveis *privacy design patterns* que poderiam contribuir para a implementação daquelas estratégias. Por último, o autor valida a sua teoria, em relação à perspectiva tecnológica e da política de privacidade, demonstrando que as oito *privacy design strategies* propostas abrangem tanto os princípios de privacidade previstos na norma ISO/IEC 29100:2011 (*Information technology; security techniques; privacy framework*) [65] quanto os estabelecidos pela Organização para a Cooperação e Desenvolvimento Econômico (*The Organisation for Economic Co-operation and Development* - OECD) [66] e podem ser aplicadas tanto em sistemas de armazenamento como em sistemas de fluxo de informação.

Koops et al. [67] demonstram que as oito *privacy design strategies* complementadas por alguns *design patterns* permitiriam implementar três requisitos considerados adequados para incorporar a abordagem *privacy by design* em plataformas genéricas da Osint: especificação de propósito; limitação de coleta e minização de dados pessoais; e qualidade dos dados.

Colesky et al. [68] aperfeiçoam as definições das oito *privacy design strategies*, renomeiam a estratégia *aggregate* para *abstract* e analisam a relação entre a abordagem estratégica e o domínio da arquitetura de software, demonstrando que a proteção da privacidade pode ser considerada um atributo de qualidade. Com base nisso, os autores definem *privacy design strategies* como a especificação de um objetivo arquitetônico distinto em *privacy by design* para atingir o atributo de qualidade de proteção de privacidade. De acordo com a Agência Espanhola de Proteção de Dados (*Agencia Española de Protección de Datos* - AEPD) [62], *privacy design strategies* fornecem um modelo acessível para que engenheiros de sistema possam definir os requisitos de privacidade identificados durante os estágios de análise e requisitos.

Além disso, Colesky et al. [68] introduzem, entre as *privacy design strategies* e os *design patterns*, as táticas, definidas como uma abordagem de *privacy by design* que contribui para alcançar o objetivo de uma abrangente *privacy design strategy*. As definições das oito *privacy design strategies* e das suas táticas associadas serão apresentadas na Seção 4.2.

Hoepman [69] esclarece que as *privacy design strategies* foram desenvolvidas para serem utilizadas nas duas primeiras fases do ciclo de vida do sistema (ideação e definição), nas quais são tomadas decisões relevantes sobre as propriedades gerais de privacidade do sistema, considerando que as ferramentas existentes (*privacy design patterns* e *privacy enhancing technologies*) se aplicam principalmente à fase de projeto e desenvolvimento. Conforme Figura 2.1 as oito fases do ciclo de vida do sistema são, nessa ordem, *ideation*,

definition, *design*, *development*, *deployment*, *operation*, *evaluation* e *decommissioning* (em tradução livre: ideação, definição, projeto, desenvolvimento, implantação, operação, avaliação e desativação).

Figura 2.3: Ciclo de vida do sistema

Fonte: Adaptado de Hoepman [69]

A AEPD [62] explica que para tornar a privacidade uma parte integrada do design do sistema, de modo que os requisitos de privacidade sejam definidos em termos de propriedades e funcionalidades totalmente implementáveis e qualquer risco de privacidade identificado seja adequadamente gerenciado pelo sistema de maneira proativa, é necessário que o desenvolvimento ocorra de forma sequencial em diferentes níveis de abstração. No mais alto nível, nas fases iniciais do desenvolvimento do conceito do objeto e da análise dos seus requisitos, é necessário definir as *privacy design strategies* e as táticas a serem seguidas durante as diferentes etapas do processamento de dados, a fim de garantir os objetivos de privacidade e o cumprimento dos princípios de proteção de dados pessoais. Em um nível intermediário, devem ser adotadas as *privacy design patterns*, definidas como soluções reutilizáveis empregadas na fase de design e que podem ser aplicadas para resolver problemas comuns de privacidade que freqüentemente surgem no desenvolvimento de produtos e sistemas. No nível mais baixo, no estágio de desenvolvimento, para implementar *privacy design patterns* com uma tecnologia concreta, são utilizadas *privacy enhancing technologies*, definidas pela Agência da União Europeia para Cibersegurança (*European Union Agency for Cybersecurity* – ENISA) [70] como todo tipo de tecnologia que apoia recursos de privacidade ou de proteção de dados pessoais, como as tecnologias que utilizam privacy design strategies ou consideram metas de proteção para engenharia de privacidade.

2.8 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

O relatório de impacto à proteção de dados pessoais (RIPD) está previsto na LGPD como "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" [9]. Embora o texto legal explicitamente associe o RIPD somente aos controladores, uma interpretação sistemática dessa lei permite concluir que também os operadores devem fazer o RIPD em benefício de suas atividades de tratamento [71].

O RIPD é um instrumento semelhante à *Data Protection Impact Assessment* (DPIA) e também funciona

como um indicador demonstrativo de conformidade com a legislação de proteção de dados pessoais [72]. A DPIA, prevista no artigo 35 do Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, é um instrumento de apoio à tomada de decisão em relação ao tratamento dos dados pessoais coerente com os princípios de *privacy by design*, haja vista que deve ser realizada na concepção da operação do tratamento de dados pessoais, mesmo que algumas das operações ainda sejam desconhecidas, e atualizada ao longo do ciclo de vida do projeto [73]. O RIPD também possui essa correlação com os princípios de *privacy by design*, pois deve ser elaborado previamente à operação do tratamento de dados pessoais e atualizado durante o ciclo de vida do projeto.

O RIPD deve ser elaborado previamente à coleta e ao uso dos dados pessoais, sob pena de esvaziamento do sentido e da função desse relevante instrumento preventivo [74], sempre que o tratamento desses dados representar elevado risco aos princípios gerais de proteção ou às liberdades civis e aos direitos fundamentais. O RIPD deverá conter os seguintes requisitos mínimos: "a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados" [9].

Além do RIPD, o art. 50, § 2º, alínea "d", da LGPD apresenta o processo de avaliação sistemática de impactos e riscos à privacidade, que é uma avaliação de impacto que antecede a elaboração do RIPD e é baseada em metodologia avaliativa de riscos e de impacto das operações de tratamento de dados pessoais em relação às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais [72]. Uma única avaliação pode abordar um conjunto de operações de tratamento de dados pessoais semelhantes que apresentem alto risco [33].

Segundo o Nist [32], as avaliações de risco de privacidade contribuem para a tomada de decisões éticas referentes ao sistema ou produto e quanto ao design e à implantação de serviços, na medida em que ajudam as organizações a distinguir riscos de privacidade e riscos de conformidade, permitindo identificar se o tratamento de dados pessoais possui o potencial de trazer risco para a privacidade dos indivíduos, mesmo quando uma organização estiver em conformidade com as leis e regulamentos aplicáveis.

Este Capítulo apresentou uma base jurídica e teórica, que é necessária para compreender a atividade de Inteligência de Estado executada pela Abin, na posição de órgão central do Sisbin, os delineamentos do direito fundamental autônomo à proteção dos dados pessoais, o detalhamento do devido processo legal, dos princípios gerais de proteção e dos direitos do titular dos dados pessoais previstos na LGPD, os sete princípios fundamentais da abordagem *privacy by design* e os conceitos de *privacy design strategies*, de suas táticas associadas, de *privacy design patterns*, de *privacy enhancing technologies* e de RIPD. A partir desse esforço, com apreciação da revisão da literatura, da legislação e da sua intepretação, tem-se possível a construção metodológica de uma análise dos fatores de risco decorrentes da aplicação da LGPD e do direito fundamental à proteção de dados na atividade de Inteligência e nas aplicações de *big data analytics* para a produção da Osint, que será objeto do próximo capítulo.

3 IDENTIFICAÇÃO E ANÁLISE DOS FATORES DE RISCO

Neste Capítulo serão apresentados e analisados os fatores de risco identificados com potencial de impactar o cumprimento da missão institucional da Abin em decorrência da incidência do direito fundamental à proteção dos dados pessoais e da LGPD na atividade de Inteligência desse órgão e nas aplicações de *big data analytics* utilizadas pelo serviço de Inteligência brasileiro para a produção da Osint. Ao final deste Capítulo serão apresentadas sugestões para futuro anteprojeto de lei de proteção de dados pessoais para segurança do Estado, com o intuito de proporcionar segurança jurídica para os agentes de tratamento da Abin e para os titulares dos dados pessoais tratados por esse órgão.

Conforme ressaltado na Seção 1.5, que trata do procedimento metodológico, o objetivo desta dissertação não é mapear e avaliar todos os riscos possíveis, mesmo que não conhecidos. Além disso, para identificar e analisar os possíveis fatores de risco, utilizou-se análise documental e comparativa, levando em consideração recentes decisões do STF sobre o direito fundamental à proteção dos dados pessoais, a legislação brasileira interpretada, o direito comparado, estudos de agências governamentais brasileiras e de outros países e artigos científicos sobre esse direito fundamental e sobre a LGPD. Finalmente, para delimitar e sistematizar os fatores de risco avaliáveis, foi utilizada a tipologia prevista no art. 18 da Instrução Normativa Conjunta MP/CGU nº 1/2016.

3.1 FATORES DE RISCO OPERACIONAL

O primeiro fator de risco operacional (FRO-1) poderia decorrer do descumprimento da obrigação de manter o registro das operações de tratamento de dados pessoais que a Abin realizar. Esse fator de risco origina-se do art. 37 da LGPD, que impõe essa obrigação aos controladores e operadores, e dos princípios da transparência e da responsabilização e prestação de contas, previstos no art. 6º, incisos VI e X, da LGPD. A ocorrência do FRO-1 poderia acarretar a anulação ou a suspensão de operações de Inteligência da Abin que envolvam tratamento de dados pessoais. Como medida de mitigação, propõe-se que a Abin mantenha o registro de todas as operações de tratamento de dados pessoais que realizar.

Cumpre esclarecer que tanto o FRO-1 quanto outros fatores de risco mencionados no decorrer deste Capítulo 3 poderão ensejar, como consequência de sua ocorrência, a anulação ou a suspensão de operações de Inteligência da Abin envolvendo dados pessoais por desconformidade com o princípio fundamental da proteção de dados pessoais e com os dispositivos da LGPD aplicáveis no caso concreto. Pietro [75] explica que anulação é o desfazimento do ato administrativo por razões de ilegalidade e pode ser feita pela própria Administração Pública, com base no seu poder de autotutela sobre os próprios atos, o denominado controle interno, e também pelo controle externo, que é aquele exercido por um dos Poderes sobre o outro.

De acordo com o STF [46], as atividades de Inteligência, ainda que acobertadas pelo sigilo, estão submetidas ao controle externo dos Poderes Legislativo e Judiciário, haja vista que a Constituição Federal repudia poder sem controle e exige que os atos administrativos sejam motivados e orientados pelos

princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

O segundo fator de risco operacional (FRO - 2) poderia ocorrer pela ausência de confecção do RIPD previamente ao tratamento de dados pessoais que possa, eventualmente, gerar riscos às liberdades civis e aos direitos fundamentais. Esse fator de risco origina-se do art. 5º, inciso XVII, da LGPD, que determina a elaboração dessa documentação, contendo a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, as medidas, as salvaguardas e os mecanismos de mitigação de risco; e do princípio da prevenção, previsto no art. 6º, inciso VIII, da LGPD. A materialização do FRO-2 poderia acarretar suspensão ou anulação de operações de Inteligência realizadas com tratamento de dados pessoais. A medida de mitigação proposta é que o controlador da Abin confeccione o RIPD previamente ao tratamento de dados pessoais nas hipóteses previstas na LGPD.

O terceiro fator de risco operacional (FRO-3) poderia ocorrer pela reutilização incompatível de dados pessoais nas operações de tratamento realizadas com o uso de aplicações de *big data analytics*. Esse fator de risco origina-se dos princípios da finalidade e da adequação, previstos no art. 6º, incisos I e II, da LGPD, que vedam o tratamento posterior de forma incompatível com os propósitos legítimos, específicos, explícitos e informados ao titular. A ocorrência do FRO-3 poderia ensejar a anulação ou suspensão de operações de Inteligência da Abin que envolvam tratamento de dados pessoais. Como medida de mitigação, propõe-se que a Abin elabore o RIPD previamente ao tratamento dos dados pessoais e implemente a engenharia de privacidade no desenvolvimento de aplicações de *big data analytics* para produção da Osint, conforme detalhado no Capítulo 4. A abordagem *privacy by design* demanda que as organizações considerem, em termos gerais, se o tratamento de dados pessoais nessas aplicações está dentro das expectativas razoáveis dos titulares dos dados pessoais. Caso a análise dos dados revele correlações inesperadas que acarretem a reutilização dos dados pessoais para novos fins, essa abordagem requer que as organizações avaliem a compatibilidade do novo propósito com a finalidade original e com as expectativas razoáveis dos indivíduos em relação ao novo tratamento, devendo existir medidas e salvaguardas adequadas tanto na operação de tratamento inicial quanto nas subsequentes [76]. Para tanto, é necessária a realização do RIPD, já que as medidas e salvaguardas adequadas para cada caso dependem do contexto e dos riscos advindos do tratamento dos dados pessoais [77].

3.2 FATORES DE RISCO DE IMAGEM OU À REPUTAÇÃO

O primeiro fator de risco de imagem ou à reputação (FRI-1) da Abin poderia ocorrer pelo tratamento de dados pessoais para fins particulares. Esse fator de risco origina-se do princípio da finalidade, previsto no art. 6º, inciso I, da LGPD, que exige um propósito legítimo para fundamentar o tratamento de dados pessoais, e da decisão do Plenário do STF proferida na ADI nº 6.529 [46], no sentido de que os órgãos componentes do Sisbin somente podem compartilhar dados e conhecimentos específicos com a Abin quando comprovado o interesse público da medida, sendo vedada a utilização desses dados para atendimento de interesses pessoais ou privados. A materialização do FRI-1 poderia repercutir negativamente na imagem do órgão perante a sociedade e ensejar a suspensão ou a anulação de operações de Inteligência que envolvam tratamento de dados pessoais, por desvio de finalidade. Por exemplo, por esse motivo, o STF determinou a suspensão da atividade de Inteligência desenvolvida pelo Ministério da Justiça e Segu-

rança Pública que envolvia compartilhamento de dados pessoais relativos a escolhas pessoais e políticas de cidadãos e servidores públicos identificados como integrantes de movimento político antifascista e de professores universitários [47]. A medida de mitigaçao proposta é que a Abin garanta que suas operações de tratamento de dados pessoais são realizadas em prol do interesse público objetivamente comprovado, em conformidade com o disposto na PNI. Essa política estabelece que a Inteligência, por ser atividade exclusiva de Estado, deve ser desenvolvida em prol do bem-comum e na defesa dos interesses da sociedade e do Estado Democrático de Direito, não se colocando a serviço de grupos, ideologias e objetivos mutáveis e sujeitos às conjunturas político-partidárias [37].

O segundo fator de risco de imagem ou à reputação (FRI-2) seria a ocorrência de acessos não autorizados aos dados pessoais ou de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer tratamento inadequado ou ilícito. Esse fator de risco origina-se dos arts. 6º, inciso VII (princípio da segurança), e 46, *caput*, ambos da LGPD, que exigem dos agentes de tratamento a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e das situações acidentais ou ilícitas mencionadas. A ocorrência do FR1-2 poderia ocasionar danos à imagem e à reputação da Abin, agravados pelo fato de que uma das missões legais desse órgão é "planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade" [14]. Cabe anotar que a Abin possui em sua estrutura o Cepesc, departamento que já desenvolve programas e ferramentas para garantir o sigilo e a transmissão segura das informações e das comunicações governamentais, inclusive dos votos nas urnas eletrônicas, por meio da criação e utilização da criptografia de Estado [38]. Como medidas de mitigação, sugere-se que a Abin disponibilize para os órgãos do Sisbin canais seguros de comunicação dos dados e de informações pessoais, estruturados com criptografia de Estado, e elabore e implemente regras de boas práticas e um programa de governança em privacidade, em consonância com o disposto no art. 50 da LGPD.

