DISSERTAÇÃO DE MESTRADO PROFISSIONAL

A POSSIBILIDADE DA REALIZAÇÃO DE VIGILÂNCIA POR MEIO DE GEOLOCALIZAÇÃO EM TEMPO REAL PELA AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

RICARDO RAMOS SAMPAIO

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

A POSSIBILIDADE DA REALIZAÇÃO DE VIGILÂNCIA POR MEIO DE GEOLOCALIZAÇÃO EM TEMPO REAL PELA AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

RICARDO RAMOS SAMPAIO

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. Ugo Silva Dias, Dr, FT/UnB _____
Orientador

Prof. Georges Daniel Amvame Nze, Dr, FT/UnB _____
Co-orientador

Prof.Edna Dias Canedo, Dra, FT/UnB _____
Examinador interno

Prof. Luiz Henrique Diniz Araújo, Dr, UFPE _____
Examinador externo

Prof. Robson de Oliveira Albuquerque, Dr, FT/UNB _____
Suplente

FICHA CATALOGRÁFICA

SAMPAIO, RICARDO
A POSSIBILIDADE DA REALIZAÇÃO DE VIGILÂNCIA POR MEIO DE GEOLOCALIZAÇÃO EM TEMPO REAL PELA AGÊNCIA BRASILEIRA DE INTELIGÊNCIA [Distrito Federal] 2023.
xvi, 108 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023). Publicação PPEE.MP.051
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Geolocalização	2. Inteligência
3. Privacidade	4. Proteção de dados
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

SAMPAIO, R. (2023). *A POSSIBILIDADE DA REALIZAÇÃO DE VIGILÂNCIA POR MEIO DE GEOLOCALIZAÇÃO EM TEMPO REAL PELA AGÊNCIA BRASILEIRA DE INTELIGÊNCIA*.
Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 108 p. Publicação PPEE.MP.051

CESSÃO DE DIREITOS

AUTOR: RICARDO RAMOS SAMPAIO
TÍTULO: A POSSIBILIDADE DA REALIZAÇÃO DE VIGILÂNCIA POR MEIO DE GEOLOCALIZAÇÃO EM TEMPO REAL PELA AGÊNCIA BRASILEIRA DE INTELIGÊNCIA.
GRAU: Mestre em Engenharia Elétrica ANO: 2023

RICARDO RAMOS SAMPAIO
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico esse trabalho aos meus pais que, certamente, no plano espiritual onde estiverem, estão olhando e zelando pela minha trajetória terrena.

AGRADECIMENTOS

À Deus por permitir que eu alcance meus objetivos, guiando meus passos e fazendo com que eu trilhe os melhores caminhos.

À minha esposa, Mariana, pelo amor, amizade e parceria. Sem esse apoio eu não teria participado dessa jornada de aprofundados e intensos estudos. Suas palavras de encorajamento fizeram com que eu acreditasse na possibilidade de desenvolver esse trabalho.

Aos meus filhos, Luísa e Henrique, pela compreensão nas minhas ausências.

Ao meu amigo Gibran que me incentivou a ingressar neste projeto.

Ao Professor Robson Albuquerque pelas orientações.

Ao meu orientador, Professor Ugo, e meu co-orientador, Professor Georges, pela paciência e serenidade na condução das diretrizes da pesquisa.

À UNB e à ABIN que me permitiram assimilar conhecimentos que serão de utilidade ímpar na minha vida acadêmica e profissional.

RESUMO

O avanço tecnológico tem produzido um processo de mudança nas técnicas operacionais utilizadas pelos serviços de inteligência ao redor do mundo. A obtenção de informações por meio de fotografias, comunicações, sinais, imagens, ondas, radiações e assinaturas eletromagnéticas desenvolveu-se rapidamente e tornou-se uma rotineira prática dos serviços de inteligência. A própria coleta de informações em fontes abertas, em conjunto com a capacidade de análise de *big data*, alcançou estágio singular. As técnicas operacionais antigas têm sido convertidas em meios de busca e coleta com uso de mecanismos tecnológicos, imprimindo um alcance e amplitude de dados sem precedentes. A geolocalização ou determinação em tempo real da localização de um indivíduo, o correspondente eletrônico da vigilância, vem sendo utilizada, sem maiores questionamentos, em diversos países. Essa constatação impulsiona o desenvolvimento desta pesquisa, que se volta a verificar se a geolocalização em tempo real pode ser utilizada pela ABIN, sem que isso afronte a legislação pátria e a privacidade dos indivíduos. É nesse contexto que se apresenta essencial esmiuçar as características dos serviços de inteligência e a evolução do direito à privacidade e da proteção de dados, traçando-se, ainda, um comparativo entre a instrumentalidade da coleta de dados pelo Estado com as empresas de tecnologia. Outro ponto importante para atingir conclusões robustas sobre o assunto é verificar se a legislação, a cadeia e competência de autorização para atuação e os mecanismos de controle dos serviços de inteligência estrangeiros se aproximam ou se distanciam do brasileiro. Por fim, um exame aprofundado de decisões judiciais do Supremo Tribunal Federal e do Superior Tribunal de Justiça a respeito da privacidade, compartilhamento de dados, da ponderação de interesses e da geolocalização estática tem como finalidade reforçar o raciocínio a respeito da possibilidade do uso da geolocalização em tempo real.

ABSTRACT

Technological advances have produced a process of change in the operational techniques used by intelligence services around the world. Obtaining information through photographs, communications, signals, images, waves, radiation and electromagnetic signatures developed rapidly and became a routine practice for intelligence services. The collection of information from open sources itself, together with the ability to analyze big data, has reached a unique stage. Old operational techniques have been converted into means of search and collection using technological mechanisms, giving an unprecedented range and breadth of data. Geolocation or determination in real time of an individual's location, the electronic correspondent of surveillance, has been used, without further questioning, in several countries. This finding drives the development of this research, which once again verifies whether real-time geolocation can be used by ABIN, without this infringing national legislation and the privacy of individuals. It is in this context that it is essential to scrutinize the characteristics of intelligence services and the evolution of the right to privacy and data protection, also drawing a comparison between the instrumentality of data collection by the State with technology companies. Another important point to reach robust conclusions on the subject is to verify if the legislation, the chain and competence of authorization to act and the control mechanisms of the foreign intelligence services approach or distance themselves from the Brazilian one. Finally, an in-depth examination of judicial decisions of the Federal Supreme Court and the Superior Court of Justice regarding privacy, data sharing, balancing of interests and static geolocation aims to reinforce the reasoning regarding the possibility of using geolocation in real time.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ABIN	Agência Brasileira de Inteligência
ACEL	Associação Nacional das Operadoras Celulares
ADI	Ação Direta de Inconstitucionalidade
ADPF	Arguição de Descumprimento de Preceito Fundamental
AGO	*Australian Geospatial Intelligence Organization*
AGU	Advocacia-Geral da União
ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
ASD	*Australian Signals Directorate*
ASIO	*Australian Security Intelligence Organization*
ASIS	*Australian Secret Intelligence Service*
BFV	*Bundesamt Für Verfassungsschutz*
BND	*Bundesnachrichtendienst*
CCAI	Comissão Mista de Controle das Atividades de Inteligência
CCPA	Lei da Califórnia de Privacidade do Consumidor
CDR	*Call Detail Record*
CIA	*Central Intelligence Agency*
CSEC	*Communications Security Establishment Canada*
CSIS	*Canadian Security Intelligence Service*
DEA	*Drug Enforcement Administration*
DENATRAN	Departamento Nacional de Trânsito
DGSE	*Direction Générale de la Sécurité Extérieure*
DGSI	*Direction Générale de la Sécurité Intérieure*
DIO	*Defense Intelligence Organization*
DNRED	*Direction Nationale du Renseignement et des Enquêtes Douanières*
DPR	*Délégation Parlementaire Au Renseignement*
DRM	*Direction du Renseignement Militaire*
DRSD	*Direction du Renseignement et de la Sécurité de la Défense*
ECHR	*European Court Of Human Rights*
ENI	Estratégia Nacional de Inteligência
EPIC	*Electronic Privacy Information Center*
ERB	Estação Rádio Base
FBI	*Federal Bureau of Investigation*
FISA	*Foreign Intelligence Surveillance Act*
FISC	*Foreign Intelligence Surveillance Court*
GCHQ	*Government Communications Headquartes*
GCSB	*Government Communications Security Bureau*

Continua na próxima página

GDPR	*General Data Protection Regulation*
GPS	*Global Position System*
HUMINT	*Human Intelligence*
IANA	*Internet Assigned Numbers Authority*
IBGE	Instituto Brasileiro de Geografia e Estatística
IGIS	Inspetor-Geral de Inteligência e Segurança
IMEI	*International Mobile Equipment Identity*
IMINT	*Imagery intelligence*
IMSI	*International Mobile Subscriber Identity*
IP	*Internet Protocol*
ISR	*L' Inspection Des Services De Renseignement*
LGPD	Lei Geral de Proteção de Dados
MASINT	*Measurement and Signature Intelligence*
MI5	*Military Service, Section 5*
MI6	*Military Service, Section 6*
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
NSA	*National Security Agency*
NSLs	*National Security Letters*
NZSIS	*New Zealand Security Intelligence Service*
OAIC	*Office of the Australian Information Commissioner*
OMD	Observação, memorização e descrição
ONA	*Office of National Assessments*
OSINT	*Open source intelligence*
OTAN	Organização do Tratado do Atlântico Norte
PL	Projeto de Lei
PNI	Política Nacional de Inteligência
RE	Recurso Extraordinário
RFB	Receita Federal do Brasil
RSF	Repórteres Sem Fronteiras
SCC	*Supreme Court of Canada*
SERPRO	Serviço Federal de Processamento de Dados
SFICI	Serviço Federal de Informações e Contra-Informações
SIGINT	*Signals intelligence*
SIS	*Secret Intelligence Service*
SISBIN	Sistema Brasileiro de Inteligência
SMP	Serviço Móvel Pessoal
SMS	*Short Message Service*
SNI	Serviço Nacional de Informações
SS	*Security Service*
SSCI	*Senate Select Committee on Intelligence*

Continua na próxima página

STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
SVA	Serviço de Valor Adicionado
TDOA	*Time Difference of Arrival*
TIA	*Telecommunications (Interception and Access)*
TRACFIN	*Cellule du Renseignement Financier*
UIF	Unidade de Inteligência Financeira
UKIC	*United Kingdom Intelligence Comunity*

Fim da Lista de Siglas

1 INTRODUÇÃO

Os serviços de inteligência ao redor do mundo têm se mostrado como uma essencial ferramenta na tomada de decisões por governantes e autoridades de diversos países. Com o avanço tecnológico, a vigilância, monitoramento, a busca e coleta de dados alcançou uma dimensão e amplitude irreversíveis na inteligência e contrainteligência.

Internacionalmente, a utilização da denominada vigilância eletrônica por geolocalização de aparelhos celulares é largamente aceita em grande parte dos países, à exemplo dos Estados Unidos [1], Reino Unido [2], Canadá [3], Austrália [4], Nova Zelândia [5], Alemanha [6] e França [7]. Assim, um estudo comparativo, dos serviços de inteligência congêneres, seus mecanismos de autorização e controle, e as decisões judiciais acerca do assunto em outros países, pode balizar interpretações e conclusões sobre o tema, em especial, se no Brasil há diferenças ou semelhanças que importem e influenciem na aceitação ou negativa da vigilância por meio da geolocalização em tempo real.

Para que se tenha uma ideia, de acordo com a Agência Nacional de Telecomunicações (ANATEL) [8], em novembro de 2022 existiam no país 254,9 milhões de acessos de telefonia móvel e, destes, 226,6 milhões possuíam banda larga móvel. Esses números representam uma densidade de 101,0 acessos/100 hab., o que demonstra a dimensão da possibilidade que a geolocalização de usuários em tempo real representa. Nesse sentido, é interessante trazer à baila por quais meios tecnológicos se efetiva a geolocalização em tempo real de um usuário do serviço móvel pessoal ou da internet. Se a geolocalização se utiliza de dados das estações móveis, se é inerente ao uso do Serviço Móvel Pessoal a localização dos terminais ou ainda, se aplicativos ou buscadores na internet captam, voluntária ou não, a localização do usuário.

Um ponto que exsurge diante dessa capacidade tecnológica de geolocalização é como ficaria o direito à privacidade e à proteção de dados. No Brasil, ainda grassa certa controvérsia, mesmo com o passar do tempo, se a proteção constitucional dos dados do usuário estaria relacionada a comunicação [9] ou a privacidade em si [10]. Diante disso, é imperioso descortinar a evolução, o conceito e a natureza do direito à privacidade e à proteção de dados.

Esses aspectos possibilitam uma compreensão mais aprofundada da convivência dos direitos fundamentais como um todo. Quão intensamente pode ser empregada a teoria da ponderação de princípios [11] para sobrelevar interesses públicos em face do direito à privacidade. Ou, ainda, como a utilização apenas da geolocalização em tempo real em contraponto à geolocalização estática pode, dentro da perspectiva de compressão de direitos fundamentais, utilizada pelo Supremo Tribunal Federal em seus julgamentos, conviver com o direito à privacidade.

O consentimento do titular dos dados sensíveis, seja genérico, seja específico, ficaria dispensado em decorrência de uma ponderação de interesses realizada pela lei, aprioristicamente, que considera mais relevantes e preponderantes os interesses de natureza pública frente aos interesses do titular, ainda que estes tenham qualidade de Direito Fundamental [12].

O enfrentamento do assunto, portanto, mais do que ser dirimido na esfera legal, passa pelo sopesamento de princípios constitucionais. Nessa perspectiva, é possível vislumbrar que a convivência de dois princípios constitucionais conflitantes significa a atribuição de primazia [11] a um deles, sem descurar a essência e validade do outro. O que se observa é que há situações em concreto que justificam a relativização de direitos estabelecidos como fundamentais na Constituição Federal de 1988. Não há direito absoluto, ainda que constitucionalmente resguardado, não havendo, inclusive, necessidade de concordância expressa do constituinte com a restrição de direitos fundamentais sempre que se fizer necessária a concretização do princípio da concordância prática entre ditames [13]. Trata-se de restrição implicitamente acatada pelo constituinte. O denominado princípio da convivência com a as liberdades públicas [14] a ensejar que o interprete, na hipótese de conflito entre dois ou mais direitos ou garantias fundamentais, realize um exercício de equilíbrio entre os bens jurídicos conflitantes, evitando que um deles seja aniquilado pelo outro. A redução proporcional do espectro de alcance dos direitos fundamentais concretiza a unicidade e harmonia do texto constitucional.

Assim, o direito à privacidade não se revela ilimitado e imune a intervenções restritivas [15]. Um dos exemplos nesse campo são os direitos a saúde e privacidade, permitindo-se que existam graus de intervenção na privacidade [16]. Nesse sentido, o que se busca na pesquisa é verificar se a vigilância através da utilização da geolocalização em tempo real atinge o direito à privacidade ou se é necessária a relativização do direito à privacidade em hipóteses de geolocalização do usuário para atender determinado interesse público. Nesse campo, é essencial traçar um paralelo entre a captação de dados pelas empresas de tecnologia, as *big techs*, e a utilização de dados do usuário pelo Poder Público. O que justifica a assimilação de dados pessoais pelo Estado e por uma empresa privada? Será que é possível estabelecer um parâmetro comparativo de importância e instrumentalidade do uso dos dados pelo Estado e pelas empresas de tecnologia?

Há que se delimitar igualmente se há restrições legais à utilização da geolocalização, enquanto uso de dados pessoais, em questões de segurança do Estado e da sociedade e a defesa nacional A questão não se mostrou elucidada pela Lei Geral de Proteção de Dados (LGPD) que, exclui da necessidade de consentimento do titular, o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos, abarcando, nesse contexto situações de interesse público. Outrossim, afastou da abrangência da LGPD o tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. É imperioso determinar quais regras e dispositivos da LGPD se aplicam ao uso da geolocalização pela inteligência ou mesmo se a experiência em outros países é capaz de delinear o assunto no Brasil.

1.1 HIPÓTESE

O ponto crucial do presente estudo é verificar em que medida a técnica operacional de vigilância empregada pelos serviços de inteligência, especificamente pela Agência Brasileira de Inteligência (ABIN) no Brasil, pode se utilizar da geolocalização de pessoas em tempo real através dos seus aparelhos celulares.

1.2 JUSTIFICATIVA

A localização do usuário do Serviço Móvel Pessoal (SMP) por meio da utilização de técnicas de geolocalização e a privacidade são temas que, necessariamente, se entrelaçam e carregam um aspecto interdisciplinar a ser examinado.

A possibilidade de localização do usuário por meio do seu aparelho celular é circunstância que tangencia aspectos da intimidade e privacidade, pois permite identificar os lugares frequentados com habitualidade, a duração de permanência em determinado local, trajetos de deslocamento utilizados, natureza e características dos locais, dentre outras situações que podem ser extraídas do cruzamento de informações.

Há intensa relevância social e contemporaneidade no assunto. Ao longo dos últimos anos houve significativa evolução nos conceitos e natureza do direito à privacidade e proteção de dados. Ao mesmo tempo, o avanço tecnológico ensejou o acesso a dados pessoais da esfera íntima do indivíduo.

Sob outro viés, e de longa data, vivencia-se a necessidade de monitoramento e acompanhamento de pessoas que sejam de interesse dos serviços de inteligência, à exemplo daquelas ligadas ao terrorismo. Além da observação e controle visual dos alvos por meio da vigilância é preciso avaliar se a geolocalização em tempo real da estação móvel pode ser utilizada como uma espécie de vigilância eletrônica.

1.3 OBJETIVOS

1.3.1 Objetivo geral

Verificar, a partir da evolução do direito à privacidade, ponderação de princípios e interesses, e comparativo com outros modelos de serviços de inteligência, se a utilização da geolocalização em tempo real como sucedâneo da vigilância atinge o direito à privacidade e encontra respaldo legal para ser adotada.

1.3.2 Objetivos específicos

1. Identificar as técnicas de geolocalização em tempo real em plataformas de estação móvel do serviço móvel pessoal (SMP).
2. Investigar, no ordenamento jurídico brasileiro, o conceito, natureza, elementos, alcance, subsídios

teóricos e práticos que envolvem o direito à privacidade, diferenciando-o de outras garantias constitucionais similares.

3. Investigar o posicionamento de tribunais brasileiros em relação a privacidade e ponderação de interesses.

4. Analisar a harmonização de direitos fundamentais individuais e coletivos entre si e aspectos do contratualismo.

5. Analisar e comparar o modelo dos serviços de inteligência estrangeiros congêneres com o brasileiro.

1.4 ESTRUTURA DA DISSERTAÇÃO

O trabalho foi dividido em 9 capítulos, excluindo-se a introdução e a conclusão, com o objetivo de contextualizar o problema, apresentar a hipótese e desenvolver os objetivos geral e específicos. Ao longo dos capítulos são estabelecidas as premissas e alicerces que servem de elementos para a conclusão.

No capítulo 2. (DEFINIÇÃO, NATUREZA, TÉCNICAS E FINALIDADE DOS SERVIÇOS DE INTELIGÊNCIA) apresentam-se os contornos de uma atividade de inteligência, ou seja, as características de órgãos/unidades que se utilizam de técnicas operacionais. São descritas, igualmente, as possibilidades técnicas de localização de um indivíduo, quais os elementos técnicos que resultam na localização de uma pessoa e quais são os detentores desse dado.

O capítulo 3. (GEOLOCALIZAÇÃO E TÉCNICAS OPERACIONAIS EM SERVIÇOS DE INTELIGÊNCIA ESTRANGEIROS) aponta a legislação, a competência para autorização e as formas de controle das técnicas operacionais de serviços de inteligência estrangeiros. Em aprofundada pesquisa são descritos os modelos de outras agências de inteligência, possibilitando que se estabeleça uma comparação com os parâmetros brasileiros e a ABIN. Em outros termos: como são realizadas e geridas as técnicas operacionais em outros países e se é possível encontrar pontos de semelhança na legislação e formas de controle.

No capítulo 4. (INAPLICABILIDADE DA LGPD À CAPTAÇÃO DA GEOLOCALIZAÇÃO PELA ATIVIDADE DE INTELIGÊNCIA) demonstra-se a partir da análise da LGPD, legislações estrangeiras, parecer da Advocacia-Geral da União e decisão do Supremo Tribunal Federal, que a Lei Geral de Proteção de Dados não se aplica em quase sua totalidade à ABIN quando atua em temas como defesa nacional e segurança do Estado.

Diante da inaplicabilidade da LGPD, no capítulo 5. (A EVOLUÇÃO DO CONCEITO E NATUREZA DO DIREITO À PRIVACIDADE) demonstra-se que os limites impostos à geolocalização estão em sede constitucional, no direito à privacidade e à proteção de dados. A evolução do instituto mostra a atualidade e contemporaneidade do tema.

No capítulo 6. (USO PRIVADO E PÚBLICO DA GEOLOCALIZAÇÃO. O CONTRATO SOCIAL

DAS *BIG TECHS* X CONTRATO SOCIAL DO ESTADO) é realizada uma análise crítica da coleta de dados pelas empresas de tecnologia em comparação com a captação pelo Poder Público.

No capítulo 7. (A PRIVACIDADE, O COMPARTILHAMENTO DE DADOS E A GEOLOCALIZAÇÃO NAS RECENTES DECISÕES JUDICIAIS NO BRASIL) são elencadas e comentadas as decisões judiciais que perpassam entendimento principalmente em relação à privacidade.

No capítulo 8. (JUÍZO DE PONDERAÇÃO. PRIVACIDADE X INTERESSE PÚBLICO. O USO DA GEOLOCALIZAÇÃO DE DADOS ESTÁTICOS) é exposto teoria alemã, acolhida pelo Supremo Tribunal Federal (STF), acerca da necessária compressão de direitos quando existem aparentes conflitos entre bens jurídicos com proteção constitucional. Tal tese lastreou decisões do Superior Tribunal de Justiça (STJ) permitindo o acesso a dados de geolocalização estática de indivíduos indeterminados.

No capítulo 9. (O USO DA GEOLOCALIZAÇÃO EM TEMPO REAL PELA INTELIGÊNCIA) demonstra-se a proximidade de institutos e modelos internacionais com a realidade brasileira. É traçado um comparativo entre a campana, atividade que não exige decisão judicial e não afeta a privacidade, e a vigilância, técnica operacional realizada pelos serviços de inteligência.

No trabalho foram feitas diversas citações diretas, principalmente a textos de leis estrangeiras e decisões de tribunais nacionais e internacionais. Esses pontos foram destacados em sua essência como “dados de pesquisa” de suma importância para realização de um comparativo com a realidade no Brasil.

2 DEFINIÇÃO, NATUREZA, TÉCNICAS E FINALIDADE DOS SERVIÇOS DE INTELIGÊNCIA

Conceitualmente, inteligência é *a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado.* [1] [17].

Para Kent[18], o termo inteligência pode ser entendido e definido a partir de três acepções:

1. inteligência enquanto organização (órgão responsável pelo desempenho da atividade);
2. inteligência como produto, o resultado que se produz ou alcança com a atividade; e
3. inteligência como atividade em si, que se efetivaria pelo procedimento de reunião, busca e obtenção de dados e produção do conhecimento .

Enquanto atividade, pode ser vista, igualmente, 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 planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado* [19].

Para o Gabinete do Diretor Nacional de Inteligência [2] Americano *"Inteligência inclui as organizações, capacidades e processos envolvidos na coleta, processamento, exploração, análise e disseminação de informações ou inteligência acabada. Os produtos de inteligência fornecem aos usuários as informações que foram coletadas e analisadas com base em seus requisitos"* [20].

O ciclo de inteligência ou, na nomenclatura do Departamento de Estado dos Estados Unidos, Processo de Inteligência, envolve o estabelecimento da Necessidade/Requisitos pelo usuário ou tomador de decisões, o Planejamento de reunião de dados e conhecimentos, Processamento, Análise e Difusão. É um ciclo que se fecha no retorno do produto para a autoridade assessorada.

A sistematização do ciclo de inteligência tem sido elencada como prioridade pela Organização do Tratado do Atlântico Norte [21] no *Joint ISR* (*Joint Intelligence, Surveillance and Reconnaissance*). Inteligência conjunta, vigilância e reconhecimento são considerados pilares da cooperação entre os integrantes da OTAN e essencial para o sucesso das operações militares.

Destarte, para o desempenho de seu mister, o órgão de inteligência, inexoravelmente, se socorre de ferramentas de busca do dado ou da informação necessária. Essa tarefa de coleta de elementos se subdivide

[1] Art. 1°, §2° da Lei n° 9.883/99

[2] O Diretor Nacional de Inteligência chefia a comunidade de inteligência nos Estados Unidos.

em HUMINT (inteligência humana), IMINT (inteligência de imagens), MASINT (inteligência de medição de assinatura), SIGINT (inteligência de sinais), OSINT (inteligência de fontes abertas), dentre outras.

Para a Doutrina Nacional de Inteligência [22], *a reunião é o processo de obtenção de conhecimentos e dados que contribuem para a produção do conhecimento, englobando diversos meios de obtenção, tanto os alicerçados exclusivamente em habilidades humanas quanto os embasados no emprego de meios tecnológicos.*

A importância do processo de reunião e coleta de dados ou informações é de tal monta que se confunde com o próprio conceito da atividade de inteligência, como bem acentua Cepik [23]:

> Nesse caso, uma definição mais restrita diz que inteligência é a coleta de informações sem o consentimento, a cooperação ou mesmo o conhecimento por parte dos alvos da ação. Nesta acepção, inteligência é o mesmo que segredo ou informação secreta.
> Mantive ao longo da pesquisa uma forte ancoragem na definição restrita de inteligência, aplicando-a ao estudo dos serviços governamentais que atuam nessa área. Ignorar a definição restrita implicaria perder de vista o que torna afinal essa atividade problemática. No mundo real, porém, as atividades dos serviços de inteligência são mais amplas do que a mera espionagem e mais restritas do que o provimento de informações sobre todos os temas relevantes para a decisão governamental [23].

Existem diversas técnicas operacionais utilizadas por serviços de inteligência pelo mundo afora, como disfarce, fotografia, filmagem, OMD (observação, memorização e descrição), estória cobertura, vigilância (incluindo-se a eletrônica, a partir de dispositivos tecnológicos), recrutamento, infiltração, interceptação de dados telefônicos, telemáticos, eletromagnéticos, assim como outras mais sofisticadas que envolvem mecanismos de vigilância em massa e análise de mega-dados coletados. A vigilância em massa, utilizada por algumas agências de inteligência, se mostra como um mecanismo muito mais amplo e com um alcance indeterminado, o que resulta em um impacto no direito à privacidade maior do que a vigilância física ou eletrônica individual[3].

A amplitude, no entanto, do alcance das ações de busca está necessariamente ligada às limitações impostas pelo arcabouço legislativo de cada país e à interpretação conferida pelos órgãos de controle e do Judiciário, inclusive em relação ao emprego de pessoal e equipamentos nas operações de inteligência.

No Brasil, o primeiro órgão de inteligência foi instituído com a edição do Decreto n° 44.489, de 15 de setembro de 1958, que criou o Serviço Federal de Informações e Contra-Informações (SFICI). Antes desse momento, a atividade de inteligência se desenvolvia no âmbito do Conselho de Defesa Nacional (1927-1934), do Conselho Superior de Segurança Nacional (1934-1937) e do Conselho de Segurança Nacional (1937-1946) [24].

Contemporaneamente[4], a atividade de inteligência no Brasil é realizada, precipuamente, pela Agência

[3] A geolocalização é uma espécie de vigilância eletrônica, capaz de determinar a localização de determinada pessoa de interesse para um serviço de inteligência. É espécie porque a vigilância eletrônica seria capaz de obter outros dados e informações do indivíduo.

[4] A ABIN foi criada pela Lei 9883/99, em 07 de dezembro de 1999.

Brasileira de Inteligência (ABIN), que, por força da Lei n° 9.883/99, coordena o Sistema Brasileiro de Inteligência [17]. Dentre as competências da ABIN encontramos a de planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência, observando, para tanto, a Política [19]e a Estratégia Nacional de Inteligência [25].

Longe do secretismo, o que baliza, portanto, a atividade de inteligência em âmbito nacional são dois documentos públicos, de acesso irrestrito, editados pelo Presidente da República, o Decreto n° 8.793/2016 e o Decreto s/n, de 15 de dezembro de 2017, que dispõem sobre os principais eixos norteadores para a consecução dos objetivos a serem trilhados pelos órgãos componentes do Sistema Brasileiro de Inteligência (SISBIN).

A Política Nacional de Inteligência (PNI) foi concebida para orientar a atividade de inteligência e define os parâmetros, limites de atuação, assim como estabelece pressupostos, objetivos, instrumentos e diretrizes, no âmbito do Sistema Brasileiro de Inteligência (SISBIN).

A Estratégia Nacional de Inteligência (ENI), por sua vez, detalha a PNI e serve de referência para a formulação do Plano Nacional de Inteligência, esse sim, um documento restrito de nível operacional e tático.

De acordo com a ENI, cabe à atividade de Inteligência acompanhar o ambiente interno e externo, buscando identificar oportunidades e possíveis ameaças e riscos aos interesses do Estado e à sociedade brasileira. As ações destinadas à produção de conhecimentos devem permitir que o Estado, de forma antecipada, direcione os recursos necessários para prevenir e neutralizar adversidades futuras e para identificar oportunidades para sua atuação.

Foram elencadas na ENI como principais ameaças capazes de pôr em perigo a integridade da sociedade e do Estado e a segurança nacional temas como espionagem, sabotagem, interferência externa, ações contrárias à soberania nacional, ataques cibernéticos, terrorismo, atividades ilegais que envolvam bens de uso dual, armas de destruição em massa, criminalidade organizada, corrupção e ações contrárias ao Estado Democrático de Direito.

A Estratégia Nacional de Inteligência também estabeleceu alguns assuntos que foram enquadrados como oportunidades para o Brasil: inserção do país no cenário internacional, cooperação internacional, desenvolvimento científico e tecnológico, inteligência cibernética, consolidação de rede logística e de infraestrutura de interesse nacional.

Em todos esses temas, de ameaças ou riscos, compete à atividade de inteligência produzir conhecimentos para auxiliar as autoridades governamentais no processo decisório. A atividade de inteligência, portanto, não se presta a desenvolver investigação e repressão criminal e, portanto, órgãos de inteligência do SISBIN não se confundem com órgãos de persecução penal, como as Polícias Judiciárias Civil e Federal.

Essa premissa é de extrema importância porque o produto da atividade de inteligência não se reveste de caráter probatório, não compõe peça de inquérito ou ação penal, ou tampouco deve ser utilizado como elemento para formação da *opinio delicti* ou, ainda, para condenação criminal[5]. O próprio Superior Tribunal de Justiça tem, recorrentemente, estabelecido a diferença entre os denominados relatórios de inteligência e as peças produzidas no contexto de persecução criminal. A Corte, em julgamentos relacionados ao controle externo exercido pelo Ministério Público Federal da atividade policial, firmou posicionamento restringindo o acesso do Parquet Federal aos documentos produzidos no curso da atividade de polícia judiciária. Importante, no particular, trazer à baila, o que explica o STJ:

> PROCESSUAL CIVIL E ADMINISTRATIVO. CONTROLE EXTERNO DO MINISTÉRIO PÚBLICO. RELATÓRIOS AVULSOS DE INTELIGÊNCIA POLICIAL. ACESSO IRRESTRITO. DIREITO. INEXISTÊNCIA.
>
> [...]
>
> 2. Entre as funções institucionais atribuídas ao Ministério Público pela Constituição Federal está o controle externo da atividade policial (CF, art. 129, VII), o que abrange o acesso a quaisquer documentos relativos àquela atividade-fim (art. 9º da LC n. 75/1993).
>
> 3. A atividade de inteligência, disciplinada pela Lei n. 9.883/1999, que instituiu o Sistema Brasileiro de Inteligência (SISBIN) e criou a Agência Brasileira de Inteligência (ABIN), consiste na "obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado".
>
> 4. "O controle e fiscalização externos da atividade de inteligência serão exercidos pelo Poder Legislativo na forma a ser estabelecida em ato do Congresso Nacional"(art. 6º daquele diploma legal).
>
> 5. A inclusão do Departamento de Polícia Federal entre os órgãos integrantes do SISBIN (art. 4º do Decreto n. 4.376/2002) permitiu àquela unidade a elaboração de relatório de inteligência (RELINT), que, de acordo com a União, "pode transcender o âmbito policial".
>
> 6. O controle externo da atividade policial exercido pelo Parquet deve circunscrever-se à atividade de polícia judiciária, conforme a dicção do art. 9º da LC n. 75/1993, cabendo-lhe, por essa razão, o acesso aos relatórios de inteligência policial de natureza persecutório-penal, ou seja, relacionados com a atividade de investigação criminal.
>
> 7. O poder fiscalizador atribuído ao Ministério Público não lhe confere o acesso irrestrito a "todos os relatórios de inteligência"produzidos pelo Departamento de Polícia Federal, incluindo aqueles não destinados a aparelhar procedimentos investigatórios criminais formalizados. [...] (Resp. AgInt no Resp 1439165/RJ. Rel. Min. Gurgel de Faria. 1ª Turma. DJ. 12/08/2019).

Nesse contexto, em que se dissocia a repressão e investigação de infrações penais e a atividade de inteligência, é que se deve examinar as ferramentas utilizadas pelas agências de inteligência.

No Brasil, a utilização de técnicas e meios sigilosos para obtenção de dados pela ABIN é tema con-

[5] Alguns órgãos se utilizam de técnicas aprimoradas de fiscalização denominando-as de "inteligência". Sem embargo, há aqueles que efetivamente produzem conhecimento a partir de metodologia própria, difundida pela Escola Nacional de Inteligência (ESINT). A doutrina tem, para além da acepção clássica, entendido a inteligência em distintas categorias, como a inteligência financeira, fiscal, econômica, sanitária, policial dentre outras. Nesse contexto, atuando os órgãos nas suas competências fiscalizatórias, o Superior Tribunal de Justiça e o Supremo Tribunal Federal tem aceito a possibilidade de compartilhamento dos dados e informações. O STF, no julgamento do RE 1.055.941/SP, com repercussão geral, entendeu que não há ilegalidade no compartilhamento dos dados obtidos pela Receita Federal no âmbito de sua atividade fiscalizatória para fins de persecução criminal. O STJ no RHC 155552/SP reconheceu a possibilidade da Receita Federal do Brasil compartilhar informações de investigação em procedimento administrativo fiscal próprio, realizando a representação para fins de investigação criminal, para fins de persecução penal, atendendo a Lei Complementar 105/2001.

troverso e que alcança certa dose de incompreensão, principalmente no âmbito dos Poderes Legislativo, Judiciário e da sociedade em geral.

A legislação não esmiuçou quais seriam os mecanismos que poderiam ser utilizados ao longo do exercício da atividade de inteligência. É o que se verifica do parágrafo único do art. 3° da Lei n° 9.883/99, norma que instituiu a ABIN e o SISBIN:

> Art. 3° Fica criada a Agência Brasileira de Inteligência - ABIN, órgão da Presidência da República, que, na posição de órgão central do Sistema Brasileiro de Inteligência, terá a seu cargo planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, obedecidas à política e às diretrizes superiormente traçadas nos termos desta Lei.
>
> Parágrafo único. As atividades de inteligência serão desenvolvidas, no que se refere aos limites de sua extensão e ao uso de técnicas e meios sigilosos, com irrestrita observância dos direitos e garantias individuais, fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado.

Se de um lado procurou-se resguardar as técnicas, evitando possíveis contra medidas de proteção de outros países e agências congêneres de inteligência, de outro criou-se um espaço jurídico interpretativo que alberga diversas matizes de pensamento, de teorias que restringem operações de busca, mencionando que a falta de discriminação legislativa reclama a edição de lei específica ou, ainda, de instrumentos regulamentadores sobre a questão, a entendimentos jurídicos que procuram acolher o uso de técnicas de inteligência que não afrontem diretamente um comando legal, sob pena de se inutilizar a previsão do próprio art. 3° da Lei n° 9.883/99.

Em outros termos, parte que se debruça no dispositivo acredita que ele não possibilita que a ABIN desenvolva qualquer técnica de inteligência. Outro segmento, por sua vez, acredita que o desenvolvimento das técnicas está limitada pelas disposições legais e constitucionais, notadamente aquelas relacionadas aos direitos e garantias individuais, permitindo-se a atuação da ABIN dentro dessa moldura.

A doutrina [26] bem pontuou a questão:

> Outro aspecto sobre o qual convém fazer referência neste Capítulo diz respeito à maneira como a sociedade e o poder público encaram a obtenção dos dados pela inteligência. Particularmente nas democracias, é constante o debate sobre o tipo de informações que são obtidas pelos serviços de inteligência e por que meios. É natural que se questione se o serviço age corretamente ao reunir um dado protegido, especialmente se esse dado for referente a um cidadão ou reunido dentro do território nacional. Afinal, agindo assim, o serviço não estaria indo de encontro a sua missão básica de proteger o cidadão? Não violaria as liberdades individuais, tão necessárias à democracia e ao Estado de direito?
>
> A resposta da comunidade de inteligência é que, ao realizar operações para reunir dados sobre determinado indivíduo ou organização que represente ou possa vir representar ameaça à sociedade, o serviço secreto está a proteger os cidadãos, o Estado e a própria democracia. Tem-se aí o dilema da necessidade de segurança versus a preservação dos direitos individuais, dilema este que não encontra solução absoluta.

A ideia de que um serviço de inteligência não pode, de forma absoluta, se valer de operações de busca para obtenção de determinado dado ou conhecimento subverte o próprio ciclo de inteligência e a etapa de

produção do conhecimento. É indissociável de qualquer serviço de inteligência a busca do dado negado, não acessível por simples consulta em fontes abertas. Pensar o contrário é acreditar que o serviço de inteligência deve, em sua atividade de análise, reproduzir as notícias da imprensa. O ponto, portanto, é encontrar a medida e o equilíbrio do processo de coleta e busca para a atividade de produção do conhecimento de inteligência em decorrência dos princípios da legalidade, proporcionalidade, razoabilidade e ponderação de interesses.

Como já dito alhures, existem diversas técnicas de inteligência, umas mais e outras menos abrangentes, esse trabalho se debruçará sobre a Geolocalização em tempo real.

O que seria, nesse contexto de inteligência, a geolocalização em tempo real?

A geolocalização de um alvo de inteligência, ou identificação da localização de determinada pessoa, pode ser vista como uma vigilância eletrônica, isto é, a partir de um mecanismo tecnológico. Essa vigilância eletrônica se traduz na identificação, em tempo real, da localização da pessoa, ou ainda, onde esteve em determinado dia e horário ou que trajeto ou percurso realizou. O meio que tem possibilitado essa vigilância eletrônica, capaz de determinar a localização do indivíduo, é o rastreamento de um aparelho de telefonia celular.

De acordo com a Agência Nacional de Telecomunicações [8], em novembro de 2022 existiam no país 254,9 milhões de acessos de telefonia móvel e, destes, 226,6 milhões possuíam banda larga móvel. Esses números representam uma densidade de 101,0 acessos/100 hab..

Como se observa dos números, o telefone celular tornou-se um objeto popular, de uso permanente e de larga utilização pela sociedade, seja pela utilização do Serviço Móvel Pessoal ou como uma plataforma capaz de acessar a internet (Serviço de Valor Adicionado - SVA) o que resulta, atualmente, pelo menos em tese, na possibilidade efetiva de localização remota de quase a totalidade da população brasileira.

Assim, o celular ou, na terminologia legal, constante da Resolução Anatel n° 477/2007, estação móvel, habilitada em uma rede de Serviço Móvel Pessoal e com serviços de dados de internet, mostra-se como a principal forma de geolocalização das pessoas.

A geolocalização tem sido utilizada com interesses econômicos e comerciais há algum tempo, sem maiores questionamentos, individuais ou coletivos, em relação à privacidade, mesmo nos casos de aceitação obrigatória de ferramentas e aplicativos que coletam e compartilham dados do usuário, inclusive a localização. O que se oferece ao usuário em contrapartida é a praticidade diária, a diminuição de etapas de interface com aplicativos e *e-commerce* e a obtenção de serviços e produtos personalizados. Para alguns *Apps*, é essencial a localização do usuário para o seu funcionamento.

Aplicativos que conferem facilidades de rotas/deslocamento (*Waze, Google Maps*) ou oferecem a possibilidade de aquisição de serviços de transporte ou entrega (Uber, 99, Cabify, Ifood, Rappi), ou proveem o usuário de ferramenta de uso da internet (navegadores de internet) ou permitem uma individualização da

experiência, a partir da localização do usuário (*AccuWeather, The Weather Chanel, Tripadvisor, Facebook, Instagram, Fitness*) em alguns casos compartilham a localização do usuário com empresas que tem por objetivo oferecer ao consumidor produtos e serviços que estejam mais adequados ao perfil de movimentação e frequência de locais pelo indivíduo.

Em outros termos, o compartilhamento da localização, em tempo real ou de locais frequentados, possibilita estabelecer perfis comportamentais e proporciona uma estratégia de alcance de potenciais consumidores a partir de uma análise das preferências dos usuários e a realização de uma publicidade direcionada. De sorte que, uma base de dados de geolocalização adquire, nesse contexto, valor econômico imensurável no campo privado.

E como se atinge a localização do usuário do telefone celular?

Seja pelo uso do Serviço Móvel Pessoal (SMP), *Apps* ou pela internet, há diversas formas de alcançar a geolocalização.

A primeira delas é pelo *Global Position System* (GPS)[6]. O Sistema de Posicionamento Global foi criado para uso militar, mas, em momento seguinte, foi franqueado um módulo para utilização civil e se mostra como ferramenta de auxílio de navegação marítima, aérea e até no cotidiano de deslocamentos urbanos. A ferramenta permite a localização de um aparelho móvel por meio de 4 ou mais satélites. Cada satélite emite um sinal de rádio padrão captado pelo aparelho receptor que calcula a diferença de tempo de emissão e recepção, determinando uma localização imaginária. A intersecção das localizações imaginárias determinadas por 4 satélites resulta na localização do usuário, definida em coordenadas geográficas (latitude, longitude e elevação) [27].

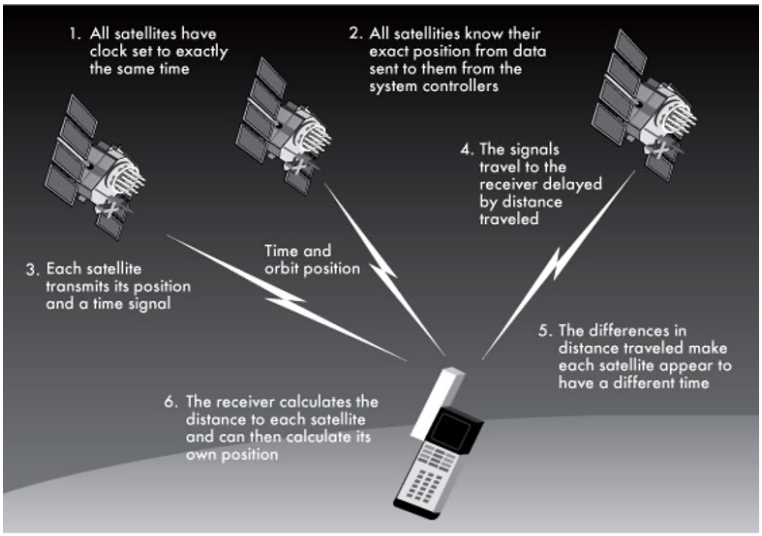

Figura 2.1: Funcionamento do GPS.
Fonte: <https://scmwiki2012.wordpress.com/g/gps-global-positioning-system/>

[6]Registre-se que há 4 sistemas mundiais de localização via satélite. GPS é o sistema americano. Glonass o sistema russo. Galileu o sistema europeu e Beidou o sistema chinês. GPS é o sistema mais popular.

Em uma representação mais clara:

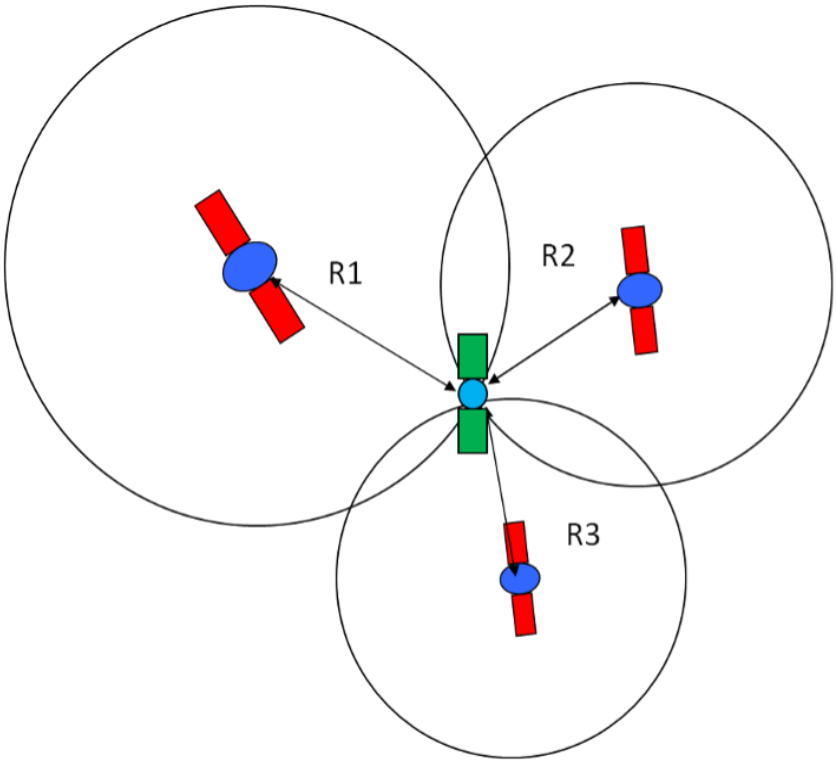

Figura 2.2: Funcionamento do GPS (2).
Fonte: <https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html/>

Grande parte dos telefones celulares atuais (*smartphones*) possuem um GPS integrado, que é acessado, por exemplo, por *Apps* interessados em determinar a localização do usuário.

O GPS determina a localização do indivíduo ainda que estejam inabilitados os serviços de *bluetooth, wi-fi* e serviços de telefonia (SMP – Serviço Móvel Pessoal). Em outros termos, é possível localizar uma pessoa durante uma viagem aérea, quando ativado o "modo avião", por meio do GPS. Daí que não se deve confundir a possibilidade de localização pelo GPS com a ativação de serviços celulares ou uso da internet.

Pela internet, e atualmente a maioria dos telefones celulares são *smartphones* e possuem um serviço de dados (internet) contratado, é possível estimar a geolocalização de um usuário por meio do endereço IP. IP é o código atribuído a um terminal de uma rede para permitir sua identificação, em outras palavras, é o seu endereço na internet.

A entidade internacional responsável pela atribuição de IP's (IANA) distribui faixas de números ou blocos de endereços por países.

Nacionalmente, o Núcleo de Informação e Coordenação do Ponto BR. (NIC.br) redistribui esses números por regiões ou cidades. A partir desse ponto, a informação a respeito da localização dos usuários é detida pelos provedores de internet, que sabem, exatamente o usuário que utilizou determinado endereço

de IP naquele momento. Esse rastreio, via IP, é que permite a geolocalização do usuário que acessou a internet por telefone celular ou computador/notebook.

O marco civil da internet, Lei n° 12.965/2014 [28], obriga os provedores a manter os dados pelo prazo de pelo menos 1 (um) ano, fornecendo-os nas seguintes condições:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
>
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
>
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Esse mecanismo de obtenção da geolocalização é mais complexo do que o rastreio via GPS ou por meio de Estações Rádio Bases, que será tratada logo mais.

Uma outra forma de obter a localização de um indivíduo é a verificação de Geotags. Em uma tradução literal da sigla, são etiquetas de localização apostas em fotos, vídeos, postagens em redes sociais, etc. Quando o usuário do telefone celular realiza uma postagem no Facebook ou Instagram, por exemplo, a rede social vincula, via acesso ao GPS, o comentário ao local onde a pessoa está naquele momento. Fotos ou vídeos também embutem essa etiqueta de localização e data/hora em que foi realizado o registro.

Os meios de localização mencionados acima não estão atrelados ao serviço de telefonia móvel em si. Há, no entanto, um mecanismo de geolocalização que é inerente ao uso do serviço móvel pessoal. Quando um indivíduo utiliza o serviço de telefonia celular ele é automaticamente geo-localizado porque é necessário vinculá-lo a uma rede do SMP, e isso se faz por meio de uma Estação Rádio Base (ERB). Ou seja, para que o serviço seja prestado, a operadora necessita que uma ERB se "conecte" ao terminal do aparelho celular. Esse processo de autenticação serve, inclusive, para dar acesso ao serviço apenas aos usuários que contrataram o SMP naquela específica operadora, o que impede, por exemplo, do usuário da empresa X realizar uma ligação telefônica pela rede da empresa Y.

Explicando melhor, quando o celular é ligado, ficando visível para todas as ERB´s de qualquer operadora naquela região de alcance, ele automaticamente envia uma mensagem com a identificação do cliente (identidade de assinante móvel internacional – IMSI) e do aparelho, o denominado IMEI. A ERB então da operadora contratada reconhece o terminal previamente cadastrado e lhe confere acesso à rede. A partir

desse momento, há uma constante comunicação entre o aparelho celular e as torres. Não é necessária a realização de uma ligação telefônica para que o aparelho celular seja identificado na rede e esteja ligado a uma ERB. Ele está, enquanto ligado, permanentemente autenticado, o que lhe permite utilizar o serviço a qualquer momento, como originador ou destinatário de uma ligação telefônica. As ERB's, por sua vez, estão ligadas à central da operadora, responsável por realizar a comutação das ligações e sms's (*short message service*) e prover internet a partir da rede mundial de computadores.

Assim, em linhas gerais, independentemente de uma busca ativa, todos os usuários da telefonia celular estão, necessariamente, sendo identificados e localizados pelas prestadoras em decorrência da necessidade de prestação do serviço. Todas as operadoras sabem exatamente, em tempo real, qual ERB está provendo o Serviço Móvel Pessoal a um determinado usuário, ou seja, em qual torre o celular está autenticado. E mais, os dados de localização, assim como diversas outras informações, como origem e destino de ligações, padrões de comportamento e localização do usuário, registro de uso da estrutura telefônica e conteúdo das mensagens de texto enviadas são armazenados nos CDR's (*Call Detail Record*) e ficam em poder da operadora por, pelo menos, 5 anos. Esses registros de utilização da rede servem como fonte de informação para aprimoramento do serviço, mas também permitem às operadoras traçar estratégias comerciais a partir desses dados.

Com o avanço e popularização da telefonia celular e a necessidade de suportar ligações simultâneas, aumentou-se a necessidade de instalação de ERB's com menores raios de ação (áreas geográficas de cobertura), principalmente em grandes centros urbanos de elevado adensamento populacional. É possível verificar esse fenômeno através da plataforma serviço móvel da Anatel (http://sistemas.anatel.gov.br/siec-servico-movel-web/). A figura 2.3 mostra a quantidade de ERBs em determinada área de São Paulo/SP. É possível identificar que na Av. Paulista o número de ERBs aumenta significativamente:

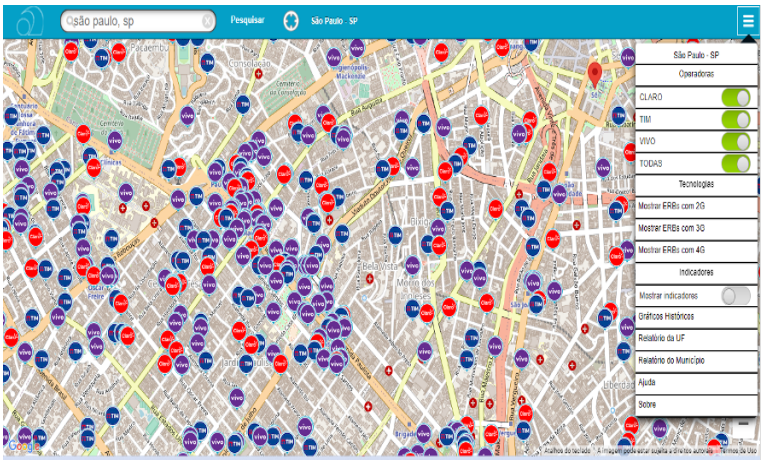

Figura 2.3: ERB's na Av. Paulista.
Fonte: <http://sistemas.anatel.gov.br/siec-servico-movel-web/>

Busca-se, portanto, dividir cada macro-célula em áreas de abrangência menores (micro-células) com torres mais baixas e com menos potência. Isso porque há uma limitação de número de usuários em cada ERB. Então se outrora uma ERB abrangia um raio, por exemplo, de 1km, vinculando os telefones celulares a essa estação, atualmente criou-se a necessidade de operação de micro ERB's. Isso resulta na diminuição

do raio de alcance, por exemplo, para 300 metros ou menos, o que significa uma maior precisão na geolocalização do usuário. Nesse caso, a se considerar que o usuário está vinculado a uma ERB, parte-se do pressuposto que ele está localizado no raio de alcance da torre.

Para além, no entanto, da ideia de geolocalização pela vinculação do usuário em uma ERB's (o que resulta em uma precisão menor quando comparado ao GPS), existem técnicas que buscam a geolocalização mais precisa do usuário, seja por meio do cálculo do tempo de envio e chegada de um sinal em relação a uma ERB (TDOA – *Time Difference of Arrival*) ou a partir da combinação de dados de múltiplas ERB's, como a triangulação, trilateração/multilateração ou *Bounding Box*.

Uma outra maneira de localização por meio de radiofrequência é o *fingerprinting*. A ideia principal da técnica é que cada aparelho/estação móvel emite informações e sinais próprios de comunicação com as ERB's. Com o parâmetro prévio de sinais de determinado aparelho celular, seria possível, a partir de uma delimitação de área geográfica, e mapeando as radiofrequências, identificar o que seria a impressão digital de comunicação de um usuário com a rede.

Para além desses mecanismos, existem diversos *Apps* que possibilitam o compartilhamento da localização do usuário em tempo real, hipótese, no entanto, que exige que o indivíduo disponibilize ativamente sua localização.

Em um apanhado geral, como no celular o fornecimento do Serviço Móvel Pessoal (ligações telefônicas) e do Serviço de Valor Agregado (internet) é realizado pela mesma empresa, é comum que a geolocalização do usuário seja atingida pela combinação do GPS com as ERB's.

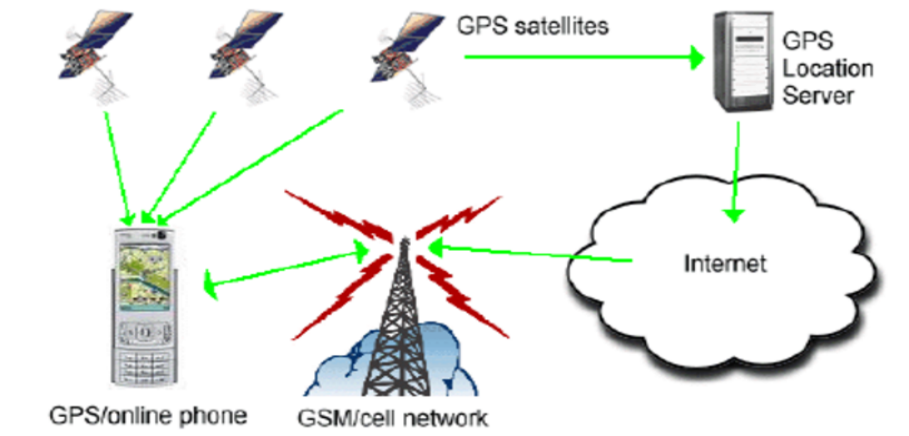

Figura 2.4: Geolocalização por GPS e ERB.
Fonte:
<https://www.researchgate.net/figure/Assisted-Global-Positioning-System-A-GPS_fig5_287156709/>

A par da possibilidade tecnológica de geolocalização de determinada pessoa, a questão que exsurge é se os órgãos de inteligência podem obter a localização de um alvo por meio destas capacidades tecnológicas.

3 GEOLOCALIZAÇÃO E TÉCNICAS OPERACIONAIS EM SERVIÇOS DE INTELIGÊNCIA ESTRANGEIROS

Com essas premissas em mente, é possível aprofundar os aspectos legislativos e de jurisprudência, buscando estabelecer um paralelo com as diversas agências de inteligência, especialmente em relação à geolocalização de alvos de inteligência.

Como é cediço, a *National Security Agency* desenvolveu programas de vigilância em massa, como o PRISM e o ECHELON, este último em parceria, inicialmente, com os países que integram o Tratado de Segurança conhecido como *Five Eyes*, englobando os Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia. Assim, iniciaremos a análise a partir da experiência desses países.

3.1 REINO UNIDO

O *Secret Intelligence Service* (SIS) ou *Military Service, Section* 6 (MI6), o *Security Service* (SS) ou *Military Service, Section* 5 (MI5) e o *Government Communications Headquarters* (GCHQ) são as três principais agências de inteligência do governo britânico.

Embora o MI6 tenha se tornado famoso em virtude de uma série de filmes abordando operações de um agente de inteligência, até meados da década de 90, o MI6 negava a própria existência. Apesar de documentos apontarem a sua criação em 1909, apenas em 1994, com a edição da *Intelligence Services Act*, concretizou-se formalmente o SIS com a missão de atuar no interesse da segurança nacional, obtendo informações sobre ações e intenções de estrangeiros. A aparente clandestinidade, no entanto, não impediu o SIS de atuar operacionalmente desde antes da 1ª Guerra Mundial.

O MI5 concentra-se na inteligência doméstica, atuando, principalmente, em contraterrorismo em solo britânico.

No Reino Unido, é possível citar a *Investigatory Powers Act* 2016 [2]. Na lei britânica incluem-se entre os dados de identificação *data which may be used to identify, or assist in identifying, the location of any person, event or thing* 263. (*General Definitions* 2 C.). Os mandados de interceptação dos dados podem ser emitidos para atender solicitações dos serviços de inteligência pelo Secretário de Estado no interesse da segurança nacional. Isso significa a possibilidade de acesso aos dados de localização dos usuários a partir de uma decisão de cunho administrativo (não judicial). No entanto, reforçando os mecanismos de controle, a *Investigatory Powers Act* 2016 estabeleceu que a autorização/mandado apenas entra em vigor após a aprovação por um juiz. A lei, na Parte 6, Capítulo 1, também menciona a possibilidade de emissão de mandados para interceptação em massa.

No campo do direito comparado, em julho de 2019, no julgamento do caso *Liberty vs Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs* [29] em que se questionava se o *Intelligence Services Act* teria conferido ao MI5 poderes excessivos para obtenção de dados em massa, sem as devidas salvaguardas suficientes contra o risco de abuso de poder, a Alta Corte de Justiça (*High Court of Justice*) não acatou a ação e os argumentos suscitados pela *Liberty*, entendendo que a *Intelligence Services Act* estaria compatível com a *Human Rights Act* 1998.

Em maio de 2021, a Corte Europeia de Direitos Humanos (*European Court of Human Rights*) [30] julgou o caso da *Big Brother Watch and Others vs*. Reino Unido. O caso se referia às denúncias de jornalistas e organizações de direitos humanos a respeito de três pontos:

1. interceptação em massa de comunicações;
2. recebimento de informações de agências de inteligência estrangeiras, oriundas de interceptação em massa, pelo Reino Unido; e
3. obtenção de dados de comunicações através dos prestadores de serviços de comunicação.

Os fatos relatados foram durante a vigência da Regulamentação de Poderes de Investigação 2000 (anterior a *Investigatory Powers Act* 2016). A *European Court of Human Rights* (ECHR) considerou que, diante da proliferação de ameaças, a realização de interceptações em massa não violaria, por si só, a Convenção, devendo-se, no entanto, estabelecer um regime de salvaguardas como a avaliação da necessidade e proporcionalidade da medida, autorização independente, supervisão e revisão. A ECHR reconheceu, todavia, que a vigilância em massa é essencial para proteger a segurança nacional.

Em relação à supervisão da atividade, deve-se mencionar o *Justice and Security Act* 2013, norma onde consta a previsão de controle externo das atividades de inteligência pelo *Intelligence and Security Committee*, colegiado composto por 9 membros da Câmara dos Comuns e Câmara dos Lordes, responsável por examinar as políticas, despesas, administração e operações das sete agências e departamentos que formam a Comunidade de Inteligência do Reino Unido (UKIC).

3.2 ESTADOS UNIDOS DA AMÉRICA

Nos Estados Unidos, a comunidade de inteligência engloba 17 agências governamentais, civis e militares, independentes entre si, e que produzem inteligência, conjunta e separadamente, interna e externa. Dentre os membros, podemos citar a CIA (*Central Intelligence Agency*), NSA, FBI, Inteligência do Departamento de Defesa, Escritório de Inteligência do Departamento de Estado, *Homeland Security*, Escritório de inteligência do DEA (*Drug Enforcement Administration*), Inteligência do Tesouro Americano, e inteligências militares [31]. A comunidade de inteligência é chefiada pelo Diretor Nacional de Inteligência.

Embora com origem na década de 60, o programa ECHELOM, voltado inicialmente para inteligência de sinais e coleta de dados na região da Rússia e Europa Ocidental, ganhou musculatura no período pós

atentados de 11/09, com a vigilância em massa de escala global. É nesse período, mais precisamente em 26 de outubro de 2001, que o então Presidente americano, George W. Bush edita o USA *Patriot Act* com o objetivo de enfrentar a ameaça terrorista, por meio do fornecimento de ferramentas voltadas a obstar o terrorismo [32].

De maneira geral, a tônica do USA *Patriot Act* foi municiar as agências de inteligência de meios para combater com maior veemência o terrorismo e estimular a obtenção e compartilhamento de informações conforme se verifica da Seção 903:

> It is the sense of Congress that officers and employees of the intelligence community of the Federal Government, acting within the course of their official duties, should be encouraged, and should make every effort, to establish and maintain intelligence relationships with any person, entity, or group for the purpose of engaging in lawful intelligence activities, including the acquisition of information on the identity, location, finances, affiliations, capabilities, plans, or intentions of a terrorist or terrorist organization, or information on any other person, entity, or group (including a foreign government) engaged in harboring, comforting, financing, aiding, or assisting a terrorist or terrorist organization.

Em 2004, é aprovado o *Intelligence Reform and Terrorism Prevention Act* [33]. Cria-se com a Lei a figura do Diretor Nacional de Inteligência, responsável por, dentre outros pontos, chefiar a comunidade de inteligência americana, garantindo o compartilhamento das informações entre as agências. Para além da reforma em si da organização do sistema de inteligência, a norma estabelece diversos pontos sobre a segurança aeroportuária, de fronteiras, imigração, assim como outras ferramentas de combate ao terrorismo e a lavagem de dinheiro.

Em julho de 2005, o USA *Patriot Act* foi prorrogado pela primeira vez pelo Congresso Americano. O USA *Patriot Improvement and Reauthorization Act of* 2005 [34], além de expandir a vigência, serviu como um aprimoramento da lei original. Alterou-se a *Intelligence Reform and Terrorism Prevention* ampliando o conceito de alvo ligado ao terrorismo para fins de monitoramento e vigilância. Foram acrescentadas salvaguardas adicionais para garantia dos direitos e privacidade dos americanos.

No campo da vigilância e dos mandados, os *National Security Letters* (NSLs)[1], expedidos por autoridades administrativas com determinação de entrega e produção de dados por investigados, destacam-se entre as alterações nas Seções 105, 106, 108 e 109:

> (Sec. 105) Amends FISA to apply provisions governing the duration of an order for electronic surveillance or a physical search to surveillance targeted against a foreign power who is not a U.S. person. Limits to one year an order (or extension) for the use of pen registers and trap and trace devices where the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a U.S. person.

[1] As denominadas Cartas de Segurança Nacional são anteriores ao USA *Patriot Act*, foram criadas em 1978, mas tiveram ênfase com a lei e sofreram questionamentos, principalmente sobre a sua constitucionalidade. A natureza é de uma ordem administrativa dirigida ao particular ou ao investigado para que entreguem ou produzam informações de interesse da segurança nacional. O ponto crítico da ordem é que havia uma obrigação de sigilo embutida, impedindo que o destinatário revelasse a determinação do FBI. Com o USA *Patriot Improvement and Reauthorization Act of* 2005 permitiu-se a revisão da ordem por uma autoridade judicial, incluindo-se a cláusula de confidencialidade.

> (Sec. 106) Amends the FISA provisions governing orders for the production of tangible things to authorize the Director of the FBI to delegate to the Deputy Director or the Executive Assistant Director for National Security the authority to make an application for such an order involving library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person. Requires an application for such an order to: (1) include a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation; (2) include an enumeration of minimization procedures adopted by the Attorney General that are applicable to the retention and dissemination by the FBI of any tangible things produced; and (3) describe the tangible things to be produced with sufficient particularity to permit them to be fairly identified.
>
> Sets forth provisions concerning review by a panel of three judges of petitions filed by recipients challenging an order's legality.
>
> Requires the Attorney General to report to specified congressional committees annually on requests and order applications for the production of tangible things and semiannually on orders for the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, and medical records that would identify a person.
>
> Sec. 108) Requires applications for roving wiretaps to include specific facts. Requires an order approving electronic surveillance where the nature and location are unknown to direct the applicant to provide notice to the court, within 10 days after the surveillance begins, of: (1) the nature and location of each new facility or place at which the electronic surveillance is directed; (2) the facts and circumstances relied upon to justify the belief that such facility is or was being used by the target of the surveillance; (3) any proposed minimization procedures that may be necessitated by a change in the facility; and (4) the total number of electronic surveillances conducted under the authority of the order. Directs the Attorney General to inform the House and Senate Judiciary Committees semiannually concerning electronic surveillance under FISA, including regarding: (1) electronic surveillance orders where the nature and location of each targeted facility are unknown; (2) criminal cases in which information acquired has been authorized for use at trial; and (3) emergency employments of electronic surveillance.
>
> (Sec. 109) Requires the Attorney General to inform such Committees regarding: (1) emergency physical searches authorized; and (2) pen registers and trap and trace devices authorized on an emergency basis.

Em 2006 ocorreu uma nova prorrogação por meio do USA *Patriot Act Additional Reauthorizing Amendments Act*, o que igualmente se operou nos anos de 2009, 2010 e 2011. O *Patriot Sunsets Extension Act of* 2011 estendeu a vigência do USA *Patriot Improvement and Reauthorization Act of* 2005 e do *Intelligence Reform and Terrorism Prevention Act of* 2004 até 01/06/2015 [35].

Em junho de 2015, o Presidente Barack Obama sancionou o USA *Freedom Act* [36]. A lei fora objeto de discussões na Câmara e no Senado americanos desde 2013 e cuidou de prorrogar dispositivos do USA *Patriot Act*, com exceção da seção 215, que cuidava da vigilância em massa. Esse assunto ficou sob a regulamentação exclusiva da *Protect America Act* e da FISA *Amendments Act of* 2008 na seção 702.

Contextualizado normativamente o período pós 11/09, que motivou a edição de uma série de leis e medidas voltadas a assegurar a segurança nacional nos Estados Unidos, iniciando-se com o *Patriot Act*, é possível trazer, especificamente, o histórico normativo que embasou o desenvolvimento do programa PRISM[2] pela NSA.

[2]PRISM foi um programa de vigilância em massa desenvolvido pela NSA a partir da captura de dados da rede de internet que trafegavam pelas principais empresas de tecnologia, incluindo-se a Microsoft, Yahoo!, AOL, Google, Facebook, Youtube, Skype e Apple.

O *Foreign Intelligence Surveillance Act* 1978 [37] originalmente exigia a menção ao status de cidadão estrangeiro para expedição pelo *Foreign Intelligence Surveillance Court* (FISC) de um mandado voltado à coleta de dados de inteligência.

Em 2007, com o *Protect America Act* [38], alterou-se o *Foreign Intelligence Surveillance Act* 1978, removendo-se a exigência de expedição de um mandado pela FISC[3] e redefinindo-se os alvos de inteligência estrangeira. A lei passou a considerar a possibilidade de coleta de dados de estrangeiros em que se supusesse estar fora dos Estados Unidos (Seção 105B)[4].