O terceiro fator de risco de imagem ou à reputação (FRI-3) poderia ocorrer pela divulgação não autorizada de dados pessoais em decorrência de inferência e reidentificação de dados dessa natureza tratados por aplicações de *big data analytics*. Assim como o FRI-2, esse fator de risco também se origina dos arts. 6º, inciso VII (princípio da segurança), e 46, *caput*, ambos da LGPD. A materializaçaõ do FRI-3 poderia gerar repercussão negativa na imagem da Abin perante a sociedade e suspensão ou anulação de operações de Inteligência que envolvam tratamento de dados pessoais. Como medidas de mitigação, propõe-se que a Abin implemente os princípios fundamentais da abordagem *privacy by design* e as *privacy design strategies* no desenvolvimento de aplicações de *big data analytics* para produção da Osint, conforme detalhado no Capítulo 4, e elabore o RIPD previamente ao tratamento dos dados pessoais. Cumpre ressaltar que a engenharia de privacidade requer uma abordagem de risco suficientemente robusta, para gerenciar os riscos de privacidade identificados, selecionando e aplicando controles para mitigá-los, incluindo arquiteturas que respeitem a privacidade, políticas de privacidade e métodos de gerenciamento de dados, tais como minimizaçao, anonimizaçao, agregação e o uso de *privacy enhancing technologies* [78].

3.3 FATOR DE RISCO LEGAL

O primeiro fator de risco legal (FRL-1) poderia ocorrer pela vigilância eletrônica em larga escala em decorrência do tratamento realizado com aplicações de *big data analytics*, o que poderia configurar violação a uma série de princípios de proteção previstos na LGPD. Esse fator de risco origina-se dos princípios da finalidade, da adequação, da necessidade e da transparência, previstos no art. 6º, incisos I, II, III e VI, da LGPD, respectivamente. A ocorrência desse fator de risco poderia ensejar a anulação ou suspensão de operações de Inteligência da Abin que envolvam tratamento de dados pessoais. Como medidas de mitigação, propõe-se que a Abin elabore o RIPD previamente ao tratamento dos dados pessoais e implemente a engenharia de privacidade no desenvolvimento de aplicações de *big data analytics* para produção da Osint, conforme detalhado no Capítulo 4. A adoção dessas medidas viabilizaria a implementação de medidas técnicas e administrativas ou organizacionais nos estágios iniciais de desenvolvimento dos *softwares* e durante todo o ciclo de vida dos dados pessoais, para mitigar de forma proativa e antecipada riscos de privacidade e de proteção de dados pessoais. Com efeito, a abordagem *privacy by design* possibilita repensar e redesenhar as operações de tratamento de dados pessoais, com a definição de novos atores e responsabilidades, e com um papel proeminente para a tecnologia como elemento de garantia, de modo que as medidas técnicas e organizacionais adequadas e as salvaguardas sejam consideradas no estágio mais cedo possível e integradas ao tratamento [58].

O segundo fator de risco legal (FRL-2) poderia decorrer da não adoção imediata do devido processo legal, dos princípios gerais de proteção e dos direitos do titular dos dados pessoais previstos na LGPD, no que forem compatíveis com a atividade de Inteligência de Estado. Esse fator de risco origina-se da ADI nº 6.649 [18] e da ADPF nº 695 [19], nas quais o STF reiterou o entendimento exposto na ADI nº 6.529 [46], no sentido de que essa atividade estatal deve observar o direito fundamental à proteção dos dados pessoais e, por conseguinte, os princípios gerais de proteção e os direitos do titular previstos na LGPD, no que forem compatíveis com o exercício dessa função estatal, mesmo diante da exceção prevista expressamente na LGPD em relação ao tratamento de dados pessoais realizado com finalidade exclusiva de segurança do Estado e da ausência da legislação específica mencionada no art. 4º, § 1º, dessa lei, conforme detalhado na Seção 2.3. Sobre o assunto, cumpre ressaltar que "as normas definidoras dos direitos e garantias fundamentais têm aplicação imediata" [20], o que significa que um direito fundamental não poderá ter sua proteção e fruição negadas pura e simplesmente por conta dos argumentos de que se trata de direito positivado como norma programática e de eficácia meramente limitada e de que o reconhecimento de uma posição subjetiva dependeria de uma interposição legislativa [21]. A ocorrência desse fator de risco legal poderia ensejar a anulação de operações de Inteligência da Abin que envolvam o tratamento de dados pessoais. Sendo assim, passa-se a analisar de que forma a Abin deveria observar o devido processo legal, os princípios gerais de proteção e os direitos do titular dos dados pessoais, para mitigar esse fator de risco.

3.3.1 Observância do devido processo legal

O devido processo "é imperativo da própria Constituição e de aplicação inafastável" [79]. Consequentemente, a Abin deveria instaurar procedimento formal para solicitar dados pessoais aos órgãos do Sisbin, registrando a fundamentação específica da finalidade, da adequação e da necessidade do tratamento, a fim

de demonstrar os propósitos legítimos, a legalidade e o atendimento do interesse público. Além disso, a transmissão dos dados pessoais deveria ocorrer sempre por meio de um canal seguro de comunicação, com registro dos acessos, para possibilitar a responsabilização em caso de eventual omissão, desvio ou abuso, sendo vedado, o compartilhamento, sem autorização judicial, de dados pessoais sujeitos à cláusula de reserva de jurisdição, como os que envolvam o sigilo dos dados e das comunicações telefônicas, ainda que presente o interesse público [16].

3.3.2 Observância dos princípios gerais de proteção

Quanto à observância dos dez princípios gerais de proteção relacionados no art. 6º da LGPD, cumpre ressaltar que esses princípios são alicerces dessa Lei e representam quase que um consenso internacional, estando presentes nas principais leis estrangeiras sobre proteção de dados [80] (Seção 2.4):

1) princípio da finalidade;

2) da adequação;

3) da necessidade;

4) do livre acesso;

5) da qualidade dos dados;

6) da transparência.

7) da segurança;

8) da prevenção;

9) da não discriminação; e

10) da responsabilização e prestação de contas.

No que diz respeito à observância do primeiro princípio geral de proteção (da finalidade), deveria constar em procedimento formal a fundamentação específica dos propósitos do tratamento, para que seja possível avaliar a necessidade, adequação e proporcionalidade em sentido estrito do tratamento de dados pessoais [59] e para evitar que as informações coletadas para uma finalidade sejam utilizadas para outra finalidade incompatível com a inicial [81]. Sobre esse assunto, Wimmer [82] discutiu parâmetros para o compartilhamento e uso secundário de dados pessoais no âmbito do Estado e concluiu que, ainda que se possa, em determinadas circunstâncias, admitir o compartilhamento de dados pessoais no âmbito do poder público com mudança das finalidades que justificaram sua coleta, seriam necessárias a adoção de salvaguardas materiais e procedimentais, a observância dos direitos e dos princípios associados à proteção de dados pessoais e a justificativa do interesse público específico a ser atingido com o uso secundário desses dados.

Além disso, o princípio da finalidade exige que o tratamento dos dados pessoais esteja amparado em uma das bases legais da LGPD. Sobre o assunto, embora Teffé e Viola [83] possuam o entendimento de que não seria necessário identificar uma base legal apropriada autorizativa do tratamento de dados pessoais para as situações que se enquadrassem nas hipóteses de exclusão de aplicação da LGPD, Wimmer [84]

esclarece que a LGPD considerou as diferenças na racionalidade de tratamento de dados entre o setor público e a iniciativa privada, prevendo duas bases legais específicas para o tratamento de dados pessoais pelo poder público, quais sejam, a execução de políticas públicas e a execução de competências legais ou o cumprimento das atribuições legais do serviço público, sendo esta última estabelecida pelo art. 23 da LGPD, em complemento às bases legais previstas nos arts. 7º e 11 dessa Lei.

Sobre a possibilidade de utilização das bases legais do consentimento e do legítimo interesse para justificar o tratamento de dados pessoais, Wimmer [84] explica que o RGPD proíbe expressamente que as autoridades públicas, no desempenho de suas atribuições, fundamentem o processamento de dados pessoais com a base legal do legítimo interesse, haja vista que o Estado deve atuar predominantemente com base em suas competências legais específicas, e que a base legal do consentimento é tratada com desconfiança, em virtude do desequilíbrio na relação entre o cidadão e o poder público, da dificuldade de caracterizar o consentimento como livre e da instabilidade decorrente da possibilidade de revogação do consentimento a qualquer tempo.

Nesse sentido e considerando que a atuação do Estado é limitada pelas competências que lhe são atribuídas por lei [84], o tratamento de dados pessoais realizado pela Abin no exercício da atividade de Inteligência, com finalidade exclusiva de segurança do Estado, encontraria amparo, como regra geral, na base legal de execução de competências legais, prevista no art. 23 da LGPD, o que tornaria desnecessário o consentimento do titular dos dados pessoais e concorreria para o cumprimento da missão legal da Abin, eis que "a efetividade das atividades de inteligência associa-se, com frequência, ao caráter sigiloso do processo e das informações coletadas" [46].

Esse entendimento quanto à base legal aplicável é corroborado pelo Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal, que previu, em seu art. 9º, apenas três bases legais para fundamentar o tratamento de dados pessoais para atividades de segurança pública e de persecução penal: o cumprimento de atribuição legal de autoridade competente, na persecução do interesse público, na forma de lei ou regulamento, o que está em consonância com o entendimento exposto acima; a execução de políticas públicas previstas em lei, na forma de regulamento; e a proteção da vida ou da incolumidade física do titular ou de terceiro, contra perigo concreto e iminente [85].

Para cumprir o segundo princípio (da adequação), as solicitações de compartilhamento de dados e informações formuladas pela Abin deveriam ser sempre acompanhadas da motivação demonstrativa da adequação da solicitação às finalidades legais, para que o Poder Judiciário, se provocado, possa realizar o controle de legalidade, examinando a conformidade da solicitação aos princípios da proporcionalidade e da razoabilidade [16].

Para atender ao terceiro princípio (da necessidade), o controlador deveria buscar atingir suas finalidades da forma menos intrusiva possível à privacidade dos titulares dos dados pessoais e com o tratamento apenas dos dados essenciais para o atingimento dos objetivos. A boa execução de tal princípio se materializaria pela rigorosa governança dos processos de tratamento, nos quais constariam os tipos de dados pessoais coletados.

No que diz respeito ao quarto princípio (do livre acesso), embora a publicidade seja a regra na Administração Pública, a Lei nº 12.527, de 18 de novembro de 2011, conhecida como Lei de Acesso à Informação, apresenta três hipóteses de restrição ao acesso à informação administrativa: quando estiver classificada

como ultrassecreta, secreta ou reservada, por ser imprescindível à segurança do Estado ou da Sociedade; quando estiver protegida por hipótese legal de sigilo, segredo de justiça e segredo industrial; ou quando envolver tratamento de informações pessoais [86]. Fora dessas hipóteses, os órgãos e entes públicos estão obrigados a divulgar todas as informações produzidas, processadas e armazenadas [87]. No caso do tratamento dos dados pessoais realizado pela Abin no exercício da atividade de Inteligência, entende-se que o interesse público prevalente limita o princípio do livre acesso nas três hipóteses mencionadas, sobretudo pelo sigilo legal decorrente dos arts. 9º e 9º-A da Lei nº 9.883/1999, amparado pelo art. 5º, inciso XXXIII, da Constituição Federal que excepciona da regra geral de acesso aquelas informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado. Saliente-se que o direito fundamental à proteção de dados pessoais não é um direito absoluto, podendo ser limitado pela aplicação de outro direito fundamental ou preceito constitucional, aplicável ao caso concreto [81].

Para atendimento do quinto princípio (da qualidade dos dados), a Abin precisaria analisar se os dados pessoais tratados estão corretos e atualizados, para assegurar a produção de conhecimentos confiáveis para o assessoramento do Presidente da República. Isso exigiria uma constante atualização técnica e auditoria, em conformidade com os mais elevados padrões.

Para cumprir o sexto princípio (da transparência), a Abin deveria manter registro das suas operações de tratamento de dados pessoais e elaborar o RIPD nas hipóteses previstas na LGPD. Essas obrigações asseguram transparência, na medida em que a documentação serve para verificar se o tratamento dos dados ocorreu de maneira lícita e para comprovar se os problemas jurídicos referentes à proteção de dados pessoais foram identificados, analisados e levados em consideração [88].

Para cumprir o sétimo princípio (da segurança), a Abin precisará prover aos integrantes do Sisbin canais seguros de compartilhamento de dados pessoais, assegurando a proteção contra acessos não autorizados e a integridade dos dados. Essa medida exigiria mais investimentos em segurança da informação, com foco nas melhores técnicas possíveis.

Para atendimento do oitavo princípio (da prevenção), a Abin precisaria produzir RIPD previamente às operações de tratamento de dados pessoais que, eventualmente, possam gerar riscos às liberdades civis e aos direitos fundamentais, além de adotar regras de boas práticas e implementar um programa de governança em privacidade.

Para cumprimento do nono princípio (da não discriminação), as operações de tratamento de dados pessoais da Abin deveriam envolver apenas os dados pessoais estritamente necessários para o atingimento de propósitos legítimos e específicos.

Finalmente, para concretizar o décimo princípio (da responsabilização e da prestação de contas), os agentes de tratamento deveriam implementar medidas adequadas e eficazes para assegurar a segurança das operações de tratamento de dados pessoais; nomear um encarregado e fixar cláusulas contratuais obrigando parceiros a nomearem encarregados pelos tratamentos de dados pessoais [89]. Mendes [11] esclarece que o encarregado tem como funções receber reclamações dos titulares de dados pessoais, comunicar-se com a ANPD e orientar os funcionários sobre como cumprir as normas de proteção de dados pessoais. Também é altamente recomendável implementar e fortalecer políticas de segurança da informação. Essas políticas precisariam, cada vez mais, se materializar no desenvolvimento de uma infraestrutura de sistemas de informação, com um nível adequado de segurança e proteção de dados pessoais [90]. Outras medidas

preventivas seriam a elaboração do RIPD nas hipóteses legais e a manutenção dos registros de todas as operações de tratamento de dados pessoais.

3.3.3 Observância dos direitos dos titulares dos dados pessoais

Em relação aos direitos dos titulares dos dados pessoais previstos nos artigos 17 e 18 da LGPD, a Abin deveria buscar resguardar às pessoas naturais os direitos fundamentais de liberdade, de intimidade e de privacidade quando realizar operações de tratamento de dados pessoais e disponibilizar para os titulares dos dados pessoais as informações relacionadas no art. 18 dessa lei, a qualquer momento e mediante requisição. Contudo, por força da supremacia do interesse público sobre o privado, nem sempre a Abin poderá disponibilizar esses dados para os titulares, notadamente quando eles estiverem classificados ou protegidos por hipóteses legais de sigilo. Essa limitação está amparada pelo art. 5º, inciso XXXIII, da Constituição Federal de 1988, o qual restringe o acesso a informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado. Essa norma constitucional é instrumentalizada pelos dispositivos referentes ao sigilo, previstos nos arts. 9º e 9º-A da Lei nº 9.883/1999, criados para assegurar o êxito das atividades sigilosas da Abin.