Em 2008, com o FISA *Amendments Act of* 2008 [37], acrescentou-se à Lei o Título VII, consolidando-se a permissão para que o Procurador-Geral e o Diretor de Inteligência Nacional possam autorizar, conjuntamente, e pelo período de 01 ano, a vigilância e obtenção de informações de uma pessoa que não esteja em território americano. A determinação está sujeita a revisão judicial e as diretrizes adotadas devem ser remetidas aos Comitês de Inteligência do Congresso Americano, as Comissões do Judiciário do Senado e da Câmara dos Deputados e ao Tribunal de Vigilância de Inteligência Estrangeira. Na hipótese de vigilância a ser realizada em cidadão americano, compete ao Tribunal de Vigilância de Inteligência Estrangeira autorizar a medida, com a anuência do Procurador Geral.

Na seção 703 do FISA *Amendments Act of* 2008 encontramos o alcance e a abrangência da Lei:

> "(a) JURISDICTION OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT.—
> "(1) IN GENERAL.—The Foreign Intelligence Surveillance Court shall have jurisdiction to review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires an order under this Act, and such acquisition is conducted within the United States.

É nesse específico ponto que se autoriza a NSA a interceptação eletrônica, captura e análise de metadados, acessar e-mails, transferências de arquivos e dados, vídeos, fotografias, comunicações de maneira geral, dados armazenados em empresas de telecomunicações, e, em especial, a geolocalização de pessoas.

[3] O Tribunal é composto por 11 juízes de tribunais distritais federais designados pelo Chief Justice of the United States. Cada juiz tem um mandato de 07 anos. A competência da Corte é examinar pedidos de vigilância eletrônica, buscas físicas e outras ações investigativas que se relacionem com a inteligência estrangeira.

[4] SEC. 105B. (a) Notwithstanding any other law, the Director of National Intelligence and the Attorney General, may for periods of up to one year authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the Director of National Intelligence and the Attorney General determine..."

Em relação aos meios de comunicação, a Lei estabelece a obrigatoriedade de colaboração:

> With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to— "(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and ' '(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition, or the aid furnished that such electronic communication service provider wishes to maintain.

Por outro lado, restou consignado uma cláusula expressa de isenção de qualquer responsabilidade perante os Tribunais por empreender colaboração com o Governo Americano:

> "(3) RELEASE FROM LIABILITY.—No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

Do ponto de vista estratégico, no próprio site da NSA [37] se extrai a informação da importância do *Foreign Intelligence Surveillance Act of* 1978 *Amendments Act of* 2008, assim como da assistência das empresas telefônicas:

> The Foreign Intelligence Surveillance Act of 1978 (FISA) regulates certain types of foreign intelligence collection including certain collection that occurs with compelled assistance from U.S. telecommunications companies. Given the techniques that NSA must employ when conducting NSA's foreign intelligence mission, NSA quite properly relies on FISA authorizations to acquire significant foreign intelligence information and will work with the FBI and other agencies to connect the dots between foreign-based actors and their activities in the U.S. The FISA Court plays an important role in helping to ensure that signals intelligence collection governed by FISA is conducted in conformity with the requirements of the statute. All three branches of the U.S. Government have responsibilities for programs conducted under FISA, and a key role of the FISA Court is to ensure that activities conducted pursuant to FISA authorizations are consistent with the statute, as well as the U.S. Constitution, including the Fourth Amendment.

De acordo com Steward Baker, ex conselheiro da NSA, "os metadados absolutamente dizem tudo sobre a vida de alguém. Se você tiver metadados suficientes, não precisará de conteúdo" [39].

Olhando a questão sob o ângulo político, a vigência do FISA *Amendments Act of* 2008 perpassou os governos titularizados por Republicanos e Democratas nos Estados Unidos. O programa PRISM foi implantado com o *Protect America Act* e o FISA *Amendments Act of* 2008 ainda sob o Governo Bush, mas em 2012 foi prorrogado já sob a titularidade do Presidente Obama pelo FISA *Amendments Act Reauthorization Act of* 2012 até 31/12/2017 [40]. E, por fim, o Presidente Donald Trump sancionou o FISA *Amendments Act Reauthorization Act of* 2017, que prorrogou a Lei até 21/12/2023 [41].

Além do PRISM, a NSA desenvolveu diversos programas de vigilância em massa, como o *Fairview, Blarney, Storm e Oakstar*. Após cerca de 6 anos de ser instituído, o assunto veio a público em 2013, em virtude do vazamento de informações promovido pelo ex-colaborador da NSA, Edward Snowden.

Com a repercussão do assunto, entidades de defesa das liberdades civis ingressaram com diversas ações judiciais. Um julgamento (nº 13-58) que merece referência é o EPIC (*Electronic Privacy Information Center*) vs NSA (*National Security Agency*) perante a Suprema Corte Americana [42]. A entidade questionou os programas de vigilância desenvolvidos pela agência de inteligência em virtude das revelações do ex colaborador do órgão, Edward Snowden. O Mandado de Segurança apresentado na Suprema Corte visava sustar autorização concedida pela FISC (*Foreign Intelligence Survellaince Court*)[5] à NSA [43] de acesso a metadados telefônicos de cidadãos americanos, incluindo sua geolocalização. A petição não foi conhecida pela Suprema Corte Americana[6] , havendo grande ressonância na mídia do tema [44].

Um outro julgamento interessante da Suprema Corte Americana, mas que envolve um procedimento criminal, e, portanto, dissociado de questões de segurança nacional dos Estados Unidos, é o caso Carpinter vs United States. O processo diz respeito à geolocalização do demandante através do celular pelo FBI que buscava confirmar a autoria de furtos.

Analisando-se 12.898 pontos de localização do usuário, em 127 dias, a partir de dados das companhias telefônicas, foi possível detectar que Timothy Carpenter estava em quatro locais onde ocorreram furtos. A Suprema Corte entendeu, no entanto, que, em decorrência da expectativa razoável de privacidade, deveria ter havido, no caso, um "mandado judicial" apoiado pelo que denominam de "causa provável", descrita na quarta emenda da Constituição Americana[7]. Em outros termos, para fins de persecução criminal, não poderia ter ocorrido a geolocalização sem uma ordem judicial. O argumento do FBI (*Federal Bureau of Investigation*) de que os dados de localização não pertenceriam ao usuário porque compartilhados voluntariamente com as empresas de telefonia não foi acolhido.

Todavia, no curso da decisão são excluídos do raciocínio utilizado sobre privacidade as seguintes situações: técnicas e ferramentas convencionais de vigilância, como câmeras de segurança; outros registros de negócios que possam acidentalmente revelar informações de localização; e outras técnicas de vigilância envolvendo assuntos externos ou segurança nacional.

Considerando a natureza do sistema jurídico (*common law*) o que a Suprema Corte salientou foi que o caso Carpinter vs United States não poderia servir de precedente, isto é, diretriz para julgamentos posteriores, nas hipóteses listadas no parágrafo anterior[8].

[5]O Tribunal de Vigilância de Inteligência Estrangeira foi estabelecido em 1978 e é composto por juízes oriundos de tribunais distritais federais designados pelo Chefe de Justiça dos Estados Unidos com mandato de 07 anos. Trata-se de um Tribunal especializado com competência para apreciar questões envolvendo inteligência e estrangeiros.

[6]O Mandado de Segurança apresentado à Suprema Corte Americana tem como um dos seus requisitos a liquidez e certeza do direito pleiteado, além da demonstração que não existem outros meios judiciais para atingir a finalidade pleiteada.

[7]Em tradução livre, a Quarta Emenda estabelece: O direito do povo de estar seguro em suas pessoas, casas, papéis e bens, contra buscas e apreensões injustificadas, não será violado, e nenhum mandado será emitido, mas por causa provável, apoiado por juramento ou afirmação e, em particular, descrevendo o local a ser revistado e as pessoas ou coisas a serem apreendidas.

[8]O assunto foi abordado pela mídia e especialistas: https://www.gazetadopovo.com.br/justica/suprema-corte-dos-eua-toma-decisao-historica-sobre-monitoramento-de-dados-4paqcwlnczzhypvl46x038r12/

Pela análise dos casos, percebe-se nítida diferença de tratamento dispensado pelo Judiciário quando o assunto diz respeito a temas como segurança nacional ou terrorismo e nas hipóteses de crimes a serem apurados na esfera criminal.

No campo do controle da atividade de inteligência, para além das medidas hierárquicas e funcionais de competência para aprovação de requerimentos e atribuições originárias de deflagração de pedidos de mandados para acesso a dados e realização de operações de inteligência, encontram-se os Comitês da Câmara e do Senado.

O *United States Senate Select Committee on Intelligence* (SSCI)[9] [45] foi criado pela Resolução 400 de 1976 do Senado Americano [46] e é composto por 15 senadores, entre republicanos, democratas, além de 5 membros *ex officio*. As atividades do Comitê estão expressamente definidas:

> Hearings: The Committee meets roughly twice a week for 1 1/2 to 2 hours, generally in closed session. Most hearings involve appearances by senior Intelligence Community officials—heads of agencies, senior program managers, and senior intelligence analysts—who present testimony and answer Senators' questions. The topics for hearings include agency activities, intelligence collection programs, and intelligence analysis on a geographic region or issue (e.g., stability in the Middle East, Iran's nuclear program, terrorism threats). The Committee occasionally meets in open session, such as annual hearings to receive intelligence testimony on the national security threats to the United States, and for the Committee to consider the President's nominees to intelligence positions requiring Senate confirmation.
>
> Legislation: The Committee writes an annual intelligence authorization bill that authorizes funding levels for intelligence activities (these set caps for agency funding) and provides legislative provisions that limit or allow intelligence conduct. The Committee also periodically considers stand-alone legislation, including laws governing surveillance of U.S. citizens (such as the Foreign Intelligence Surveillance Act, known as "FISA"). On occasion, the Committee reviews intelligence aspects of treaties as part of the Senate's ratification process. Investigations and Reviews: The Committee conducts reviews of intelligence programs or events, ranging from routine and continuing study (the conduct of covert action programs and intelligence operations) to formal inquiries.
>
> Confirmations: The Committee considers and makes recommendations to the Senate for the President's nominees to serve in intelligence positions requiring the Senate's confirmation. Analysis: The Committee receives and reviews intelligence analysis on a broad range of topics to inform policy decisions.
>
> Daily Oversight: The Committee, through its staff, tracks the regular collection and analysis activities of the Intelligence Community, enabling the Committee to engage with the Intelligence Community early on if it becomes aware of an issue. The Committee's Audit and Oversight staff conducts longer-term oversight projects. [47].

Tradução livre:

> Audiências: O Comitê se reúne aproximadamente duas vezes por semana durante 1 1/2 a 2 horas, geralmente em sessões fechadas. A maioria das audiências envolve aparições de altos funcionários da Comunidade de Inteligência – chefes de agências, gerentes de programas seniores e analistas de inteligência seniores – que apresentam testemunho e respondem às perguntas dos senadores. Os tópicos das audiências incluem atividades da agência, programas de coleta de inteligência e análise de inteligência sobre uma região geográfica ou questão (por exemplo, estabilidade no Oriente Médio, programa nuclear do Irã, ameaças terroristas). O Comitê ocasionalmente

[9] O United States Senate Select Committee on Intelligence é muitas vezes referido apenas como Intelligence Committee

> se reúne em sessões abertas, como audiências anuais para receber testemunhos de inteligência sobre as ameaças à segurança nacional dos Estados Unidos e para o Comitê considerar os indicados do presidente para cargos de inteligência que exigem confirmação do Senado.
>
> Legislação: O Comitê elabora um projeto de lei anual de autorização de inteligência que autoriza os níveis de financiamento para atividades de inteligência (estes estabelecem limites para o financiamento de agências) e fornece disposições legislativas que limitam ou permitem a conduta de inteligência. O Comitê também considera periodicamente legislação autônoma, incluindo leis que regem a vigilância de cidadãos americanos (como o Foreign Intelligence Lei de Fiscalização, conhecida como "FISA"). Ocasionalmente, o Comitê revisa aspectos de inteligência de tratados como parte do processo de ratificação do Senado.
>
> Investigações e Revisões: O Comitê realiza revisões de programas ou eventos de inteligência, variando de estudos de rotina e contínuos (condução de programas de ação secreta e operações de inteligência) a investigações formais.
>
> Confirmações: O Comitê considera e faz recomendações ao Senado para os indicados pelo Presidente para servir em cargos de inteligência que requerem a confirmação do Senado.
>
> Análise: O Comitê recebe e revisa a análise de inteligência em uma ampla gama de tópicos para informar as decisões políticas.
>
> Supervisão diária: O Comitê, por meio de sua equipe, rastreia as atividades regulares de coleta e análise da Comunidade de Inteligência, permitindo que o Comitê se envolva com a Comunidade de Inteligência desde o início, caso tome conhecimento de um problema. A equipe de auditoria e supervisão do Comitê conduz projetos de supervisão de longo prazo.

À toda evidência, percebe-se uma supervisão, acompanhamento e envolvimento direto do *United States Senate Select Committee on Intelligence* (SSCI) com as atividades diárias e rotineiras de inteligência, além das estratégicas. O SSCI se reúne semanalmente com chefes das agências de inteligência, questionam conjunturas e analisam relatórios.

Anualmente, o Comitê autoriza dotações orçamentárias para as atividades de inteligência [48]. Em outra frente de atuação, opinam acerca das indicações do Presidente Americano para ocupação nas agências de cargos de inteligência.

Ainda no campo do legislativo, a Câmara dos Representantes[10] mantém o *The Permanent Select Committee on Intelligence* [49] com atribuições igualmente de supervisionar as agências de inteligência americanas.

Do ponto de vista de controle interno, isto é, realizado pelos próprios órgãos de inteligência e por entidades governamentais do Poder Executivo, é possível citar o Conselho Nacional de Segurança, o Conselho Consultivo de Inteligência do Presidente, o Conselho de Supervisão de Inteligência, o Conselho de Supervisão de Privacidade e Liberdades Civis, além da figura dos Inspetores Gerais, correspondente no Brasil aos Corregedores-Gerais dos órgãos, o Procurador Geral, que unifica nos Estados Unidos o correspondente ao Advogado-Geral da União e o Procurador-Geral da República do Brasil.

Como principal baliza para o exercício da inteligência pelas agências americanas, foi editada pelo Presidente Reagan, em 04/12/1981, a Ordem Executiva 12333[11] . Um ponto a se destacar nas diretrizes emanadas do Presidente da República são as técnicas de coleta:

[10] A Câmara dos Representantes nos Estados Unidos corresponde à Câmara dos Deputados Federais no Brasil.

[11] O texto original sofreu alterações das Ordens Executivas 13284 (2003), 13355 (2004) e 13470 (2008. A Ordem Executiva

> 2.4 Collection Techniques. Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes [50].

Em tradução livre:

> 2.4 Técnicas de Coleta. As agências dentro da Comunidade de Inteligência devem usar as técnicas de coleta menos intrusivas viáveis dentro dos Estados Unidos ou dirigidas contra pessoas dos Estados Unidos no exterior. As agências não estão autorizadas a usar técnicas como vigilância eletrônica, busca física não consentida, vigilância de correio, vigilância física ou dispositivos de monitoramento, a menos que estejam de acordo com os procedimentos estabelecidos pelo chefe da agência em questão e aprovados pelo Procurador-Geral. Tais procedimentos devem proteger os direitos constitucionais e outros direitos legais e limitar o uso de tais informações para fins governamentais legais.

Pelo que se depreende, a vigilância eletrônica deve seguir os procedimentos delineados em parâmetros estabelecidos pelo Chefe da respectiva agência de inteligência e com a aprovação do Procurador Geral.

No campo jurisdicional, adotou-se uma espécie de órgão especializado para examinar os pedidos oriundos do governo americano em relação a buscas físicas, vigilância eletrônica e outras medidas investigativas relativas à inteligência estrangeira. O *Foreign Intelligence Surveillance Court* foi criado em 1978 com a Lei de Vigilância de Inteligência Estrangeira. O Tribunal é composto por 11 juízes de tribunais distritais federais, que possuem mandato por 7 anos. Os questionamentos da sociedade civil e entidades privadas são submetidos ao Judiciário de maneira geral.

3.3 CANADÁ

No Canadá existem duas agências de inteligência: o Serviço Canadense de Inteligência de Segurança (CSIS) e o Serviço de Segurança de Comunicações Canadense (CSEC), esta última responsável pela coleta de sinais eletrônicos ou inteligência de sinais (SIGINT), o congênere canadense da NSA (Agência de Segurança Nacional americana). As duas agências têm cooperação acentuada com os serviços americanos, especialmente a CIA e a NSA, no escopo da Aliança dos Cinco Olhos (*Five Eyes*).

A Lei do Serviço de Inteligência de Segurança Canadense [3], com as alterações posteriores, Lei Anti-

12333 encontra similitude no Brasil com a Política Nacional de Inteligência e a Estratégia Nacional de Inteligência, ambas editadas por meio de Decreto n° 8793/2016 e Decreto s/n, de 15/12/2017.

terrorista de 2015[12] /C-51 e C59[13], dispõe que o Serviço pode coletar quaisquer dados que sejam de fontes abertas, relacionados a estrangeiros ou aprovados previamente pelo Ministro da Segurança Pública. Neste último universo se integram todos os dados que possam gerar resultados relevantes para o desempenho dos deveres e funções do Serviço definidas anualmente em documento pelo Ministro. Nesse aspecto, a competência ficou delineada no item 12 (1) da Lei:

> Collection, analysis and retention
>
> 12 (1) The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada
>
> Measures to reduce threats to the security of Canada 12.1 (1) If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat.
>
> Marginal note: Limits
>
> (2) The measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures, the reasonable availability of other means to reduce the threat and the reasonably foreseeable effects on third parties, including on their right to privacy.

Em tradução livre:

> Coleta, análise e retenção
>
> 12 (1) O Serviço deve coletar, por investigação ou de outra forma, na medida do estritamente necessário, e analisar e reter informações e inteligência a respeito de atividades que possam, por motivos razoáveis, ser suspeitas de constituir ameaças à segurança do Canadá e, em relação a isso, informará e aconselhará o Governo do Canadá.
>
> Medidas para reduzir as ameaças à segurança do Canadá 12.1 (1) Se houver motivos razoáveis para acreditar que uma determinada atividade constitui uma ameaça à segurança do Canadá, o Serviço poderá tomar medidas, dentro ou fora do Canadá, para reduzir a ameaça.
>
> Limites
>
> 12.1 (2) As medidas devem ser razoáveis e proporcionais às circunstâncias, tendo em conta a natureza da ameaça, a natureza das medidas, a disponibilidade razoável de outros meios para reduzir a ameaça e os efeitos razoavelmente previsíveis sobre terceiros, incluindo em seu direito à privacidade.

Com as alterações empreendidas pelo projeto C-59, aprovado em 21/06/2019, estabeleceu-se um regime voltado a disciplinar a coleta, retenção, consulta, gestão e exploração do conjunto de dados buscado pelo Serviço de Inteligência.

No Canadá o sistema jurídico é peculiar, se utiliza da *common law* em nove províncias e da *civil law*

[12] Após os ataques ao Parliament Hill e o assassinato do subtenente Patrice Vincent, foi aprovado o projeto C-51 que resultou na Lei Antiterrorista de 2015 no Canadá. A lei fez alterações na Lei do Serviço de Inteligência de Segurança Canadense e em outras normas. Encarada como uma ofensiva ao crescimento do grupo terrorista Estado Islâmico, a lei sofreu duras críticas e foi comparada ao USA Patriot Act, legislação americana que conferiu amplos poderes aos Estados Unidos para combater o terrorismo.

[13] O projeto de lei C59 teve como escopo equilibrar a previsão dos direitos e liberdades com a necessidade de garantir a segurança nacional

na província de Quebec. A Suprema Corte Canadense é integrada por 9 membros, sendo 6 juízes oriundos da *common law* e 3 da *civil law*.

Dois julgamentos da Suprema Corte do Canadá (SCC) merecem referência.

No caso Hassan Almrei, Harkat e Charkaoui vs Canada (*The Minister of Citizenship and Immigration*) [51], a Suprema Corte Canadense entendeu que o procedimento da Lei de Imigração e Refugiados de emissão das ordens de segurança de inadmissibilidade de ingresso em solo canadense e a detenção de Almrei e Harkat violaram a Carta Canadense de Direitos e Liberdades. Almei e Harkat foram presos em outubro de 2001 em virtude de suspeitas de envolvimento com grupos terroristas.

Em 2008, após a decisão da SCC, foram editados novos procedimentos para certificados de segurança na Lei de Imigração e Proteção de Refugiados. Reeditou-se, na sequência, uma nova ordem em face de Harkat, o que resultou em nova provocação à Corte Suprema. No caso Mohamed Harkat vs Canadá (*The Minister of Citizenship and Immigration and the Minister of Public Safety and Emergency Preparedness*) a SCC textualmente afirmou que não haveria dúvidas que tanto a segurança pública quanto a segurança nacional estariam entre as maiores preocupações do governo, mas que a garantia a um processo judicial justo era essencial. Nesse aspecto, seria imperioso alcançar um equilíbrio entre essas duas prioridades democráticas. Com essa toada, instou que o Parlamento Canadense atuasse para produzir uma legislação que harmonizasse e equilibrasse constitucionalmente os dois interesses da sociedade.

O que se discutia no novo processo Mohamed Harkat vs Canadá [52] é se para resguardar a segurança nacional poderia ser restringido o acesso do acusado ao seu defensor, a documentos constantes no processo acusatório e às testemunhas. A Corte Suprema Canadense entendeu que as limitações eram excessivamente amplas e ofendiam o s.7 (*Toda pessoa tem direito à vida, à liberdade e à segurança da pessoa e o direito de não ser privada delas, exceto de acordo com os princípios fundamentais da justiça*) da Carta Canadense de Direitos e Liberdades, Parte I do Ato Constitucional de 1982 [53].

Sobre a geolocalização de pessoas, o Tribunal Superior de Justiça de Ontário (CANADÁ, 2016 [54] foi instado por duas empresas telefônicas, a *Rogers Communications* e a *Telus Communications*, acerca de um pedido da polícia que buscava informações de metadados de usuários. Com o intuito de investigar uma série de assaltos na região de Brampton, a polícia solicitou às operadoras informações de usuários que estariam utilizando as torres (ERBs) na região, assim como dados de origem e destinação das chamadas, endereços dos usuários e informações bancárias.

Na decisão, o Tribunal Superior de Justiça de Ontário considerou que os usuários tem uma expectativa razoável de privacidade em seus registros telefônicos. Mas a importância dessa decisão passa pelas orientações que foram firmadas pelo Ministro Sproat para as hipóteses de pedidos semelhantes (*tower dump*) realizados pela polícia:

> "The police should include the following in the information to obtain a production order: a statement or explanation that demonstrates that the officer seeking the order is aware of the principles of incrementalism and minimal intrusion and has tailored the requested order with that

> in mind; an explanation as to why all of the named locations or cell towers, and all of the requested dates and time parameters, are relevant to the investigation; an explanation as to why all of the types of records sought are relevant; any other details or parameters which might permit the target of the production order to conduct a narrower search and produce fewer records; and a request for a report based on specified data instead of a request for the underlying data itself. If there is a request for the underlying data, there should be a justification for the request. The police should also include confirmation that the types and amounts of data that are requested can be meaningfully reviewed. Issuing justices should generally insist upon the police providing the information, [page694] confirmations and explanations outlined in those guidelines."

Em suma, o Tribunal Superior de Justiça de Ontário estabelece parâmetros a partir da ideia de proporcionalidade e relevância das informações, com a mínima intrusividade da ação estatal na esfera de privacidade dos usuários. De acordo com a Corte, o pedido deve demonstrar porque os registros de torres específicas em determinado período de tempo (vinculação geográfica e temporal) são capazes de auxiliar na investigação. O objetivo claro é reduzir a extração de metadados que sejam desnecessários para a finalidade policial.

De acordo com a Lei, as medidas que limitem um direito ou liberdade, garantidos pela Carta Canadense de Direitos e Liberdades, devem ser deferidas por um juiz, que expedirá um mandado para essa finalidade com prazo e escopo específico.

Além do controle judicial, a Lei do Serviço de Inteligência de Segurança Canadense estabeleceu a apresentação de um relatório anual de atividades ao Parlamento, o acompanhamento do Serviço por uma Agência de Revisão e, em casos de indícios de ilegalidade na atuação, a comunicação dos fatos ao Procurador-Geral do Canadá.

3.4 AUSTRÁLIA

Na Austrália, a comunidade de inteligência é composta pelas agências: *Australian Security Intelligence Organization* (ASIO), *Australian Secret Intelligence Service* (ASIS), *Australian Signals Directorate* (ASD) e *Australian Geospatial Intelligence Organization* (AGO), *Office of National Assessments* (ONA) e *Defense Intelligence Organization* (DIO).

A principal delas, a *Australian Security Intelligence Organization* (ASIO), com funções de coleta e análise[14], tem suas competências descritas no *Australian Security Intelligence Organization Act*, de 1979, *Intelligence Services Act* 2001 e *Telecommunications* (*Interception and Access*) *Act* 1979 [4]. De maneira geral, as competências descritas na seção 17 da Lei da ASIO não destoam de outras agências de inteligência. São atribuições da ASIO coletar e buscar informações relevantes para a segurança nacional e assessorar as autoridades em relação a esses assuntos.

Entre os poderes especiais conferidos à ASIO encontram-se a instalação e o monitoramento de dispo-

[14]Na Austrália, a regra é que cada agência fique responsável pelo processo de coleta ou de análise.

sitivos de vigilância, o monitoramento de telecomunicações e o acesso remoto a computadores, atividades que podem ser realizadas com a obtenção de um mandado, submetido à aprovação do Procurador Geral (TIA, 1979). Os registros de chamadas telefônicas e a titularidade das linhas, por sua vez, podem ser acessados diretamente junto às empresas de telefonia pelos serviços de inteligência[15].

A ASIO é comandada pelo Diretor-Geral de Segurança e subordinada ao Ministro do Interior da Austrália. Entre os elementos de controle e supervisão, é possível citar a apresentação de um relatório anual perante o Parlamento Australiano, a fiscalização do Inspetor-Geral de Inteligência e Segurança (IGIS), a supervisão dos poderes especiais pelo Procurador-Geral e a avaliação da administração e despesas pela Comissão Parlamentar de Inteligência e Segurança.

Em 2022, o Gabinete do Comissário de Informação Australiano (OAIC), órgão regulador de privacidade na Austrália, apresentou um modelo de reforma e unificação da estrutura legislativa de vigilância eletrônica. De acordo com o OIAC, as agências de inteligência australianas ficaram imunes à lei de privacidade de 1988, sendo necessária uma regulação que alcançasse os seis serviços, mas garantindo os poderes especiais da ASIO e das agências para proteção da segurança nacional [56].

3.5 NOVA ZELÂNDIA

Na Nova Zelândia, as duas principais agências de inteligência são o *Government Communications Security Bureau* (GCSB), especializado em inteligência de sinais e garantia de informações e atividades de segurança cibernética, e o *New Zealand Security Intelligence Service* (NZSIS), especializado em atividades de inteligência humana.

Em 2017 foi aprovada a Lei de Inteligência e Segurança, unificando a legislação que regulamenta a atividade dos dois serviços de inteligência [5]. A lei trouxe em seu bojo os objetivos, as funções e obrigações dos serviços de inteligência, a possibilidade de utilização do que denominou de *Assumed identities*[16], criação e manutenção de uma pessoa jurídica com o objetivo de expandir a capacidade das agências e manter a atividade em sigilo, as hipóteses, requisitos e competência de autorizações de operações ilegais, dentre outras questões. Enquanto outros países trilharam o caminho de apenas mencionar objetivos e finalidades dos serviços de inteligência, ficando, implicitamente, o mandato para atuar com maior ou menor amplitude de acordo com as autorizações conferidas no caso em concreto pela autoridade competente, a Nova Zelândia optou por regulamentar, detalhadamente, os aspectos que envolvem o *Government Communications Security Bureau* e o *New Zealand Security Intelligence Service*.

De acordo com a legislação, os objetivos das agências de inteligência são contribuir para a proteção da segurança nacional, as relações internacionais e o bem estar da Nova Zelândia. Para atingir esses objetivos,

[15] Embora não aplicável aos serviços de inteligência, se circunscrevendo aos órgãos de segurança pública, é interessante registrar a edição, em 2004, da Surveillance Devices Act, ou, em tradução livre, a Lei de Vigilância de Dispositivos [55].

[16] As Assumed identities é a possibilidade de utilização de uma identidade falsa pelo agente de inteligência visando preservar e proteger a sua identidade real, assim como permitir que a atividade desenvolvida seja sigilosa.

as agências se utilizam das funções de coletar e analisar informações, o que pode exigir, se caracterizar uma atividade ilegal, uma autorização que se instrumentaliza por um mandado de inteligência do tipo 1 ou 2. As autorizações elaboradas pelo Diretor-Geral e deferidas pelo Ministro, autoridade hierárquica da agência, ou o Comissário-Chefe de Autorizações de Mandado de Inteligência se revestem de uma exclusão de ilicitude para as atividades desenvolvidas pela agência de inteligência sob aquele manto:

> Part 4
>
> Authorisations
>
> 46 - Purpose of Part
>
> The purpose of this Part is to establish an authorisation regime for the intelligence and security agencies that—
>
> (a)
>
> authorises as lawful the carrying out of an activity by an intelligence and security agency that would otherwise be unlawful, if certain criteria are satisfied; and
>
> (b)
>
> confers on an intelligence and security agency specified powers for the purpose of giving effect to an authorisation.

As atividades que podem ser autorizadas pelas autoridades competentes estão, exemplificativamente, dispostas na Lei:

> Authorised activities and powers
>
> 67Authorised activities
>
> (1) An intelligence warrant may authorise the carrying out of 1 or more of the following activities that would otherwise be unlawful:
>
> (a) conducting surveillance in respect of 1 or more—
>
> (i) persons or classes of persons:
>
> (ii) places or classes of places:
>
> (iii) things or classes of things:
>
> (b) intercepting any private communications or classes of private communications:
>
> (c) searching 1 or more—
>
> (i) places or classes of places:
>
> (ii) things or classes of things:
>
> (d) seizing—
>
> (i) 1 or more communications or classes of communications:
>
> (ii) information or 1 or more classes of information:
>
> (iii) 1 or more things or classes of things:
>
> (e) requesting the government of, or an entity in, another jurisdiction to carry out an activity that, if carried out by an intelligence and security agency, would be an unlawful activity:
>
> (f) taking any action to protect a covert collection capability:
>
> (g) any human intelligence activity to be carried out for the purpose of collecting intelligence, not being an activity that—
>
> (i) involves the use or threat of violence against a person; or

(ii) perverts, or attempts to pervert, the course of justice.

(2) An intelligence warrant issued to the Director-General of the Government Communications Security Bureau may, in addition to any of the activities specified in subsection (1), authorise the doing of any other act that is necessary or desirable to protect the security and integrity of communications and information infrastructures of importance to the Government of New Zealand (including identifying and responding to threats or potential threats to those communications or infrastructures) without the consent of any person.

Antes da edição da Lei de Inteligência e Segurança, de 2017, dois julgamentos da Suprema Corte da Nova Zelândia podem ser citados. No caso Hamed & Ors v. R [57] se examinou a possibilidade da polícia ingressar em ambiente privado e inserir mecanismo de vigilância sem previsão legal. A Suprema Corte entendeu que a polícia não obteve uma autorização específica para a investigação, não sendo suficiente o mandado que havia sido requerido para a investigação contínua de vigilância em face dos acusados, violando o *Bill of Rights Act* 1990. Apesar disso, ponderando os direitos dos acusados e os crimes cometidos, a Suprema Corte admitiu as provas produzidas pela vigilância em face de 4 acusados, afastando-as em relação aos demais. Exarada em 2011, a decisão da Suprema Corte revela a sua preocupação acerca do direito à privacidade em contraponto ao interesse da sociedade na elucidação de crimes graves, embora, em última instância tenha sobressaído, em juízo de ponderação, o segundo.

Um outro julgamento bem interessante, a respeito do juízo de ponderação envolvendo segurança nacional, é o caso Zaoui v. Procurador Geral [58]. A questão de fundo concernia na possibilidade de um estrangeiro, com condição de refugiado concedida pelo governo neozelandês, ser deportado para o país de origem. Zaoui ingressou na Nova Zelândia e solicitou refúgio, mas foi considerado um risco à segurança nacional pelo *New Zealand Security Intelligence Service* (NZSIS). No curso da análise da Apelação ao Inspetor-Geral de Inteligência, que visava reverter a decisão do (NZSIS), foi concedido o status de refugiado a Zaoui. A Suprema Corte se deparou com o art. 33, §1° do Estatuto de Refugiados que prevê a impossibilidade de deportação ou expulsão de refugiados nas hipóteses de risco à vida ou liberdade no país de origem. De outro lado, o Inspetor-Geral de Inteligência, confirmando a manifestação da NZSIS, considerou o Sr. Zaoui como um risco à Nova Zelândia. Diante desse quadro, entendeu a Corte Maior que não cabia ao Inspetor-Geral perquirir eventual risco do refugiado em caso de expulsão ou deportação, devendo se ater às questões de segurança nacional para a aplicação do instituto. Ademais, levou em consideração que a própria Convenção das Nações Unidas acolhe a hipótese de expulsão do refugiado que seja considerado um perigo à situação do país que o acolheu. Em síntese, prevaleceu o ato e o entendimento do NZSIS, pela deportação de Zaoui em virtude do risco à segurança nacional.

A supervisão externa do *Government Communications Security Bureau* e do *New Zealand Security Intelligence Service* é realizada pelo Comitê de Inteligência e Segurança, que realiza o escrutínio parlamentar das políticas, administração e despesas das agências de inteligência e segurança, e pelo Inspetor-Geral de Inteligência e Segurança, a quem compete conduzir uma avaliação acerca das atividades finalísticas dos serviços em referência, à exemplo da emissão das autorizações. Na esfera interna, as agências devem produzir um relatório anual e submetê-lo aos respectivos Ministros.

3.6 ALEMANHA

Na Alemanha há dois serviços de inteligência que se destacam, o *Bundesnachrichtendienst* (BND), Serviço Federal de Inteligência, e o *Bundesamt für Verfassungsschutz* (BFV), Escritório de Proteção à Constituição.

Fundado em 1956, o BND se concentra na inteligência estrangeira, política, econômica e militar [59]. Os tópicos de atuação são ataques cibernéticos originados no exterior, investigação de redes de terroristas no exterior, situação política, econômica, militar e de conflito em países, crime organizado e proliferação indesejada de armas de destruição em massa no mundo.

O BFV, por sua vez, tem como foco de análise e acompanhamento o extremismo de direita, extremismo de esquerda, cidadãos do Reich e autogovernadores, islamismo e terrorismo islâmico, extremismo relacionado ao exterior, contra-inteligência e proliferação, proteção de segredos e sabotagem, defesa cibernética, proteção econômica e científica e deslegitimação do Estado.

O BND *Act* [6] confere poderes (§2°) ao Serviço Federal de Inteligência para coletar, processar e usar as informações necessárias sobre operações no exterior que sejam de importância para a segurança da Alemanha, inclusive solicitando informações de empresas de telecomunicações (§2°b).

Ao final de 2017, as entidades *Reporters Without Borders* (Repórteres Sem Fronteiras - RSF) e a *Society for Civil Liberties*, uma ONG de direitos civis, ingressaram com uma reclamação no Tribunal Constitucional Federal Alemão (*Bundesverfassungsgericht*) questionando a vigilância em massa do BND. Em termos gerais, questionava-se as autorizações do Serviço Federal de Inteligência para acesso às telecomunicações estrangeiro-estrangeiro, o compartilhamento irrestrito dos dados captados com órgãos nacionais e internacionais e a cooperação com órgãos de inteligência de outros países nesse contexto. Especificamente, a ação proposta apontava que a vigilância era demasiadamente ampla e atingia, inclusive, o sigilo da fonte dos profissionais de mídia. Não havia proteção das comunicações das fontes e a imprensa[17]. Os dispositivos questionados da Lei do Serviço Federal de Inteligência decorreram de alterações promovidas pela Lei de Adaptação do Regulamento Geral de Proteção de Dados (Diretiva 679/2016 da União Europeia) de 30 de junho de 2017.

Em maio de 2020, o Tribunal Constitucional Federal Alemão [60] decidiu pela inconstitucionalidade de alguns dispositivos da lei, optando, no entanto, por manter a validade da norma, fixando o prazo de 31 de dezembro de 2021 para que o Legislativo promovesse alterações na lei a partir das premissas estabelecidas na decisão. Reconheceu o Tribunal que a retirada imediata da Lei do mundo jurídico removeria a base para a proteção de bens primordiais. Assim, exercendo uma ponderação com os direitos fundamentais afetados, optou por não realizar uma suspensão abrupta da norma. No dizer do Tribunal, *é mais aceitável a manutenção temporária das disposições inconstitucionais do que a sua eliminação até que seja previsível uma nova regulamentação*.

[17] Essa ação foi motivada pela denúncia do colaborador da NSA, Edward Snowden, da existência de um sistema de coleta em massa de dados. Na sequência se comprovaram as ligações entre o BND e a NSA.

O Tribunal Constitucional Federal Alemão apontou alguns parâmetros para revisão da norma:

1. que a vinculação e observância pelo Estado dos direitos fundamentais não se limita ao território nacional alemão;
2. que a proteção aos direitos fundamentais pode receber tratamento diverso na Alemanha e no exterior;
3. há que se buscar um equilíbrio entre a manutenção da segurança e os direitos fundamentais;
4. a Constituição não se opõe ao instrumento da vigilância estratégica e da cooperação conexa com outros serviços de inteligência;
5. a necessidade de regulação dos poderes do órgão de inteligência não significa que a atividade não será desempenhada em sigilo;
6. a vigilância estratégica das telecomunicações serve ao fim legítimo de ajudar a identificar perigos em um estágio inicial, salvaguardando a capacidade de ação do Estado e fornecendo informações sobre política externa e segurança, e é adequada e necessária para a sua realização de acordo com o princípio da proporcionalidade;
7. os detalhes técnicos e práticos de todo o processo de coleta e avaliação, a cooperação e a transmissão de dados são regulados por regulamentos de serviço não público;
8. deve-se especificar com suficiente precisão as finalidades para que a vigilância de telecomunicações e os conhecimentos adquiridos no processo possam ser utilizados;
9. os órgãos de controle devem ter todos os poderes necessários para um controle efetivo perante o Serviço Federal de Inteligência;

Primeiro ponto que o Tribunal ultrapassou foi a questão da extraterritorialidade da Constituição Alemã. Mais do que o aspecto territorial, a Corte firmou posicionamento pela inviolabilidade absoluta da dignidade da pessoa humana em decorrência dos preceitos constitucionais. Reafirmou-se, no entanto, na linha da jurisprudência da Corte, notadamente no julgamento do caso Census Act, que, individualmente, o cidadão deveria tolerar restrições decorrentes da necessidade de proteção do interesse público. Sem embargo, o Tribunal estabeleceu que é dever do Estado criar uma regulamentação sobre o assunto. A coleta, de acordo com o Tribunal, deve observar ao princípio constitucional da legalidade (*Gesetzmäßigkeit der Verwaltung*). Na grande maioria dos países europeus, tais disposições regulamentadoras não existem, e o poder das agências de inteligência estrangeiras para conduzir programas de vigilância deriva de poderes gerais [61].

A decisão se mostra bem interessante para a presente pesquisa, considerando que o Brasil sorve da experiência de países europeus que adotam a *civil law*, como Alemanha, França, Portugal e Itália. Ademais, o Tribunal Constitucional Federal Alemão faz uma análise bastante minuciosa da importância do processo de coleta versus a inafastável garantia de preservação dos direitos fundamentais, dentre eles, a privacidade. Saliente-se, por oportuno, que a lei expressamente consigna na sua seção 68 a restrição aos direitos fundamentais ao sigilo das cartas, correios e telecomunicações (artigo 10.º da Lei Básica) e o direito fundamental à inviolabilidade do domicílio (artigo 13, da Lei Básica).

A decisão do *Bundesverfassungsgericht* motivou a aprovação, em dezembro de 2020, pelo *Bundestag* (Parlamento alemão) do projeto de alteração da lei submetido pelo Governo. Após críticas, principalmente da RSF, a lei sofreu nova alteração, em julho de 2021. Certo é que a lei, em seu capítulo 21 (§21), vedou a possibilidade de coleta de dados pessoais com a finalidade de obter informações de uma relação confidencial[18].

No campo da supervisão ou *oversight*, o próprio BND *Act* estabeleceu mecanismos de controle da atividade de coleta, ou monitoramento estratégico das telecomunicações, por meio do Conselho de Controle Independente, composto por 6 membros nomeados para um mandato de 12 anos, sem direito à recondução, dentre magistrados do Tribunal de Justiça Federal ou Tribunal Administrativo Federal. Para além do Conselho de Controle Independente, criado por ocasião da reforma da lei do BND em 2021, três outros órgãos tem a atribuição de exercer o controle dos órgãos de inteligência na Alemanha:

1. o Painel de Supervisão Parlamentar, responsável por fiscalizar as atividades de inteligência de maneira geral, abarcando o BND e o BFV;
2. a Comissão do G10 analisa a interferência dos serviços de inteligência no sigilo das telecomunicações; e
3. o Comissário Federal para Proteção de Dados e Liberdade de Informação cuida, por sua vez, na atuação dos órgãos de inteligência em relação ao direito fundamental de proteção de dados.

3.7 FRANÇA

Na França, a Coordenação Nacional de Inteligência e Combate ao Terrorismo, criada em 2017, coordena a comunidade de inteligência composta por 6 entidades [62]:

1. a Diretoria Geral da Segurança Externa – DGSE (*Direction Générale de la Sécurité Extérieure*);
2. a Diretoria Geral de Segurança Interna – DGSI (*Direction Générale de la Sécurité Intérieure*);
3. a Diretoria de Inteligência e Segurança de Defesa - DRSD (*Direction du Renseignement et de la Sécurité de la Défense*);
4. a Diretoria de Inteligência Militar - DRM (*Direction du Renseignement Militaire*);
5. a Diretoria Nacional de Informações e Investigações Aduaneiras – DNRED (*Direction Nationale du Renseignement et des Enquêtes Douanières*); e
6. a Unidade de Inteligência Financeira – TRACFIN (*Cellule du Renseignement Financier*)

A Diretoria Geral de Segurança Interna é responsável pelas seguintes tarefas em âmbito interno [63]:

[18] Considerou-se protegida por sigilo a relação com clérigos, advogados e jornalistas.

1. combate ao terrorismo e extremismo violento;
2. detecção e prevenção de ameaças de interferência estrangeira sobre atores econômicos estratégicos franceses;
3. atuação como polícia judiciária especializada nas hipóteses de violação de sigilo que envolva defesa nacional e terrorismo;
4. contra-inteligência;
5. defesa cibernética; e
6. combate a proliferação de armas.

A atividade de inteligência desenvolvida pela Diretoria Geral de Segurança Interna é supervisionada por instâncias internas (controle hierárquico) e por meio do Ministério de Interior.

A Diretoria Geral da Segurança Externa, ligada ao Ministério da Defesa concentra sua atuação nos seguintes temas com enfoque externo [64]:

1. combate ao terrorismo;
2. proliferação de armas de destruição em massa;
3. geopolítica internacional;
4. contra-inteligência (interferência externa e espionagem); e
5. defesa cibernética.

Assim como no Brasil, a França fixou na Estratégia Nacional de Inteligência [65] os objetivos a serem perseguidos e as questões prioritárias, decorrentes da avaliação das ameaças e das oportunidades de ação. Em julho de 2019, o documento apontou quatro questões: ameaça terrorista, antecipar crises e os riscos de ruptura, defesa e promoção dos interesses econômicos e industriais da França e a luta contra ameaças transversais, como ameaça cibernética, interferência, espionagem, crime organizado e proliferação de armas.

Desde 2015, o Código de Segurança Interna, lei que rege a atividade de inteligência e, especificamente, a coleta de dados e informações, estabeleceu a necessidade de autorização do primeiro-ministro para utilização de técnicas de inteligência como a interceptação de segurança, geolocalização, recolhimento de dados computacionais e gravação de sons e imagens. A autorização somente pode ser emitida por um período de tempo determinado, após a avaliação e concordância de uma autoridade administrativa independente, a Comissão Nacional de Controle das Técnicas de Inteligência [7], e apenas para determinados fins estabelecidos exaustivamente pela lei:

1. defesa nacional e integridade territorial;

2. prevenção de interferência externa, defesa e promoção dos interesses de política externa, execução de compromissos europeus e internacionais da França;

3. defesa e promoção de grandes interesses econômicos, industriais e científicos da França;

4. prevenção do terrorismo, do crime organizado e da proliferação de armas de destruição em massa; e

5. prevenção de ataques à forma republicana de instituições, violência coletiva susceptível de prejudicar gravemente a paz pública.

Já há, nesse caso, pode-se afirmar, um juízo de ponderação do legislador apontando situações, em tese, que permitem ou ensejam a utilização de técnicas de inteligência que afetam o direito à privacidade.

Especificamente sobre o uso da geolocalização estabeleceu:

> Art. L. 851-5.-Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisée l'utilisation d'un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet. Si la mise en œuvre de cette technique nécessite l'introduction dans un véhicule ou dans un lieu privé, cette mesure s'effectue selon les modalités définies à l'article L. 853-3.

em tradução livre:

> Arte. L. 851-5.-Sob as condições previstas no Capítulo I do Título II deste livro, pode ser autorizada a utilização de um dispositivo técnico que permita a localização em tempo real de uma pessoa, um veículo ou um objeto. "Se a implementação desta técnica exigir a introdução em veículo ou em local privado, esta medição é efetuada de acordo com os métodos definidos no artigo L. 853-3.

As condições referidas no capítulo I, do Título II são *ex vi legis*:

> Titre II
>
> DE LA PROCÉDURE APPLICABLE AUX TECHNIQUES DE RECUEIL DE RENSEIGNEMENT SOUMISES À AUTORISATION
>
> Chapitre Ier
>
> De l'autorisation de mise en œuvre
>
> Art. L. 821-1.-La mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées au titre V du présent livre est soumise à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement.
>
> Ces techniques ne peuvent être mises en œuvre que par des agents individuellement désignés et habilités.

Em tradução livre:

> Título II
>
> "PROCEDIMENTO APLICÁVEL ÀS TÉCNICAS DE COBRANÇA DE INTELIGÊNCIA SUJEITO A AUTORIZAÇÃO
>
> “Capítulo I
>
> “Autorização para implementar
>
> "Arte. L. 821-1.- A implementação em território nacional das técnicas de recolha de informações referidas no Título V deste livro está sujeita a autorização prévia do Primeiro-Ministro, emitida após parecer da Comissão Nacional de Controlo das Técnicas de Inteligência .
>
> “Essas técnicas só podem ser implementadas por agentes designados e autorizados individualmente.

A Comissão Nacional de Controle das Técnicas de Inteligência realiza, igualmente, um controle concomitante e *a posteriori* do uso das técnicas de inteligência. A Comissão é composta por nove membros, sendo dois deputados e dois senadores, com períodos de atuação que coincidem com seus mandatos na Assembleia Geral e no Senado, dois membros do Conselho de Estado, dois magistrados do Tribunal de Cassação e um membro com conhecimentos de comunicações eletrônicas, designado pelo Presidente da Autoridade Reguladora das Comunicações Eletrônicas e Postais. O mandato dos membros, com exceção dos parlamentares, é de seis anos.

Além do controle das técnicas, há um órgão administrativo específico, criado em julho de 2014, responsável pela inspeção dos serviços de inteligência, que pode ser provocado diretamente pelo primeiro ministro francês, o ISR (*l'inspection des Services de Renseignement*) [66].

No campo legislativo, a Delegação Parlamentar de Inteligência (*Délégation Parlementaire au Renseignement* - DPR), criada em 2007, que representa o Senado e a Assembleia Nacional, tem por escopo fiscalizar a atividade fim de inteligência, sendo-lhe conferida, inclusive, a possibilidade de convocar o Diretor Geral de Segurança Interna para prestar esclarecimentos [67]. A Comissão Especial de Verificação de Fundos tem por função o controle das contas dos órgãos de inteligência.

Sob a ótica judicial, algumas questões foram submetidas ao Conselho Constitucional[19].

Em 2015, o Conselho Constitucional analisou, por meio da ação n° 2015-713 DC, e considerou constitucionais, dentre outros, os dispositivos L. 851-4, L. 851-5 e L. 851-6 do Código de Segurança Interna. Tais dispositivos se referem à possibilidade de utilização da geolocalização como técnica de inteligência. *In verbis*:

> 4. DROITS ET LIBERTÉS. 4.5. DROIT AU RESPECT DE LA VIE PRIVÉE (voir également ci-dessous Droits des étrangers et droit d'asile, Liberté individuelle et Liberté personnelle) 4.5.6. Géolocalisation
>
> L'article L. 851-4 du code de la sécurité intérieure autorise l'autorité administrative à requérir des opérateurs la transmission en temps réel des données techniques relatives à la localisation des

[19] O Conselho Constitucional é encarregado do controle constitucional e se caracteriza como a mais alta autoridade constitucional na França, é independente dos demais poderes, inclusive do Poder Judiciário francês. Na França há duas Supremas Cortes, a Corte de Cassação e o Conselho de Estado, em virtude da dualidade de jurisdição, judicial e administrativa, e um órgão especializado, de controle de constitucionalidade, o Conselho Constitucional. Diferente do modelo austríaco de Hans Kelsen, o modelo francês adota uma espécie singular de terceira via para o exame concentrado de constitucionalidade das leis.

équipements terminaux utilisés mentionnés à l'article L. 851-1 et selon l'article L. 851-5, l'autorité administrative peut utiliser un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet et l'article L. 851-6 prévoit la possibilité pour cette même autorité de recueillir, au moyen d'un appareil ou d'un dispositif permettant d'intercepter, sans le consentement de leur auteur, des paroles ou des correspondances émises, transmises ou reçues par la voie électronique ou d'accéder à des données informatiques les données relatives à la localisation des équipements terminaux utilisés.

Ces techniques de recueil de renseignement s'exercent, sauf disposition spécifique, dans les conditions prévues au chapitre Ier du titre II du code de la sécurité intérieure : elles sont autorisées par le Premier ministre, sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur ou des ministres chargés de l'économie, du budget ou des douanes, après avis préalable de la commission nationale de contrôle des techniques de renseignement et elles ne peuvent être mises en œuvre que par des agents individuellement désignés et habilités ; elles sont réalisées sous le contrôle de la commission nationale de contrôle des techniques de renseignement dont la composition et l'organisation sont définies aux articles L. 831-1 à L. 832-5 dans des conditions qui assurent son indépendance et dont les missions sont définies aux articles L. 833-1 à L. 833-11 dans des conditions qui assurent l'effectivité de son contrôle ; conformément aux dispositions de l'article L. 841-1, le Conseil d'État peut être saisi par toute personne souhaitant vérifier qu'aucune technique de recueil de renseignement n'est irrégulièrement mise en œuvre à son égard ou par la commission nationale de contrôle des techniques de renseignement ; en application des dispositions de l'article L. 871-6, les opérations matérielles nécessaires à la mise en place des techniques mentionnés à l'article L. 851-4 ne peuvent être exécutées, dans leurs réseaux respectifs, que par des agents qualifiés des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou des exploitants de réseaux ou fournisseurs de services de télécommunications.

Par ailleurs, ces tehniques sont mises en œuvre pour les finalités énumérées à l'article L. 811-3; lorsque la mise en œuvre de la technique prévue à l'article L. 851-5 impose l'introduction dans un véhicule ou dans un lieu privé, cette mesure s'effectue selon les modalités définies à l'article L. 853-3; l'autorisation d'utilisation de la technique prévue à l'article L. 851-6 est délivrée pour une durée de deux mois renouvelable dans les mêmes conditions de durée ; les appareils ou dispositifs utilisés dans le cadre de cette dernière technique font l'objet d'une inscription dans un registre spécial tenu à la disposition de la commission nationale de contrôle des techniques de renseignement; le nombre maximal de ces appareils ou dispositifs pouvant être utilisés simultanément est arrêté par le Premier ministre, après avis de cette commission ; les informations ou documents recueillis par ces appareils ou dispositifs doivent être détruits dès qu'il apparaît qu'ils ne sont pas en rapport avec l'autorisation de mise en œuvre et, en tout état de cause, dans un délai maximal de quatre-vingt-dix jours à compter de leur recueil. Dans ces conditions, les dispositions des articles L. 851-4, L. 851-5 et L. 851-6 du code de la sécurité intérieure ne portent pas une atteinte manifestement disproportionnée au droit au respect de la vie privée.

(2015-713 DC, 23 juillet 2015, cons. 51, 61, 63, JORF n°0171 du 26 juillet 2015 page 12751, texte n° 4)

Em tradução livre:

4. DIREITOS E LIBERDADES. 4.5. DIREITO AO RESPEITO À PRIVACIDADE. 4.5.6. Geolocalização.

O artigo L. 851-4 do Código de Segurança Interna autoriza a autoridade administrativa a exigir que os operadores transmitam em tempo real dados técnicos relativos à localização dos equipamentos terminais utilizados mencionados no artigo L. 851-1 e de acordo com o artigo L. 851-5; a autoridade administrativa pode utilizar dispositivo técnico que permita a localização em tempo real de uma pessoa, veículo ou objeto e o artigo L. 851-6 prevê a possibilidade de esta mesma autoridade recolher, por meio de dispositivo ou dispositivo que permita interceptar, sem o consentimento de seu autor, palavras ou correspondências emitidas, transmitidas ou recebidas por meio eletrônico ou acessar dados informáticos relativos à localização do equipamento terminal utilizado.

Essas técnicas de coleta de informações são exercidas, salvo disposição específica, nas condições previstas no Capítulo do Título II do Código de Segurança Interna: são autorizados pelo

> Primeiro-Ministro, a pedido escrito e fundamentado do Ministro da Defesa, do Ministro do Interior ou dos ministros responsáveis pela economia, orçamento ou alfândegas, após prévio parecer da comissão nacional de controle de técnicas de inteligência e só podem ser implementadas por agentes individualmente designados e autorizados; são realizados sob o controle da comissão nacional para o controle das técnicas de inteligência cuja composição e organização são definidas nos artigos L. 831-1 a L. 832-5 em condições que garantam a sua independência e cujas missões são definidas nos artigos L 833-1 a L. 833-11 em condições que assegurem a eficácia de seu controle; de acordo com o disposto no artigo L. 841-1, o Conselho de Estado pode ser instado por qualquer pessoa que pretenda verificar se nenhuma técnica de coleta de informações foi implementada irregularmente a seu respeito ou pela comissão nacional de controle de técnicas de inteligência; nos termos do disposto no artigo L. 871-6, as operações materiais necessárias à implementação das técnicas referidas no artigo L. 851-4 só podem ser realizadas, nas respetivas redes, por serviços ou entidades de agentes qualificados colocados sob a alçada de autoridade ou supervisão do Ministro responsável pelas comunicações eletrônicas ou operadores de rede ou prestadores de serviços de telecomunicações.
>
> Além disso, essas técnicas são implementadas para os fins listados no Artigo L. 811-3;
>
> quando a aplicação da técnica prevista no artigo L. 851-5 exigir a introdução num veículo ou em local privado, esta ação é efetuada de acordo com os procedimentos definidos no artigo L. 853-3;
>
> a autorização de utilização da técnica prevista no artigo L. 851-6 é emitida por um período de dois meses, renovável nas mesmas condições de duração;
>
> os dispositivos utilizados no âmbito desta última técnica são objeto de registro especial mantido à disposição da comissão nacional de controle das técnicas de inteligência;
>
> o número máximo destes dispositivos que podem ser utilizados em simultâneo é fixado pelo Primeiro-Ministro, após consulta a esta comissão;
>
> as informações ou documentos recolhidos por esses dispositivos devem ser destruídos logo que se verifique que não estão relacionados com a autorização de implementação e, em qualquer caso, no prazo máximo de noventa dias a contar da sua coleta. Nestas condições, as disposições dos artigos L. 851-4, L. 851-5 e L. 851-6 do Código de Segurança Interna não constituem uma violação manifestamente desproporcional do direito ao respeito da vida privada.
>
> (2015-713 DC , 23 de julho de 2015, cons. 51 , 61 , 63 , JORF n° 0171 de 26 de julho de 2015 página 12751, texto n° 4)

Do Inteiro Teor da decisão destaca-se raciocínio plenamente aplicável às atividades de inteligência em qualquer país:

> 9. Considérant que le recueil de renseignement au moyen des techniques définies au titre V du livre VIII du code de la sécurité intérieure par les services spécialisés de renseignement pour l'exercice de leurs missions respectives relève de la seule police administrative ; qu'il ne peut donc avoir d'autre but que de préserver l'ordre public et de prévenir les infractions; qu'il ne peut être mis en œuvre pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs;

Em tradução livre:

> 9. Considerando que a coleta de informações com recurso às técnicas definidas no Título V do Livro VIII do Código de Segurança Interna pelos serviços especializados de informações para o exercício das respectivas missões é da exclusiva responsabilidade da polícia administrativa; que, portanto, não pode ter outro propósito senão preservar a ordem pública e prevenir delitos; que não pode ser utilizado para detectar infracções ao direito penal, recolher provas ou encontrar os autores;

Em outros termos, o que afirmou o Conselho Constitucional foi que a coleta da geolocalização realizada pelos serviços de inteligência franceses não pode ser utilizada para a persecução penal, ou seja, para investigações e processos de natureza criminal, que, ao fim e ao cabo, resultam na limitação da liberdade de ir e vir, direito fundamental que pressupõe as garantias da ampla defesa e contraditório, ainda que diferidas, isto é, em momento posterior no curso de um processo penal.

Ainda em 2015, o Conselho Constitucional examinou, na ação n° 2015-722 DC [68], se as medidas de vigilância de comunicações eletrônicas internacionais estavam em harmonia com o direito à privacidade, o sigilo da correspondência e o direito a um recurso judicial. No julgamento se considerou que os dispositivos L. 854-1, L. 854-2, L. 854-5 e L. 854-9 do Código de Segurança Interna eram constitucionais. É o destaque *ipsis litteris* de trecho da decisão:

> DROITS ET LIBERTÉS. 4.19. LIBERTÉ PERSONNELLE. 4.19.3. Liberté personnelle et police administrative.
>
> L'article L. 854-1 autorise la surveillance des communications qui sont émises ou reçues à l'étranger et délimite le champ de celles de ces communications qui sont susceptibles de faire l'objet de mesures de surveillance dans les conditions prévues par les autres dispositions du chapitre IV du titre V du livre VIII du code de la sécurité intérieure. Le recueil de renseignement au moyen des mesures de surveillance prévues au chapitre IV du titre V du livre VIII du code de la sécurité intérieure par les services spécialisés de renseignement pour l'exercice de leurs missions respectives relève de la seule police administrative. Il ne peut donc avoir d'autre but que de préserver l'ordre public et de prévenir les infractions. Il ne peut être mis en œuvre pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs.
>
> L'article L. 854-1 permet la surveillance aux seules fins de défense et de promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 . Ainsi, le législateur a précisément circonscrit les finalités permettant de recourir au régime d'autorisation des mesures de surveillance des communications émises ou reçues à l'étranger prévu par l'article L. 854-1 et n'a pas retenu des critères en inadéquation avec l'objectif poursuivi par ces mesures de police administrative.
>
> L'autorisation d'intercepter des communications électroniques émises ou reçues à l'étranger est délivrée par le Premier ministre et désigne les réseaux de communication sur lesquels les interceptions sont admises. L'autorisation d'exploiter ces interceptions est délivrée par le Premier ministre ou par l'un de ses délégués sur demande motivée des ministres de la défense, de l'intérieur ou chargés de l'économie, du budget ou des douanes ou de leurs délégués. Cette exploitation est réalisée par un service spécialisé de renseignement; que les autorisations d'interception ou d'exploitation sont délivrées pour une durée limitée. L'autorisation d'exploiter de manière non individualisée les données de connexion interceptées précise le type de traitements automatisés pouvant être mis en œuvre.
>
> Le législateur a prévu des durées de conservation en fonction des caractéristiques des renseignements collectés ainsi qu'une durée maximale de conservation de huit ans à compter du recueil des renseignements chiffrés, au-delà desquelles les renseignements collectés doivent être détruits. En outre, en vertu de l'article L. 854-6, les transcriptions ou extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite des finalités mentionnées à l'article L. 811-3.
>
> Le législateur a prévu que la commission nationale de contrôle des techniques de renseignement reçoit communication de toutes les décisions et autorisations du Premier ministre mentionnées à l'article L. 854-2 et qu'elle dispose d'un accès permanent, complet et direct aux dispositifs de traçabilité, aux renseignements collectés, aux transcriptions et extractions réalisées ainsi qu'aux relevés mentionnés au quatrième alinéa de l'article L. 854-6 retraçant les opérations de destruction, de transcription et d'extraction. La commission peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de sa mission. Sont applicables aux contrôles pratiqués par la commission sur les mesures de surveillance internationale les dispositions de l'article L. 833-3 qui réprime de peines délictuelles les actes d'entrave à l'action de la commission.
>
> Il résulte de tout ce qui précède que les dispositions des articles L. 854-1, L. 854-2, L. 854-5

et des premier à troisième et sixième alinéas de l'article L. 854-9 ne portent pas d'atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances.

Em tradução livre:

> 4. DIREITOS E LIBERDADES. 4.19. LIBERDADE PESSOAL. 4.19.3. Liberdade pessoal e polícia administrativa
>
> O artigo L. 854-1 autoriza a vigilância das comunicações enviadas ou recebidas no estrangeiro e delimita o âmbito das comunicações susceptíveis de serem objeto de medidas de vigilância nas condições previstas nas demais disposições do Capítulo IV do Título V do Livro VIII do Código de Segurança Interna.
>
> A coleta de informações por meio das medidas de vigilância previstas no Capítulo IV do Título V do Livro VIII do Código de Segurança Interna pelos serviços de inteligência especializados para o exercício das respectivas missões é da exclusiva responsabilidade da polícia administrativa. Por conseguinte, não pode ter outra finalidade que não a preservação da ordem pública e a prevenção de infracções. Não pode ser usado para detectar violações da lei penal;
>
> O artigo L. 854-1 permite a vigilância "com o único propósito de defender e promover os interesses fundamentais da Nação mencionados no artigo L. 811-3". Assim, o legislador circunscreveu precisamente as finalidades que permitem recorrer ao sistema de autorização de medidas de vigilância de comunicações emitidas ou recebidas no estrangeiro previsto no artigo L. 854-1 e não manteve critérios inadequados. medidas de polícia administrativa.
>
> A autorização de interceptação de comunicações eletrônicas enviadas ou recebidas no estrangeiro é emitida pelo Primeiro-Ministro e designa as redes de comunicações nas quais é permitida a interceptação. A autorização para explorar estas intercepções é emitida pelo Primeiro-Ministro ou por um dos seus delegados a pedido fundamentado dos ministros da defesa, do interior ou responsáveis pela economia, orçamento ou alfândegas ou seus delegados. Essa exploração é realizada por um serviço de inteligência especializado; que as autorizações de interceptação ou exploração sejam emitidas por um período limitado. A autorização para usar os dados de conexão interceptados de forma não individualizada especifica o tipo de processamento automatizado que pode ser implementado.
>
> O legislador previu prazos de conservação em função das características da informação recolhida, bem como um período máximo de conservação de oito anos a partir da coleta da informação encriptada, para além do qual a informação recolhida deve ser destruída. Além disso, nos termos do artigo L. 854-6, as transcrições ou excertos devem ser destruídos logo que a sua conservação deixe de ser indispensável à prossecução dos fins referidos no artigo L. 811-3.
>
> O legislador previu que a comissão nacional de controle das técnicas de inteligência receba a comunicação de todas as decisões e autorizações do Primeiro-Ministro referidas no artigo L. 854-2 e que tenha acesso permanente, completo e direto aos dispositivos de rastreabilidade, a informações coletadas, as transcrições e extrações realizadas, bem como as declarações mencionadas no parágrafo quarto do artigo L. 854-6 que refazem as operações de destruição, transcrição e extração. A comissão pode solicitar ao Primeiro-Ministro todos os elementos necessários ao cumprimento da sua missão. As disposições do artigo L. 833-3.
>
> Decorre de tudo o que precede que as disposições dos artigos L. 854-1, L. 854-2, L. 854-5 e o primeiro ao terceiro e sexto parágrafos do artigo L. 854-9 não interferem desproporcionalmente com o direito a vida privada e ao sigilo da correspondência.
>
> (2015-722 DC, 26 de novembro de 2015, cons. 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, JORF nº 0278 de 1º de dezembro de 2015 página 22187, texto nº 2).

Em síntese, a decisão aponta para a constitucionalidade das disposições normativas, essencialmente por considerar que ficou estabelecido um rito procedimental administrativo para a deflagração das medidas de coleta de dados, assim como se previu que tais providências seriam adotadas com a finalidade de defesa e promoção dos interesses fundamentais da Nação.

De acordo com o art. 4° do Tratado da União Europeia [69], a União respeita as funções essenciais do Estado, nomeadamente as que se destinam a garantir a integridade territorial, a manter a ordem pública e a salvaguardar a segurança nacional. Em especial, a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro.

Diante desse panorama, é interessante, para uma melhor visualização, destacar, resumidamente, como cada país lida com as técnicas de inteligência.

Tabela 3.1: Comparativo de Legislação de Serviços de Inteligência Estrangeiros

País	**Legislação**
Estados Unidos	USA *Patriot Act*. *Intelligence Reform and Terrorism Prevention Act*. USA *Patriot Improvement and Reauthorization Act of* 2005. USA *Patriot Act Additional Reauthorization Amendments Act*. *Patriot Sunsets Extension Act of* 2011. USA *Freedom Act*. *Protect America Act*. FISA *Amendments Act of* 2008. *Foreign Intelligence Surveillance Act* 1978. FISA *Amendments Act Reauthorization Act of* 2017.
Reino Unido	*Investigatory Powers Act* 2016 incluiu a geolocalização entre os dados que podem ser acessados.
Canadá	Lei do Serviço de Inteligência Canadense, com alterações das Lei Antiterrorista de 2015, C-51 e C-59.
Austrália	Australian Security Intelligence Organization Act 1979, Intelligence Services Act 2001 e Telecommunications Act 1979.
Nova Zelândia	Lei de Inteligência e Segurança, 2017.
Alemanha	BND Act, 1990 (Lei do Serviço Federal de Inteligência). A BND Act foi alterada pela Lei de Adaptação do Regulamento Geral de Proteção de Dados. Em 2020 e 2021 a BND Act foi alterada seguindo as diretrizes do Tribunal Constitucional Federal Alemão.
França	Código de Segurança Interna e Estratégia Nacional de Inteligência.

Tabela 3.2: Comparativo de Competência para autorização de técnicas operacionais em Serviços de Inteligência Estrangeiros

País	Autorização para utilização de técnica operacional
Estados Unidos	Procurador-Geral e *Foreign Intelligence Surveillance Court* (FISC).
Reino Unido	Mandado do Secretário de Estado aprovado por um juiz.
Canadá	Juiz.
Austrália	Acesso direto. Em casos como monitoramento de telecomunicações e instalação de dispositivos de vigilância a autorização se realiza por aprovação do Procurador-Geral.
Nova Zelândia	Mandados, tipo 1 ou 2, deferidos pelo Ministro ou pelo Comissário-Chefe de Autorizações de Mandado de Inteligência.
Alemanha	Presidente do BND e Diretor-Geral do BFV.
França	Autorização do Primeiro Ministro.