Os arts. 9º e 9º-A da Lei nº 9.883/1999 veiculam a obrigatoriedade de publicação em extrato dos atos cuja publicidade possa comprometer as atividades sigilosas da Abin, incluídos os referentes ao seu peculiar funcionamento, à atuação, às atribuições e às movimentações de seus titulares; e a atribuição de competência privativa do Ministro ao qual esse órgão está subordinado para disponibilizar informações ou documentos sobre as atividades e assuntos de Inteligência produzidos, em curso ou sob a custódia da Abin, observado o respectivo grau de sigilo conferido com base na legislação em vigor, excluídos aqueles cujo sigilo seja imprescindível à segurança da sociedade e do Estado [14].

A propósito, Coutinho [91] explica que os serviços britânicos de Inteligência como o *Security Service*, conhecido como MI5 (*Military Intelligence, Section* 5), o *Secret Intelligence Service*, conhecido como MI6 (*Military Intelligence, Section 6*), e o *Government Communications Headquarters* (GCHQ) tratam dados pessoais mediante a observação de uma série de outras medidas legislativas, como o *Investigatory Powers Act* de 2016 e o *Data Protection Act* de 2018, sendo que este último possui parte específica para regular o tratamento de dados pessoais pelos serviços de Inteligência britânicos, levando em consideração as peculiaridades da atividade de Inteligência. Por exemplo, o *Data Protection Act* de 2018 trata, dentre outros assuntos, dos princípios de proteção de dados pessoais e dos direitos dos titulares desses dados em relação ao tratamento realizado pelos serviços de Inteligência, e determina que esses princípios e direitos podem deixar de ser aplicados para salvaguardar a segurança nacional, desde que seja emitido um certificado assinado por um Ministro da Coroa justificando a necessidade da isenção. Esse poder conferido a um Ministro da Coroa pode ser exercido por um Ministro que seja membro do Gabinete, ou pelo Procurador-Geral ou pelo Advogado-Geral da Escócia [92]. Essa disposição do *Data Protection Act* de 2018 é semelhante aos instrumentos de sigilo previstos nos arts. 9º e 9º-A da Lei nº 9.883/1999 e é justificada pela natureza estratégica e sigilosa da atividade de Inteligência.

3.4 FATORES DE RISCO FINANCEIRO OU ORÇAMENTÁRIO

Os fatores de risco financeiro ou orçamentário estão intimamente ligados àqueles referentes à imagem ou à reputação. O primeiro fator de risco financeiro ou orçamentário (FRF-1) poderia decorrer da utilização dos dados pessoais para atendimento de interesses pessoais ou para fins discriminatórios ilícitos ou abusivos. Esse fator de risco origina-se dos princípios da finalidade, da adequação e da não discriminação, previstos no art. 6º, incisos I, II e IX, da LGPD. O segundo fator de risco financeiro ou orçamentário (FRF-2) poderia ocorrer por acessos não autorizados aos dados pessoais, sobretudo dados pessoais sensíveis. Esse fator de risco tem origem nos princípios da segurança e da prevenção, previstos nos arts. 6º, incisos VII e VIII, da LGPD, que exigem dos agentes de tratamento a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e a prevenir a ocorrência de danos em virtude do tratamento de dados dessa natureza. O terceiro fator de risco financeiro ou orçamentário (FRF-3) poderia decorrer da tomada de decisões baseadas unicamente em tratamento automatizado de dados pessoais que afete interesses dos seus titulares, incluídas as decisões destinadas a definir o perfil pessoal, profissional, de consumo e de crédito ou os aspectos da personalidade, em razão da utilização de aplicações de *big data analytics* desenvolvidas com critérios discriminatórios ilícitos ou abusivos. Esse fator de risco origina-se do princípio da não-discriminação (art. 6º, inciso IX, da LGPD).

A materialização do FRF-1, do FRF-2 e do FRF-3 poderia ensejar o ajuizamento de ações judiciais de indenização por danos morais, por força do art. 5º, inciso X, da Constituição Federal, segundo o qual "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" [20]. Nesse sentido, o STF decidiu que o tratamento de dados pessoais promovido por órgãos públicos em desconformidade com os parâmetros legais e constitucionais importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da LGPD, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de culpa ou dolo [18], [19].

Como medidas de mitigação do FRF-1 e do FR-2, sugere-se que a Abin desenvolva suas atividades de Inteligência com irrestrita observância dos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado brasileiro, conforme determina o art. 3º, parágrafo único, da Lei nº 9.883/1999 [14], e com respeito ao direito fundamental à proteção de dados pessoais e aos dispositivos da LGPD que lhe são aplicáveis. Para mitigar o FRF-3, propõe-se que a Abin elabore o RIPD previamente ao tratamento dos dados pessoais nas hipóteses previstas na LGPD, implemente a engenharia de privacidade no desenvolvimento de aplicações de *big data analytics* para produção da Osint, conforme detalhado no Capítulo 4, e, quando solicitado pelo titular dos dados pessoais, forneça informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, conforme determina o art. 20, § 1º, da LGPD. A quantificação dos riscos do tratamento de dados pessoais, por meio de uma abordagem baseada em risco, permite aos controladores adotar medidas adequadas que sejam proporcionais à probabilidade e à gravidade dos riscos para os direitos e liberdades dos titulares de dados pessoais, com o intuito de atingir conformidade com as normas de proteção de dados pessoais e de implementar a abordagem *privacy by design* [93].

3.5 RESUMO DOS FATORES DE RISCO IDENTIFICADOS

A Tabela 3.1 apresenta um resumo dos principais fatores de risco com potencial de impactar o cumprimento da missão institucional da Abin, das suas origens, das possíveis consequências decorrentes da sua ocorrência e das medidas de mitigação propostas.

Tabela 3.1: Resumo dos fatores de risco, das suas origens, das suas possíveis consequências e das medidas de mitigação propostas.

Identificador do fator de risco	Fator de risco específico	Origem do fator de risco	Possíveis consequências	Medidas de mitigação propostas
FRO-1	Descumprimento da obrigação de manutenção do registro das operações de tratamento de dados pessoais.	Art. 6º, incisos VI e X, da LGPD (princípios da transparência e da responsabilização e prestação de contas) e art. 37 da LGPD.	Anulação ou suspensão de operações de Inteligência da Abin, por violação do princípio da transparência.	A Abin deveria manter o registro de todas as operações de tratamento de dados pessoais que realizar.
FRO-2	Não confecção prévia do RIPD.	Art. 5º, inciso XVII, da LGPD e art. 6º, inciso VIII, dessa lei (princípio da prevenção).	Anulação ou suspensão de operações de Inteligência da Abin.	Os agentes de tratamento da Abin deveriam confeccionar o RIPD nas hipóteses previstas na LGPD.
FRO-3	Reutilização incompatível de dados pessoais nas operações de tratamento realizadas com a utilização de aplicações de big data analytics destinadas à produção da Osint.	Art. 6º, incisos I e II, da LGPD (princípios da finalidade e da adequação).	Anulação ou suspensão de operações de Inteligência da Abin.	A Abin poderia elaborar o RIPD previamente ao tratamento dos dados pessoais e desenvolver suas próprias aplicações de *big data analytic*s para produção da Osint, utilizando a engenharia de privacidade.
FRI-1	Tratamento de dados pessoais para fins particulares.	Art. 6º, inciso I, da LGPD (princípio da finalidade) e ADI nº 6.529.	Repercussão negativa na imagem da Abin perante a sociedade e/ou suspensão ou anulação de operações de Inteligência .	A Abin deveria garantir que suas operações de tratamento de dados pessoais são realizadas em prol do interesse público objetivamente comprovado e na defesa dos interesses da sociedade e do Estado.

FRI-2	Acessos não autorizados aos dados pessoais e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão ou qualquer forma de tratamento inadequado ou ilícito.	Art. 6º, inciso VI da LGPD (princípio da segurança) e art 46, *caput,* dessa lei.	Repercussão negativa na imagem da Abin perante a sociedade e/ou suspensão ou anulação de operações de Inteligência.	A Abin deveria disponibilizar para os órgãos do Sisbin canal seguro de comunicação dos dados e informações pessoais, estruturado com criptografia de Estado e que atenda aos requisitos de segurança e aos princípios gerais previstos na LGPD.
FRI-3	Divulgação não autorizada de dados pessoais em decorrência de inferência e reidentificação de dados dessa natureza tratados por aplicações de *big data analytic*s para obtenção da Osint.	Art. 6º, inciso VI da LGPD (princípio da segurança) e art 46, *caput*, dessa lei.	Repercussão negativa na imagem da Abin perante a sociedade e/ou suspensão ou anulação de operações de Inteligência.	A Abin poderia elaborar o RIPD previamente ao tratamento dos dados pessoais e desenvolver suas próprias aplicações de *big data analytics* para produção da Osint, utilizando a engenharia de privacidade.
FRL-1	Vigilância eletrônica em larga escala em decorrência do tratamento realizado com aplicações de *big data analytics* para obtenção da Osint.	Art. 6º, incisos I, II, III e VI, da LGPD (princípios da finalidade, da adequação, da necessidade e da transparência).	Anulação ou suspensão de operações de Inteligência da Abin.	A Abin poderia elaborar o RIPD previamente ao tratamento dos dados pessoais e desenvolver suas próprias aplicações de *big data analytics* para produção da Osint, utilizando a engenharia de privacidade.
FRL-2	Não adoção imediata das disposições da LGPD relativas ao devido processo legal, aos princípios gerais de proteção e aos direitos do titular dos dados pessoais, no que forem compatíveis com a atividade de Inteligência de Estado.	Direito fundamental à proteção dos dados pessoais, ADI nº 6.529 [46], ADI nº 6.649 [18] e ADPF nº 695 [19].	Anulação ou suspensão de operações de Inteligência da Abin.	A Abin deveria adotar imediatamente os dispositivos da LGPD relativos ao devido processo legal, aos princípios gerais de proteção e aos direitos do titular dos dados pessoais.

FRF-1	Utilização dos dados pessoais para atendimento de interesses pessoais ou para fins discriminatórios ilícitos ou abusivos.	Art. 6º, incisos I, II e IX, da LGPD (princípios da finalidade, da adequação e da não discriminação).	Ajuizamento de ações judiciais de indenização por danos morais.	A Abin deveria exercer sua atividade de Inteligência com irrestrita observância do direito fundamental à proteção de dados pessoais e aos dispositivos da LGPD que lhe são aplicáveis.
FRF-2	Acessos não autorizado aos dados pessoais, sobretudo dados pessoais sensíveis.	Art. 6º, incisos VII e VIII, da LGPD (princípios da segurança e da prevenção) .	Ajuizamento de ações judiciais de indenização por danos morais.	A Abin deveria exercer sua atividade de Inteligência com irrestrita observância do direito fundamental à proteção de dados pessoais e aos dispositivos da LGPD que lhe são aplicáveis.
FRF-3	Tomada de decisões baseadas unicamente em tratamento automatizado de dados pessoais que afete interesses dos seus titulares, usando aplicações de *big data analytics* com critérios discriminatórios abusivos ou ilícitos.	Art. 6º, inciso IX, da LGPD (princípio da não-discriminação).	Ajuizamento de ações judiciais de indenização por danos morais.	A Abin poderia elaborar o RIPD previamente ao tratamento dos dados pessoais e desenvolver suas próprias aplicações de *big data analytics* para produção da Osint, utilizando a engenharia de privacidade.

3.6 SUGESTÕES PARA FUTURO ANTEPROJETO DE LEI

Considerando que a própria LGPD remete à necessidade de produção de uma legislação específica para regular o tratamento de dados pessoais realizados para fins exclusivos de segurança do Estado, depreende-se que há peculiaridades da atividade de Inteligência que justificam um tratamento diferenciado. Por esse motivo e para proporcionar segurança jurídica para os agentes de tratamento da Abin e para os titulares dos dados pessoais tratados por esse órgão, este trabalho propõe quatro sugestões para subsidiar a elaboração de um futuro Anteprojeto de Lei de Proteção de Dados Pessoais nas Atividades de Segurança do Estado.

A primeira sugestão é que o futuro anteprojeto de Lei preveja expressamente mecanismos para limitar o princípio do livre acesso e os direitos do titular dos dados pessoais, com amparo no art. 5º, inciso XXXIII, da Constituição Federal de 1988 e em conformidade com os requisitos de necessidade e proporcionalidade, para não comprometer as atividades sigilosas da Abin que envolvam tratamento de dados pessoais e para assegurar a segurança da sociedade e do Estado, conforme argumentado nos Seções 3.3.2 e 3.3.3.

A segunda sugestão é que o Anteprojeto defina como base legal autorizativa do tratamento de dados pessoais na atividade de Inteligência de Estado o cumprimento das atribuições legais do serviço público. A propósito, o cumprimento de atribuição legal de autoridade competente é a base legal que autoriza o tratamento de dados pessoais pela *European Union Agency for Law Enforcement Cooperation* (Europol), agência da União Europeia que presta apoio aos Estados-Membros no combate às formas graves de criminalidade internacional e ao terrorismo. Com efeito, o Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, autoriza que essa agência obtenha e trate informações, incluindo dados pessoais, existentes em bases de dados informatizadas nacionais ou internacionais, caso seja necessário para o exercício das suas atribuições (art. 17, § 3º), e transfira dados pessoais para organismos da União Europeia e para países terceiros e organizações internacionais se eles forem necessários para a prevenção e combate dos crimes abrangidos pelos objetivos da Europol (art. 23, § 6º) [94].

A terceira sugestão é o estabelecimento de regras claras para a realização de acordos de cooperação disciplinando as hipóteses e termos de transferência internacional de dados pessoais entre a Abin e órgãos de Inteligência estrangeiros, países terceiros ou organizações internacionais, garantindo que as transferências ocorram com um nível de proteção equivalente ao da União Europeia. Ainda, sugere-se que o tratamento seja limitado aos dados estritamente necessários para a atividade de Inteligência e que sejam assegurados direitos efetivos aos titulares dos dados pessoais transferidos. Ressalte-se que, em 16 de julho de 2020, o Tribunal de Justiça da União Europeia invalidou o programa *Privacy Shield*, desenvolvido pela União Europeia e pelos Estados Unidos da América para facilitar as transferências transfronteiriças de dados pessoais para fins comerciais. O Tribunal entendeu que a *Presidential Policy Directive* nº 28 não fornecia aos titulares dos dados pessoais direitos oponíveis às autoridades americanas nos tribunais e que o Decreto Executivo nº 12333 e a Seção 702 do *Foreign Intelligence Surveillance Act* (Fisa), que autoriza a vigilância de pessoas não americanas localizadas fora dos Estados Unidos da América, não asseguram um nível de proteção substancialmente equivalente ao garantido na União Europeia pelo RGPD, pois permitem que as agências de Inteligência norte-americanas coletem mais informações do que as estritamente necessárias para cumprir os objetivos legítimos [95]. Esse debate está longe de terminar e envolve uma grande discussão sobre as transferências internacionais de dados pessoais [96], [97].

Finalmente, a quarta sugestão é que o Anteprojeto preveja sanções administrativas pelo tratamento ilegal ou irregular de dados pessoais e estabeleça um sistema de supervisão eficiente, autônomo e transparente, que assegure aos titulares dos dados pessoais o direito de apresentarem reclamação à ANPD ou para outro órgão de controle externo da atividade de Inteligência. Essa sugestão encontra sintonia com o direito da União Europeia, que prevê, por exemplo, na Diretiva 2016/680 (UE), que a autoridade de controle de dados pessoais da área administrativa, cível e comercial poderá cumular essa competência com a área criminal e de segurança pública. Ou, ainda, que poderá ser criada outra entidade autônoma para desempenhar tal função [98].

4 PROPOSTA DE COMO A ABIN PODERIA IMPLEMENTAR A ENGENHARIA DE PRIVACIDADE

Este Capítulo apresenta uma proposta de como a Abin poderia implementar a engenharia de privacidade no desenvolvimento de aplicações de *big data analytics* para a produção da Osint, ainda na fase de sua concepção, com vistas a mitigar os fatores de risco cujos identificadores são FRO-3, FRI-3, FRL-1 e FRF-3 (Capítulo 3) e, com isso, compatibilizar o uso dessa técnica analítica pelo órgão de Inteligência brasileiro com o direito fundamental à proteção de dados pessoais.

Embora a Abin, na condição de órgão público federal, possa adquirir, por meio de licitação, aplicações de *big data analytics* para a produção da Osint, o ideal, por razões de segurança do Estado e de soberania nacional, seria a Abin desenvolver suas próprias aplicações, valendo-se de seus agentes públicos lotados no Cepesc. A propósito, Brustolin et al. [99] e Miller [100] analisaram documentos que demonstram que a empresa suíça Crypto AG era secretamente controlada pela *Central Intelligence Agency* (CIA), serviço de Inteligência norte-americano, e, durante algum tempo, também pela *Bundesnachrichtendienst* (BND), serviço de Inteligência alemão, e que essa empresa, com o apoio técnico da *National Security Agency* (NSA), agência de segurança dos Estados Unidos especializada em Inteligência de sinais, adulterou os equipamentos de criptografia que comercializava, para permitir que os referidos serviços de Inteligência lessem, durante décadas, as comunicações criptografadas de países aliados e adversários que adquiriram esses equipamentos, dentre os quais o Brasil.

A despeito de potenciais vulnerabilidades para o Estado brasileiro que podem advir de eventual aquisição de aplicações de *big data analytics* desenvolvidas por empresas privadas, Hoepman [69] ressalta que as *privacy design strategies* podem ser relevantes para subsidiar a elaboração das especificações nos editais de licitações destinadas a adquirir esse tipo de aplicação.

Para implementar na Abin a engenharia de privacidade no desenvolvimento de aplicações de *big data analytics* para produção da Osint, com o intuito de mitigar os fatores de risco identificados como FRO-3, FRI-3, FRL-1 e FRF-3 (Capítulo 3), esta dissertação propõe a adoção de [62], guia sobre *privacy by design* editado pela AEPD em 2019, complementado por [53], relatório sobre privacy by design em big data produzido pela Enisa em 2015, pelos motivos apresentados a seguir.

Esses dois documentos contemplam medidas administrativas ou organizacionais e técnicas, as quais podem ser entendidas em um sentido amplo como qualquer método ou meio que um controlador pode empregar para que o tratamento de dados pessoais seja feito de forma eficaz, respeitando os princípios de proteção, sendo exemplos de medida técnica o uso de avançadas soluções tecnológicas e de medida administrativa ou organizacional a formação básica dos funcionários da organização em proteção de dados pessoais [77].

A adoção de medidas administrativas ou organizacionais e técnicas é uma imposição da LGPD, que determina, em seu art. 46, *caput*, e § 2º, que desde a fase de concepção do produto ou do serviço até a sua execução, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição,

perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

As medidas administrativas ou organizacionais apresentadas no guia da AEPD estão em consonância com o RGPD, norma que serviu de inspiração para a criação da LGPD, e foram baseadas em [61] e [101], dois artigos da pesquisadora Ann Cavoukian, idealizadora dos sete princípios fundamentais de *privacy by design*, com vistas a implementar esses princípios no desenvolvimento de *softwares* que tratam dados pessoais, desde a sua concepção, para que seja preservada a privacidade dos titulares desses dados.

As medidas técnicas do relatório da Enisa também estão em consonância com o RGPD e foram baseadas em [64], [68] e [69], que tratam das oito *privacy design strategies*, cuja aplicação foi sugerida pela Enisa em [102] e [53]; pela Autoridade de Proteção de Dados da Noruega (*The Norwegian Data Protection Authority*) em [103]; e pelo governo federal brasileiro em [104], guia para fomentar orientações básicas aos desenvolvedores de aplicativos da Administração Pública Federal sobre o desenvolvimento seguro de aplicativos móveis, o que evidencia a robustez e a atualidade dessa teoria.

Ressalte-se que quando a Enisa publicou os dois relatórios [102] e [53], sugerindo a adoção das *privacy design strategies* para a implementação da abordagem *privacy by design*, essa agência era a única instituição a nível da União Europeia dotada de competências e recursos para realizar atividades de investigação e aconselhamento específicas em matéria de privacidade e proteção de dados por *design* e por padrão e em *privacy enhancing technologies*, conforme reconhecido pela Autoridade Europeia para a Proteção de Dados (*European Data Protection Supervisor* - EDPS) em [105] e [106]. Atualmente, a Enisa é a agência da União Europeia dedicada a alcançar um elevado nível comum de cibersegurança em toda a Europa [107].

Finalmente, a utilização das *privacy design strategies* para viabilizar a implementação de uma abordagem de *privacy by design* em plataformas genéricas da Osint foi validada por Koops et al. em [67].

Relativamente à necessidade de complementar o guia da AEPD sobre *privacy by design* com o relatório da Enisa sobre *privacy by design em big data*, essa situação decorre da inovação apresentada nesse último documento consistente na demonstração de como as *privacy design strategies* podem ser inseridas nas fases da cadeia de valor de *big data analytics* e implementadas por medidas técnicas.

Nas próximas Seções deste Capítulo será demonstrado como as medidas administrativas e técnicas provenientes, respectivamente, dos sete princípios fundamentais de *privacy by design* e das oito *privacy design strategies* viabilizam a implementação da engenharia de privacidade no desenvolvimento de *softwares*, inclusive de *big data analytics* para a produção da Osint, e o cumprimento dos princípios gerais de proteção de dados pessoais e dos direitos do titular previstos na LGPD.

4.1 MEDIDAS ADMINISTRATIVAS PARA IMPLEMENTAR OS PRINCÍPIOS FUNDAMENTAIS DA ABORDAGEM PRIVACY BY DESIGN

Os sete princípios fundamentais da abordagem *privacy by design* servem para orientar um programa de privacidade que as organizações devem traduzir em práticas específicas [50]. Nesse sentido, a LGPD estabeleceu a necessidade de observância do *privacy by design* por organizações privadas e públicas ao determinar, expressamente, a indispensabilidade de um programa de governança em privacidade, para

evidenciar algumas regras de boas práticas que devem ser observadas no tratamento dos dados pessoais, tendo como base a natureza do tratamento, seus objetivos e fins e a probabilidade e gravidade dos riscos, sopesados com os benefícios a serem auferidos [57].

Dentre as medidas administrativas ou organizacionais previstas na LGPD, destacam-se a confecção do RIPD previamente ao tratamento de dados pessoais que possa, eventualmente, gerar riscos às liberdades civis e aos direitos fundamentais (art. 5º, inciso XVII); o tratamento apenas dos dados pessoais estritamente necessários para o atingimento de propósitos legítimos e específicos (art. 6º, incisos I, II e III), sendo que as pessoas jurídicas de direito público deverão fazê-lo para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (art. 23, *caput*); o dever imposto aos controladores e operadores de manterem o registro das operações de tratamento de dados pessoais que realizarem (art. 37); a indicação de um encarregado pelo tratamento de dados pessoais pelo controlador e a divulgação da identidade e das informações de contato do encarregado, preferencialmente no sítio eletrônico do controlador (art. 41, *caput* e § 1º); e a formulação de regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (art. 50, *caput*) [9]. Essas medidas administrativas também contribuem para mitigar os fatores de risco cujos identificadores são FRO-3, FRI-3, FRL-1 e FRF-3 (Capítulo 3).

De acordo com Bachlechner et al. [108], as organizações devem possuir encarregados de dados pessoais conhecedores da legislação e capazes de avaliar o impacto e os riscos envolvidos em relação ao tratamento dos dados pessoais coletados. Franzolin e Valente [89] recomenda que as organizações fixem cláusulas contratuais obrigando parceiros a nomearem encarregados pelo tratamento de dados pessoais.

Bachlechner et al. [108] explica que, em geral, as tecnologias por si só não são suficientes para assegurar a proteção dos dados pessoais, sendo necessário adotar, em algum nível, as medidas não técnicas para assegurar que uma determinada tecnologia funcione conforme o esperado.

As medidas administrativas propostas pela AEPD [62] para implementar os princípios fundamentais da abordagem *privacy by design* servem, também, para viabilizar a incorporação da engenharia de privacidade no desenvolvimento de *softwares*, inclusive de *big data analytics* para a produção da Osint, desde a sua concepção, o cumprimento dos princípios gerais de proteção de dados pessoais e dos direitos do titular previstos na LGPD e a mitigação dos fatores de risco cujos identificadores são FRO-3, FRI-3, FRL-1 e FRF-3 (Capítulo 3), conforme evidenciado na Tabela 4.1.

Tabela 4.1: Correlação entre as medidas administrativas, os princípios e direitos previstos na LGPD e os fatores de risco.

Princípios fundamentais de *privacy by design* [61]	**Medidas administrativas ou organizacionais propostas pela AEPD [62]**	**Princípios e direitos na LGPD atendidos pelas medidas administrativas**	**Fatores de risco mitigados pelas medidas administrativas**
1. Proativo e não reativo: a abordagem *privacy by design* é caracterizada pela adoção de medidas proativas para prever e prevenir riscos de privacidade antes que estes se concretizem.	• Compromisso da organização quanto à proteção dos dados pessoais, desde os mais altos níveis da Administração; • desenvolver cultura de comprometimento e melhoria contínua dos trabalhadores; • atribuir responsabilidades para que cada membro da organização esteja ciente de suas tarefas para preservar a privacidade; e • desenvolver métodos sistemáticos baseados em indicadores para a detecção precoce de processos e práticas deficientes em garantir a privacidade.	Princípios da segurança; da prevenção; da não discriminação e da responsabilização e prestação de contas. Direito fundamental de privacidade.	FRI-3 e FRF-3.
2. Privacidade como configuração padrão: *privacy by design* busca garantir que os dados pessoais sejam automaticamente protegidos em qualquer sistema ou prática de negócio. A privacidade é integrada ao sistema como configuração padrão.	• Estabelecer critérios para restringir coleta de dados pessoais ao mínimo necessário; • limitar o uso de dados pessoais aos objetivos para os quais foram coletados e garantir que haja uma base legítima para o tratamento; • restringir o acesso aos dados pessoais de acordo com o "princípio da necessidade de conhecer"e com os perfis de acesso diferenciados; e • definir e cumprir prazos rígidos de retenção.	Princípios da finalidade; da necessidade; e da adequação. Direitos fundamentais de liberdade, de intimidade e de privacidade.	FRO-3 e FRL-1.
3. Privacidade incorporada ao design: *privacy by design* deve ser incorporada no projeto e na arquitetura dos sistemas de TI e nas práticas de negócios, sem diminuir a funcionalidade.	• Considerar a privacidade como um requisito essencial dentro do ciclo de vida dos sistemas e serviços e no desenho de processos organizacionais; • realizar uma análise de risco de privacidade e, quando aplicável, realizar RIPD previamente ao tratamento de dados pessoais; e • documentar todas as decisões da organização relacionadas com privacidade.	Princípios da adequação; segurança; da prevenção; da transparência e da responsabilização e prestação de contas.	FRO-3, FRI-3 e FRL-1.

4. Funcionalidade total: *privacy by design* procura acomodar todos os interesses e objetivos legítimos, evitando a pretensão de falsas dicotomias, como privacidade *versus* segurança, já que é possível ter ambas.	• Identificar e avaliar os diferentes e legítimos interesses da organização e dos titulares dos dados pessoais; • estabelecer canais de comunicação, para compreender os múltiplos interesses que, à primeira vista, possam parecer divergentes; e • gerenciar adequadamente os riscos à privacidade.	Princípios da transparência; da qualidade dos dados; e da prevenção.	FRL-1 e FRF-3
5. Segurança de ponta a ponta: *privacy by design* gerencia com segurança os dados pessoais, de ponta a ponta, ao longo de todo o ciclo de vida desses dados, retendo-os com segurança e os destruindo ao final do tratamento, em tempo hábil.	• Classificar e organizar os dados e as operações de tratamento de dados pessoais com base em perfis de acesso; e • assegurar a destruição segura da informação no final do seu ciclo de vida.	Princípio da segurança. Direitos fundamentais de liberdade, de intimidade e de privacidade.	FRI-3.
6. Visibilidade e Transparência: *privacy by design* busca garantir a todas as partes interessadas que o tratamento dos dados pessoais é realizado de acordo com as promessas e objetivos declarados, sujeitos a verificação independente, seja qual for a prática de negócios ou a tecnologia envolvida.	• Publicizar as políticas de privacidade que regem a organização; • elaborar e publicar cláusulas informativas concisas, claras e compreensíveis, facilmente acessíveis sobre o tratamento dos dados pessoais, os riscos envolvidos e como os direitos dos titulares podem ser exercidos; • compartilhar a identidade e detalhes de contato do controlador; e • estabelecer mecanismos de comunicação e reclamação acessíveis, simples e eficazes para os titulares dos dados pessoais.	Princípio da finalidade; da adequação; e da transparência. Direitos previstos nos arts. 17 e 18 da LGPD.	FRO-3 e FRL-1.

7. Respeito pela privacidade do usuário: *privacy by design e*xige que os desenvolvedores dos sistemas e os agentes de tratamento mantenham os interesses dos titulares dos dados em primeiro lugar.	• Disponibilizar informação completa e adequada que conduza a um consentimento informado, livre, específico e inequívoco que deve ser explícito em todos os casos que o requeiram; • proporcionar aos titulares dos dados o acesso aos seus dados pessoais e a informações detalhadas sobre os objetivos do tratamento; e • implementar mecanismos que permitam aos titulares dos dados exercer os seus direitos em matéria de proteção de dados.	Princípios da finalidade; da adequação; do livre acesso; da qualidade dos dados; da transparência; e da não discriminação. Direitos previstos nos arts. 17 e 18 da LGPD.	FRO-3 e FRF-3.

Fonte: Autor, com base em Cavoukian [61], AEPD [62] e LGPD [9].

O Gabinete do Comissário de Informação do Reino Unido (*Information Commissioner's Office* - ICO) [76] ressalta que as organizações que utilizam aplicações de *big data analytics* precisam justificar desde a concepção do tratamento a necessidade da coleta de conjunto de dados pessoais específicos, para definir as finalidades do tratamento e estabelecer os dados que serão relevantes, com o intuito de minimizar a coleta e o tratamento; e cumprir cronogramas apropriados de retenção dos dados pessoais de acordo com requisitos regulatórios quanto ao tempo em que os registros devem ser mantidos.