Tabela 3.3: Comparativo de Controle Interno e Externo nos Serviços de Inteligência Estrangeiros

País	Controle Interno e Externo
Estados Unidos	**Controle Hierárquico/Interno:** Inspetores Gerais, Procurador-Geral, Conselho Nacional de Segurança, o Conselho Consultivo de Inteligência do Presidente, o Conselho de Supervisão de Inteligência, o Conselho de Supervisão de Privacidade e Liberdades Civis. **Controle Parlamentar:** *United States Senate Select Committee on Intelligence* e o *Permanent Select Committee on Intelligence*. **Controle Judicial:** *Foreign Intelligence Surveillance Court* (FISC).
Reino Unido	O Controle Parlamentar é realizado pelo *Intelligence and Security Committee* com membros da Câmara dos Comuns e dos Lordes.
Canadá	Agência de Revisão das atividades de inteligência. Obrigatoriedade de apresentação de um Relatório ao Parlamento.
Austrália	Controle Hierárquico; Envio de relatório anual ao Parlamento Australiano, Fiscalização pelo Inspetor-Geral de Inteligência e Segurança, Supervisão dos poderes especiais pelo Procurador-Geral e avaliação das despesas pela Comissão Parlamentar de Inteligência e Segurança.
Continua na próxima página	

Tabela 3.3 – Continuação da página anterior

País	Controle Interno e Externo
Nova Zelândia	Controle Hierárquico; Comitê de Inteligência e Segurança (Parlamento) e Inspetor-Geral de Inteligência e Segurança.
Alemanha	Conselho de Controle Independente, Painel de Supervisão Parlamentar, Comissão do G10 (analisa interferência no sigilo das comunicações) e Comissário Federal para a Proteção de Dados e Liberdade de Informação.
França	1) Controle Hierárquico realizado pelo Ministério do Interior e Ministério da Defesa. 2) Comissão Nacional de Controle de Técnicas de Inteligência; 3) Inspeção dos Serviços de Inteligência; 4) Delegação Parlamentar de Inteligência (controle legislativo). 5) Comissão Especial de Verificação de Fundos (controle de contas)

Tabela 3.4: Comparativo de Decisões Judiciais em relação aos Serviços de Inteligência Estrangeiros

País	Jurisprudência
Estados Unidos	Suprema Corte Americana: ação que questionava os programas de vigilância sequer foi conhecida pela Corte.
Reino Unido	*High Court of Justice: Intelligence Services Act* está de acordo com o *Human Rights Act* 1998.
Canadá	**Suprema Corte do Canadá:** Equilíbrio entre segurança nacional e restrições de direitos dos acusados. **Tribunal Superior de Justiça de Ontário:** é possível a geolocalização. Proporcionalidade e Relevância das Informações.
Austrália	A pesquisa não detectou decisões judiciais relacionadas ao assunto
Nova Zelândia	Suprema Corte: em casos diversos, em juízo de ponderação de interesses, prevaleceu o interesse da sociedade e a segurança nacional em comparação com direitos individuais.
Alemanha	Tribunal Constitucional Federal Alemão: processo de coleta vs direitos fundamentais. A vigilância estratégica das telecomunicações é legítima, adequada e necessária mas deve ser utilizada com proporcionalidade.

Continua na próxima página

Tabela 3.4 – Continuação da página anterior

País	Jurisprudência
França	Conselho Constitucional: a geolocalização como técnica de inteligência interna é constitucional. A vigilância em massa no exterior não afronta o direito à privacidade.

4 INAPLICABILIDADE DA LGPD À CAPTAÇÃO DA GEOLOCALIZAÇÃO PELA ATIVIDADE DE INTELIGÊNCIA

Em princípio, é imperioso afastar o argumento que a geolocalização implicaria na interceptação telefônica da estação móvel (aparelho celular). O sigilo das comunicações telefônicas é protegido constitucionalmente no art. 5°, inciso XII, da Carta Magna. A proteção constitucional conferida às comunicações somente pode ser excepcionada nas hipóteses de investigação criminal ou instrução processual penal. Disso resulta que, em nenhuma hipótese, é possível que se obtenha informações a partir de interceptações das comunicações para fins de inteligência ou em processos judiciais de natureza cível. Mas não se aplica o regramento à geolocalização uma vez que o dado obtido para determinar a localização do alvo não se caracteriza como comunicação.

E como se caracterizaria essa informação de localização do indivíduo a partir de uma estação móvel? Trata-se de um dado pessoal obtido através de um meio tecnológico, como o GPS do aparelho celular ou as Estações Rádio Bases, fornecedoras do serviço celular. E qual arcabouço jurídico resguarda os dados pessoais? Em sua redação original, a Constituição Federal protegeu o direito à privacidade no inciso X, do art. 5° (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). Em 2022, por meio da Emenda Constitucional n° 115, inseriu-se no rol de direitos e garantias fundamentais o direito à proteção dos dados pessoais. Destarte, o que se ampara, de maneira geral, em relação ao dado de geolocalização é a privacidade do indivíduo e a proteção enquanto dado pessoal.

Dito isto, há que se verificar se a Lei Geral de Proteção de Dados (LGPD) disciplina o acesso a um dado pessoal, e especificamente à geolocalização, para a finalidade de inteligência. Ou seja, se a vigilância eletrônica, voltada a identificar a geolocalização de um indivíduo encontra algum respaldo ou vedação no âmbito da LGPD.

A Lei Geral de Proteção de Dados [70], de 14 de agosto de 2018 foi editada e impulsionada na conjuntura[1] da *General Data Protection Regulation* (GDPR) [71], legislação europeia que consolidou a proteção do tratamento de dados, e do escândalo da Cambridge Analytica, envolvendo dados da rede social Facebook [72] . O assunto, no entanto, foi amadurecido a partir da constatação que os dados dos usuários e, principalmente, seu comportamento na rede mundial de computadores se traduzem em ativo econômico, merecendo a devida proteção na linha do que foi realizado em outros países.

Cuidou a Lei de definir, em seu art. 5°, inciso X, o tratamento de dados como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso,

[1] O Projeto de Lei n° 4060/2012 é da relatoria do Dep. Milton Monti. Em 2016, foi apensado à matéria o PL n° 5276/2016, encaminhado pelo Poder Executivo e mais abrangente, contendo 56 artigos divididos em nove capítulos. Após o episódio da Cambridge Analytica, em março de 2018, citado expressamente no relatório pelo Dep. Orlando Silva, o assunto ganhou impulso, tendo sido aprovado requerimento de urgência, e, na sequência, a redação final pelo plenário, em 29/05/2018.

reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração". Nesse contexto, a coleta do dado de geolocalização, seja por meio do GPS ou da ERB, estaria caracterizada como tratamento de dados pessoais.

Todavia, a Lei Geral de Proteção de Dados estipulou, em seu artigo 4°, hipóteses de inaplicabilidade da norma, à exemplo do tratamento de dados pessoais realizados para fins exclusivamente jornalísticos, artísticos e acadêmicos, assim como aqueles efetivados por pessoa natural, com fins particulares e não econômicos. Especificamente no inciso III, do artigo em referência, estão englobados, como exceção, o tratamento de dados com fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
>
> II - realizado para fins exclusivamente:
>
> a) jornalístico e artísticos; ou
>
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
>
> III - realizado para fins exclusivos de:
>
> a) segurança pública;
>
> b) defesa nacional;
>
> c) segurança do Estado; ou
>
> d) atividades de investigação e repressão de infrações penais
>
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. (BRASIL, 2018)

A corroborar o inciso III, do art. 4°, o §1° do mesmo dispositivo da LGPD dispõe que o tratamento de dados pessoais previsto no inciso III deve ser regido por legislação específica. Portanto, esse plexo de comandos e atividades, constantes da definição do que é tratamento de dados, citado no art. 5°, inciso X, não estão abarcados pela Lei, quando disser respeito, exclusivamente, à segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, uma vez que a norma remeteu a disciplina do tema à lei a ser editada em momento posterior.

Analisando a questão sobre outro prisma, extrai-se da exposição de motivos do Anteprojeto de lei elaborado pelo Ministério da Justiça, que resultou no PL 5276/2016 [73], apensado ao PL 4060/2012, e na LGPD, após a sanção presidencial:

> A minuta proposta abarca o tratamento de informações pessoais processadas tanto pelo setor público como pelo setor privado. Estão excluídos do âmbito de proteção da norma, no entanto, aqueles tratamentos de dados pessoais realizados para fins exclusivamente pessoais, bem como aqueles que tem por objeto o exercício regular da atividade jornalística, artística, literária ou acadêmica. Quanto à regulação referente à segurança pública, esta deverá respeitar os princípios

> gerais estabelecidos no texto, porém contará com legislação específica posterior a esta proposta. (BRASIL, Câmara dos Deputados, 2016)

Depreende-se do último período do parágrafo que o intuito daqueles que elaboraram o Anteprojeto era remeter a disciplina do tratamento de dados das hipóteses do art. 4°, inciso III, da LGPD, para uma legislação específica.

Avançando na interpretação da LGPD, em 2020, a Advocacia-Geral da União firmou, por meio do Parecer n. 00088/2020/DECOR/CGU/AGU, com as alterações do Despacho n. 00357/2021/DECOR/CGU/AGU, exarados no processo NUP 08000.066064/2019-01 posicionamento acerca da aplicabilidade imediata dos princípios gerais de proteção e dos direitos do titular dos dados previstos na LGPD para o tratamento de dados de segurança pública e que envolvesse atividades de investigação e repressão de infrações penais. São esclarecedores os termos do Despacho n. 00357/2021/DECOR/CGU/AGU:

> 18. O § 1º do art. 4º da LGPD estabelece que o tratamento de dados pessoais para referenciadas finalidades será objeto de lei específica, a qual deverá disciplinar a matéria sem olvidar as peculiaridades que são próprias destas finalidades e do interesse público perseguido, vocacionado para combater com eficiência a criminalidade. Assim o tratamento dos dados para execução das referenciadas políticas públicas será objeto de lei especial, que preverá cautelas específicas e compatíveis com a finalidade pública almejada, de maneira que o legislador ordinário editará comandos próprios para resguardar os direitos dos titulares dos dados sem comprometer a eficiente persecução penal.
>
> 19. Assim, o legislador ordinário, ao prever que referenciada lei específica a ser editada deverá resguardar a proporcionalidade, o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD está, na verdade, expressando que a matéria não está tratada na LGPD, bem como que será disciplinada em lei própria, especial, não cabendo, salvo melhor juízo, aplicar de imediato disposições da LGPD para o tratamento de dados para as finalidades de segurança pública, investigação e repressão de crimes justamente porque para tais finalidades foi prevista a incidência de lei própria, a ser editada especificamente para disciplinar tais hipóteses, e que, portanto, estabelecerá salvaguardas e ponderações próprias e especiais, que acautelem os direitos dos titulares dos dados sem comprometer a eficiente persecução penal.
>
> 20. As salvaguardas postas ao final do § 1º do art. 4º da LGPD, pois, compreendem um plexo de diretrizes que devem ser consideradas na elaboração da lei vindoura, e não se prestam para determinar a incidência imediata de dispositivos da LGPD, ainda que materialmente relacionados aos preceitos jurídicos referenciados no aludido § 1º do art. 4º da LGPD.
>
> 26. O § 1º do referenciado artigo 4º, pois, além de prever que a matéria especificamente relacionada ao tratamento de dados para fins de segurança pública e investigação e repressão de crimes será disciplinada por legislação própria, o que não é previsto para as demais hipóteses em que a incidência da Lei nº 13.709, de 2018, foi afastada pelos incisos do art. 4º, também delimita as diretrizes, inclusive de patamar constitucional, que devem ser observadas pelos Poderes Constituídos no trâmite da norma, revelando-se, salvo melhor juízo, impróprio e paradoxal que, a partir de tais diretrizes, seja investigada a incidência ou não de determinados artigos da LGPD para as hipóteses que a própria LGPD fixou sua não incidência e ainda teve o cuidado de prever lei própria para sua disciplina.
>
> [...]
>
> 31. Portanto, a melhor exegese do inciso II, alínea "b"; do inciso III, alíneas "a" e "d"; e dos §§ 1º a 4º; todos do art. 4º da LGPD; determina que: (a) a LGPD não se aplica para o tratamentos de dados com fins de segurança pública, investigação e repressão de ilícitos, ressalvado o disposto nos §§ 2º a 4º do seu art. 4º; (b) o tratamento dos dados para estas finalidades será disciplinado em lei especial; (c) os Poderes constituídos, na proposição e trâmite da lei especial, devem considerar as diretrizes, inclusive de patamar constitucional, de que cuida a parte final do § 1º do art. 4º da LGPD; e (d) a não incidência da LGPD não enseja a interrupção da execução das políticas

> públicas de segurança e persecução penal nem tampouco a absoluta ausência de salvaguardas, de governança e de reserva no tratamento dos dados pessoais para tais finalidades, devendo as Pastas envolvidas aplicar os preceitos constitucionais e as normas legais e infralegais em vigor até que sobrevenha a legislação especial.

A questão dirimida pela AGU teve como foco o tratamento de dados no contexto de segurança pública, investigação e repressão de infrações penais, alíneas "a" e "d" do inciso III do art. 4°. O raciocínio utilizado, no entanto, por decorrência lógica, aplica-se às outras alíneas, "b" e "c" do mesmo dispositivo. Dito de outro modo, o tratamento de dados para fins exclusivos de defesa nacional e segurança do Estado não está regido pela LGPD, excetuando-se os §§ 2° e 4° do art. 4°.

No campo judicial, o Supremo Tribunal Federal tangenciou o tema ao ser instado a se manifestar em virtude da Arguição de Descumprimento de Preceito Fundamental, tombada sob o n° 695, e protocolizada em 15/06/2020. Os instrumentos normativos atacados foram o Decreto n° 10.046/2019, Portaria n° 15/2016 [74] e Termo de Autorização n° 07/2020, ambos do Departamento Nacional de Trânsito (DENATRAN). Na ação, questionou-se o compartilhamento de dados do DENATRAN com a Agência Brasileira de Inteligência (ABIN).

Sob a relatoria do Ministro Gilmar Mendes foi proferida decisão em sede de Medida Cautelar em que se reconheceu *que o próprio texto da LGPD escusa a aplicação dos seus princípios e diretrizes ao tratamento de dados para fins de segurança pública, defesa nacional ou segurança do estado (art. 4º, inciso III)* [74].

Merece registro a decisão do Tribunal de Justiça de São Paulo, nos autos da Apelação Cível n° 1090663-42.2018.8.26.0100 que julgou improcedente a irresignação do Metrô de São Paulo que buscava a reforma da sentença em ação proposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) e a Defensoria Pública do Estado de São Paulo.

No caso em concreto, a Concessionaria da linha 4 do Metrô de São Paulo S.A. implantou sistema de coleta, utilização e armazenamento de dados, por meio de câmeras com captação facial, em suas instalações sem conhecimento ou consentimento dos usuários do serviço de transporte. A decisão, na linha da Lei Geral de Proteção de Dados, diferencia a finalidade da captação dos dados. Vejamos:

> A situação exposta no caso concreto é muito diferente da captação de imagens por sistemas de segurança com objetivo de melhoria na prestação do serviço, segurança dos usuários ou manutenção da ordem, o que seria não só aceitável, mas necessário diante da obrigação da fornecedora de serviço público zelar pela segurança de seus usuários dentro de suas dependências. É evidente que a captação da imagem ora discutida é utilizada para fins publicitários e consequente cunho comercial, já que, em linhas gerais, se busca detectar as principais características dos indivíduos que circulam em determinados locais e horários, bem como emoções e reações apresentadas à publicidade veiculada no equipamento [75].

Por fim, é importante pontuar, na esteira de se confirmar a inaplicabilidade da LGPD ao tratamento de dados promovidos exclusivamente para os fins do art. 4°, inciso III, que, por Ato do Presidente da

Câmara dos Deputados, de 26 de novembro de 2019, foi constituída Comissão de Juristas para elaboração do Anteprojeto da Lei de Proteção de Dados para segurança pública e persecução penal (LGPD-Penal).

O Anteprojeto foi apresentado pela Comissão que reafirmou, na exposição de motivos, a opção do legislador, durante às discussões da LGPD, acerca da necessidade de edição de legislação específica que contemplasse a regulação do art. 4°, inciso III, da LGPD. Em sua proposta de texto normativo, a LGPD-Penal estabeleceu a sua abrangência: *Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de defesa nacional e segurança do Estado* [76].

O Anteprojeto contemplou 12 capítulos, perfazendo 68 artigos, mas limitou-se a regulamentar as alíneas "a" e "d" do inciso III, do art. 4°, isto é, o tratamento de dados relacionados à segurança pública e atividades de investigação e repressão de infrações penais, deixando de lado as alíneas "b" e "c", respectivamente defesa nacional e segurança do Estado, que permanecem alheios à regulamentação da LGPD e LGPD-Penal, o que pode gerar, com o vácuo legiferante, inúmeras novas interpretações sobre o ponto.

Seguindo na linha de extrair a melhor interpretação da LGPD e se a lei abarcou, ou não, o regramento de coleta e utilização de dados pessoais por órgãos de inteligência, é interessante observar a legislação de outros países.

Na *Ley de Protección de los Datos Personales, Ley* 25.326/2000, a correspondente argentina da nossa Lei Geral de Proteção de Dados, em seu artigo 5°, 2.b) conjugado com o artigo 17, 1. e 2. já se reconhecia, pouco menos que 20 anos antes da edição da LGPD, as especificidades do tratamento de dados nas hipóteses de defesa nacional, segurança pública e investigação de infrações penais. É a redação:

> Articulo 5° — (Consentimiento).
>
> 2. No será necesario el consentimiento cuando:
>
> b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtudde una obligación legal.
>
> Articulo 17. — (Excepciones)
>
> 1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.
>
> 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado [77].

A lei de proteção de dados colombiana, *Ley Estatutaria* 1581 de 2012, disciplina a questão afastando do seu âmbito de aplicação dados de segurança e defesa nacional, lavagem de dinheiro e financiamento do terrorismo, inteligência e contra-inteligência. (art. 2, b) e c) e art. 10). *In verbis*:

> Artículo 2°. Ámbito de Aplicación. Los principios y disposiciones contenidas en la presente

> ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.
>
> El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:
>
> b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;
>
> c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;
>
> Artículo 10. Casos en que no es necesaria la autorización.
>
> La autorización del Titular no será necesaria cuando se trate de:
>
> a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial [78].

Na Costa Rica, na *Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales*, Lei n° 8968/2011, podem ser impostas limitações a autodeterminação informativa, definidos como conjunto de princípios e garantias, nas hipóteses de segurança do Estado e investigação, prevenção e repressão de infrações penais (art. 8°, a) e c)).

> Artículo 8.- Excepciones a la autodeterminación informativa del ciudadano
>
> a) La seguridad del Estado
>
> [...]
>
> c) La prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología en las profesiones [79].

Isso, significa, em outros termos, que, embora aplicável irrestritamente, a lei costa-riquenha preferiu dar tratamento específico ao assunto na própria legislação geral.

A *Ley* nº 29.733, *Ley de Protección de Datos Personales*, editada em 3 de julho de 2011, no Peru excluiu do seu âmbito de abrangência (art. 3°) o tratamento de dados quando for necessário para o desempenho de competências dos órgãos públicos de defesa nacional, segurança pública e investigação e repressão de crimes.

> Artículo 3. Ámbito de aplicación La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles. Las disposiciones de esta Ley no son de aplicación a los siguientes datos personales:
>
> [. . .]
>
> 2. A los contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito [80].

A lei mexicana, *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, em

seu art. 80 e seguintes, explicita que o tratamento de dados pessoais realizado pelas autoridades de segurança nacional deve obedecer aos corolários de proporcionalidade, adequação e finalidade, devendo, ainda, estabelecer medidas de proteção em seus bancos de dados que garantam a disponibilidade, integridade e confidencialidade das informações.

> Artículo 80. La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de las sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto. Las autoridades que accedan y almacenen los datos personales que se recaben por los particulares en cumplimiento de las disposiciones legales correspondientes, deberán cumplir con las disposiciones señaladas en el presente Capítulo.
>
> Artículo 81. En el tratamiento de datos personales así como en el uso de las bases de datos para su almacenamiento, que realicen los sujetos obligados competentes de las instancias de seguridad, procuración y administración de justicia deberá cumplir con los principios establecidos en el Título Segundo de la presente Ley. Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.
>
> Artículo 82. Los responsables de las bases de datos a que se refiere este Capítulo, deberán establecer medidas de seguridad de nivel alto, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado [81]

Assim como na lei da Costa Rica, o México optou por em capítulo próprio da sua lei geral de proteção de dados conferir tratamento diferenciado às hipóteses de segurança nacional, segurança pública, ou para a prevenção ou perseguição dos delitos.

No Panamá, assim como no Brasil, a Lei de Dados Pessoais (*Ley* n° 81/2019) é recente, tendo entrado em vigor apenas em 2021. Em seu art 3°, excepciona-se da aplicação da norma os tratamentos de dados pessoais realizados com a finalidade de prevenção, investigação, detecção ou repressão de infrações penais ou nas hipóteses de inteligência financeira e segurança nacional.

> Artículo 3. Se exceptúan del ámbito de esta Ley aquellos tratamientos que expressamente se encuentren regulados por leyes especiales o por las normativas que las desarrollen, además de los tratamientos de datos personales siguientes:
>
> [...]
>
> 2. Los que realicen autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.
>
> 3. Los que se efectúen para el análisis de inteligencia financiera y relativos a la seguridad nacional de conformidad con las legislaciones, tratados o convênios internacionales que regulen estas materias [82].

A lei uruguaia, *ley* 18331/2008 – *Proteccíon de Datos Personales Y Acción de "habeas data"*, estabelece em seu art. 27 que a norma não se aplica quando os dados possam afetar a defesa nacional, segurança pública e repressão de crimes.

> Artículo 27. Excepciones al derecho a la información.-
>
> Lo dispuesto en la presente ley no será aplicable a la recolección de datos, cuando la información del titular afecte a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales [83].

A Lei n° 172/13, *Ley Orgánica sobre Protección de Datos de Carácter Personal*, da República Dominicana, seguiu a linha das demais legislações ressalvando de sua aplicabilidade os arquivos dos organismos de inteligência e investigação e prevenção de crimes (art. 4° 2.).

> Artículo 4.- Restricciones. El régimen de protección de los datos de carácter personal no aplicará:
>
> 2. A los archivos de datos personales establecidos por los organismos de investigación y de inteligencia de la República Dominicana encargados de la prevención, persecución y castigo de los crímenes y delitos [84].

No Chile, com a Lei n° 19.628/99, não é necessário o consentimento do titular dos dados se o tratamento for realizado por entidade pública que detenha competência para realizar a atividade (art. 15 e 20). Para além disso, o titular dos dados não pode solicitar o acesso, modificação, cancelamento ou bloqueio de dados em órgãos públicos quando haja prejuízo à função investigatória e ao interesse nacional. É a dicção da lei chilena:

> Artículo 15.- No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional.
>
> [...]
>
> Artículo 20.- El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular [85].

Como se observa, a lei chilena, assim como a mexicana e a costa riquenha, igualmente estabeleceu, no seu próprio regime geral, disposições especiais acerca do tratamento de dados realizado com a finalidade investigativa e de segurança nacional.

Por fim, importante citar a *General Data Protection Regulation* (GDPR), legislação do bloco da comunidade europeia que revogou a Diretiva de Proteção de Dados 95/46/CE e entrou em vigor em 25 de maio de 2018, inspirando a elaboração da Lei Geral de Proteção de Dados brasileira.

O Regulamento Geral sobre a Proteção de Dados excluiu (art. 2°), expressamente, do seu escopo de abrangência o tratamento de dados pessoais realizados pelas autoridades competentes para prevenção, investigação, detecção ou repressão de infracções penais, incluindo-se, nesse contexto, a proteção e prevenção de ameaças à segurança pública.

> Art. 2 – Material Scope

> 2. This Regulation does not apply to the processing of personal data: (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. (EUROPEIA, 2016)

A Lei da Califórnia de Privacidade do Consumidor (CCPA), de 28 de junho de 2018, Estado Americano onde se concentram empresas como Google, Apple, Facebook, Instagram, WhatsApp e Twitter estabeleceu em seu item 1798.145 que as obrigações impostas às empresas não devem impedir que elas cumpram outras leis de caráter federal, estadual ou municipal, ou mesmo que auxiliem autoridades em investigações cíveis ou criminais.

> 1798.145.
>
> (a) The obligations imposed on businesses by this title shall not restrict a business's ability to:
>
> (1) Comply with federal, state, or local laws.
>
> (2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
>
> (3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law [86].

Com esse extenso apanhado de Leis estrangeiras de proteção de dados, é possível afirmar que a LGPD não destoou, nesse particular, de normas congêneres. Em regra, portanto, sistemas de direito positivo não adotaram normas gerais e abstratas que abarcaram tratamento de dados de segurança pública, defesa nacional, segurança do Estado, atividades de inteligência, investigação e repressão de infrações penais. Em uma interpretação não restrita à hermenêutica do dispositivo em si, mas, a partir de uma análise de textos normativos de proteção de dados em mais de 20 países, utilizando-os como fontes de estudos juscomparativos, assim como dos entendimentos da Advocacia Geral da União e do Supremo Tribunal Federal, é possível dizer que a Lei Geral de Proteção de Dados afastou quase que por completo a sua aplicabilidade ao tratamento de dados realizado com fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

A própria designação de Comissão de Juristas pelo Presidente de Câmara dos Deputados e o reconhecimento na exposição de motivos que o tratamento de dados para os fins exclusivos das alíneas do inciso III, do art. 4° deve ser objeto de legislação específica, reforçam a ideia da inaplicabilidade da LGPD a esses temas.

Em contrapartida, o Anteprojeto da Lei Geral de Proteção de Dados Penal, embrião da legislação especial suscitada pelo art. 4° §1° da LGPD, teve poucos avanços no processo legislativo e limita-se, até então, a regulamentar as hipóteses de inaplicabilidade das alíneas "a" e "d" do inciso III, do art. 4°. Se por um lado, andou bem ao dissociar a regulamentação de temas de natureza diversa, tratamento de dados em repressão de infrações penais e o manejo de informações em situações de defesa nacional e segurança do Estado, por outro deu aparência de cumprimento e exaurimento do comando de atuação legislativa

determinado pela LGPD. Essa circunstância contribui para manter o carente arcabouço normativo das atividades que envolvem o essencial aparato de inteligência nacional.

De todo modo, constata-se que a interpretação do art. 4°, inciso III e §1° da LGPD que afasta a aplicabilidade de quase a totalidade da norma para o tratamento de dados realizado com fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais está alinhada com o arcabouço legislativo dos demais países.

O que se verifica, portanto, é que a Lei Geral de Proteção de Dados (LGPD) não disciplina, respalda ou veda o acesso a um dado pessoal, e especificamente à geolocalização, para a finalidade de inteligência. Destarte, enquanto não editada a LGPD Penal a vigilância eletrônica, que identifica a geolocalização de um alvo de interesse da inteligência em tempo real, está regida e limitada pela proteção constitucional que se confere à intimidade e privacidade (art. 5°, inciso X) e aos dados pessoais (art. 5°, inciso LXXIX).

A partir dessa constatação, é interessante a análise dos contornos do direito à privacidade e da proteção dos dados pessoais.

5 A EVOLUÇÃO DO CONCEITO E NATUREZA DO DIREITO À PRIVACIDADE

O embrião do direito à privacidade[1] e intimidade surge com a ideia do direito de "ser deixado só" (*to be let alone*). Samuel Warren e Louis Brandeis[2] [87], então estudantes de direito na Universidade de Harvard, escreveram a obra *"The Right to Privacy"*. De acordo com os autores, mudanças políticas, econômicas e sociais implicam no reconhecimento de novos direitos. O direito de ser deixado sozinho parte do raciocínio de evolução e dinâmica dos direitos. Gradualmente o direito à vida e à propriedade deram origem (ou ganharam novas facetas) ao direito de aproveitar a vida e o direito à propriedade evoluiu para o reconhecimento de direitos civis. Para os autores as invenções que surgiam naquele momento motivavam uma resposta jurídica protetiva ao indivíduo.

O interessante é que o contexto fático retratado pelos autores de evolução tecnológica era o avanço da fotografia, o surgimento de gravadores de voz e a disseminação de imagens em jornais (*The press is overstepping in every direction the obvious bounds of propriety and of decency*). E diante desse conjunto é que se defendeu o direito de estar só (*The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual*).

Sustenta-se, em suma, que deve ser do indivíduo a decisão de tornar determinado fato público ou não (*In every such case the individual is entitled to decide whether that which is his slhall be given to the public*). O direito à privacidade não se confunde com o direito autoral, o que se protege naquele são os pensamentos, sentimentos e emoções expressos em uma obra de arte ou escrito, além da vontade de tornar pública, nesse aspecto, a própria obra.

Apesar da defesa veemente da autonomia do direito à privacidade a partir do comparativo com o direito autoral e da proteção conferida por figuras jurídicas como a calúnia ou difamação, Warren e Brandeis já naquele momento consideraram que o direito à privacidade não seria absoluto e encontraria limite no interesse público.

Com pouco avanço até a metade do século XX, a proposta de autonomia de um direito à privacidade autônomo foi revisitada no estudo do professor William Prosser, *Privacy*, na década de 60. Para Prossner

[1] A privacidade em si é uma noção que remonta a 350 a.c. quando Aristóteles escreve a obra "A Política" e aborda as duas esferas distintas da vida, a esfera da vida privada, familiar, e a esfera da vida pública, política. Cuida-se acima do direito à privacidade

[2] Importante dizer que Brandeis tornou-se juiz da Suprema Corte Americana e participou do julgamento do caso Olmstead vs United States em que se discutia a legalidade de interceptações telefônicas. No caso, como as escutas não haviam sido implantadas na residência dos investigados, mas em cabos telefônicos na rua, não se considerou violação à quarta emenda da constituição americana, que garante a inviolabilidade da pessoa e seus bens contra buscas e apreensões indevidas. Embora derrotado, o juiz Brandeis, defendeu a necessidade da obtenção de um mandado para a interceptação telefônica, uma vez que a constituição protegeria o cidadão contra qualquer violação injustificada de sua privacidade.

[88], um dos maiores estudiosos americanos da responsabilidade civil, o direito à privacidade não seria uno mas uma violação de quatro aspectos do núcleo central da ideia do "direito de estar só". Seriam eles:

1. intrusão na reclusão ou solidão do autor;
2. divulgação de fatos privados;
3. publicidade de fatos inverídicos que afetam a imagem da pessoa perante a comunidade; e
4. apropriação do nome ou sinais do autor para auferir vantagem própria.

A tutela da privacidade passaria pela proteção da reputação, da tranquilidade emocional e da propriedade imaterial.

Ainda na década de 60, Bloustein [89] se propõe a escrever uma teoria geral da privacidade individual, resgatando os alicerces conceituais de Warren e Brandeis a respeito da unicidade do bem jurídico protegido no direito à privacidade. Rebatendo Prossner, entendeu que existia um bem jurídico a reunir as situações que outrora se confundiam com figuras jurídicas tradicionais, como direito autoral, à honra e propriedade. O bem jurídico a ser protegido no direito à privacidade seria a dignidade da pessoa humana. É nesse momento que o direito à privacidade ultrapassa a esfera individual, do direito à vida privada, intimidade e família, para alcançar uma dimensão coletiva, de direito fundamental.

Na Alemanha, Hubmann [90] concebeu uma teoria concêntrica ou teoria das esferas (*Sphärentheorie*) a respeito dos graus de intensidade de proteção e percepção individual de limitação de divulgação. Assim, para ele, da camada mais exterior para o centro, existiria a camada individual (*Individualsphäre*), a privada (*Privatsphäre*) e a secreta (*Geheimsphäre*), esta última a mais profunda e protegida. Atualmente, predomina na doutrina e restou aplicada nos tribunais alemães a teoria das três esferas, embora existam críticas a respeito da utilidade prática da compartimentação. Mas, de maneira geral, acredita-se que o núcleo central, a esfera da intimidade, teria proteção absoluta em face do princípio da dignidade da pessoa humana, enquanto nas demais esferas, o acesso aos dados poderia ser relativizado em decorrência de interesses públicos e direitos de patamar semelhante ou superior à privacidade. Diga-se, por oportuno, que a teoria de Hubmann encontrou eco também na doutrina portuguesa, conforme bem pontua Paulo Mota Pinto [91].

É nesse momento histórico, entre 1960 e 1970, que, mundialmente, a proteção ao direito à privacidade começa a se entrelaçar com a proteção aos dados pessoais, conforme já expusemos acima. É o processo de funcionalização da privacidade, nas palavras de Danilo Doneda [92], isto é, a continuação da proteção a partir de outros meios.

No Brasil, Tércio Sampaio escreveu paradigmático artigo [10] acerca do sigilo de dados, privacidade e limites da atuação estatal. Se debruçando sobre a garantia constitucional do sigilo de dados e das telecomunicações (art. 5°, inciso XII, da CF/88) e sua correlação com o direito à privacidade (art. 5°, inciso X, da CF/88), o trabalho serviu de fundamento doutrinário para diversas decisões do Supremo Tribunal Federal, notadamente no Ag. Reg no HC 124.322-RS, RE n° 418.416-SC, MS n° 21.729-DF, RO em HC n° 132.062-RS e HC 91.867-PA. Em suma, a partir das premissas firmadas no artigo, a Corte Constitucional

firmou posicionamento no sentido que a inviolabilidade das comunicações telefônicas refere-se aos dados de voz e identificação de receptor e transmissor da mensagem em trânsito. O acesso estatal à comunicação telefônica (quebra de sigilo telefônico), nos termos constitucionais, deve ocorrer apenas com autorização judicial e encontra-se restrito para os fins de investigação criminal ou instrução processual penal. Por outro lado, os dados estáticos armazenados em escritos, anotações, pastas, arquivos, em meio físico e eletrônico, poderiam ser objeto de busca e apreensão administrativa, desde que não violassem a privacidade do indivíduo. Assim, para ele, o sigilo não é o fim em si mesmo, ele é instrumental, e visa a proteção dos dados relacionados à vida privada, honra, imagem e intimidade das pessoas. Não faria sentido opor ao Estado restrição a dados cadastrais de elementos identificadores e de convivência social, como nome, endereço, filiação, profissão, idade, estado civil, números de registro civil. Esses dados seriam compartilhados em maior ou menor grau nas relações sociais.

A ideia, portanto, nos remete à visão de Hubmann, de que existiriam graus de sensibilidade no dado pessoal, representando a intimidade "um âmbito exclusivo que alguém reserva para si, sem nenhuma repercussão social". Já se vê, portanto, o paralelo de proteção de dados e intimidade.

Após aproximadamente 25 anos, interessante trabalho foi elaborado [93] para avaliar a contemporaneidade do artigo de Tércio Sampaio Ferraz. A obra resgata o espírito do trabalho do eminente professor da Faculdade de Direito da Universidade de São Paulo:

> Ao relacionar dados pessoais à privacidade, e ao mesmo tempo reconhecer a importância desse valor para a dignidade humana, Ferraz Júnior foi importante em desenhar a moldura axiomática dentro da qual os debates sobre proteção e acesso a dados pessoais devem ser pensados. Ainda que indolor, silencioso e discreto, o acesso a dados pessoais pode trazer graves implicações à privacidade, afetando, por consequência, a dignidade dos sujeitos. Nessa linha, "Sigilo de dados" reconhece que há uma dimensão das vidas privadas cujo simples acesso não autorizado por terceiros, por mais discreto que seja, é incompatível com o próprio status humano. É intrinsecamente humano e, portanto, valoroso enquanto característica indissociável da humanidade, guardar espaços de nossa intimidade em relação aos quais se decide, sem interferências ostensivas ou sorrateiras, quem deles pode participar. Compartilhar segredos mais recônditos e intimidades mais reclusas apenas com quem se escolhe é uma forma de expressar confiança, amizade e amor. Não reconhecer este espaço de exclusividade, eliminando, em consequência, a possibilidade do exercício desses julgamentos afetivos, implica violação a algo inerentemente humano e valoroso, mesmo quando tal devassa se dá de modo discreto e imperceptível.