Considerando que o art. 4º, § 1º, da LGPD determina que o tratamento de dados pessoais realizado para fins exclusivos de segurança do Estado será regido por legislação específica que preverá medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD [9], as medidas administrativas propostas pela AEPD [62] para implementar os princípios fundamentais da abordagem *privacy by design* podem ser de grande utilidade para a Abin, por contribuirem para o atingimento da conformidade com os princípios gerais de proteção de dados pessoais e dos direitos do titular previstos naquela lei no desenvolvimento de aplicações de *big data analytics* para a produção da Osint e por servirem para mitigar os fatores de risco identificados como FRO-3, FRI-3, FRL-1 e FRF-3 (Capítulo 3).

4.2 MEDIDAS TÉCNICAS PARA IMPLEMENTAR AS PRIVACY DESIGN STRATEGIES

Colesky et al. [68] dividiram as oito *privacy design strategies* em duas categorias diferentes: estratégias orientadas a dados e estratégias orientadas a processos. A primeira categoria, estratégias orientadas a dados, objetiva mitigar riscos de privacidade e compreende as seguintes estratégias: *hide, minimize, separate* e *abstract*. De acordo com Hoepman [69], a segunda categoria, estratégias orientadas a processos, foca nos processos, para que o tratamento de dados pessoais seja feito de forma responsável, abrangendo aspectos organizacionais e procedimentais, e compreende quatro estratégias: *inform, control, enforce* e *demonstrate*.

As *privacy design strategies* funcionam como pontes entre os princípios de proteção dos dados pessoais impostos por lei e a implementação da privacidade em soluções concretas e estão centradas em mitigar riscos à privacidade decorrentes das operações de tratamento de dados pessoais, sendo desejável que todas as estratégias ou a maioria deles sejam implementadas, a fim de tornar os sistemas mais amigáveis à privacidade [62].

Esta dissertação apresenta as definições das oito *privacy design strategies* e das suas táticas associadas, conforme [68] e [69], e as correlaciona com os princípios gerais de proteção de dados pessoais e com os direitos do titular previstos na LGPD e com os fatores de risco identificados como FRO-3, FRI-3, FRL-1 e FRF-3 (Capítulo 3), consoante evidenciado na Tabela 4.2. Com isso, pretende-se demonstrar que as *privacy design strategies* e as suas táticas associadas servem para implementar os princípios e direitos da LGPD ainda na fase de concepção do desenvolvimento de *softwares* que respeitam o direito fundamental à proteção de dados pessoais, incluindo aplicações de *big data analytics* para produção da Osint, e para mitigar os quatro fatores de risco mencionados.

Tabela 4.2: Correlação das *privacy design strategies* e das suas táticas com os princípios e direitos previstos na LGPD e com os fatores de risco.

Privacy design strategies	**Táticas associadas**	**Princípios e direitos na LGPD atendidos pelas estratégias e táticas associadas / Fatores de risco mitigados**
1 - ***Minimize***: limitar o tratamento, coletando dados de menos pessoas ou menos dados pessoais.	*Select*: selecionar previamente quais pessoas e atributos são relevantes, tratando apenas dados pessoais estritamente necessários que satisfaçam os critérios da seleção. Usar uma lista branca.	Princípios da finalidade; da adequação; da necessidade; da segurança; da prevenção; e da transparência. Direito ao bloqueio ou à eliminação de dados desnecessários ou excessivos. / FRO-3 e FRL-1.
	Exclude: determinar previamente quais pessoas e atributos são irrelevantes, não tratando esses dados ou excluindo-os logo após a coleta. Usar uma lista negra.	
	Strip: estabelecer prazos de retenção e mecanismos de exclusão automática dos dados pessoais na camada de aplicação quando o período expirar ou quando não forem mais necessário.	
	Destroy: apagar definitivamente os dados pessoais na camada de armazenamento físico quando deixarem de ser relevantes, usando meios técnicos para impossibilitar sua recuperação.	
2 - ***Separate***: separar o tratamento de dados pessoais.	*Isolate*: coletar e tratar dados pessoais em diferentes bancos de dados ou aplicações, separados logicamente em *hardwares* diferentes.	Princípios da segurança; da prevenção. Direito de privacidade. / FRI-3.
	Distribute: distribuir o tratamento por diferentes locais físicos que não estejam sob o controle de uma única entidade, por meio de arquiteturas de sistemas distribuídos ou descentralizados.	
3 - ***Abstract***: limitar o tratamento dos detalhes dos dados pessoais.	*Summarise*: resumir atributos detalhados em atributos gerais e com mais granularidade. Por exemplo, usar uma faixa etária em vez de uma data de nascimento específica.	Princípios da segurança; da prevenção; e da não discriminação. Direito de privacidade. / FRI-3 e FRF-3.
	Group: agregar informações médias de um grupo de pessoas em vez de tratar dados pessoais de um indivíduo específico.	
	Perturb: tratar dados pessoais modificados por valores aproximados ou por ruído aleatório.	

4 - ***Hide***: restringir acesso aos dados pessoais ou torná-los indissociáveis ou inobserváveis.	*Restrict*: restringir o acesso a dados pessoais, por meio de uma política rígida de controle de acesso, baseada no princípio da "necessidade de conhecer". Dificultar o compartilhamento acidental ou vazamento de dados pessoais .	Princípios da segurança; da prevenção; e da responsabilização e prestação de contas. Direitos de intimidade e de privacidade. / FRI-3.
	Obfuscate: usar criptografia e *hashing*, para tornar os dados pessoais ininteligíveis para quem não esteja autorizado a acessá-los.	Princípios da segurança e da prevenção. Direito de privacidade. / FRI-3.
	Dissociate: remover os dados de identificação direta, para evitar correlação entre eventos, pessoas e dados pessoais.	Princípios da segurança; da prevenção; e da responsabilização e prestação de contas. Direito de privacidade. / FRI-3.
	Mix: misturar dados pessoais, para ocultar a fonte ou suas interrelações; ou anonimizar dados pessoais.	Princípios da segurança; e da prevenção. Direito de privacidade e anonimização. / FRI-3.
5 - ***Inform***: informar os titulares dos dados sobre o tratamento de forma oportuna e adequada.	*Supply*: fornecer informações sobre quais dados pessoais são tratados, finalidade do tratamento, tempo de retenção e terceiros com os quais os dados são compartilhados e disponibilizar contato do encarregado e política de privacidade.	Princípios da finalidade; da adequação; e da transparência. Direitos de liberdade; de privacidade; e de obter do controlador informação das entidades públicas e privadas com as quais houve uso compartilhado de dados. / FRO-3 e FRL-1.
	Explain: explicar em linguagem clara e simples quais dados pessoais são tratados, necessidade e finalidade do tratamento.	Princípios da finalidade; da adequação; da transparência. Direitos de liberdade e de privacidade. / FRO-3.
	Notify: notificar os titulares quando seus dados forem tratados ou compartilhados com terceiros e quando houver violação de segurança com risco para suas liberdades e direitos. Permitir aos usuários controlar as notificações que querem receber.	Princípios da transparência; da segurança; e da prevenção.Direitos de liberdade; de privacidade e de obter do controlador informação das entidades públicas e privadas com as quais houve uso compartilhado de dados. / FRO-3 e FRI-3.
6 - ***Control***: fornecer aos titulares controle sobre o tratamento de seus dados pessoais.	*Consent*: adquirir consentimento explícito e informado dos titulares dos dados para o tratamento de seus dados pessoais, em caso de inexistência de outra base legal para o tratamento, e possibilitar a retratação do consentimento.	Princípios da transparência; e da prevenção. Direitos de liberdade; e de obter do controlador eliminação dos dados pessoais tratados com o consentimento; informação sobre possibilidade de não fornecer consentimento e consequências da negativa; e revogação do consentimento. / FRO-3.

	Choose: a funcionalidade básica deve ser acessível para pessoas que não consentem com o tratamento de seus dados pessoais. Oferecer alternativa com funcionalidades avançadas.	Princípio da não discriminação. Direitos de liberdade; e de obter do controlador informação sobre possibilidade de não fornecer consentimento e suas consequências. / FRO-3.
	Update: oferecer aos usuários meios para revisar e atualizar os dados pessoais coletados sobre eles, o que pode ser combinado com uma abordagem que permita aos usuários visualizar os dados pessoais coletados.	Princípios do livre acesso; da qualidade dos dados; da transparência; e da não discriminação. Direito de obter do controlador confirmação da existência de tratamento; acesso aos dados; correção e eliminação de dados. / FRO-3, FRL-1 e FRF-3.
	Retract: fornecer mecanismos para que os titulares possam excluir seus dados pessoais ou solicitarem essa exclusão, o que pode ser feito por meio de um *dashboard*.	Princípios do livre acesso; da qualidade dos dados; da transparência. Direitos de liberdade; de privacidade; e de obter do controlador eliminação dos dados. / FRO-3 e FRL-1 .
7 - ***Enforce***: observar a privacidade no tratamento e implementar medidas necessárias.	*Create*: criar uma política de privacidade, destinar recursos para executar esta política e especificar a finalidade e o fundamento legal de cada processo de tratamento.	Princípios da transparência; da segurança; da prevenção; da não discriminação; e da responsabilização e prestação de contas. Direito de privacidade. / FRO-3, FRI-3, FRL-1 e FRF-3.
	Mantain: manter política de privacidade com implementação de controles; atribuir responsabilidades; treinar o pessoal e exigir que terceiros processadores cumpram essa política.	
	Uphold: revisar a política de privacidade regularmente e ajustá-la quando necessário, de modo que essa política fique alinhada com o plano geral de negócios e a missão da organização.	
8 - ***Demonstrate***: demonstrar para a ANPD que o tratamento respeita a privacidade.	*Record*: documentar e fundamentar as decisões sobre o tratamento de dados pessoais; coletar *logs* do sistema e respostas a anomalias.	Princípios da transparência; da segurança; da prevenção; da não discriminação; e da responsabilização e prestação de contas. Direito de privacidade. / FRO-3, FRI-3, FRL-1 e FRF-3.
	Audit: auditar regularmente os *logs*, os processos organizacionais e os processos de tratamento.	
	Report: relatar os resultados das auditorias à ANPD ou guardá-los para referência futura e consultá-la quando necessário.	

Fonte: Autor, com base em Hoepman [69] e na LGPD [9].

No que diz respeito à estratégia *minimize*, Hoepman [69] ressalta que mesmo na mineração de dados, no aprendizado de máquina e no tratamento de *big data* é necessário considerar maneiras de minimizar o conjunto final de dados pessoais retidos, selecionando apenas os dados que que sejam relevantes e descartando o restante. Isso deve ser levado em consideração no desenvolvimento de aplicações de *big data analytics* para produção da Osint.

Relativamente à estratégia *control*, Hoepman [69] esclarece que o consentimento nem sempre é necessário para tratar dados pessoais, haja vista que, além do consentimento, há outras bases legais autorizativas do tratamento, e que nem sempre é possível ou mesmo necessário permitir que os titulares corrijam seus dados pessoais ou tenham a solicitação de exclusão desses dados atendida pelos agentes de tratamento. Conforme demonstrado anteriormente nas Seções 3.3.2 e 3.3.3, o tratamento de dados pessoais realizado pela Abin no exercício da atividade de Inteligência, com finalidade exclusiva de segurança do Estado, está amparado, como regra geral, na base legal de execução de competências legais, prevista no art. 23 da LGPD, o que tornaria desnecessário o consentimento do titular dos dados pessoais. Além disso, a Abin pode restringir o acesso dos titulares aos seus dados pessoais, quando tais dados estiverem classificados ou protegidos por hipóteses legais de sigilo. Essa restrição está prevista no art. 5º, inciso XXXIII, da Constituição Federal de 1988, e é aplicável a informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado. No plano infraconstitucional, esse mandamento constitucional é complementado pelos arts. 9º e 9º-A da Lei nº 9.883/1999, criados para assegurar o êxito das atividades sigilosas e estratégicas da Abin.

Consoante mencionado anteriormente, [62], guia da AEPD, deve ser complementado por [53], relatório da Enisa sobre *privacy by design* em *big data* que demonstra como as *privacy design strategies* podem ser inseridas em cada fase da cadeia de valor de *big data analytics* e que apresenta possíveis medidas técnicas para implementá-las. Outras medidas técnicas também são apresentadas por Saltarella et al. em [109], artigo científico de revisão da literatura que sistematizou as melhores práticas para implementar as *privacy design strategies*, do ponto de vista tecnológico, obtidas a partir dos requisitos do RGPD e da análise de noventa e um artigos científicos selecionados no estudo.

A Tabela 4.3 sistematiza os resultados obtidos pela Enisa [53] em relação à inserção das *privacy design strategies* em cada fase da cadeia de valor de *big data analytics* e os correlaciona com as possíveis medidas técnicas para implementá-las e com os fatores de risco identificados como como FRO-3, FRI-3, FRL-1 e FRF-3 (Capítulo 3).

Tabela 4.3: Possíveis medidas técnicas para implementar as *privacy design strategies* na cadeia de valor de *big data analytics* e sua correlação com os fatores de risco.

Ordem	**Fase da cadeia de valor de *big data analytics***	***Privacy design strategies***	**Possíveis medidas técnicas para implementar as *privacy design strategies* / Fatores de risco mitigados pelas medidas técnicas**
1	**Aquisição e coleta**	*Minimize*	Definir quais dados pessoais são necessários para a finalidade do tratamento e períodos de retenção; excluir dados pessoais desnecessários; reduzir os detalhes; fornecer mecanismos de exclusão; e elaborar RIPD, para limitar o tratamento aos dados necessários para a finalidade. / FRO-3 e FRL-1.
		Abstract	Anonimizar localmente (na fonte) os dados pessoais antes de liberá-los para análise; e produzir RIPD, para identificar situações em que é possível utilizar informações agregadas em vez dos dados pessoais, como ocorre na análise estatística de fontes distribuídas. / FRI-3 e FRF-3.
		Hide	Usar *privacy enhancing technologies*, como ferramentas antirrastreamento, criptografia, mascaramento de identidade e compartilhamento seguro de arquivos./ FRI-3.
		Inform	Fornecer avisos aos titulares sobre o tratamento de seus dados pessoais; e usar mecanismos de transparência durante todo o tratamento de *big data*, para obter consentimento informado. / FRO-3 e FRI-3.
		Control	Implementar mecanismos de obtenção e exclusão do consentimento do titular dos dados pessoais, se esta for a base legal para o tratamento, e adotar políticas de privacidade adesivas. / FRO-3.
2	**Análise e curadoria**	*Abstract*	Utilizar técnicas de anonimização, tais como k-anonimato, privacidade diferencial, etc. / FRI-3.
		Hide	Utilizar criptografia pesquisável, criptografia homomórfica e computações multipartidárias seguras, especialmente no contexto da realização de pesquisas e cálculos sobre dados criptografados. / FRI-3.
3	**Armazenamento**	*Hide*	Criptografar os dados pessoais armazenados; e implementar mecanismos de autenticação e de controle de acesso, para proteger dados pessoais em bancos de dados./ FRI-3.
		Separate	Armazenar e analisar os dados pessoais de forma distribuída e descentralizada; e adotar medidas de controle de acesso e técnicas de criptografia. / FRI-3.
4	**Uso dos dados**	*Abstract*	Assegurar a qualidade e a proveniência dos dados pessoais no decurso da tomada de decisão baseada em *big data*. / FRF-3.
5	**Aplicáveis em todas as quatro fases.**	*Enforce e Demonstrate*	Utilizar ferramentas automatizadas de definição de políticas de privacidade, atribuir responsabilidades e buscar conformidade com as políticas de privacidade. / FRO-3, FRI-3, FRL-1 e FRF-3.

Fonte: Adaptado de Enisa [53].

Após definir as *privacy design strategies*, é necessário implementá-las nas fases de projeto e de desenvolvimento do sistema, por meio dos *privacy design patterns* e das *privacy enhancing technologies*. De acordo com a AEPD [62], um mesmo *privacy design pattern* pode responder a múltiplas *privacy design strategies*, fornecendo soluções para diferentes problemas que aparecem ao longo das atividades de processamento de dados, e uma única *privacy enhancing technology* pode ser usada para implementar vários *privacy design patterns*.

Na fase de projeto, para implementar as *privacy design strategies* podem ser utilizados os *privacy design patterns*, definidos como soluções reutilizáveis para resolver problemas de privacidade comuns e reiterados que aparecem repetidamente em um contexto específico durante o desenvolvimento de produtos e sistemas [62]. Geralmente, a descrição dos *privacy design patterns* contém pelo menos seu nome, sua finalidade, seu contexto de aplicação, objetivos, estrutura, implementação (relação com outros padrões), as consequências de sua aplicação e usos conhecidos. Exemplos de *privacy design patterns* e sua descrição podem ser obtidos em [110] e [111].

Na fase de desenvolvimento, são utilizadas as *privacy enhancing technologies*, grupo organizado e coerente de soluções de tecnologia da informação e comunicações que reduzem os riscos de privacidade através da implementação de estratégias e padrões previamente definidos [62]. As *privacy enhancing technologies* podem variar de uma única ferramenta técnica a uma implantação completa, dependendo do contexto, do escopo e da própria operação de tratamento de dados pessoais [58], e a sua eficácia pode variar em função da evolução tecnológica, o que dificulta a elaboração de uma classificação e tipologia atualizadas [62].

A despeito dessa dificuldade, a AEPD [62] propõe uma classificação das *privacy enhancing technologies* baseada nos objetivos dessas tecnologias, dividindo-as nas que se destinam a proteger a privacidade (por exemplo, ocultar dados pessoais ou eliminar a necessidade de identificação) e nas que buscam gerenciá-la (criptografia de comunicações seguras, anonimizadores, anti-rastreadores etc.). A Enisa [58] apresenta as principais *privacy enhancing technologies*, seus pontos fortes e sua aplicabilidade em relação ao cumprimento dos princípios de proteção de dados pessoais previstos no artigo 5º do RGPD. Jordan et al. [112] propõem uma classificação dessas tecnologias em três categorias: algorítmica, arquitetural ou de aumento. A algorítmica protege a privacidade alterando a forma como os dados são representados, mas mantendo as informações necessárias para permitir seu uso, sendo exemplos a criptografia homomórfica, a privacidade diferencial e as provas de conhecimento zero; a arquitetural foca na troca confidencial de informações entre várias partes sem compartilhar os dados subjacentes e incluem aprendizado federado e computação multipartidária; e a categoria de aumento protege a privacidade usando distribuições históricas para direcionar a geração de dados realistas que aumentam as fontes de dados existentes, sendo exemplos os dados sintéticos e *digital twinning*.

As soluções tecnológicas para mitigar os problemas de privacidade causados pelo tratamento de dados pessoais em larga escala são múltiplas, estão em rápido desenvolvimento [113], intimamente ligadas entre si e, na prática, precisam ser combinadas para serem eficazes, inexistindo uma classe única de tecnologias mais importante [108].

A adoção de medidas técnicas e administrativas ou organizacionais está em consonância com os princípios da segurança e da prevenção, previstos no art. 6º, inciso VII e VIII, da LGPD, respectivamente. O

princípio da segurança determina que os agentes de tratamento devem utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; enquanto o da prevenção exige que sejam adotadas medidas para prevenir a ocorrência de danos nas operações de tratamento de dados pessoais. Em complemento, o art. 46, § 1º, da LGPD atribui à ANPD a possibilidade de regulamentar padrões técnicos mínimos sobre essas medidas, considerando a natureza das informações tratadas, as características específicas do tratamento, o estado atual da tecnologia e os princípios gerais de proteção [9].

Incorporar a proteção de dados pessoais ainda na concepção do software é cada vez mais reconhecida como a abordagem certa para garantir uma conformidade durável e eficiente com a lei de proteção de dados [93], haja vista que as violações de privacidade de dados pessoais podem ser evitadas se os requisitos de privacidade forem devidamente obtidos na fase de especificação dos requisitos funcionais e não funcionais, ainda no início do desenvolvimento de software [114]. Os requisitos funcionais definem a principal finalidade do negócio e as especificidades do sistema a ser desenvolvido, enquanto os requisitos não funcionais são aplicáveis a todos os sistemas e dizem respeito a questões horizontais, como necessidades de segurança e cumprimento das leis aplicáveis [106]. Na engenharia de sistemas, a privacidade geralmente é incluída como um requisito não funcional, haja vista que na maioria das aplicações ela é auxiliar ao objetivo principal do sistema, apesar de a privacidade também poder aparecer como um requisito funcional de uma determinada aplicação, como o sistema de anonimato Tor [78]. Os requisitos de privacidade do sistema são obtidos principalmente de leis, regulamentos, padrões e expectativas das partes interessadas [33].

Para garantir a incorporação da privacidade nos estágios iniciais do desenvolvimento de *software*, é necessário considerar a privacidade como uma exigência essencial dentro do ciclo de vida de sistemas e serviços e na concepção de processos organizacionais; analisar os riscos aos direitos e liberdades das pessoas naturais e, quando aplicável, realizar relatório de impacto à proteção de dados pessoais, como parte integrante de qualquer nova iniciativa de tratamento [62], haja vista que, a partir da avaliação das vulnerabilidades potenciais do sistema e das possíveis ameaças, é possível selecionar controles técnicos e gerenciais adequados para prevenir ou mitigar os riscos [33].

Portanto, assim como as medidas administrativas propostas pela AEPD [62] para implementar os princípios fundamentais da abordagem *privacy by design*, as medidas técnicas decorrentes das *privacy design strategies* também podem ser de grande utilidade para a Abin, por contribuirem para o atingimento da conformidade com os princípios gerais de proteção de dados pessoais e com os direitos do titular previstos na LGPD no desenvolvimento de aplicações de big data analytics para a produção da Osint. Além disso, essas medidas técnicas servem para mitigar os fatores de risco cujos identificadores são FRO-3, FRI-3, FRL-1 e FRF-3 (Capítulo 3).

5 CONCLUSÃO

A atividade de Inteligência de Estado configura uma política pública prevista na Lei nº 9.883/1999, regulamentada pelo Decreto nº 8.793/2016 e executada pela Abin, na qualidade de órgão central do Sisbin. A Abin realiza tratamento de dados pessoais com finalidade exclusiva de segurança do Estado, conforme se depreende das competências legais desse órgão, e, por esse motivo, as disposições da LGPD, em tese, não incidiriam sobre essa atividade, por força do disposto no inciso III, alínea "c", do art. 4º dessa lei. Entretanto, mesmo diante dessa exceção legal, o direito fundamental à proteção de dados pessoais e a LGPD incidem na atividade de Inteligência da Abin, em virtude da aplicação imediata das normas definidoras dos direitos e garantias fundamentais.

Os objetivos deste trabalho foram a identificação, a análise e o tratamentos dos possíveis fatores de risco para a Abin decorrentes dessa incidência. Foram analisados acórdãos recentes do STF versando sobre a proteção de dados pessoais. Em dois desses acórdãos, a Suprema Corte brasileira reconheceu que essa proteção é direito fundamental autônomo e, à época, implícito no texto constitucional. Com isso, também se demonstrou haver uma interpretação desse direito, antes mesmo do advento da LGPD. Posteriormente, essa proteção foi incluída, também, entre os direitos e garantias fundamentais da Constituição Federal de 1988, por meio da Emenda Constitucional nº 115, promulgada em 10 de fevereiro de 2022.

Com base na legislação, no direito comparado, em recentes decisões do STF sobre o direito fundamental à proteção dos dados pessoais, em estudos de agências governamentais brasileiras e de outros países e em artigos científicos, este trabalho obteve como principais resultados a identificação dos possíveis fatores de risco para a Abin decorrentes da incidência daquele direito fundamental e da LGPD na atividade de Inteligência de Estado e nas aplicações de *big data analytics* utilizadas pelo serviço de Inteligência brasileiro para a produção da Osint; a análise das consequências de eventual materialização desses fatores; a proposição de medidas para mitigá-los e a demonstração de que o direito fundamental à proteção de dados pessoais e a LGPD podem ser limitados pelo art. 5º, inciso XXXIII, da Constituição Federal de 1988, que restringe o acesso a informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado, a fim de assegurar o êxito das atividades sigilosas da Abin.

Embora o objetivo deste trabalho não fosse o mapeamento e a avaliação de todos os riscos potenciais, utilizou-se a tipologia prevista no art. 18 da Instrução Normativa Conjunta MP/CGU nº 1/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Essa tipologia é útil para classificar alguns fatores de risco identificados e divididos em: operacionais, de imagem ou à reputação, legais e financeiros ou orçamentários. Demonstrou-se, por exemplo, que a eventual ocorrência dos fatores de risco identificados poderia acarretar a suspensão ou a anulação de operações de Inteligência desenvolvidas pela Abin que envolvam tratamento de dados pessoais. Ainda, que isso poderia atrair uma repercussão negativa na imagem do órgão perante a sociedade. Ou, ainda, isso poderia ensejar o ajuizamento de ações judiciais de indenização por danos morais pela inobservância do direito fundamental à proteção de dados pessoais na atividade de Inteligência desempenhada pela Abin.

Assim, como pesquisa aplicada, foram propostas algumas medidas para mitigar os riscos identificados,

abrangendo o cumprimento pela Abin de deveres previstos na LGPD, como o registro de todas as operações de dados pessoais e a confecção do RIPD nas hipóteses previstas nessa Lei. Foram sugeridas, ainda, o estabelecimento de regras de boas práticas, bem como a implementação de um programa de governança em privacidade e a imediata observância do devido processo legal, dos princípios gerais de proteção e dos direitos do titular dos dados pessoais.

Além disso, considerando que a maioria dos conhecimentos produzidos pelos serviços de Inteligência se valem de dados, inclusive pessoais, coletados em fontes abertas no contexto de *big data*, este trabalho demonstrou que os fatores de risco para a Abin relacionados com o tratamento de dados pessoais obtidos por meio de aplicações de *big data analytics* para a produção da Osint poderiam ser mitigados pela elaboração do RIPD previamente ao tratamento desses dados e pelo desenvolvimento, por meio do Cepesc, de suas próprias aplicações de *big data analytics*, para produção da Osint, com observância dos princípios fundamentais da abordagem *privacy by design* e das *privacy design strategies*.

Com isso, confirmou-se a hipótese de que, se o direito fundamental à proteção dos dados pessoais e a LGPD – ao menos em parte – incidem na atividade de Inteligência da Abin, inclusive nas aplicações de *big data analytics* utilizadas por esse órgão para a produção da Osint, então poderão decorrer para esse órgão fatores de risco com potencial de impactar o cumprimento de sua missão institucional.

Na sequência, esta dissertação apresentou a sua primeira contribuição, qual seja, a proposição de sugestões para futuro Anteprojeto de Lei de Proteção de Dados Pessoais nas Atividades de Segurança do Estado, levando em consideração as peculiaridades da atividade de Inteligência da Abin e a necessidade de assegurar os direitos dos titulares dos dados pessoais.

Recomendou-se por exemplo que o futuro Anteprojeto estabeleça como base autorizativa do tratamento de dados pessoais na atividade de Inteligência de Estado o cumprimento das atribuições legais do serviço público, de forma semelhante com a base autorizativa prevista no regulamento da Europol. Ainda, que o Anteprojeto preveja regras sobre a realização de acordos de cooperação para disciplinar com nível de proteção equivalente ao da União Europeia as transferências internacionais de dados pessoais entre a Abin e órgãos de Inteligência estrangeiros, países terceiros ou organizações internacionais; tudo para assegurar direitos efetivos aos titulares dos dados pessoais transferidos.

Finalmente, este trabalho apresentou a sua segunda contribuição como pesquisa aplicada, qual seja, proposta para implementar na Abin a engenharia de privacidade no desenvolvimento de aplicações de *big data analytics* para a produção da Osint, ainda na fase de concepção desses *softwares*, por meio da adoção de medidas administrativas para implantar os princípios fundamentais da abordagem *privacy by design* e de medidas técnicas decorrentes das *privacy design strategies*. Com isso, a Abin conseguiria compatibilizar a utilização de aplicações de *big data analytics* em sua atividade de Inteligência de Estado com a observância da LGPD e do direito fundamental à proteção de dados pessoais.

Espera-se que esta dissertação auxilie a Abin a mitigar o elevado risco de privacidade decorrente do uso de aplicações de *big data analytics* em suas operações de tratamento de dados pessoais e, ao mesmo, a ampliar a sua capacidade de coleta e análise de grandes volumes de dados, inclusive pessoais, disponíveis em *big data*, por meio do desenvolvimento de suas próprias aplicações analíticas para a produção da Osint, com o necessário respeito ao direito fundamental à proteção dos dados pessoais, considerando que o modelo de negócio desse órgão é produzir conhecimentos a partir de dados, para assessorar de forma oportuna

e relevante o Presidente da República. Em última análise, entende-se que a adoção das sugestões contidas neste trabalho contribuiria para aumentar a confiança da sociedade na Inteligência de Estado, a qual, por determinação legal, deve ser exercida com irrestrita observância dos direitos e garantias individuais.

Como trabalho futuro, propõe-se a realização de pesquisa sobre metodologia específica para a elaboração de RIPD para aplicações de *big data analytics* destinadas para a produção da Osint, com vistas a mitigar os riscos decorrentes da utilização dessa técnica analítica no tratamento de dados pessoais e, com isso, resguardar os direitos dos titulares dos dados pessoais e, ao mesmo tempo, maximizar, na medida do possível, a coleta e análise de dados disponíveis em fontes abertas.

REFERÊNCIAS BIBLIOGRÁFICAS

1 HRIBAR, G.; PODBREGAR, I.; IVANUŠA, T. Osint: a “grey zone”? *International Journal of Intelligence and CounterIntelligence*, v. 27, n. 3, p. 529–549, 2014. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/08850607.2014.900295>. Acesso em: 23/02/2023.

2 SOUZA, D. F. de; BOMFIM, D. R. D. do. Ciência de dados e produção de conhecimentos de inteligência. *Revista Brasileira de Inteligência*, n. 16, p. 53–77, 2021. Disponível em: <https://rbi.enap.gov.br/index.php/RBI/article/view/196>. Acesso em: 23/02/2023.

3 POTZ, T. *The Increasing Importance of OSINT as a Source of Intelligence*. Tese (Doutorado) — University of Zagreb. The Faculty of Political Science. International Relations and Security Studies, 2021. Disponível em: <https://repozitorij.unizg.hr/islandora/object/fpzg:1381>. Acesso em: 24/02/2023.

4 BRASIL. *Decreto de 15 de dezembro de 2017*. Aprova a Estratégia Nacional de Inteligência. Brasília, DF: Presidência da República, 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm>. Acesso em: 25/10/2021.

5 SARLET, I. W. 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*, Belo Horizonte: Fórum, v. 14, n. 42, p. 179–218, 2020. Disponível em: <http://dfj.emnuvens.com.br/dfj/article/view/875>. Acesso em: 29/06/2022.

6 GOSAIN, A.; CHUGH, N. Privacy preservation in big data. *International Journal of Computer Applications*, v. 100, n. 17, p. 44–47, ago. 2014. Disponível em: <https://www.ijcaonline.org/archives/volume100/number17/17619-8322>. Acesso em: 24/02/2023.