Ponce e Queiroz chegam à seguinte conclusão acerca da atualidade da obra de Ferraz Junior:

> Como pontos ainda atuais, destacam-se:
>
> (i) a centralidade do princípio da dignidade humana como parâmetro normativo que dá sentido ao direito à privacidade e à proteção de dados pessoais, orientando a aplicação desses direitos;
>
> (ii) o reconhecimento de que dados importam à privacidade individual, impondo limites à atuação fiscalizadora do Estado–conforme imprimido no próprio título do texto seminal; e
>
> (iii) a distinção entre as comunicações que deixam vestígios físicos e aquelas instantâneas como critério de interpretação da exceção constitucional ao sigilo de comunicações – isto é, para a identificação de quais tipos de interceptação são permitidos.
>
> Já como pontos que merecem reflexão atualizadora, destacam-se os seguintes:

> (i) o direito à privacidade não mais se estrutura como uma liberdade de negação, por meio da proteção de dados pessoais, ela se reveste de um aspecto positivo de controle dos próprios dados pessoais;
>
> (ii) a proteção de dados pessoais deve ser pensada em uma perspectiva relacional, em detrimento da natureza individualista associada à concepção tradicional de privacidade;
>
> (iii) a distinção rígida entre dados em trânsito e dados armazenados não mais se sustenta como critério de interpretação da inviolabilidade do sigilo de dados veiculada por meio do artigo 5°, inciso XII da Constituição Federal; e
>
> (iv) na sociedade da informação, a atividade fiscalizadora do Estado não é mais a grande ameaça à privacidade–alinhando-se a agentes privados.

Um outro estudioso que merece referência no Brasil, inclusive por ter tido papel destacado na proteção dos dados, com a consequente edição da LGPD, é Danilo Doneda. Em obra das mais citadas sobre o assunto atualmente, o autor [92] aborda a privacidade sob o prisma da complexidade decorrente da dificuldade de entendê-la com a natureza de direito subjetivo. Para ele a privacidade é um valor que se reveste de pressuposto para o livre desenvolvimento da personalidade e construção da individualidade sem ingerências externas e mecanismos de controle social. A privacidade assume uma característica coletiva em contraponto à visão patrimonialista.

Essa correlação de privacidade e proteção de dados, encontra reflexão bastante elucidativa em Ponce e Queiroz. Destaque-se, novamente, a seguinte passagem do artigo já citado acima:

> Embora se possa discutir a natureza autônoma do direito de dados pessoais com relação à privacidade, parece inquestionável que essa nova matéria, embora dotada de um campo prático de atuação cada vez mais autônomo, mantém-se ao menos em parte fortemente relacionada com a privacidade, mas em via de mão dupla: da mesma forma que recebe da privacidade a preocupação com a preservação da esfera de autonomia e individualidade dos cidadãos, a disciplina jurídica da proteção de dados pessoais informa a doutrina da privacidade sobre a natureza relacional e difusa desses objetos merecedores de proteção [93].

Por fim, na Itália, um dos maiores expoentes no estudo do direito à privacidade, Stefano Rodotà, considera que a privacidade é *"o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada"* [92].

Rodotá, com atualidade e sem perder de vista os aspectos práticos, relaciona a privacidade com o avanço tecnológico intenso dos últimos anos. Não passa despercebido de seus textos e manifestações a crescente coleta e mineração de dados (*data mining*) realizada pelas *big techs*, assim como a vigilância em massa realizada pelos países no contexto do pós ataques às torres gêmeas no 11 de setembro de 2001. Em discurso de encerramento na 26ª Conferência Internacional sobre Privacidade e Proteção de Dados Pessoais na Polônia, Rodotà [94] afirmou que há uma evolução crescente e progressiva na proteção e configuração contemporânea da privacidade. Nessa trajetória, a função sócio-política da privacidade extrapola a ideia de individualidade, transformando-se em um componente integrante da própria cidadania. Mas uma preocupação constante de Rodotà é com a vigilância em massa mesmo no combate ao terrorismo, diante do risco que a coleta massiva de dados resulte no controle opressivo da sociedade. Para ele, a video-vigilância se

tornou um mecanismo capaz de avaliar o comportamento das pessoas, resgatando suas condutas pretéritas.

Em termos de positivação do direito à privacidade, é possível citar a Declaração Universal dos Direitos do Homem [95] que estabeleceu em seu art. 12 que *ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à proteção da lei*.

Datada de 1950 e atualizada nos anos seguintes, a Convenção Europeia dos Direitos do Homem [96] consignou em seu art. 8° que *qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência*.

Com redação bem semelhante à Declaração Universal dos Direitos do Homem, a Convenção Americana sobre Direitos Humanos [97], assevera que *ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação*.

Para além dos pactos e declarações, cada país iniciou a inserção do direito à privacidade nas respectivas legislações. O Código Civil Francês [98] sofreu alteração pela Lei n° 70-643, de 17 de julho de 1970, modificando a redação da seção 9 para: *Todos têm direito ao respeito pela sua vida privada*. A Espanha inseriu em sua Constituição [99], no art. 18, 1. que *é garantido o direito à honra, à intimidade pessoal e familiar e à própria imagem*. Na Lei Maior Portuguesa [100] constou no art. 26. 1. que *a todos são reconhecidos os direitos [...] à reserva da intimidade da vida privada e familiar*. Na Itália, conforme bem ensinam Colombo e Berni [101], o *Right Of Privacy, diritto alla riservatezza, diritto al riserbo ,al segretto della vita privata e diritto ad essere lasciati soli*, foi paulatinamente sendo incorporado na jurisprudência e restou embutido na Constituição em dispositivos de proteção a inviolabilidade da personalidade, inviolabilidade de domicílio e segredo de correspondência e comunicações. Em leis ordinárias a proteção se deu por meio da tutela de dados pessoais.

No Brasil, a Constituição Federal, de 1988, alocou no capítulo dos direitos e deveres individuais e coletivos tanto a garantia a privacidade e intimidade das pessoas, considerando-as invioláveis, quanto a proteção aos dados pessoais, inclusive nos meios digitais. O Código Civil [102] não caminhou diferente, fazendo referência, em seu art. 21, igualmente, à inviolabilidade da vida privada.

O que se observa nesse apanhado doutrinário e legislativo é uma evolução do conceito e da natureza do direito à privacidade. Passando de uma perspectiva individual para coletiva e de uma posição passiva, de expectativa de não interferência na esfera privada, para ativa, na autodeterminação informativa e no controle dos dados pessoais.

6 USO PRIVADO E PÚBLICO DA GEOLOCALIZAÇÃO. O CONTRATO SOCIAL DAS BIG TECHS X CONTRATO SOCIAL DO ESTADO

Quando nos debruçamos na evolução legislativa, conceitual e, principalmente, doutrinária da privacidade e proteção de dados é comum esbarrar, sobretudo na literatura recente, com textos que combatem com veemência o acesso a dados dos indivíduos por órgãos públicos.

O que chama a atenção, no entanto, é uma timidez nas críticas às entidades privadas, principalmente às *big techs*, e uma cobrança severa da postura estatal na coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão e extração de dados.

Em outros termos, o que transparece é que a doutrina não encara a captação e comercialização de dados pessoais pelas empresas privadas como um fato que inspire igual ou maior preocupação que a gestão de dados dos cidadãos pelo Estado. Antes mesmo, no entanto, de uma análise a respeito da finalidade e legitimidade do acesso aos dados dos cidadãos por empresas privadas ou pelo Estado, é importante, ainda que não exaustivamente, elencarmos algumas situações de captação de dados por cada um desses atores.

No campo privado, para que tenhamos uma ideia da dimensão dos dados colhidos, o site Stock Apps [103] realizou um levantamento e fez um ranking da quantidade de dados captados dos usuários pelas principais *big techs*:

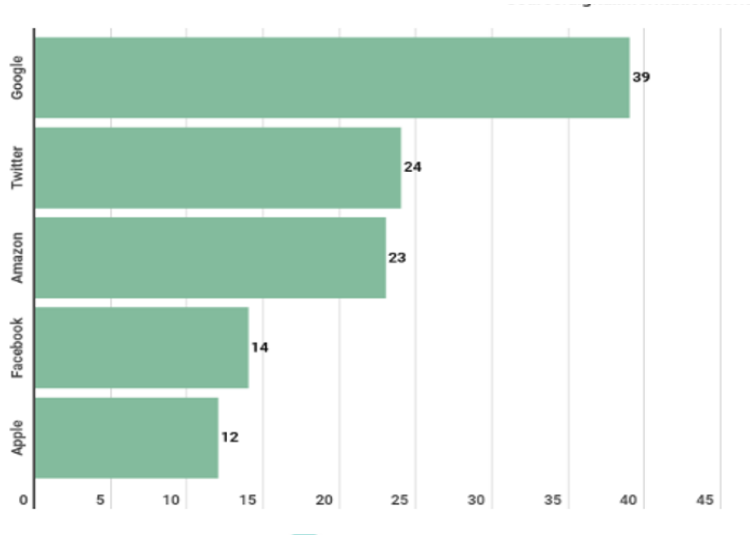

Figura 6.1: Dados coletados por *Big Tech's*.
Fonte:digitalinformationworld

O Google encabeçou a lista como plataforma que, disparadamente, é a que mais capta dados dos usuários. Da geolocalização ao histórico de navegação, a empresa digital diversifica a coleta de dados com a finalidade de segmentação e direcionamento de publicidade, embora diga que não comercializa dados pessoais e que sua missão é *"organizar as informações do mundo e torná-las universalmente acessíveis e úteis"*. Apesar dessa informação, a empresa admite que seu modelo de negócio tem alicerce na publicidade [104].

As demais *big techs*, Twiter, Amazon, Facebook e Apple, completam a lista das cinco empresas digitais que mais coletam informações dos usuários. Com a massiva captação de dados pelas *big techs*, estabelecimento de perfis, predição e modificação comportamental, as empresas digitais estão dominando a estrutura global de mercado. Dos computadores, *smartphones*, *smart tvs*, aplicativos, veículos, e, até mesmo, aspiradores de pó (os famosos roomba capazes de mapear o tamanho das residências, escadas, distância entre móveis e etc e compartilhar esses dados com o fabricante) os indivíduos estão imersos em uma atmosfera de coleta de seus dados pessoais com o objetivo de direta ou indiretamente comercializá-los. Esse fenômeno foi denominado por Shoshana Zuboff, professora da *Harvard Business School*, como Capitalismo de Vigilância [105].

Os dados pessoais dos usuários são o principal insumo a ser extraído e monetizado pelas empresas. Não se cuida mais apenas de coleta de dados isolados. Com a análise dos dados comportamentais com mecanismos de inteligência artificial chegou-se ao passo seguinte, a identificação e, eventualmente, a modificação do comportamento futuro do indivíduo. É nesse ponto que se insere a predição e, até a tentativa de manipulação comportamental, o que se viu mais claramente, no campo político, com o caso da Cambridge Analytica[1], envolvendo dados da rede social Facebook, quando se objetivava prever e influenciar escolhas nas urnas.

Resumidamente, os lucros das *big techs* dependem da sua capacidade de vigilância e de captação, análise e transformação de dados dos indivíduos em informações. Com esse objetivo, quanto mais tempo o indivíduo permanece monitorado, acessando *Apps*, ferramentas, aplicativos e interagindo na internet, mais dados são coletados e produzidos e mais acesso ao conteúdo publicitário direcionado ocorre, um mecanismo que se retroalimenta. Os dados se tornaram uma *commodity* e entramos na era da *data economy*.

Uma amostra da dimensão dos ganhos financeiros das empresas digitais restou revelado quando a Apple decidiu, em abril de 2021, implantar uma ferramenta de controle de privacidade e preservação de dados, denominada de *App Tracking Transparency*. Com a atualização do sistema operacional para o IOS 14.5, os usuários de Iphones passaram a ser consultados se autorizavam a coleta e o rastreamento de seus dados por aplicativos. Com essa medida, e a negativa de acesso aos seus dados por 62% dos usuários dos Iphones, o que gerou degradação na performance de publicidade, o Facebook perdeu R$ 53 bilhões em anúncios em 2021 [106].

[1] Estima-se que a Cambridge Analytica, empresa de mineração e análise de dados, tenha acessado, através do Facebook, dados de cerca de 87 milhões de usuários, repassando-os a clientes que tinham por objetivo influenciar as eleições em diversos países.

Há quem diga que a solução da questão estaria aí, no consentimento do usuário à "política de privacidade" ou aos "termos e condições" do aplicativo, ferramenta ou site. No entanto, tendo em vista o avanço tecnológico, circunstância que motivou Warren e Brandeis na escrita da obra *Right to the Privacy*, o que se observa atualmente é uma dependência das pessoas de aplicativos, buscadores de palavras, navegadores de internet e a interconexão digital de objetos (IOT). Todas essas facilidades oferecidas aos usuários acoplam captação de dados comportamentais e pessoais, coleta de informações do usuário, como sua localização, seu trajeto, seus hábitos e interesses, que locais frequenta, quanto tempo se atém a determinada notícia ou publicidade. E o indivíduo se vê obrigado a "aceitar" os termos de uso, como um contrato de adesão que realiza com a empresa que lhe fornece energia elétrica. Ou acata as condições impostas ou não usufrui de ferramentas de interação social e profissional, facilidades de compra de produtos e serviços, busca de locais e informações na internet e, até serviços de emergência privados[2].

Daí que a alegação de que os usuários consentiram com a captação de seus dados, e, especificamente, para o presente estudo, com sua geolocalização, não é verdadeira. A dependência enviesa as três premissas clássicas da autonomia da vontade na formação dos contratos: liberdade de contratar propriamente dita (optar pela contratação ou não), liberdade de escolher o contratado e liberdade de estipular ou discutir o conteúdo do contrato.

Sobre esse ponto, é precisa a análise de Reads no estudo da Stock Apps [103]:

> A maioria das pessoas não tem tempo ou paciência para ler as políticas de privacidade que podem ter várias páginas para cada site que visitam. Além disso, é bastante improvável que todos os usuários tenham experiência em direito para compreender adequadamente a política de privacidade. Além disso, os usuários não têm tempo, paciência ou energia para tentar descobrir quais informações os sites estão armazenando e como estão usando isso a seu favor. Como resultado, os usuários acabam permitindo que o Google colete todos os dados de que precisam, concordando com os termos da política de privacidade.

Como bem ensina Zuboff, trata-se de *uma escolha fundamentalmente ilegítima, que os indivíduos do século XXI não deveriam ter de fazer, e essa normalização nos deixa aprisionados, mas com a sensação de felicidade*. Ser rastreado por grandes empresas digitais passou a ser o novo normal. Uma circunstância aceita socialmente, até mesmo por parte da doutrina que escreve sobre privacidade.

Assim, em verdade, a natureza dos "termos e condições" apresentados aos usuários pelas *bigh techs* e sites é de um contrato eletrônico de adesão em que há pré-disposição das cláusulas, unilateralidade e rigidez em sua forma e conteúdo. Não há opção. O mais grave, entretanto, é que se induz o usuário a acreditar que a coleta dos seus dados não lhe é nociva e se realiza em seu próprio benefício e da sociedade em geral (recorde-se aqui a missão que o Google afirma ter: *"organizar as informações do mundo e torná-las universalmente acessíveis e úteis"*). Esse é o "contrato social" que as *big techs* oferecem. Inobstante, propositalmente não se torna público que a parcela de liberdade, com o fornecimento diuturno de seus

[2] Alguns veículos detêm hoje uma tecnologia de pedido de socorro por acionamento direto de um serviço de ajuda da montadora. Como o veículo está interconectado com a empresa, é possível por telemetria diagnosticar o defeito e, até mesmo, encaminhar uma equipe ao local pela identificação da geolocalização, bastando ao usuário apertar um único botão.

dados às *big techs*, que o usuário renuncia é desproporcionalmente maior diante dos benefícios que acredita acumular com o uso dos aplicativos e ferramentas disponibilizadas pelo mundo digital.

Isso tudo reforça a ideia do quão mais grave e profunda é a apreensão dos dados pessoais e informações dos usuários pelas empresas digitais, afastando o argumento de que um pseudo consentimento poderia legitimar a atuação das *big techs*.

É como bem ensina Stefano Rodotá: "*a contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações.*" [107].

Na outra vertente encontra-se a coleta de dados efetuada pelo Poder Público.

Antes de ingressar em pontos relacionados à legalidade e legitimidade do ente estatal em adotar essa ou outra medida, é imperioso lançar luzes sobre a própria dimensão de surgimento do Estado.

Em apertada síntese, a partir das concepções de Thomas Hobbes, John Locke e Jean-Jacques Rousseau, filósofos do século XVII e XVIII, adeptos da teoria contratualista, antes do surgimento do Estado existia o "estado da natureza". Nesse momento prévio à organização civil vigia a liberdade irrestrita, a possibilidade incondicional de conquistar terras, alimentos e objetos a partir do confronto direto, sujeitando os demais à vontade própria. Prevalecia o individualismo ou, no máximo, os interesses comuns momentâneos de um grupo, desencadeando a autotutela, a solução dos conflitos a partir da força, das batalhas e das guerras.

Hobbes, diante desse homem natural e da necessidade da organização de um "poder", concebe a ideia do homem artificial, do grande Leviatã, a que se chama Estado, ou Cidade (em latim *Civitas*). Destaque-se interessante passagem da sua obra Leviatã:

> A única maneira de instituir um tal poder comum, capaz de defendê-los das invasões dos estrangeiros e das injúrias uns dos outros, garantindo-lhes assim uma segurança suficiente para que, mediante seu próprio labor e graças aos frutos da terra, possam alimentar-se e viver satisfeitos, é conferir toda sua força e poder a um homem, ou a uma assembléia de homens, que possa reduzir suas diversas vontades, por pluralidade de votos, a uma só vontade. O que equivale a dizer: designar um homem ou uma assembléia de homens como representante de suas pessoas, considerando-se e reconhecendo-se cada um como autor de todos os atos que aquele que representa sua pessoa praticar ou levar a praticar, em tudo o que disser respeito à paz e segurança comuns; todos submetendo assim suas vontades à vontade do representante, e suas decisões a sua decisão. Isto é mais do que consentimento, ou concórdia, é uma verdadeira unidade de todos eles, numa só e mesma pessoa, realizada por um pacto de cada homem com todos os homens, de um modo que é como se cada homem dissesse a cada homem: Cedo e transfiro meu direito de governar-me a mim mesmo a este homem, ou a esta assembléia de homens, com a condição de transferires a ele teu direito, autorizando de maneira semelhante todas as suas ações. Feito isto, à multidão assim unida numa só pessoa se chama Estado, em latim civitas. É esta a geração daquele grande Leviatã, ou antes (para falar em termos mais reverentes) daquele Deus Mortal, ao qual devemos, abaixo do Deus Imortal, nossa paz e defesa. Pois graças a esta autoridade que lhe é dada por cada indivíduo no Estado, é-lhe conferido o uso de tamanho poder e força que o terror assim inspirado o torna capaz

de conformar as vontades de todos eles, no sentido da paz em seu próprio país, e ela ajuda mútua contra os inimigos estrangeiros. É nele que consiste a essência do testado, a qual pode ser assim definida: Uma pessoa de cujos atos uma grande multidão, mediante pactos recíprocos uns com os outros, foi instituída por cada um como autora, de modo a ela poder usar a força e os recursos de todos, da maneira que considerar conveniente, para assegurara paz e a defesa comum [108].

Na mesma linha, Locke:

DO INÍCIO DAS SOCIEDADES POLÍTICAS

95. Se todos os homens são, como se tem dito, livres, iguais e independentes por natureza, ninguém pode ser retirado deste estado e se sujeitar ao poder político de outro sem o seu próprio consentimento. A única maneira pela qual alguém se despoja de sua liberdade natural e se coloca dentro das limitações da sociedade civil é através de acordo com outros homens para se associarem e se unirem em uma comunidade para uma vida confortável, segura e pacífica uns com os outros, desfrutando com segurança de suas propriedades e melhor protegidos contra aqueles que não são daquela comunidade. Esses homens podem agir desta forma porque isso não prejudica a liberdade dos outros, que permanecem como antes, na liberdade do estado de natureza. Quando qualquer número de homens decide constituir uma comunidade ou um governo, isto os associa e eles formam um corpo político em que a maioria tem o direito de agir e decidir pelo restante.

[...]

123. Se o homem é tão livre no estado de natureza como se tem dito, se ele é o senhor absoluto de sua própria pessoa e de seus bens, igual aos maiores e súdito de ninguém, por que renunciaria a sua liberdade, a este império, para sujeitar-se à dominação e ao controle de qualquer outro poder? A resposta é evidente: ainda que no estado de natureza ele tenha tantos direitos, o gozo deles é muito precário e constantemente exposto às invasões de outros. Todos são tão reis quanto ele, todos são iguais, mas a maior parte não respeita estritamente, nem a igualdade nem a justiça, o que torna o gozo da propriedade que ele possui neste estado muito perigoso e muito inseguro. Isso faz com que ele deseje abandonar esta condição, que, embora livre, está repleta de medos e perigos contínuos; e não é sem razão que ele solicita e deseja se unir em sociedade com outros, que já estão reunidos ou que planejam se unir, visando a salvaguarda mútua de suas vidas, liberdades e bens, o que designo pelo nome geral de propriedade.

[...]

131. Mas, embora os homens ao entrarem na sociedade renunciem à igualdade, à liberdade e ao poder executivo que possuíam no estado de natureza, que é então depositado nas mãos da sociedade, para que o legislativo deles disponha na medida em que o bem da sociedade assim o requeira, cada um age dessa forma apenas com o objetivo de melhor proteger sua liberdade e sua propriedade (pois não se pode supor que nenhuma criatura racional mude suas condições de vida para ficar pior), e não se pode jamais presumir que o poder da sociedade, ou o poder legislativo por ela instituído, se estenda além do bem comum; ele tem a obrigação de garantir a cada um sua propriedade, remediando aqueles três defeitos acima mencionados que tornam o estado de natureza tão inseguro e inquietante. Seja quem for que detenha o poder legislativo, ou o poder supremo, de uma comunidade civil, deve governar através de leis estabelecidas e permanentes, promulgadas e conhecidas do povo, e não por meio de decretos improvisados; por juízes imparciais e íntegros, que irão decidir as controvérsias conforme estas leis; e só deve empregar a força da comunidade, em seu interior, para assegurar a aplicação destas leis, e, no exterior, para prevenir ou reparar as agressões do estrangeiro, pondo a comunidade ao abrigo das usurpações e da invasão. E tudo isso não deve visar outro objetivo senão a paz, a segurança e o bem público do povo [109].

Sob a mesma roupagem, Rousseau denomina essa reunião de vontades dos indivíduos de contrato social:

VI – Do pacto social.

> Eu imagino os homens chegados ao ponto em que os obstáculos, prejudiciais à sua conservação no estado natural, os arrastam, por sua resistência, sobre as forças que podem ser empregadas por cada indivíduo a fim de se manter em tal estado. Então esse estado primitivo não mais tem condições de subsistir, e o gênero humano pereceria se não mudasse sua maneira de ser.
>
> Ora, como é impossível aos homens engendrar novas forças, mas apenas unir e dirigir as existentes, não lhes resta outro meio, para se conservarem, senão formando, por agregação, uma soma de forças que possa arrastá-los sobre a resistência, pô-los em movimento por um único móbil e fazê-los agir de comum acordo.
>
> Essa soma de forças só pode nascer do concurso de diversos; contudo, sendo a força e a liberdade de cada homem os primeiros instrumentos de sua conservação, como as empregará ele, sem se prejudicar, sem negligenciar os cuidados que se deve? Esta dificuldade, reconduzida ao meu assunto, pode ser enunciada nos seguintes termos.
>
> "Encontrar uma forma de associação que defenda e proteja de toda a força comum a pessoa e os bens de cada associado, e pela qual, cada um, unindo-se a todos, não obedeça portanto senão a si mesmo, e permaneça tão livre como anteriormente." Tal é o problema fundamental cuja solução é dada pelo contrato social.
>
> [...]
>
> Portanto, se afastarmos do pacto social o que não constitui a sua essência, acharemos que ele se reduz aos seguintes termos:
>
> "Cada um de nós põe em comum sua pessoa e toda a sua autoridade, sob o supremo comando da vontade geral, e recebemos em conjunto cada membro como parte indivisível do todo."
>
> Logo, ao invés da pessoa particular de cada contratante, esse ato de associação produz um corpo moral e coletivo, composto de tantos membros quanto a assembléia de vozes, o qual recebe desse mesmo ato sua unidade, seu eu comum, sua vida e sua vontade. A pessoa pública, formada assim pela união de todas as outras, tomava outrora o nome de cidade (3), e toma hoje o de república ou corpo político, o qual é chamado por seus membros: Estado, quando é passivo; soberano, quando é ativo; autoridade, quando comparado a seus semelhantes. No que concerne aos associados, adquirem coletivamente o nome de povo, e se chamam particularmente cidadãos, na qualidade de participantes na autoridade soberana, e vassalos, quando sujeitos às leis do Estado [110].

Em outros termos, o surgimento do Estado decorre de um pacto social, a partir da ideia que uma instituição de poder supra individual promoveria segurança aos indivíduos, evitando que as disputas fossem resolvidas pela autotutela. Em troca de ceder parcela de sua infinita liberdade (o estado da natureza), o Estado regeria as relações entre os indivíduos.

Contemporaneamente, isso significa que o Estado detém a atribuição de estabelecer regramentos e adotar medidas para o bem estar da sociedade. Tome-se como exemplo, para melhor compreensão, o poder de polícia.

O poder de polícia encontrou definição positivada no Código Tributário Nacional[3]:

> Art. 78. Considera-se poder de polícia atividade da administração pública que, limitando ou disciplinando direito, interesse ou liberdade, regula a prática de ato ou abstenção de fato, em razão de interesse público concernente à segurança, à higiene, à ordem, aos costumes, à disciplina da produção e do mercado, ao exercício de atividades econômicas dependentes de concessão ou

[3] Apesar da definição legal constar do Código Tributário Nacional, a sua definição é aplicada nos demais ramos do direito, não se restringindo ao contexto do CTN.

> autorização do Poder Público, à tranquilidade pública ou ao respeito à propriedade e aos direitos individuais ou coletivos.

Extremamente interessante é cotejar os conceitos doutrinários do poder de polícia a partir dos textos dos filósofos contratualistas. Para Celso Antônio Bandeira de Mello poder de polícia se traduz:

> [...] a atividade da Administração Pública, expressa em atos normativos ou concretos, de condicionar, com fundamento em sua supremacia geral e na forma da lei, a liberdade e a propriedade dos indivíduos, mediante ação ora fiscalizadora, ora preventiva, ora repressiva, impondo coercitivamente aos particulares um dever de abstenção ('non facere') a fim de conforma-lhes os comportamentos aos interesses sociais consagrados no sistema normativo [111].

Carvalho Filho bem registra a definição de Marcelo Caetano:

> É o modo de atuar da autoridade administrativa que consiste em intervir no exercício das atividades individuais suscetíveis de fazer perigar interesses gerais, tendo por objetivo evitar que produzam, ampliem ou generalizem os danos sociais que a lei procura prevenir.
>
> De nossa parte, entendemos se possa conceituar o poder de polícia como a prerrogativa de direito público que, calcada na lei, autoriza a Administração Pública a restringir o uso e o gozo da liberdade e da propriedade em favor do interesse da coletividade [112].

Marçal Justen Filho [113], por sua vez entende que *o poder de polícia administrativa é a competência para disciplinar o exercício da autonomia privada para a realização de direitos fundamentais e da democracia, segundo os princípios da legalidade e da proporcionalidade*.

O retrato da capacidade estatal de disciplinar a atuação dos particulares com o fito de promover o bem comum está revelada no dia a dia. Sem estabelecer uma diferenciação entre as atribuições da União, Estados (membros), Municípios e suas respectivas autarquias e agências reguladoras, é certo que é o Estado que:

1. certifica a habilitação para dirigir veículos automotores;
2. autoriza a abertura de empresas;
3. concede a terceiros a prestação de serviços públicos, como o de telecomunicações e energia elétrica;
4. concede o registro de medicamentos e produtos para saúde, atestando a sua qualidade, segurança e eficácia, o que possibilita sua oferta ao público;
5. regula uma infinidade de serviços (transporte terrestre, aquaviário, aviação civil; e
6. concede alvará, autorizando a realização de construções, dentre outras atividades.

Inexoravelmente, o Estado acessará dados pessoais dos indivíduos e isso ocorre do início ao final da vida das pessoas naturais ou jurídicas em virtude da necessidade de conferir segurança nas relações jurídicas, o que motivou a própria criação do Estado. Por exemplo, quando o Estado emite certidão de

nascimento comprova o início da pessoa natural, a nacionalidade, naturalidade, filiação, e as consequências advindas do nascimento de um indivíduo. Na outra ponta, quando certifica óbito determina a abertura da sucessão hereditária, afasta ou confirma comoriência, fixa termo final para extinção de contratos e outras repercussões decorrentes do falecimento de uma pessoa. Não é diferente com uma pessoa jurídica.

O importante é que a coleta desses dados esteja atrelada a uma competência de um órgão do Estado, que se volta por sua vez a prestar uma atividade para o próprio indivíduo ou para sociedade de maneira geral. Ou seja, a finalidade em última instância é pública. Há uma instrumentalidade, os dados são captados em decorrência da necessidade de se atingir a atribuição do órgão descrita na Lei. E nesse ponto, há uma grande diferença em relação ao dado captado pelas *big techs*. Nas entidades privadas o objetivo final é monetizar o dado, ampliando os lucros das empresas digitais.

Não se pode negar, outrossim, que a capacidade de coleta e cruzamento de dados pelo Estado, especificamente o Brasil, ainda se mostra quase que rudimentar quando comparamos com as empresas digitais. Tome-se como exemplo a concessão do Auxílio Emergencial, programa do governo que teve como objetivo atenuar os impactos financeiros decorrentes da pandemia de COVID-19. Em relatório da Controladoria-Geral da União, avaliando o programa no ano de 2021 (06.04.2021 a 19.11.2021), chegou-se à conclusão que foram pagos indevidamente o valor global de R$ 1.072.132.386,00 a 3.020.914 beneficiários. Deste universo, o pagamento foi realizado após o óbito a 118.060 beneficiários, 2.737 beneficiários tinham vínculo com o Poder Executivo Federal registrado no SIAPE, 595 beneficiários com vínculo ativo com empresas estatais federais, 1.091 beneficiários com vínculo ativo com as Forças Armadas, 81.227 beneficiários com vínculos em entes federativos (municipais, estaduais ou distritais). Dados que seriam facilmente cruzados com base de dados estatais. Sem referenciar aqueles que recebiam, simultaneamente, benefício previdenciário ou assistencial ou tinham renda familiar superior à permitida para concessão do Auxílio, situações que foram igualmente identificadas após uma avaliação da Controladoria-Geral da União. [114].

O Relatório constata um prejuízo superior a 1 bilhão de reais aos cofres públicos em decorrência da validação de concessão do Auxílio Emergencial a pessoas que não teriam o direito. Isto é, os sistemas utilizados pelo Ministério da Cidadania foram incapazes de detectar um grande número de inelegibilidades e impedir o pagamento indevido de benefícios. A própria CGU elenca entre as razões a deficiência na utilização e necessidade de ajustes de registros nas bases de dados.

Nesse caso, se fala do cruzamento de dados cadastrais, em bases governamentais, bem longe das informações colhidas pelas empresas privadas, de hábitos pessoais, locais frequentados, perfil de compras, poder aquisitivo, situações que, na maioria dos casos, ingressam na esfera de privacidade mais íntima do indivíduo.

Por conseguinte, aparentemente, a conduta estatal está muito mais aderente aos preceitos da Lei Geral de Proteção de Dados do que o comportamento das *big techs*. Fundamentos como autodeterminação informativa, respeito à privacidade, inviolabilidade da intimidade e da imagem e livre desenvolvimento da personalidade encontram mais fertilidade para se desenvolver no seio público do que em terreno privado.

Apesar dessas conclusões, percebe-se que há um certo discurso maniqueísta que aponta o Estado como a entidade que capta indevidamente os dados do cidadão para fins prejudiciais e, de outro lado, estão as empresas que "ofertam" aplicativos, ferramentas e sites gratuitamente, sem nada requerer do indivíduo. Isso se reflete, de maneira geral, na sociedade como um todo, incluído o Poder Judiciário.

Dados da própria Autoridade Nacional de Proteção de Dados (ANPD) sugerem que os entes públicos são objeto de maior fiscalização e rigor nas apurações. De acordo com lista de processos sancionatórios divulgada pela ANPD em 04.04.2023, existem na entidade 8 processos punitivos, dos quais apenas 1 não se refere ao setor público [115].

Todavia, recentemente, em abril de 2023, o Ministro do Supremo, Alexandre de Moraes, deu declarações referindo-se às *big techs* dizendo que é necessário exigir uma maior transparência dos algoritmos, não é possível tratar as plataformas como terra de ninguém [116]. Na sua compreensão, deve ocorrer uma regulação das plataformas digitais e eventual responsabilização pelo impulsionamento de conteúdo antidemocrático [117].

Esse movimento já foi trilhado pela Europa. Em julho de 2022, o Parlamento Europeu aprovou a Lei sobre Serviços Digitais (DSA), *Regulation* (EU) 2022/2065 [118] e o Regulamento sobre Mercados Digitais (DMA – *Digital Markets Act*), *Regulation* (EU) 2022/1925 [119].

Mostra-se, portanto, imperioso lançar luzes e comparar a conduta de entes privados na coleta de dados com órgãos públicos, desmistificando a instrumentalidade da coleta levada a efeito pelo Estado.