7 SHERE, A. Reading the investigators their rights: a review of literature on the general data protection regulation and open-source intelligence gathering and analysis. *The New Collection*, v. 3, p. 3–21, 2020. Disponível em: <https://mcrweb-18.new.ox.ac.uk/docs/NewCollection2020.pdf#page=11>. Acesso em: 24/02/2023.

8 BOTELHO, M. C. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a Lei Geral de Pproteção de Dados Pessoais. *Argumenta Journal Law*, n. 32, p. 191–207, jan./jun. 2020. Disponível em: <http://www.seer.uenp.edu.br/index.php/argumenta/article/view/1840>. Acesso em: 24/02/2023.

9 BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709compilado.htm>. Acesso em: 25/10/2021.

10 RUARO, R. L.; SARLET, G. B. S. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) - L. 13.709/2018. *Revista direitos fundamentais & democracia (UniBrasil)*, v. 26, n. 2, p. 81–106, 2021. Disponível em: <https://repositorio.pucrs.br/dspace/handle/10923/20146>. Acesso em: 24/02/2023.

11 MENDES, L. S. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *In*: SOUZA, C. A; MAGRANI, E.; SILVA, P. (org.). *Lei Geral de Proteção de Dados - Caderno Especial*, São Paulo: Ed. Revista dos Tribunais, p. 35–56, 2019.

12 LIMBERGER, T. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. *Revista do Direito*, n. 30, p. 138–160, jul./dez. 2008. Disponível em: <https://online.unisc.br/seer/index.php/direito/article/view/580>. Acesso em: 24/02/2023.

13 NEGRI, S. M. C. d. Á.; OLIVEIRA, S. R. de; COSTA, R. S. O uso de tecnologias de reconhecimento facial baseadas em inteligência artificial e o direito à proteção de dados. *Revista Direito Público*, v. 17, n. 93, p. 82–10, maio/jun. 2020. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740>. Acesso em: 29/06/2022.

14 BRASIL. *Lei nº 9.883, de 7 de dezembro de 1999*. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Brasília, DF: Presidência da República, 1999. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm>. Acesso em: 25/10/2021.

15 BRASIL. Supremo Tribunal Federal. *Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387*. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Intimado: Presidente da República. Relatora: Min. Rosa Weber, 7 maio 2020. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf>. Acesso em: 29/06/2022.

16 BRASIL. Supremo Tribunal Federal. *Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.529*. Requerentes: Rede Sustentabilidade e Partido Socialista Brasileiro. Intimados: Presidente da República e Congresso Nacional. Relatora: Min. Cármen Lúcia, 13 ago. 2020. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344695258&ext=.pdf>. Acesso em: 29/06/2022.

17 BRASIL. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Congresso Nacional, 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm>. Acesso em: 24/02/2023.

18 BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 6.649*. Requerente: Conselho Federal da Ordem dos Advogados do Brasil. Intimado: Presidente da República. Relator: Min. Gilmar Mendes, 15 set. 2022. Disponível em: <https://portal.stf.jus.br/processos/downloadTexto.asp?id=5641150&ext=RTF>. Acesso em: 24/02/2023.

19 BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental nº 695*. Requerente: Partido Socialista Brasileiro. Intimado: União. Relator: Min. Gilmar Mendes, 15 set. 2022. Disponível em: <https://portal.stf.jus.br/processos/downloadTexto.asp?id=5641211&ext=RTF>. Acesso em: 24/02/2023.

20 BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, [2023]. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm>. Acesso em: 24/02/2023.

21 SARLET, I. W.; MARINONI, L. G.; MITIDIERO, D. *Curso de Direito Constitucional.* 11ª ed. rev. e atual. São Paulo: Saraiva Educação, 2022. *E–book*. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786553620490/>. Acesso em: 04/08/2022.

22 SOUZA, S. M. P. C. d. *Possíveis impactos da LGPD na atividade de inteligência do Cade.* Monografia (Especialização). - Brasília: Escola Nacional de Administração Pública (Enap). Planejamento e Orçamento, jun. 2020. Disponível em: <http://repositorio.enap.gov.br/handle/1/6283>. Acesso em: 29/06/2022.

23 GIL, A. C. *Como elaborar projetos de pesquisa.* 7ª ed. Barueri: Atlas, 2022. *E–book*. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559771653/>. Acesso em: 29/06/2022.

24 WAZLAWICK, R. S. *Metodologia de Pesquisa para Ciência da Computação.* 3ª ed. Rio de Janeiro: LTC, 2021. *E–book*. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788595157712/>. Acesso em: 29/06/2022.

25 BRASIL. Controladoria-Geral da União. *Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016*. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Brasília, DF, p. 1–3, 10 maio 2016. Disponível em: <https://repositorio.cgu.gov.br/handle/1/33947>. Acesso em: 29/11/2021.

26 RIBEIRO, M. M.; NUNES, R. R.; GIOZZA, W. F. Inteligência de Estado, aplicações de big data analytics e o direito fundamental à proteção de dados pessoais. In: *V Congresso de Gestão de Operações e Projetos em Organizações Públicas*. Brasília: Universidade de Brasília, 2022. Disponível em: <https://drive.google.com/file/d/1uUUgPdZKRIgLrH4EzLPh_fD2j4AiqbcL/view>. Acesso em: 26/02/2023.

27 CYBOK.ORG. *CyBOK. The Cyber Security Body of Knowledge*. Versão 1.1.0, 31 jul. 2021. Disponível em: <https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf>. Acesso em: 29/03/2023.

28 CYBOK.ORG. *Opening up the world of cyber security: How the online landscape calls for increased knowledge*. 2021. Disponível em: <https://www.cybok.org/news/cybok-version-11-now-live>. Acesso em: 29/03/2023.

29 OORSCHOT, P. C. van. Coevolution of Security's Body of Knowledge and Curricula. *IEEE Security Privacy*, v. 19, n. 5, p. 83–89, 2021. Disponível em: <https://ieeexplore.ieee.org/document/9529234>. Acesso em: 29/03/2023.

30 OLUKOYA, O. Assessing frameworks for eliciting privacy security requirements from laws and regulations. *Computers Security*, v. 117, p. 102697, 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404822000955>. Acesso em: 29/03/2023.

31 BARRETT, M. *Framework for Improving Critical Infrastructure Cybersecurity*. NIST Cybersecurity Framework, versão 1.1, 16 abr. 2018. Disponível em: <https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11>. Acesso em: 30/03/2023.

32 NIST. National Institute of Standards and Technology. *NIST Privacy Framework. A Tool for Improving Privacy Through Enterprise Risk Management*. versão 1.0, mar. 2020. Disponível em: <https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf>. Acesso em: 23/06/2022.

33 STALLINGS, W. *Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices*. Boston: Addison-Wesley Professional, 2019.

34 UNB. Universidade de Brasília. Programa de Pós-Graduação Profissional em Engenharia Elétrica. *Edital nº 8/2020*. Seleção de candidatos às vagas do Programa de Pós-Graduação Profissional em Engenharia Elétrica para turma específica do curso de mestrado profissional, ingresso no segundo semestre letivo de 2020, 2020. Disponível em: <https://ppee.unb.br/wp-content/uploads/2020/09/01092020_EDITAL_16-2020_metadados.pdf>. Acesso em: 29/03/2023.

35 BRASIL. Congresso Nacional. Resolução nº 2, de 2013-CN. Dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do Congresso Nacional, órgão de controle e fiscalização externos da atividade de inteligência, previsto no art. 6º da Lei nº 9.883, de 7 de dezembro de 1999. *Diário Oficial da União*, seção 1. Brasília, DF, ano 228, p. 1-3, 25 nov. 2013.

36 BRASIL. *SISBIN*. Brasília, DF: Agência Brasileira de Inteligência, 2021. Disponível em: <https://www.gov.br/abin/pt-br/assuntos/sisbin>. Acesso em: 29/06/2022.

37 BRASIL. *Decreto nº 8.793, de 29 de junho de 2016*. Fixa a Política Nacional de Inteligência. Brasília, DF: Presidência da República, 2016. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8793.htm>. Acesso em: 25/10/2021.

38 BRASIL. *Tecnologia*. Brasília, DF: Agência Brasileira de Inteligência, 2022. Disponível em: <https://www.gov.br/abin/pt-br/assuntos/tecnologia>. Acesso em: 29/06/2023.

39 BRASIL. *Decreto nº 11.327, de 1º de janeiro de 2023*. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das Gratificações da Agência Brasileira de Inteligência e remaneja cargos em comissão, funções de confiança e gratificações. Brasília, DF: Presidência da República, 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11327.htm#anexo1>. Acesso em: 26/02/2023.

40 BRASIL. *ABIN lança criptografia com algoritmos pós-quânticos para as eleições*. Brasília, DF: Agência Brasileira de Inteligência, 2023. Disponível em: <https://www.gov.br/abin/pt-br/assuntos/noticias/abin-lanca-criptografia-com-algoritmos-pos-quanticos-para-as-eleicoes>. Acesso em: 26/02/2023.

41 COSTA, V. L. D.; CAMPONOGARA, Â.; LÓPEZ, J.; RIBEIRO, M. V. The Feasibility of the CRYSTALS-Kyber Scheme for Smart Metering Systems. *IEEE Access*, IEEE, v. 10, p. 131303–131317, 15 dez. 2022. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9987505/>. Acesso em: 26/02/2023.

42 BRASIL. *Lei nº 14.460, de 25 de outubro de 2022*. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. Brasília, DF: Presidência da República, 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm>. Acesso em: 26/02/2023.

43 MACHADO, D. C.; MENDES, L. S. Tecnologias de perfilamento e dados agregados de geolocalização no combate à covid-19 no Brasil: uma análise dos riscos individuais e coletivos à luz da LGPD. *Revista Brasileira de Direitos Fundamentais & Justiça*, Belo Horizonte: Fórum, v. 14, n. 1, p. 105–148, 22 dez. 2020. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1020>. Acesso em: 29/06/2022.

44 SARLET, I. W.; SAAVEDRA, G. A. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais. *Revista Direito Público*, v. 17, n. 93, p. 33–57, maio/jun. 2020. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315>. Acesso em: 29/06/2022.

45 SARTORI, E. C. M.; BAHIA, C. J. A. Big Brother is watching you: da distopia orwelliana ao direito fundamental à proteção de dados pessoais. *Revista de Direitos e Garantias Fundamentais*, v. 20, n. 3, p. 225–248, 20 dez. 2019. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1785>. Acesso em: 29/06/2022.

46 BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade nº 6.529*. Requerentes: Rede Sustentabilidade e Partido Socialista Brasileiro. Intimados: Presidente da República e Congresso Nacional. Relatora: Min. Cármen Lúcia, 11 out. 2021. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15348384228&ext=.pdf>. Acesso em: 29/06/2022.

47 BRASIL. Supremo Tribunal Federal. *Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental nº 722*. Requerente: Rede Sustentabilidade. Intimado: Ministro de Estado da Justiça e Segurança Pública. Relatora: Min. Cármen Lúcia, 20 ago. 2020. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344764619&ext=.pdf>. Acesso em: 29/06/2022.

48 PINHEIRO, V. S.; BONNA, A. P. Sociedade da informação e direito à privacidade no Marco Civil da Internet: fundamentação filosófica do Estado de Direito. *Revista de Direitos e Garantias Fundamentais*, v. 21, n. 3, p. 365–394, set./dez. 2020. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1555>. Acesso em: 29/06/2022.

49 BRASIL. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. Doutrina Nacional da Atividade de Inteligência: fundamentos doutrinários. Anexo à Portaria no 244-ABIN/GSI/PR, de 23 de agosto de 2016, que aprova os fundamentos doutrinários da Doutrina Nacional da Atividade de Inteligência. *Boletim de Serviço Especial da Agência Brasileira de Inteligência*. n. 1, p. 5, 25 ago. 2016.

50 DREWER, D.; MILADINOVA, V. The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation. *Computer law & security review*, Elsevier, v. 33, n. 3, p. 298–308, jun. 2017. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364917300699>. Acesso em: 27/02/2023.

51 CHUY, J. F. M. O sistema de investigação brasileiro, a "LGPD penal" e a efetiva garantia de direitos fundamentais. *V Concurso de Artigos Científicos em Polícia Judiciária e Investigação Criminal*, Associação Nacional dos Delegados de Polícia Federal (ADPF), 26 fev. 2021. Disponível em: <https://web.adpf.org.br/wp-content/uploads/2021/03/2-Artigo_JOSE-FERNANDO-MORAES-CHUY.pdf>. Acesso em: 27/02/2023.

52 EPRS. European Parliamentary Research Service. The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. *Panel for the Future of Science and Technology*, jun. 2020. Disponível em: <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf>. Acesso em: 23/06/2022.

53 ENISA. European Union Agency for Cybersecurity. *Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics*. 17 dez. 2015. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: 22/06/2022.

54 RHAHLA, M.; ALLEGUE, S.; ABDELLATIF, T. Guidelines for GDPR compliance in big data systems. *Journal of Information Security and Applications*, Elsevier, v. 61, p. 102896, set. 2021. Disponível em: <https://www.sciencedirect.com/science/article/pii/S221421262100123X>. Acesso em: 23/06/2022.

55 ALVES, P. M. d. M. R. O impacto de big data na atividade de inteligência. *Revista Brasileira de Inteligência*, n. 13, p. 99–116, dez. 2018. Disponível em: <https://repositorio.enap.gov.br/handle/1/4658>. Acesso em: 23/06/2022.

56 GEORGIADIS, G.; POELS, G. Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: a systematic literature review. *Computer Law & Security Review*, Elsevier, v. 44, p. 105640, abr. 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364921001138>. Acesso em: 23/06/2022.

57 NETO, A. B. S.; ISHIKAWA, L.; MACIEL, M. O tratamento de dados pessoais pelo poder público e o papel dos Tribunais de Contas. *Revista Direitos Culturais*, v. 16, n. 40, p. 163–177, 23 dez. 2021. Disponível em: <https://san.uri.br/revistas/index.php/direitosculturais/article/view/604>. Acesso em: 03/05/2022.

58 ENISA. European Union Agency for Cybersecurity. *Data protection engineering: from theory to practice*. 27 jan. 2022. Disponível em: <https://www.enisa.europa.eu/publications/data-protection-engineering>. Acesso em: 23/06/2022.

59 RAGAZZO, C. E. J.; BALERONI, M. R. C.; JUNIOR, D. W. M. L. Limites ao acesso de autoridades públicas a big data: evolução legislativa e governança regulatória. *Revista da Faculdade de Direito UFPR*, v. 66, n. 2, p. 9–30, maio/ago. 2021. Disponível em: <https://revistas.ufpr.br/direito/article/view/67003>. Acesso em: 29/06/2022.

60 RAJAMÄKI, J.; SIMOLA, J. How to apply Privacy by Design in OSINT and big data analytics? In: *ECCWS 2019 18th European Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 2019. p. 364–371. Disponível em: <https://www.proquest.com/docview/2261006646/fulltextPDF/659E29A5987C47DBPQ/1?accountid=26646>. Acesso em: 23/06/2022.

61 CAVOUKIAN, A. Privacy by design: The 7 foundational principles. *Information & Privacy Commissioner of Ontario, Canada*, ago. 2009. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>. Acesso em: 23/06/2022.

62 AEPD. Agencia Española de Protección de Datos . *A Guide to Privacy by Design*. out. 2019. Disponível em: <https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf>. Acesso em: 23/06/2022.