Deve-se lembrar, neste aspecto, pensamento da Professora Laura Schertel Mendes [120], segundo a qual não *existem mais dados insignificantes nas circunstâncias modernas do processamento automatizado dos dados", assim "o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados mesmos (ou no fato que quão sensíveis ou íntimos eles são)*".

7 A PRIVACIDADE, O COMPARTILHAMENTO DE DADOS E A GEOLOCALIZAÇÃO NA RECENTES DECISÕES JUDICIAIS NO BRASIL

Em pesquisas aprofundadas no sítio eletrônico do Supremo Tribunal Federal (STF) foi possível detectar decisões judiciais que abordam a questão da privacidade, da proteção de dados e da geolocalização.

O objetivo é destacar principalmente as decisões judicias mais recentes e que tem o condão de balizar o entendimento jurídico do Poder Judiciário e a reflexão dos estudiosos a respeito do tema objeto de aprofundamento.

É interessante, neste aspecto, utilizar uma metodologia que permita uma compreensão mais aprofundada dos julgados. Nesse sentido, destacaremos os principais julgados do STF e STJ em ordem cronológica.

Um tema que recorrentemente era discutido no âmbito do STF era a possibilidade de compartilhamento com o Ministério Público, para fins penais, dos dados bancários e fiscais, obtidos pela Receita Federal do Brasil (RFB) e pela Unidade de Inteligência Financeira (UIF) em suas atividades fiscalizatórias, sem autorização prévia do Poder Judiciário. O tema foi eleito pelo STF como de repercussão geral, sendo firmada, no âmbito do Recurso Extraordinário n° 1055941/SP [121], a seguinte tese:

> Tese: É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil, que define o lançamento do tributo, com os órgãos de persecução penal para fins criminais, sem a obrigatoriedade de prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional; II – O compartilhamento pela UIF e pela RFB, referente ao item anterior, deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.
>
> Acórdão: Constitucional. Processual Penal. Compartilhamento dos Relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil com os órgãos de persecução penal para fins criminais. Desnecessidade de prévia autorização judicial. Constitucionalidade reconhecida. Recurso ao qual se dá provimento para restabelecer a sentença condenatória de 1º grau. Revogada a liminar de suspensão nacional (art. 1.035, § 5º, do CPC). Fixação das seguintes teses: 1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil - em que se define o lançamento do tributo - com os órgãos de persecução penal para fins criminais sem prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional; 2. O compartilhamento pela UIF e pela RFB referido no item anterior deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios. (RE 1055941/SP. Rel. Min. Dias Toffoli. Data do julgamento: 04/12/2019. Data da Publicação: 18/03/2021).

Temos, neste julgado, dois pontos de essencial interesse.

O STF entendeu pela possibilidade de compartilhamento, para fins penais, de dados protegidos pelo sigilo fiscal e bancário entre a RFB e UIF e o Ministério Público, sem qualquer necessidade de decisão ou autorização judicial. Isso significa que a RFB e a UIF podem repassar dados que foram obtidos em sua atividade fiscalizatória ao Ministério Público. A linha de raciocínio utilizada é que se órgãos de fiscalização se depararem com indícios de infração penal é imperioso que promovam as devidas providências, repassando ao titular da ação penal, as informações, ainda que revestidas de sigilo fiscal e bancário. Tal providência estaria no contexto de obrigação funcional e institucional da RFB e da UIF por força do arcabouço normativo, restando esvaziada uma decisão judicial que lhes autorizasse o compartilhamento.

Sob outra vertente, ainda que considerando que os dados fiscais e bancários foram colhidos em atividade fiscalizatória da RFB e da UIP, o STF entendeu que seria possível o seu compartilhamento com o Ministério Público, mesmo para fins penais. Isto é, dados sigilosos que foram coletados sem uma autorização judicial e no contexto de poder de polícia administrativo poderiam dar ensejo a uma investigação criminal e, em última instância, motivar a propositura de uma ação penal.

Na mesma linha é possível encontrar o RE 1296829/RS [122] possibilitando o compartilhamento de dados entre a Receita Federal do Brasil e o Ministério Público Eleitoral.

> Tese: Constitucionalidade do compartilhamento com o Ministério Público Eleitoral, para fins de apuração de irregularidades em doações eleitorais, dos dados fiscais de pessoas físicas e jurídicas obtidos com base em convênio firmado entre a Receita Federal e o Tribunal Superior Eleitoral, sem autorização prévia do Poder Judiciário.
>
> Acórdão: RECURSO EXTRAORDINÁRIO REPRESENTATIVO DA CONTROVÉRSIA. ELEITORAL. DOAÇÃO DE RECURSOS ACIMA DO LIMITE LEGAL. MINISTÉRIO PÚBLICO ELEITORAL. OBTENÇÃO DE DADOS FISCAIS DO DOADOR SEM PRÉVIA AUTORIZAÇÃO JUDICIAL. PORTARIA CONJUNTA SRF-TSE 74/2006. QUEBRA DO SIGILO FISCAL. LICITUDE DA PROVA. RELEVÂNCIA DA QUESTÃO CONSTITUCIONAL. MANIFESTAÇÃO PELA EXISTÊNCIA DE REPERCUSSÃO GERAL. (RE 1296829 RG/RS. Rel. Min. Luiz Fux. Data do Julgamento: 17/12/2020. Data da publicação: 08/01/2021.)

As decisões demonstram que o STF não é contrário ao compartilhamento de dados, mas é necessário que órgãos envolvidos atendam condições e demonstrem a necessidade dessa partilha. Isso é confirmado nos julgados seguintes.

Já durante a pandemia da COVID 19, o Governo Federal editou a Medida Provisória n° 954/2020, de 17/04/2020. A norma determinava que a empresas de telecomunicações, prestadoras do Serviço Telefônico Fixo Comutado (STFC) e do Serviço Móvel Pessoal (SMP), compartilhassem com o IBGE a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas e jurídicas. O objetivo seria que o IBGE a partir dessas informações pudesse continuar realizando suas pesquisas para elaboração de relatórios oficiais estatísticos sem a necessidade de visitas domiciliares, em virtude das medidas de restrição de locomoção e contato em face da situação de emergência de saúde.

Algumas entidades ingressaram com uma Ação Direta de Inconstitucionalidade, a ADI 6387/DF [123], requerendo, inclusive, uma medida cautelar em face da Medida Provisória 954/2020. Em 07/05/2020, a Ministra Relatora, Rosa Weber, proferiu decisão, referendada pelo Pleno, na medida cautelar:

> MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO.
>
> 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.
>
> 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. **O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados**.
>
> 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d").
>
> 4. **Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia**.
>
> 5. **Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades**.
>
> 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros.
>
> 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada.
>
> 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020.
>
> 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição.
>
> 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à

> intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada. (Grifos nossos) (MC na ADI 6387/DF. Rel. Min. Rosa Weber. Data do Julgamento: 07/05/2020. Data da Publicação: 12/11/2020.

Algumas passagens da decisão mostram que não há impedimento intransponível que impeça o compartilhamento dos dados dos usuários dos serviços de STFC e SMP com o IBGE. Veja-se os seguintes trechos da decisão judicial que fazem referência aos termos em que editada a Medida Provisória: *O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados; (...) não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia; Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades*.

O que resta evidente pela leitura da decisão na Medida Cautela na ADI 6387/DF (BRASIL, 2020)[123] é que a Medida Provisória n° 954/2020 não atendeu às condições normativas indispensáveis para que ocorresse o compartilhamento de dados entre as empresas de telecomunicações e o IBGE. Na decisão judicial não se veda a possibilidade de compartilhamento em si, apenas se diz que, naqueles moldes, a partir do texto da MP 954/2020, não seria possível.

Interessante compreensão acerca da privacidade e do fornecimento de dados pessoais é possível verificar na ADI 4924/DF [124]. Nesta Ação Direta de Inconstitucionalidade, a Associação Nacional das Operadoras Celulares – ACEL questionou a constitucionalidade de Lei do Estado do Paraná que obrigava as empresas de telefonia celular a fornecer os dados cadastrais dos usuários que tivessem praticado trote em ligações para os serviços de emergência do Paraná. A partir desses dados o Estado do Paraná objetivava punir administrativamente o usuário infrator. Veja-se a decisão:

> Ação direta de inconstitucionalidade. Constitucional. Administrativo. Direitos fundamentais. Lei 17.107/12, do Estado do Paraná, que dispõe sobre penalidades ao responsável pelo acionamento indevido dos serviços telefônicos de atendimento a emergências envolvendo remoções ou resgates, combate a incêndios, ocorrências policiais ou atendimento de desastres (trote telefônico). [...]
>
> 5. Alegação de inconstitucionalidade material, por suposta violação ao direito à privacidade, pela quebra do sigilo de dados sem ordem judicial e em situação desproporcional – art. 5º, X e XII, da CF. Proporcionalidade da medida, desde que observadas as exigências que decorrem dos dispositivos constitucionais indicados. Quebra de sigilo limitada aos dados pessoais. Exigência de um procedimento administrativo em curso. Infração administrativa grave, com possíveis repercussões criminais e potencial de produzir considerável risco à comunidade.
>
> 6. Conhecimento parcial da ação, apenas em relação ao art. 2º, caput, e § 1º. Quanto a estes, pedido julgado improcedente. (ADI 4924/DF. Rel. Min. Gilmar Mendes. Data do Julgamento: 04/11/2021. Data da publicação: 29/03/2022)

Em outros termos, o STF entendeu ser possível que as empresas de telefonia celular fossem instadas a fornecer dados de usuário, sem a necessidade de uma decisão judicial, a partir de um número telefônico, em

decorrência de um fato determinado (um trote) em apuração em um processo administrativo (não criminal). O STF admite repasse de dados de usuário pelas empresas de telefonia em virtude de solicitação estatal para instrução de processo administrativo punitivo.

Em outro julgado, ADI 6529/DF [125], o Supremo Tribunal Federal analisou questionamento acerca da constitucionalidade do parágrafo único do art. 4° da Lei 9883/99 (Lei que institui o Sistema Brasileiro de Inteligência e cria a Agência Brasileira de Inteligência). Vejamos a redação do dispositivo:

> Art. 4°
>
> [...]
>
> Parágrafo único. Os órgãos componentes do Sistema Brasileiro de Inteligência fornecerão à ABIN, nos termos e condições a serem aprovados mediante ato presidencial, para fins de integração, dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais.

O cerne da questão envolveu a compreensão a respeito do compartilhamento de dados entre os órgãos componentes do Sistema Brasileiro de Inteligência.

> AÇÃO DIRETA DE INCONSTITUCIONALIDADE. AÇÃO PARCIALMENTE CONHECIDA: PARÁGRAFO ÚNICO DO ART. 4º DA LEI N. 9.883/1999. VEDAÇÃO AO ABUSO DE DIREITO E AO DESVIO DE FINALIDADE. OBRIGATORIEDADE DE MOTIVAÇÃO DO ATO ADMINISTRATIVO DE SOLICITAÇÃO DE DADOS DE INTELIGÊNCIA AOS ÓRGÃOS DO SISTEMA BRASILEIRO DE INTELIGÊNCIA. NECESSÁRIA OBSERVÂNCIA DA CLÁUSULA DE RESERVA DE JURISDIÇÃO. CONFIRMAÇÃO DA CAUTELAR DEFERIDA PELO PLENÁRIO. AÇÃO JULGADA PARCIALMENTE PROCEDENTE PARA DAR INTERPRETAÇÃO CONFORME AO PARÁGRAFO ÚNICO DO ART. 4º DA LEI N. 9.883/1999.
>
> 1. A jurisprudência deste Supremo Tribunal é firme no sentido da necessidade de se identificarem as normas questionadas na ação direta de inconstitucionalidade, esclarecendo-se os argumentos justificadores do pleito. Ação conhecida parcialmente, quanto ao parágrafo único do art. 4º da Lei n. 9.883/1999.
>
> 2. A efetividade das atividades de inteligência associa-se, com frequência, ao caráter sigiloso do processo e das informações coletadas. No Estado Democrático de Direito essa função submete-se ao controle externo do Poder Legislativo (inc. X do art. 49 da Constituição) e do Poder Judiciário (inc. XXXV do art. 5º da Constituição) para aferição da adequação do sigilo decretado às estritas finalidades públicas a que se dirige.
>
> 3. Para validade do texto legal e integral cumprimento ao comando normativo infralegal do Poder Executivo, há de se adotar como única interpretação e aplicação juridicamente legítima aquela que conforma a norma à Constituição da República. É imprescindível vincularem-se os dados a serem fornecidos ao interesse público objetivamente comprovado e com motivação específica.
>
> 4. O fornecimento de informação entre órgãos que não cumpra os rigores formais do direito nem atenda estritamente ao interesse público, rotulado legalmente como defesa das instituições e do interesse nacional, configura abuso do direito, contrariando a finalidade legítima posta na norma legal.
>
> 5. Práticas de atos contra ou à margem do interesse público objetivamente demonstrado, especificado em cada categoria jurídica, devem ser afastadas pelo Poder Judiciário, quando comprovado o desvio de finalidade.
>
> 6. A ausência de motivação expressa impede o exame da legitimidade de atos da Administração Pública, incluídos aqueles relativos às atividades de inteligência, pelo que a motivação é imprescindível.

> 7. A prática de atos motivados pelo interesse público não torna juridicamente válidos comportamentos de órgãos do Sistema Brasileiro de Inteligência para fornecerem à ABIN dados configuradores de quebra do sigilo telefônico ou de dados. Competência constitucional do Poder Judiciário.
>
> 8. Ação direta de inconstitucionalidade julgada parcialmente procedente para, confirmando-se o julgado cautelar, dar interpretação conforme ao parágrafo único do art. 4º da Lei n. 9.883/1999 estabelecendo-se que: **a) os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados; b) qualquer solicitação de dados deverá ser devidamente motivada para eventual controle de legalidade pelo Poder Judiciário; c) mesmo presente interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo legal, decorrente do imperativo de respeito aos direitos fundamentais; d) nas hipóteses cabíveis de fornecimento de informações e dados à ABIN, são imprescindíveis procedimento formalmente instaurado e existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abuso**. Grifos nossos. (ADI 6529/DF. Rel. Min. Carmen Lúcia. Data do Julgamento: 11/10/2021. Data da Publicação: 22/10/2021)

Analisando-se o julgado, percebe-se que o STF reafirma três princípios administrativo constitucionais quando estabelece a interpretação do parágrafo único do art. 4° da Lei n° 9883/99.

O primeiro é a necessidade que esteja presente o interesse público quando do compartilhamento de informações entre os órgãos integrantes do SISBIN. O princípio da impessoalidade inserto no caput do art. 37 da Constituição Federal impede que qualquer ato administrativo em qualquer instância e esfera de um órgão público, seja federal, estadual e municipal, tenha por motivação interesses pessoais ou privados.

O segundo é a fundamentação do ato administrativo. As solicitações de compartilhamento de informações devem conter os motivos, as razões que impulsionam o solicitante a requerer os dados e informações.

Por último, já na alínea "d", o STF menciona a necessidade que exista um procedimento formal em que se registre e identifique os servidores públicos que tiveram acesso às informações repassadas por outros órgãos.

Tais assertivas, alíneas "a)", "b)" e "d)", encerram comandos para a ABIN e os órgãos que compõem o Sistema Brasileiro de Inteligência coincidentes com a Constituição Federal e, principalmente, com a Lei n° 9784/99, que regula o processo administrativo no âmbito da administração pública federal. São práticas administrativas que deveriam ser adotadas por todos órgãos públicos (inclusive estaduais e municipais) antes mesmo da edição da Lei n° 9.784/99 porque decorrem de princípios constitucionais da legalidade, impessoalidade e eficiência.

Quanto à alínea "c" do item 8 do julgado, não há reparos a serem anotados. Os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados sob pena

de se extrapolar o âmbito da investigação criminal para órgãos que não detém atribuições de persecução penal. A produção de conhecimento destinada a assessorar o Presidente da República não passa pela edição de relatório de inteligência ou informe que aborde estritamente inquérito policial ou ação penal em que se projeta uma condenação criminal.

Ademais, não se deve olvidar, quando se compulsa a Política Nacional de Inteligência e a Estratégia Nacional de Inteligência percebe-se que existem diversos temas a serem acompanhados pela Inteligência Nacional. Daí que não se deve resumir o papel de um órgão de inteligência de Estado ao contexto de segurança pública.

Por fim, há que se destacar ainda o julgamento de mérito na Arguição de Descumprimento de Preceito Fundamental tombada sob o n° 695. Nesta ação, um partido político questionou o compartilhamento da base de dados do Departamento Nacional de Trânsito (DENATRAN), hospedada no SERPRO (Serviço Federal de Processamento de Dados).

A Corte Constitucional estabeleceu como paradigma os contornos da decisão ADI 6529/DF (comentada acima):

> 4. O compartilhamento de informações pessoais em atividades de inteligência observará o disposto em legislação específica e os parâmetros fixados no julgamento da ADI 6.529, Rel. Min. Cármen Lúcia, quais sejam: (i) adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; (ii) instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; (iii) utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e (iv) observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal. (BRASIL, 2022) (ADPF 695/DF. Rel Min. Gilmar Mendes. Data de Julgamento: 15/09/2022. Ata de julgamento publicada no DJE de 23/09/2022)

Um gradiente que foi acrescentado nesta última decisão sobre o assunto, em setembro de 2022, é o item "iv". O STF, talvez vislumbrando um horizonte amplo para aprovação de uma legislação específica que discipline a atividade de tratamento de dados pessoais na esfera penal e de inteligência, entendeu pela aplicação, no que couber, dos princípios gerais e direitos disciplinados na LGPD no compartilhamento de informações pessoais em atividades de inteligência. O posicionamento do STF não descura que a proteção dos dados pessoais foi alçada a direito fundamental com a aprovação da Emenda Constitucional n° 115, de 10 de fevereiro de 2022, o que significa que a LGPD deve funcionar como uma bússola na definição de condutas a serem adotadas no compartilhamento de dados relacionados à segurança nacional e segurança do Estado, temas que foram excluídos da abrangência da Lei.

Especificamente em relação à geolocalização, alguns Estados como Rondônia, [126], Piauí, [127], e Minas Gerais, [128], editaram leis estaduais com o fito de obrigar as prestadoras de telefonia fixa e móvel a informarem a localização dos aparelhos às autoridades policiais quando requisitadas as informações. O assunto foi objeto de Ações Declaratórias de Inconstitucionalidade, à exemplo do leading case ADI 4401:

> Ação direta de inconstitucionalidade. 2. Lei 18.721/2010 do Estado de Minas Gerais, que dispõe sobre o fornecimento de informações por concessionária de telefonia fixa e móvel para fins de segurança pública. 3. Competência privativa da União para legislar sobre telecomunicações. Violação ao art. 22, inciso IV, da Constituição. Precedentes. 4. Ação direta de inconstitucionalidade julgada procedente, confirmando os termos da medida cautelar anteriormente deferida, para declarar a inconstitucionalidade da Lei 18.721/2010, do Estado de Minas Gerais.

Nos julgados mencionados, ADI 4739, ADI 5040 e ADI 4401, o que se observa é que o Pretório Excelso reconheceu a inconstitucionalidade das legislações estaduais, mas não porque a medida que se buscava impor às prestadoras afrontava a privacidade do usuário. O que motivou a declaração de inconstitucionalidade foi o reconhecimento de que os Estados não detêm competência para legislar sobre telecomunicações. E nesse aspecto é importante destacarmos o Voto do Ministro Relator na ADI 4739 [126]:

> No rol das garantias constitucionais desfrutadas pelos brasileiros e estrangeiros – pressupostos da estabilidade e da segurança demandadas pela vida gregária –, figura a inviolabilidade do sigilo "de dados e das comunicações telefônicas", a teor do inciso XII do artigo 5º da Constituição Federal. Eis a regra geral consagrada no texto constitucional, correndo a exceção à conta de atuação do Estado-juiz por meio da formalização de decisão fundamentada, nas situações e formas contempladas em lei.
>
> Fixada a premissa, indaga-se: ao impor às companhias operadoras de telefonia móvel a obrigação de fornecer à polícia judiciária estadual, ante solicitação, a localização dos aparelhos utilizados pelos usuários, a norma questionada institui hipótese de afastamento de sigilo de dados, ausente submissão ao crivo de órgão judicial equidistante, a vulnerar a privacidade do cidadão?
>
> A resposta é negativa. Surge impertinente, tendo em vista mera autorização ao compartilhamento de "informações sobre a localização de aparelhos de clientes", articular com a existência de quebra de sigilo, a qual, todos o sabem, constitui prerrogativa do Judiciário.
>
> A razão é única: conforme assentado, pelo Pleno, no julgamento do recurso extraordinário nº 389.808, da minha relatoria, com acórdão publicado no Diário da Justiça de 10 de maio de 2011, a vedação contida no inciso XII do artigo 5º refere-se à correspondência, às comunicações e aos dados porventura existentes nos referidos aparelhos, alcançando não apenas as chamadas telefônicas realizadas e recebidas mas também o acesso à agenda eletrônica e ao conteúdo das mensagens de texto, arquivos e documentos eletrônicos.
>
> Tem-se circunstância diversa considerada a diretriz normativa constante do diploma impugnado, o qual não trata de acesso às informações, às mensagens ou a quaisquer dados armazenados em aparelho celular, versando apenas a comunicação, à autoridade policial, de informação alusiva à localização do dispositivo móvel – a qual não se enquadra no conceito de "dado", na forma tutelada pelo constituinte. (ADI 4739. Rel. Min. Marco Aurélio de Mello. Data do Julgamento: 17/02/2021. Data da publicação: 15/04/2021)

O que se observa pela análise acima é que as decisões judiciais transparecem o posicionamento do Supremo Tribunal Federal principalmente em relação ao tratamento e coleta de dados e o direito fundamental à privacidade. O ponto convergente é que não há vedação absoluta e intransponível ao compartilhamento de dados pessoais de indivíduos entre órgãos públicos, sendo, no entanto, indispensável atender a algumas condições.

8 JUÍZO DE PONDERAÇÃO. PRIVACIDADE X INTERESSE PÚBLICO. O USO DA GEOLOCALIZAÇÃO DE DADOS ESTÁTICOS

No capítulo anterior concluímos que existem condições para que o tratamento de dados seja realizado preservando-se a privacidade do indivíduo e respeitando-se, especialmente, os princípios da finalidade, adequação, necessidade e segurança. Além das disposições da Lei Geral de Proteção de Dados, o STF continuamente reafirmou em seus julgados a necessidade de observância dos princípios vetores para a proteção dos dados e, consequentemente da privacidade.

No campo da inteligência, a Corte Suprema indicou diretrizes para o escorreito compartilhamento de dados no âmbito do SISBIN e entre órgãos da administração pública federal.

Concretamente estão sedimentadas as condições para a transição da natureza do direito à privacidade, naquilo que Rodotà [129] concebeu como a mudança de paradigma de "pessoa-informação-segredo" para "pessoa-informação-circulação-controle".

Mas existem situações em que o direito à privacidade (art. 5°, inciso X) e o direito à proteção de dados (art. 5°, inciso LXXIX), ambos com sede constitucional, colidem com outros direitos igualmente contemplados na Constituição Federal. Esse choque entre direitos fundamentais motivou a elaboração de teorias voltadas a tentar solucionar essa aparente antinomia da Lei Maior[1].

Um dos maiores expoentes do constitucionalismo, o alemão Robert Alexy [11] propôs em seu livro a Teoria dos Direitos Fundamentais (*Theorie der Grundrechte*) a "lei da colisão". Assim, para Alexy *a solução consiste no estabelecimento de uma relação de precedência condicionada entre os princípios, com base nas circunstâncias do caso concreto*.

Didaticamente, Sarmento [130] explica que a ponderação de interesses consiste em um equacionamento do problema para a resolução dos conflitos constitucionais a partir de um método casuístico em que se utiliza o princípio da proporcionalidade.

Esse juízo de ponderação, que se traduz no sopesamento (*Abwagung*, na dogmática constitucional alemã) de interesses que se sobrelevam no exame do caso em concreto, foi objeto de interessante estudo em sede de tese de doutorado de Paulo Gustavo Gonet Branco, na Universidade de Brasília, originando, na sequência, a obra Juízo de Ponderação na Jurisdição Constitucional. O escólio traz essencial raciocínio:

[1] Se diz aparente porque o ordenamento jurídico é concebido como uma unidade. Como um sistema, deve-se compreender cada regra e princípio a partir da sua relação harmônica com os demais.

> Desse modo, enquanto um princípio pode ser cumprido em maior ou menor escala, "as regras somente podem ser cumpridas ou não. Se uma regra é válida, então há de se fazer exatamente o que ela exige, sem mais nem menos".
>
> A distinção se torna crucial para apreender as peculiaridades dos conflitos entre direitos fundamentais. A estrutura que se observa num caso de colisão de regras distancia-se daquela que peculiariza uma colisão de princípios.
>
> A colisão de princípios, da mesma forma que a colisão de regras, refere-se à situação em que a aplicação de ambas as normas ao caso concreto engendra consequências contraditórias entre si. A solução para o conflito entre regras, porém, não é a mesma para o caso de colisão entre princípios.
>
> Um conflito entre regras é solucionado tomando-se uma das regras como cláusula de exceção da outra ou declarando-se inválida uma delas.
>
> Já os princípios, quando se contrapõem, não estariam exatamente em contradição, mas em tensão, que deve ser resolvida com referência ao caso que, à primeira vista, os atrai. Os princípios apresentam pesos ou importâncias diferentes para o caso analisado, mesmo que, considerados em abstrato, nenhum ostente primazia sobre o outro. O que há de se realizar é uma ponderação entre os princípios, com vistas a apurar qual o que se refere a interesse de maior monta no episódio a ser avaliado [131].

À título de exemplo da colidência de princípios e regras constitucionais é possível citar diversas situações em concreto.

O STF ao julgar a ADI 3311/DF [132] entendeu que a propaganda comercial (exercício da liberdade de expressão) de produtos derivados do tabaco encontra-se limitada em face da tutela da saúde e da proteção da criança e do adolescente.

> AÇÃO DIRETA DE INCONSTITUCIONALIDADE. ART. 3º, CAPUT e §§ 2º, 3º, 4º, 5º E 6º, DA LEI Nº 9.294/1996. PRODUTOS FUMÍGENOS, DERIVADOS OU NÃO DO TABACO. RESTRIÇÕES À PROPAGANDA COMERCIAL. ADVERTÊNCIAS SANITÁRIAS NAS EMBALAGENS. PRELIMINARES REJEITADAS. ADITAMENTO ACOLHIDO. EPIDEMIA DO TABAGISMO. CONVENÇÃO-QUADRO DAS NAÇÕES UNIDAS PARA O CONTROLE DO TABACO (CQCT). OBSERVÂNCIA DO PRINCÍPIO DA PROPORCIONALIDADE. PREVALÊNCIA DA TUTELA DA SAÚDE. PRIORIDADE ABSOLUTA DA PROTEÇÃO DE CRIANÇAS E ADOLESCENTES. CONCRETIZAÇÃO DOS OBJETIVOS FUNDAMENTAIS DA REPÚBLICA. IMPROCEDÊNCIA.
>
> [...]
>
> 3. A propaganda comercial encontra proteção constitucional, por ser manifestação da liberdade de expressão e comunicação. Na arquitetura dos direitos fundamentais, que não comporta direitos absolutos, sujeita-se a restrições, desde que proporcionais, na proteção de outros valores públicos.
>
> 4. A atividade empresarial, em todas as suas facetas, inclusive a publicitária, submete-se aos princípios da ordem econômica e há compatibilizar-se com a concretização dos demais direitos fundamentais.
>
> 5. O art. 220, § 4º, CF, no sentido de que a propaganda do "tabaco, bebidas alcoólicas, agrotóxicos, medicamentos e terapias" pode sofrer "restrições legais" explicita a possibilidade e a importância das limitações publicitárias dos produtos notadamente nocivos.
>
> 6. A propaganda comercial pode sofrer restrição legal de variada intensidade e, de modo proporcional, ser afastada para a tutela de outros direitos fundamentais. A expressão "restrição", no art. 220, § 4º, CF, não traduz limitação apriorística à ponderação de valores resultante da aplicação do princípio da proporcionalidade no caso concreto.
>
> 7. Surgem constitucionais as restrições da publicidade dos produtos fumígenos, derivados ou não do tabaco, limitada à exposição dos produtos nos postos de venda, e a imposição de advertência sanitária acompanhada de imagem, por se mostraram adequadas, necessárias e proporcionais

em sentido estrito, no contexto multifacetado das políticas públicas de combate ao fumo e de controle do tabaco.

8. Prevalência da tutela da saúde (art. 6º, CF) e incidência da proteção prioritária da criança e do adolescente (art. 227, CF). Concretização dos objetivos fundamentais da República (art. 3º, CF), mediante o estabelecimento de limites à atividade empresarial, no trato de problema de saúde pública de grande proporção. Limitada a livre iniciativa, na dimensão expressiva e comunicativa, para a construção de uma sociedade mais livre, justa e solidária, o desenvolvimento nacional sustentável, a redução de desigualdades e a promoção do bem de todos. (ADI 3311/DF. Rel. Min. Rosa Weber. Data do Julgamento: 14/09/2022 Data da Publicação 29/09/2022)

Na ADI 4815 [133], a Suprema Corte julgou a liberdade de expressão e de informação versus o direito à intimidade e privacidade. Tratou-se da possibilidade de edição de biografias sem a necessidade de autorização prévia da pessoa, o que poderia caracterizar censura prévia.

AÇÃO DIRETA DE INCONSTITUCIONALIDADE. ARTS. 20 E 21 DA LEI N. 10.406/2002 (CÓDIGO CIVIL). PRELIMINAR DE ILEGITIMIDADE ATIVA REJEITADA. REQUISITOS LEGAIS OBSERVADOS. MÉRITO: APARENTE CONFLITO ENTRE PRINCÍPIOS CONSTITUCIONAIS: LIBERDADE DE EXPRESSÃO, DE INFORMAÇÃO, ARTÍSTICA E CULTURAL, INDEPENDENTE DE CENSURA OU AUTORIZAÇÃO PRÉVIA (ART. 5º INCS. IV, IX, XIV; 220, §§ 1º E 2º) E INVIOLABILIDADE DA INTIMIDADE, VIDA PRIVADA, HONRA E IMAGEM DAS PESSOAS (ART. 5º, INC. X). ADOÇÃO DE CRITÉRIO DA PONDERAÇÃO PARA INTERPRETAÇÃO DE PRINCÍPIO CONSTITUCIONAL. PROIBIÇÃO DE CENSURA (ESTATAL OU PARTICULAR). GARANTIA CONSTITUCIONAL DE INDENIZAÇÃO E DE DIREITO DE RESPOSTA. AÇÃO DIRETA JULGADA PROCEDENTE PARA DAR INTERPRETAÇÃO CONFORME À CONSTITUIÇÃO AOS ARTS. 20 E 21 DO CÓDIGO CIVIL, SEM REDUÇÃO DE TEXTO.

[...]

4. O direito de informação, constitucionalmente garantido, contém a liberdade de informar, de se informar e de ser informado. O primeiro refere-se à formação da opinião pública, considerado cada qual dos cidadãos que pode receber livremente dados sobre assuntos de interesse da coletividade e sobre as pessoas cujas ações, público-estatais ou público-sociais, interferem em sua esfera do acervo do direito de saber, de aprender sobre temas relacionados a suas legítimas cogitações.

5. Biografia é história. A vida não se desenvolve apenas a partir da soleira da porta de casa. 6. Autorização prévia para biografia constitui censura prévia particular. O recolhimento de obras é censura judicial, a substituir a administrativa. O risco é próprio do viver. Erros corrigem-se segundo o direito, não se coartando liberdades conquistadas. A reparação de danos e o direito de resposta devem ser exercidos nos termos da lei.

7. A liberdade é constitucionalmente garantida, não se podendo anular por outra norma constitucional (inc. IV do art. 60), menos ainda por norma de hierarquia inferior (lei civil), ainda que sob o argumento de se estar a resguardar e proteger outro direito constitucionalmente assegurado, qual seja, o da inviolabilidade do direito à intimidade, à privacidade, à honra e à imagem.

8. Para a coexistência das normas constitucionais dos incs. IV, IX e X do art. 5º, há de se acolher o balanceamento de direitos, conjugando-se o direito às liberdades com a inviolabilidade da intimidade, da privacidade, da honra e da imagem da pessoa biografada e daqueles que pretendem elaborar as biografias. (ADI 4815. Rel. Min. Carmen Lúcia. Data de Julgamento: 10/06/2015. Data de Publicação 01/02/2016)

Um outro caso julgado pelo STF [134], desta feita que equacionou o direito de greve de servidores da área policial e o interesse público na manutenção da segurança interna e ordem pública, merece o destaque.

CONSTITUCIONAL. GARANTIA DA SEGURANÇA INTERNA, ORDEM PÚBLICA E PAZ SOCIAL. INTERPRETAÇÃO TELEOLÓGICA DOS ART. 9 º, § 1 º, ART. 37, VII, E ART.

> 144, DA CF. VEDAÇÃO ABSOLUTA AO EXERCÍCIO DO DIREITO DE GREVE AOS SERVIDORES PÚBLICOS INTEGRANTES DAS CARREIRAS DE SEGURANÇA PÚBLICA.
>
> [...]
>
> 2. Aparente colisão de direitos. Prevalência do interesse público e social na manutenção da segurança interna, da ordem pública e da paz social sobre o interesse individual de determinada categoria de servidores públicos. Impossibilidade absoluta do exercício do direito de greve às carreiras policiais. Interpretação teleológica do texto constitucional, em especial dos artigos 9º, § 1º, 37, VII e 144. (RE 654432/GO. Rel Min. Edson Fachin. Redator do Acórdão Min. Alexandre de Moraes. Data do Julgamento: 05/04/2017. Data da Publicação: 11/06/2018)

Como se vê, são diversas situações no campo fático em que se verifica um conflito de dois princípios ou normas constitucionais sendo sopesadas pelo Supremo Tribunal Federal. Há hipóteses, igualmente, que sequer são judicializadas mas não deixam de merecer a devida atenção no campo acadêmico. Em pesquisas no google acadêmico é possível encontrar artigos que analisam o direito à privacidade x o direito à saúde/vida no contexto da pandemia.