63 GPA. Global Privacy Assembly. Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalém, Israel, 27-29 out. 2010. Disponível em: <https://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf>. Acesso em: 23/06/2022.

64 HOEPMAN, J.-H. Privacy design strategies. *ArXiv*, abs/1210.6621, 2012. Disponível em: <https://arxiv.org/abs/1210.6621>. Acesso em: 27/02/2023.

65 ISO. International Organization for Standardization. *ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework*, Genebra, Suíça, 2011. Disponível em: <https://www.iso.org/standard/45123.html>. Acesso em: 27/02/2023.

66 OECD. The Organisation for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD Publishing, 2002. 64 p. Disponível em: <https://www.oecd-ilibrary.org/content/publication/9789264196391-en>. Acesso em: 27/02/2023.

67 KOOPS, B.-J.; HOEPMAN, J.-H.; LEENES, R. Open-source intelligence and privacy by design. *Computer Law & Security Review*, Elsevier, v. 29, n. 6, p. 676–688, dez. 2013. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0267364913001672>. Acesso em: 26/06/2022.

68 COLESKY, M.; HOEPMAN, J.-H.; HILLEN, C. A critical analysis of privacy design strategies. In: IEEE. *2016 IEEE security and privacy workshops (SPW)*. San Jose, CA, USA, 2016. p. 33–40. Disponível em: <https://ieeexplore.ieee.org/abstract/document/7527750>. Acesso em: 26/06/2022.

69 HOEPMAN, J.-H. *Privacy design strategies (the little blue book)*. Nijmegen: Radboud University, 19 abr. 2022. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>. Acesso em: 27/02/2023.

70 ENISA. European Union Agency for Cybersecurity. *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies*. 31 mar. 2016. Disponível em: <https://www.enisa.europa.eu/publications/pets>. Acesso em: 27/02/2023.

71 GOMES, M. C. O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. *In:* Lima, A. P. Hissa, C., Saldanha, P. M. (org.). *Direito Digital: Debates Contemporâneos*, São Paulo: Revista dos Tribunais, p. 141–153, 2019.

72 GOMES, M. C. O. Relatório de impacto à proteção de dados pessoais. Uma breve análise da sua definição e papel na LGPD. *Revista do Advogado*, Associação dos Advogados de São Paulo, n. 144, p. 174–183, nov. 2019. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html>. Acesso em: 27/02/2023.

73 WP29. Article 29 Data Protection Working Party. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, (wp248rev.01)*. 4 out 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/items/611236>. Acesso em: 29/06/2022.

74 FERREIRA KEILA PACHECO; RESENDE, A. P. B. A. Histórico normativo da proteção de dados pessoais no ordenamento jurídico brasileiro: avanços e retrocessos na tutela da privacidade. *Revista de Direito do Consumidor*, São Paulo: Ed. RT, ano 30, v. 137, p. 85–112, set./out. 2021. Disponível em: <https://proview.thomsonreuters.com/title.html?redirect=true&titleKey=rt%2Fperiodical%2F92900151%2Fv20210137.2&titleStage=F&titleAcct=7e24544628ff414181334d7dce4443f4#sl=0&eid=9ab847c2930e6f40749cd619bc05d3d5&eat=1_index&pg=RR-4.1&psl=p&nvgS=false&tmp=571>. Acesso em: 25/10/2021.

75 PIETRO, M. S. Z. D. *Direito Administrativo.* 36ª ed. Rio de Janeiro: Forense, 2023. *E–book*. Disponível em: <ttps://integrada.minhabiblioteca.com.br/#/books/9786559646784/>. Acesso em: 30/03/2023.

76 ICO. Information Commissioner's Office. *Big data, artificial intelligence, machine learning and data protection*. Versão 2.2, 2017. Disponível em: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. Acesso em: 29/06/2022.

77 EDPB. European Data Protection Board. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* . Versão 2.0, 20 out. 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en>. Acesso em: 29/06/2022.

78 CAVOUKIAN, A.; SHAPIRO, S.; CRONK, R. J. Privacy engineering: proactively embedding privacy, by design. *Information and privacy commissioner of Ontario, Canada*, jan. 2014. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-priv-engineering.pdf>. Acesso em: 28/02/2023.

79 ABREU, J. d. S. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD *In:* BIONI, B.; MENDES, L. S.; DONEDA, D.; SARLET, I. W.; JR., O. L. R (org.). *Tratado de proteção de dados pessoais*, Rio de Janeiro: Forense, 2021. *E–book*. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/>. Acesso em: 29/11/2021.

80 SOUZA, C. A. P.; VIOLA, M.; PADRÃO, V. Considerações iniciais sobre os interesses legítimos do controlador na Lei Geral de Pproteção de Dados Pessoais. *Revista Direito Público*, v. 16, n. 90, dez. 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3744>. Acesso em: 29/06/2022.

81 MENDES, L. S. F. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. *Revista Brasileira de Direitos Fundamentais & Justiça*, Belo Horizonte: Fórum, v. 12, n. 39, p. 185–216, jul./dez 2018. Disponível em: <http://dfj.emnuvens.com.br/dfj/article/view/655>. Acesso em: 29/06/2022.

82 WIMMER, M. Limites e possibilidade para o uso secundário de dados pessoais no poder público: lições da pandemia. *Revista Brasileira de Políticas Públicas*, v. 11, n. 1, p. 123–142, abr. 2021. Disponível em: <https://www.publicacoes.uniceub.br/RBPP/article/view/7136>. Acesso em: 13/07/2022.

83 TEFFé, C. S. d.; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *civilistica.com*, v. 9, n. 1, p. 1–38, maio 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510>. Acesso em: 29/11/2021.

84 WIMMER, M. O regime jurídico do tratamento de dados pessoais pelo poder público *In:* BIONI, B.; MENDES, L. S.; DONEDA, D.; SARLET, I. W.; JR., O. L. R (org.). *Tratado de proteção de dados pessoais*, Rio de Janeiro: Forense, 2021. *E–book*. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/>. Acesso em: 29/11/2021.

85 BRASIL. Câmara dos Deputados. Comissão de Juristas sobre Segurança Pública. *Anteprojeto de lei de proteção de dados para segurança pública e persecução penal*. Brasília, DF: Câmara dos Deputados, 2021. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf>. Acesso em: 29/06/2022.

86 BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 25/10/2021.

87 GASIOLA, G. G.; MACHADO, D.; MENDES, L. S. A administração Pública entre transparência e proteção de dados. *Revista de Direito do Consumidor*, São Paulo: Ed. RT, ano 30, v. 135, p. 179–201, maio/jun. 2021. Disponível em: <https://proview.thomsonreuters.com/title.html?redirect=true&titleKey=rt%2Fperiodical%2F92900151%2Fv20210135.1&titleStage=F&titleAcct=7e24544628ff414181334d7dce4443f4#sl=0&eid=758bd3fecf9204b160a9a436648c9191&eat=%5Bereid%3D%22758bd3fecf9204b160a9a436648c9191%22%5D&pg=I&psl=p&nvgS=false>. Acesso em: 25/10/2021.

88 DöHMANN, I. S. g. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. *Revista Direito Público*, Brasília, v. 17, n. 93, p. 9–32, jul. 2020. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4235>. Acesso em: 29/06/2022.

89 FRANZOLIN, C. J.; VALENTE, V. A. E. Alguns apontamentos sobre a responsabilidade ativa mediante a prestação de contas e a prevenção de danos por meio de conformidades. *Revista de Direito do Consumidor*, São Paulo: Ed. RT, ano 30, v. 133, p. 75–106, jan./fev. 2021. Disponível em: <https://proview.thomsonreuters.com/title.html?redirect=true&titleKey=rt%2Fperiodical%2F92900151%2Fv20210133.2&titleStage=F&titleAcct=7e24544628ff414181334d7dce4443f4#sl=p&eid=f9561e3f6959aa75069c31b96914aa0c&eat=a-259632651&pg=RR-2.1&psl=&nvgS=false&tmp=893>. Acesso em: 25/10/2021.

90 FERNANDES, M. A. d. S.; OLIVEIRA, F. G. de; FERRAZ, F. S.; SILVA, D. A. da; CANEDO, E. D.; JR, R. T. d. S. Impactos da Lei de Proteção de Dados (LGPD) brasileira no uso da computação em nuvem. *Revista Ibérica de Sistemas e Tecnologias de Informação*, Lousada, Porto, Portugal, n. E42, p. 374–385, fev. 2021. Disponível em: <https://www.proquest.com/openview/bf09afd72a0cfbb9c3a995f1529d6751/1.pdf?pq-origsite=gscholar&cbl=1006393>. Acesso em: 08/12/2021.

91 COUTINHO, L. LGPD e Inteligência: os limites no tratamento de dados pessoais coletados em fontes abertas. *Revista Brasileira de Inteligência*, n. 15, p. 99–116, dez. 2020. Disponível em: <https://rbi.enap.gov.br/index.php/RBI/article/view/183>. Acesso em: 25/10/2021.

92 GB. Reino Unido. *Data Protection Act, 2018*. 23 maio 2018. Disponível em: <https://www.legislation.gov.uk/ukpga/2018/12/contents>. Acesso em: 25/10/2021.

93 SION, L.; DEWITTE, P.; LANDUYT, D. V.; WUYTS, K.; VALCKE, P.; JOOSEN, W. DPMF: a modeling framework for data protection by design. *Enterprise Modelling and Information Systems Architectures (EMISAJ)*, v. 15, n. 10, p. 1–53, 2020. Disponível em: <https://www.emisa-journal.org/emisa/article/view/240>. Acesso em: 23/06/2022.

94 UE. UNIÃO EUROPEIA. Parlamento Europeu; Conselho da União Europeia. Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016. Cria a Agência da União Europeia para a Cooperação Policial (Europol) e substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho. *Jornal Oficial da União Europeia*. n. L. 135, p. 53–114, 24 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0794>. Acesso em: 06/12/2021.

95 UE. UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia (Grande Seção). *Processo C-311/18*. Requerente: Data Protection Commissioner. Requeridos: Facebook Ireland Ltd. e Maximillian Schrems. Relator: T. von Danwitz. 16 jul. 2020. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62018CJ0311>. Acesso em: 07/12/2021.

96 VERONESE, A. Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão no brasil e na américa latina *In:* BIONI, B.; MENDES, L. S.; DONEDA, D.; SARLET, I. W.; JR., O. L. R (Org.). *Tratado de proteção de dados pessoais*, Rio de Janeiro: Forense, 2021. *E–book*. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/>. Acesso em: 29/11/2021.

97 VERONESE, A.; SANTOS, L. M. d. S. B. Padrões de conformidade nacionais de proteção de dados pessoais: anotações na perspectiva de compliance após a invalidação do Privacy Shield firmado entre os Estados Unidos da América e a União Europeia *In:* FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (Org.). *Compliance e políticas de proteção de dados*, São Paulo: Editora Revista dos Tribunais, p. 93–136, 2021.

98 UE. UNIÃO EUROPEIA. Parlamento Europeu; Conselho da União Europeia. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. *Jornal Oficial da União Europeia*. n. L. 119, p. 89, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:02016L0680-20160504&from=EN>. Acesso em: 29/06/2022.

99 BRUSTOLIN, V.; OLIVEIRA, D. de; PERON, A. E. dos R. Exploring the relationship between crypto ag and the cia in the use of rigged encryption machines for espionage in brazil. *Cambridge Review of International Affairs*, Routledge, p. 1–34, 2020. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/09557571.2020.1842328?journalCode=ccam20>. Acesso em: 24/02/2023.

100 MILLER, G. The Washington Post *"The intelligence coup of the century". For decades, the CIA read the encrypted communications of allies and adversaries*. 11 fev. 2020. Disponível em: <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/>. Acesso em: 23/02/2023.

101 CAVOUKIAN, A. Operationalizing Privacy by Design. A guide to implementing strong privacy practices. *Information and privacy commissioner of Ontario, Canada*, dez. 2012. Disponível em:

<https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf>. Acesso em: 23/02/2023.

102 ENISA. European Union Agency for Cybersecurity. *Privacy and Data Protection by Design – from policy to engineering*. 12 jan. 2015. Disponível em: <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>. Acesso em: 22/06/2022.

103 NDPA. Norwegian Data Protection Authority. *Software development with Data Protection by Design and by Default*. 28 nov. 2017. Disponível em: <https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default>. Acesso em: 26/06/2022.

104 BRASIL. Ministério da Economia. *Guia de Requisitos Mínimos de Segurança e Privacidade para Aplicativos Móveis – LGPD*. Versão 1.0, 24 nov. 2021. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_seguranca_apps.pdf/view>. Acesso em: 23/02/2023.

105 EDPS. European Data Protection Supervisor. *Formal comments of the EDPS on the Cybersecurity package* . 24 dez. 2021. Disponível em: <https://edps.europa.eu/data-protection/our-work/publications/comments/cybersecurity-package_en>. Acesso em: 29/06/2022.

106 EDPS. European Data Protection Supervisor. *Opinion 5/2018: Preliminary Opinion on privacy by design*. 31 maio 2018. Disponível em: <https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en>. Acesso em: 29/06/2022.

107 ENISA. European Union Agency for Cybersecurity. *About ENISA*. Disponível em: <https://www.enisa.europa.eu/about-enisa>. Acesso em: 28/02/2023.

108 BACHLECHNER, D.; FORS, K. L.; SEARS, A. M. The role of privacy-preserving technologies in the age of big data. In: *WISP 2018 Proceedings*. [s.n.], 2018. Disponível em: <https://aisel.aisnet.org/wisp2018/28>. Acesso em: 27/02/2023.

109 SALTARELLA, M.; DESOLDA, G.; LANZILOTTI, R. Privacy Design Strategies and the GDPR: A Systematic Literature Review. In: MOALLEM, A. (Ed.). *HCI for Cybersecurity, Privacy and Trust*. Cham: Springer International Publishing, 2021. p. 241–257. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-030-77392-2_16>. Acesso em: 27/02/2023.

110 PRIVACYPATTERNS.EU. *privacypatterns.eu - collecting patterns for better privacy*. 2023. Disponível em: <https://privacypatterns.eu/#/?limit=6&offset=0>. Acesso em: 27/02/2023.

111 PRIVACYPATTERNS.ORG. *privacypatterns.org*. 2023. Disponível em: <https://privacypatterns.org/>. Acesso em: 27/02/2023.

112 JORDAN, S.; FONTAINE, C.; HENDRICKS-STURRUP, R. Selecting Privacy-Enhancing Technologies for Managing Health Data Use. *Frontiers in Public Health*, v. 10, 2022. Disponível em: <https://www.frontiersin.org/articles/10.3389/fpubh.2022.814163>. Acesso em: 28/02/2023.

113 TIMAN, T.; MANN, Z. Data Protection in the Era of Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies. In: CURRY, E.; METZGER, A.; ZILLNER, S.; PAZZAGLIA, J.-C.; ROBLES, A. G. (Ed.). *The Elements of Big Data Value: Foundations of the Research and Innovation Ecosystem*. Cham: Springer International Publishing, 2021. p. 153–175. Disponível em: <https://doi.org/10.1007/978-3-030-68176-0_7>. Acesso em: 26/06/2022.

114 CANEDO, E. D.; CALAZANS, A. T. S.; MASSON, E. T. S.; COSTA, P. H. T.; LIMA, F. Perceptions of ICT Practitioners Regarding Software Privacy. *Entropy*, v. 22, n. 4, 2020. Disponível em: <https://www.mdpi.com/1099-4300/22/4/429>. Acesso em: 26/06/2022.