Com a disseminação do coronavírus a partir do contato físico da pessoa infectada com outro indivíduo proliferaram medidas ao redor do mundo de restrições de locomoção e isolamento social. Uma das formas que autoridades propuseram para mensurar a movimentação das pessoas e, até, evitar ou minimizar o contágio pelo vírus, era verificar a geolocalização dos indivíduos por meio das prestadoras do serviço de SMP ou por Apps. Nesse contexto, alguns estudiosos [135], [136] e [16] acreditaram ser possível a flexibilização do direito à privacidade em virtude do direito à saúde pública.

O que se busca demonstrar com esse apanhado de decisões judiciais e opiniões doutrinárias é que não existe direito absoluto, conforme sobejamente declarado pelo STF.

Ingressando, especificamente, na questão da geolocalização constata-se que há inúmeras decisões do Superior Tribunal de Justiça possibilitando a denominada quebra de dados estáticos do usuário, resultando, dentre outras coisas, em sua geolocalização. Há quem se refira à medida como busca reversa de dados de localização [137].

Em princípio, deve-se recordar que a geolocalização através do acesso a dados estáticos permite que a investigação refaça trajetos dos indivíduos, realize o cruzamento de dados com câmeras de vigilância de vias públicas e de ambientes privados, estabeleça conexão entre pessoas que estiveram em locais diferentes (indivíduos que se portam como estranhos mas que estão em vários locais juntos). Em algumas ordens judiciais determina-se ao provedor de internet que informe se houve, naquela região e durante intervalo de tempo definido, alguma pesquisa em sites buscadores de palavra de termos ligados à vítima e seus hábitos ou elementos que tenham conexão com o crime perpetrado. Assim, a geolocalização de dados estáticos se mostra bastante efetiva mas é, sem dúvida nenhuma, muita mais invasiva à privacidade que a geolocalização em tempo real.

Esse ponto é importante considerando que a geolocalização de dados estáticos necessariamente resulta no acesso à localização e dados de pessoas que não estão vinculadas ao fato delituoso. Em outros termos,

o STJ entendeu que o acesso a dados de localização de indivíduos inocentes seria uma espécie de “dano colateral”, “mal menor” a ser suportado por qualquer pessoa em troca de se alcançar informações que pudessem indicar a autoria de um crime. Ou seja, afasta-se uma dimensão da esfera da privacidade de determinadas pessoas para que se atinja o interesse público de avanço de investigações de natureza criminal. Embora não o tenha realizado explicitamente, o STJ, nas entrelinhas, estabeleceu um segundo juízo de ponderação. Existe um ônus a ser suportado pela sociedade para que haja uma evolução e modernização das apurações de infrações penais. E esse ônus é relativizar sua privacidade. Daí que, neste caso, de fato se justifica uma autorização judicial para a medida.

Destaque-se o leading case:

> RECURSO EM MANDADO DE SEGURANÇA. DIREITO À PRIVACIDADE E À INTIMIDADE. IDENTIFICAÇÃO DE USUÁRIOS EM DETERMINADA LOCALIZAÇÃO GEOGRÁFICA. IMPOSIÇÃO QUE NÃO INDICA PESSOA INDIVIDUALIZADA. AUSÊNCIA DE ILEGALIDADE OU DE VIOLAÇÃO DOS PRINCÍPIOS E GARANTIAS CONSTITUCIONAIS. FUNDAMENTAÇÃO DA MEDIDA. OCORRÊNCIA. PROPORCIONALIDADE. RECURSO EM MANDADO DE SEGURANÇA NÃO PROVIDO.
>
> 1. Os direitos à vida privada e à intimidade fazem parte do núcleo de direitos relacionados às liberdades individuais, sendo, portanto, protegidos em diversos países e em praticamente todos os documentos importantes de tutela dos direitos humanos. No Brasil, a Constituição Federal, no art. 5º, X, estabelece que: "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". A ideia de sigilo expressa verdadeiro direito da personalidade, notadamente porque se traduz em garantia constitucional de inviolabilidade dos dados e informações inerentes a pessoa, advindas também de suas relações no âmbito digital.
>
> 2. Mesmo com tal característica, o direito ao sigilo não possui, na compreensão da jurisprudência pátria, dimensão absoluta. De fato, embora deva ser preservado na sua essência, este Superior Tribunal de Justiça, assim como a Suprema Corte, entende que é possível afastar sua proteção quando presentes circunstâncias que denotem a existência de interesse público relevante, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios que devem ser, em tese, suficientes à configuração de suposta ocorrência de crime sujeito à ação penal pública.
>
> 3. Na espécie, a ordem judicial direcionou-se a dados estáticos (registros), relacionados à identificação de usuários em determinada localização geográfica que, de alguma forma, possam ter algum ponto em comum com os fatos objeto de investigação por crimes de homicídio.
>
> 4. A determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, as quais dão acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. Há uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Decerto que o art. 5º, X, da CF/88 garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, o acesso a esses dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma.
>
> 5. Os dispositivos que se referem às interceptações das comunicações indicados pelos recorrentes não se ajustam ao caso sub examine. O procedimento de que trata o art. 2º da Lei n. 9.296/1996, cujas rotinas estão previstas na Resolução n. 59/2008 (com alterações ocorridas em 2016) do CNJ, os quais regulamentam o art. 5º, XII, da CF, não se aplica a procedimento que visa a obter dados pessoais estáticos armazenados em seus servidores e sistemas informatizados de um provedor de serviços de internet. A quebra do sigilo de dados, na hipótese, corresponde à obtenção de registros informáticos existentes ou dados já coletados.

> 6. Não há como pretender dar uma interpretação extensiva aos referidos dispositivos, de modo a abranger a requisição feita em primeiro grau, porque a ordem é dirigida a um provedor de serviço de conexão ou aplicações de internet, cuja relação é devidamente prevista no Marco Civil da Internet, o qual não impõe, entre os requisitos para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios.
>
> 7. Os arts. 22 e 23 do Marco Civil da Internet, que tratam especificamente do procedimento de que cuidam os autos, não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Assim, para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros. Não é necessário, portanto, que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação, tampouco que justifique a indispensabilidade da medida, ou seja, que a prova da infração não pode ser realizada por outros meios, o que, aliás, seria até, na espécie - se houvesse tal obrigatoriedade legal - plenamente dedutível da complexidade e da dificuldade de identificação da autoria mediata dos crimes investigados.
>
> 8. Logo, a quebra do sigilo de dados armazenados, de forma autônoma ou associada a outros dados pessoais e informações, não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas, até porque o objetivo precípuo dessa medida, na expressiva maioria dos casos, é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado.
>
> 9. Conforme dispõe o art. 93, IX, da CF, "todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação". Na espécie, tanto os indícios da prática do crime, como a justificativa quanto à utilização da medida e o período ao qual se referem os registros foram minimamente explicitados pelo Magistrado de primeiro grau.
>
> 10. Quanto à proporcionalidade da quebra de dados informáticos, ela é adequada, na medida em que serve como mais um instrumento que pode auxiliar na elucidação dos delitos, cuja investigação se arrasta por dois anos, sem que haja uma conclusão definitiva; é necessária, diante da complexidade do caso e da não evidência de outros meios não gravosos para se alcançarem os legítimos fins investigativos; e, por fim, é proporcional em sentido estrito, porque a restrição a direitos fundamentais que dela redundam - tendo como finalidade a apuração de crimes dolosos contra a vida, de repercussão internacional - não enseja gravame às pessoas eventualmente afetadas, as quais não terão seu sigilo de dados registrais publicizados, os quais, se não constatada sua conexão com o fato investigado, serão descartados.
>
> 11. Logo, a ordem judicial para quebra do sigilo dos registros, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, não se mostra medida desproporcional, porquanto, tendo como norte a apuração de gravíssimos crimes cometidos por agentes públicos contra as vidas de três pessoas - mormente a de quem era alvo da emboscada, pessoa dedicada, em sua atividade parlamentar, à defesa dos direitos de minorias que sofrem com a ação desse segmento podre da estrutura estatal fluminense - não impõe risco desmedido à privacidade e à intimidade dos usuários possivelmente atingidos pela diligência questionada.
>
> 12. Recurso em mandado de segurança não provido. (RMS 62143/RJ. Rel. Min. Rogério Schietti Cruz. Data de Julgamento: 26/08/2020. Data de Publicação: 08/09/2020) [138].

Alguns pontos que merecem o realce:

1. o direito à privacidade não possui, dimensão absoluta, sendo possível afastar sua proteção quando presentes circunstâncias que denotem a existência de interesse público relevante. Se dois enunciados normativos ou princípios constitucionais apontam para soluções divergentes em uma situação fática é necessária a solução do conflito pelo sopesamento dos valores envolvidos;

2. não se aplica ao caso o regramento da Lei n° 9.296/1996 porque não se trata de quebra de sigilo das

comunicações ou telemático; e

3. A medida de acesso aos dados estáticos é tida pelo STJ como mais um instrumento que pode auxiliar na elucidação dos delitos.

Isso significa que se trata de meio investigatório atípico que deve virar regra em inquéritos policiais.

Em relação ao último ponto, o que se constata é que de fato as investigações criminais passaram a utilizar a busca reversa de dados de localização (AgRg no HC 746463/RS, AgRg no RMS 68487/PE, AgRg no RMS 68119/RJ, AgRg no RMS 67750/SP, AgRg no RMS 66791/CE, AgRg no RMS 66668/MT).

Como dito, a quebra de sigilo de dados estáticos se mostra muito mais ampla que a simples busca pela localização em tempo real. As informações fornecidas pelas empresas de tecnologia, na hipótese da busca reversa de dados, englobam os registros de conexão, acesso a aplicações de internet, dados pessoais e de busca na internet de um universo de pessoas indeterminado. São dados que revelam com maior extensão e profundidade a vida privada do indivíduo. E de grande parte de pessoas que não são objeto de investigação.

Em última instância, no entanto, o que se observa é que não há direito absoluto e que, a partir da teoria da ponderação de interesses se mostra possível realizar a compressão do direito à privacidade quando em aparente confronto com situações de segurança do Estado e defesa nacional.

9 O USO DA GEOLOCALIZAÇÃO EM TEMPO REAL PELA INTELIGÊNCIA

Para delimitação do campo de atuação dos órgãos de inteligência é imperioso diferenciar precisamente as ferramentas e técnicas a serem utilizadas. Não se pode olvidar, por exemplo, que o constituinte brasileiro optou por restringir a quebra de sigilo das comunicações telefônicas para as hipóteses de investigação criminal ou instrução processual penal.

Especificamente em relação à geolocalização verifica-se que se notabilizou na jurisprudência a geolocalização estática, ou seja, aquela que se fundamenta nos artigos 22 e 23 do Marco Civil da Internet e busca o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Nesse manto estão abarcadas, dentre outras informações, buscas na internet, dados pessoais dos usuários, informações sobre proximidade e trajetos coincidentes de usuários e a localização aproximada de todos os indivíduos em determinada área delimitada em um intervalo de tempo. O pedido em si de busca reversa dos dados não engloba o registro e o conteúdo de ligações telefônicas, regido pela Lei n° 9296/96 e com requisitos mais rigorosos para o seu atendimento, assim como as informações fornecidas pelo responsável pela guarda não são obtidas através do serviço de telefonia celular.

A geolocalização em tempo real se volta a fornecer ao solicitante apenas a localização ou trajeto do usuário naquele exato momento. Nada a mais. Essa informação pode ser obtida pelas Estações Rádio Base ou através de dados de localização captados por aplicativos de celular ou sites da internet. O que muda é que o detentor do dado será originalmente a empresa de telecomunicações prestadora do SMP ou alguma big tech com quem o usuário compartilha voluntária ou involuntariamente sua localização. Secundariamente os dados de localização de um usuário obtidos por uma big tech podem ser compartilhados com outras empresas.

Com essas considerações, é importante correlacionar a geolocalização em tempo real, o que se pode chamar de localização eletrônica do indivíduo, com as praticas desenvolvidas “analogicamente”, à moda antiga, pelas polícias judiciárias e órgãos de inteligência.

Nas polícias judiciárias (civil ou federal), uma das medidas de investigação de determinado fato é a campana ou monitoramento. Essa técnica ou providência não está descrita no Código de Processo Penal como medida a ser adotada pela autoridade policial em um inquérito policial:

> Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
>
> I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais;
>
> II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;
>
> III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias; IV - ouvir o ofendido;

> V - ouvir o indiciado, com observância, no que for aplicável, do disposto no Capítulo III do Título Vll, deste Livro, devendo o respectivo termo ser assinado por duas testemunhas que Ihe tenham ouvido a leitura;
>
> VI - proceder a reconhecimento de pessoas e coisas e a acareações;
>
> VII - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;
>
> VIII - ordenar a identificação do indiciado pelo processo datiloscópico, se possível, e fazer juntar aos autos sua folha de antecedentes;
>
> IX - averiguar a vida pregressa do indiciado, sob o ponto de vista individual, familiar e social, sua condição econômica, sua atitude e estado de ânimo antes e depois do crime e durante ele, e quaisquer outros elementos que contribuírem para a apreciação do seu temperamento e caráter;
>
> X - colher informações sobre a existência de filhos, respectivas idades e se possuem alguma deficiência e o nome e o contato de eventual responsável pelos cuidados dos filhos, indicado pela pessoa presa.

Campana, de acordo com Nogueira Cobra apud Marques [139], significa observação discreta, para conhecer os movimentos de pessoa ou pessoas ou para fiscalizar a chegada ou aparecimento de alguém, ou ainda, seguimento de alguém de modo discreto para conhecer seus movimentos e ligações.

Apesar de não haver previsão expressa, é uma medida rotineira nas polícias judiciárias, reconhecida como eficaz pelo próprio Judiciário e que não afeta a privacidade do indivíduo. Destaque-se a decisão do Superior Tribunal de Justiça:

> DIREITO PENAL E PROCESSUAL PENAL. AGRAVO REGIMENTAL NO HABEAS CORPUS SUBSTITUTIVO DE RECURSO PRÓPRIO. TRÁFICO ILÍCITO DE ENTORPECENTES. ARGUIÇÃO DE NULIDADE. ALEGAÇÃO DE OCORRÊNCIA DE AÇÃO CONTROLADA. INEXISTÊNCIA DE AUTORIZAÇÃO JUDICIAL. TESE DEFENSIVA RECHAÇADA. MERA OBSERVAÇÃO/MONITORAMENTO DISCRETO E À DISTÂNCIA DA MOVIMENTAÇÃO DE SUSPEITO. [...]
>
> II – Arguição de nulidade. Alegação de ocorrência de ação controlada. Inexistência de autorização judicial. Tese defensiva rechaçada. Segundo o quadro fático probatório dos autos, as instâncias ordinárias afirmaram não se tratar de ação controlada; mas, sim, de observação/monitoramento discreto e à distância da movimentação de suspeito. O prolongamento no tempo da campana se deu unicamente, a fim de que os policiais constatassem, com a devida segurança, a efetiva ocorrência do tráfico de entorpecentes. Tal proceder mostra-se lídimo e consentâneo com o Estado Democrático de Direito, uma vez que os agentes públicos, imbuídos de prudência necessária, não invadiram a esfera de privacidade do paciente sem que a mera suspeita se tornasse densa o suficiente. Nesse contexto, o acolhimento da pretensão defensiva, segundo as alegações vertidas na impetração, requer aprofundamento cognitivo no acervo fático-probatório, situação vedada no âmbito do remédio heroico. [...] (HC 674031/SP. Rel. Min. JESUÍNO RISSATO. Data do Julgamento: 14/09/2021. Data da Publicação: 27/09/2021) [140].

A campana, portanto, nada mais é que o monitoramento e registro da localização e deslocamento de pessoas e suas atitudes ou a observação da movimentação em locais.

Talvez não seja exagero dizer que não há uma única agência de inteligência no mundo que não se utilize da técnica de vigilância. Importante dizer que Vigilância é técnica de inteligência e não se confunde com a “Perseguição” ou “Campana” que é uma atividade tipicamente policial voltada a captura do infrator.

A vigilância nada mais é que a observação do alvo em ambiente público, de trânsito acessível por qualquer popular. Observando o significado da palavra, é estar atento. Do inglês, *surveillance*, a etimologia aponta vigiar (*veillance*) de cima (*sur*). Para Haggerty and Ericson [141] vigilância é a coleta e análise das informações.

E o que se extrai da vigilância? É possível determinar o trajeto e os locais visitados pela pessoa, assim como eventuais contatos que possam interessar ao objeto de avaliação da missão/operação de inteligência.

A Vigilância, portanto, é direcionada, tem um alvo certo e delimitado. E, nesse sentido, difere-se por completo da denominada vigilância em massa, utilizada, por exemplo, no programa PRISM da NSA, que se mostra geral e indiscriminada, não sendo possível determinar um alvo específico, que mais parece o panoptismo onividente e onipresente de Bentham [142].

Para melhor compreensão, passa-se a idealizar uma situação fictícia. Imagine-se que uma agência de inteligência estrangeira comunica ao Brasil que determinado suspeito de integrar o grupo terrorista *Al Qaeda* desembarcará no Brasil e não se sabe a finalidade da viagem. É presumível o interesse tanto da agência comunicante quanto das autoridades nacionais em saber a motivação para o ingresso em território nacional. Se existem células da organização terrorista no Brasil. Se há fontes de financiamento financeiro a atos terroristas. Se há planos de um ataque terrorista em solo nacional, dentre outras informações. Para alguns dos questionamentos a vigilância física é mais efetiva que a geolocalização eletrônica. Esta última visa identificar a localização do alvo ou seu trajeto mas é incapaz de alcançar detalhes próprios da observação presencial de uma vigilância física.

Nesse raciocínio, se é possível a vigilância realizada a partir da observância real, com acompanhamento do alvo a partir de uma ou mais equipes designadas para a atividade, com obtenção de informações mais completas, parece ser permitida a geolocalização a partir da identificação da localização ou trajeto do alvo através do GPS do celular ou das Estações Rádio Base. A resposta para o assunto, no entanto, é mais complexa.

A ideia da utilização de meios tecnológicos para localização de um alvo por um órgão de inteligência nacional causa, de maneira geral, certa desconfiança.

A vigilância, termo utilizado no âmbito da inteligência, se difere da campana no tocante a finalidade do ato. Se na campana o que se objetiva é colher elementos, indícios de autoria e/ou materialidade em relação a um crime, na vigilância a observação visa subsidiar uma análise de inteligência.

No contexto de uma investigação criminal, a campana coleta elementos, que podem se materializar em fotos, vídeos ou, até mesmo um relatório de policiais a respeito do que foi observado, que comporão um inquérito policial a subsidiar a propositura de ação penal e eventual condenação do investigado.

A vigilância, por sua vez, pode igualmente utilizar de meios como a fotografia, vídeo ou descrição dos

fatos observados, mas resultará na elaboração de um informe ou um relatório de inteligência, peças que servirão de assessoramento para uma autoridade. Com um objetivo diferente, a situação a ser observada recebe um enfoque diverso.

É possível traçar um paralelo, reforçando que a inteligência não se resume aos aspectos de segurança pública. A campana se direciona a responsabilização penal individual, enquanto a vigilância pode resultar no desenvolvimento de políticas de criminalização ou reforço de medidas de proteção e combate de crimes em determinada localidade. O interesse, por conseguinte, da inteligência não é a condenação de um determinado membro de uma organização criminosa, é se esse grupo é capaz de afrontar as instituições de Estado ou se infiltrar nelas.

Uma outra circunstância que distingue a campana da vigilância é a metodologia de elaboração e formalização do documento produto da observação. Na campana, o documento que exprime e descreve os fatos precisa identificar os policiais que realizaram a atividade, compõe o inquérito policial e está sujeita ao contraditório. Na vigilância, o documento resultante agregará dados e informações a um outro documento, de análise, produzido pela inteligência e que subsidiará e assessorará as autoridades. Como na área de inteligência as informações produzidas não instruirão e não fundamentarão uma ação penal é inadequado fazer referência a possibilidade de exercício do direito ao contraditório.

Verifica-se que há semelhanças e diferenças entre a campana policial e a vigilância, mas um dos elementos coincidentes é que ambas se utilizam da observação de fatos e pessoas em público. E, nesse ponto, o Judiciário não apontou que haveria uma violação do direito à privacidade do indivíduo ter sua rotina, trajeto e localização monitoradas pelo Poder Público. É óbvio que tanto a campana quanto a vigilância exigem uma motivação para serem realizadas. Não se trata do monitoramento de qualquer indivíduo. Na área policial, o que impulsiona uma campana é uma desconfiança do cometimento de um crime. No campo da inteligência, o objetivo é verificar um determinado aspecto de interesse definido em um documento devidamente aprovado que autoriza a missão.

Estabelecida a premissa de que a vigilância não afeta o direito à privacidade há que se perguntar: se na vigilância é possível observar, além da localização do indivíduo, detalhes comportamentais, eventuais encontros com outras pessoas, se o indivíduo carrega consigo objetos e tantos outros aspectos, por qual motivo não se poderia obter apenas a localização da pessoa eletronicamente, através das Estações Rádio Base, da internet ou aplicativos?

A questão é tão incompreensível que alguém poderia apor o argumento que com possibilidade do uso da ferramenta de geolocalização em tempo real seria possível determinar a "primeira" localização. E, apenas a partir disso é que se poderia empreender a vigilância. Então seria essa primeira localização que importaria em violação da vida privada do indivíduo? O que é determinante na privacidade é se ele está na Av. Paulista em São Paulo, na Av. Boa Viagem em Recife ou na Av. Atlântica no Rio de Janeiro?

A experiência em outros países mostra que não. Não se trata de uma ferramenta recente e muito menos utilizada apenas pelo Brasil. As ferramentas de geolocalização em tempo real tem amplo uso pelas

agências de inteligência estrangeiras, sem qualquer questionamento em relação ao direito à privacidade. O que preocupa as entidades de proteção de direitos civis em outros países é a constante coleta em massa e indiscriminada de dados e informações da sociedade de maneira geral, programas de vigilância em massa que são capazes de varrer comunicações telefônicas, telemáticas, buscas na internet, *deep web* e tudo que for alçado a dado, palavra ou informação de interesse.

Pois bem. Com essas premissas estabelecidas, é necessário traçar um paralelo entre a ABIN e serviços de inteligência estrangeiros observando três pilares:

1. regulamentação e enumeração das técnicas operacionais;
2. autorização para realização de vigilância ou obtenção da geolocalização em tempo real;
3. estrutura de fiscalização e controle da atividade de inteligência.

De maneira geral, a legislação concernente à atividade de inteligência em outros países, assim como ocorre no Brasil, procura fixar escopo, finalidades e temas a serem acompanhados pelos serviços de inteligência. Ou seja, faz uma descrição genérica de poderes a partir de objetivos, sem ingressar especificamente nas técnicas operacionais que poderão ser utilizadas. Essa circunstância não implica em amplo e irrestrito espectro de escolha. Ao optar pela não exposição de seus métodos, as agências visam preservar sua peculiar forma de atuação. Já há, nessa estratégia, a intenção de se resguardar em relação à inteligência adversa (contrainteligência) e não expor suas capacidades. Isso não significa que não exista internamente, em cada serviço de inteligência, normas e manuais que prevejam e detalhem cada uma das técnicas operacionais, o que lhes confere uma metodologia de uso e a possibilidade de controle pelas unidades internas e órgãos externos.

A regulamentação e enumeração do uso das técnicas operacionais em normas internas dos órgãos de inteligência, e em especial, na ABIN, atende ao princípio da legalidade estrita. Como dito no capítulo acima, em grande parte dos países europeus sequer existem disposições regulamentadoras das técnicas de inteligência, ancorando-se a atividade apenas nos poderes genéricos dispostos nas leis.

Mas a constatação de que a natureza de um órgão de inteligência implica na interpretação do princípio da legalidade estrita sob essa ótica não se aplica apenas no Brasil, essa tese encontra precedente na Alemanha. Em julgamento em 2020, o Tribunal Constitucional Alemão reconheceu que o detalhamento do processo de coleta de dados deveria ser realizado por instrumento normativo interno e restrito do Serviço Federal de Inteligência, uma vez que a necessidade de regulação não significava que o desempenho da atividade não deveria se realizar em sigilo.

Sob outra perspectiva, em relação à competência para autorizar a vigilância ou a busca da geolocalização em tempo real, há diversos modelos nos países.

Existem situações em que a técnica operacional é aprovada por uma autoridade judicial. Nestes casos, o mais comum é que exista um órgão do Judiciário especializado na matéria de inteligência. Ou seja, criado para lidar especificamente com operações de inteligência. É o que se observa no Reino Unido.

Em outra vertente, a mais comum, a obtenção dos dados por meio de coleta ou busca, situação em que se insere a geolocalização em tempo real, é autorizada por uma autoridade no âmbito do serviço de inteligência ou que está acima do chefe da agência, por exemplo, o Ministro. No mais das vezes, conforme exposto na pesquisa acima, o grau hierárquico a ser alçada a questão depende do aprofundamento da operação de busca e coleta e da duração da atividade. Certo é que, no universo pesquisado, das maiores agências de inteligência, grande parte se utiliza de um modelo de autorização administrativa, isto é, sem a participação do Judiciário. É o que ocorre, por exemplo, na Alemanha, na França, na Austrália, na Nova Zelândia e no Brasil.

Em um terceiro modelo, o misto, é possível que a autorização seja emanada de uma autoridade administrativa ou por uma justiça especializada. Adotado pelos Estados Unidos.

Um outro argumento que poderia ser usado em contrário à ferramenta de geolocalização em tempo real é a possível utilização indevida da ferramenta ou a falta de controle.

Essa alegação remete à fiscalização e ao controle da atividade de inteligência em si e a um protocolo de uso e auditoria das técnicas e ferramentas utilizadas. Mais ainda, suscitar esses "pontos negativos" tangencia a desconfiança com o órgão de inteligência central do Brasil, a ABIN. Dito tudo isto, é imperioso trazer à colação as feições da ABIN, seus limites legais e arcabouço de controle interno e externo.

Em breve escorço histórico, retomando a evolução da inteligência no Brasil descrita em capítulo anterior, deve-se registrar que em decorrência da Medida Provisória nº 150, de 15 de março de 1990, convertida na Lei nº 8.028, de 12 de abril do mesmo ano, restou extinto o Serviço Nacional de Informações (SNI), que fora criado pela Lei n° 4341, de 13 de junho de 1964.

A extinção do SNI resultou na assunção das atribuições da área de inteligência pela então Secretaria de Assuntos Estratégicos. Não foi nesse momento que se criou o serviço de inteligência atual, não tendo ocorrido sucessão direta.

Em 05/12/96, o Presidente Fernando Henrique Cardoso, em cerimônia de encerramento de cursos de inteligência do Centro de Formação e Aperfeiçoamento de Recursos Humanos da Subsecretária de Inteligência da Casa Militar, enfatizou a importância de o Brasil, dentro de uma ordem democrática, dispor de profissionais competentes na área de Inteligência. Na ocasião fez referência que:

> a Inteligência de Estado não pode ser contaminada por visão ideológica dos processos político e social brasileiros. Salientou, ainda, que a Inteligência deve prestar contas à sociedade de suas ações pelos meios legais adequados. Por fim, afirmou que o serviço de Inteligência é parte do Estado brasileiro, tendo lugar definido na sua estrutura, o que impõe uma percepção clara de funções, competências e limites de atribuições [19].

Em outras palavras, em interpretação própria, o que se queria afirmar é que, independentemente da atuação do SNI e de visões ideológicas dos processos políticos que o país atravessara, era importante instituir um serviço de inteligência. É ínsito à organização estatal de países de expressão a existência de

um serviço de inteligência.

Na sequência, menos de um ano depois, o Poder Executivo submeteu ao Congresso Nacional o Projeto de Lei n° 3.651, de 19 de setembro de 1997 [143], merecendo o destaque à Exposição de Motivos:

> A presente iniciativa resulta das diretrizes traçadas por Vossa Excelência para dar resposta efetiva à necessidade, essencial ao Estado Democrático de Direito, de **municiar o Governo com informações estratégicas, produzidas em tempo hábil e em absoluta sintonia com a Constituição e as Leis do País, assegurando-lhe o conhecimento antecipado de fatos e fatores relacionados com o desenvolvimento e a segurança do Estado, em todas as áreas da vida nacional**.
>
> Para atender a esses objetivos, o novo sistema de inteligência e seu órgão central, a Agência Brasileira de Inteligência-ABIN, **proverão o Governo, a exemplo do que ocorre em outros países, de dados de natureza estratégica acerca das dificuldades, potencialidades e impedimentos ao cumprimento de suas elevadas funções, em todos os setores de sua atuação**.
>
> No art. 1°, o projeto institui o Sistema Brasileiro de Inteligência, que integra as atividades de planejamento e execução dos procedimentos de inteligência no País. Introduz-se uma regra da mais alta importância para o disciplinamento das atividades de inteligência. **Limitam-se as ações do Sistema à observância incondicional dos Princípios Fundamentais que a Constituição Federal estabeleceu para o País, no seu parágrafo único. Assim como a nossa Lei Máxima erigiu como regra inicial a imposição desses princípios, para dar expressiva demonstração de seu significado também o projeto procura erigir a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana como linhas mestras de cada ato administrativo a ser praticado pelos agentes públicos. Não se trata aqui de imagem de retórica, mas de definição de diretrizes para o efetivo controle que o Poder Legislativo e o Poder Judiciário poderão e deverão fazer das atividades do setor**.
>
> No parágrafo único desse artigo, **mais uma vez o projeto limita a atividade de inteligência, porque condiciona o uso de técnicas e meios sigilosos à irrestrita observância dos direitos e garantias individuais, à fidelidade às instituições e aos princípios éticos que regem os interesses e a segurança do Estado**.
>
> O art. 4° define a competência da ABIN, que deverá assessorar o Chefe de Estado no desempenho de suas elevadas funções, sobretudo em caráter preventivo, avaliando ameaças internas e externas à ordem constitucional e aperfeiçoando seu pessoal para o exercício de suas atribuições. **O parágrafo único prevê a remessa à ABIN dos dados necessários à defesa das instituições**. (grifos nossos)

Após dois anos, na linha do preconizado no Projeto de Lei e no discurso do então Presidente Fernando Henrique Cardoso, foi editada a Lei n° 9.883/99 estipulando funções, competências e limites de atribuições da Agência Brasileira de Inteligência.

Coube à ABIN exercer a função de órgão central do Sistema Brasileiro de Inteligência (SISBIN) obedecendo à política nacional de inteligência e as diretrizes traçadas. Isto é, o mandato conferido ao novel serviço de inteligência brasileiro não era aberto, deveria ser exercido nos contornos da moldura a ser fixada pelo Poder Executivo sob a supervisão das Casas Legislativas. E, nos termos do parágrafo único do art. 5° da Lei n° 9883/99, deve a política nacional de inteligência ser submetida, antes de sua edição, ao órgão de controle externo do Poder Legislativo para exame e sugestões.

Assim, tanto as diretrizes quanto a execução da atividade de inteligência ficam sob a supervisão do Parlamento. Foi na Resolução n° 2, de 2013, do Congresso Nacional [144], parte integrante do Regimento Interno das Casas, que se dispôs sobre a Comissão Mista de Controle das Atividades de Inteligência, órgão

que ficou com a responsabilidade de fiscalizar e exercer o controle externo das atividades de inteligência e contrainteligência.

A referida Resolução não se furtou a indicar o que representaria a fiscalização em seu art. 2° §§ 1° e 2°:

> § 1°. **Entende-se por fiscalização e controle [...] todas as ações referentes à supervisão, verificação e inspeção das atividades** de pessoas, órgãos e entidades relacionados à inteligência e contrainteligência, bem como à salvaguarda de informações sigilosas, visando à defesa do Estado Democrático de Direito e à proteção do Estado e da sociedade. (não se restringe a ABIN – trata da atividade de inteligência)
>
> §2°. **O controle da atividade de inteligência realizado pelo Congresso Nacional compreende as atividades exercidas pelos órgãos componentes do SISBIN** em todo o ciclo da inteligência, **entre as quais as de reunião, por coleta ou busca**, análise de informações, produção de conhecimento, e difusão, bem como a função de contrainteligência e quaisquer operações a elas subordinadas. (grifos nossos)

Se o controle da atividade de inteligência exercido pela Comissão Mista de Controle das Atividades de Inteligência engloba as etapas de coleta e busca do dado é porque a CCAI pode fiscalizar as operações de inteligência, incluindo-se a utilização de ferramentas e mecanismos de captação do dado, a geolocalização em tempo real, por exemplo.

Em 2015, a Comissão Mista de Controle das Atividades de Inteligência [145], elaborou marcante relatório de suas atividades apontando:

> O presente relatório expõe, de forma sucinta, as atividades promovidas, visitas e debates realizados pelos integrantes da COMISSÃO DE CONTROLE DA ATIVIDADE DE INTELIGÊNCIA-CCAI, refletindo a permanente busca de difundir, na sociedade, o sentido estratégico das atividades de Inteligência para a defesa do Estado brasileiro.
>
> As grandes potências possuem uma forte e ativa atividade de inteligência, incluindo investimentos em modernos sistemas e em infraestrutura própria para sua sustentação. Estabelecem seus planos de desenvolvimento a partir das informações produzidas pelos seus órgãos e agentes. E mais, promovem uma indústria cultural de valorização de seus agentes e organismos, muito além do julgamento de sua missão.
>
> [...]
>
> Constatação de alta relevância é de que não existe democracia desenvolvida no mundo que não disponha de serviços secretos eficientes, eficazes e efetivos. De fato, democracia e inteligência são plenamente compatíveis. E nações que buscam ocupar papel de destaque no cenário internacional precisam de serviços de inteligência de qualidade.
>
> [...]
>
> Ora, então, se os serviços secretos lidam com tanto poder e são importante instrumento a serviço do Estado (e, em democracias, da sociedade), como evitar que, em regimes democráticos, esses serviços extrapolem suas funções, acumulem significativo poder e cometam arbitrariedades contra aqueles que deveriam defender? A resposta está exatamente no estabelecimento de rígidos mecanismos de fiscalização e controle, tanto internos quanto externos. É o controle que garantirá que a inteligência atue em consonância com a democracia.

Em paralelo, assim como ocorre em outros órgãos da administração pública federal, na estrutura da ABIN há unidades de controle como a Ouvidoria, Corregedoria-Geral (unidade setorial do Sistema de

Correição do Poder Executivo Federal), Assessoria de Governança e Conformidade e Assessoria Jurídica (unidade da Advocacia-geral da União), além do poder hierárquico exercido pelo Diretor-Geral e pelo Ministro Chefe da Casa Civil[1]. Ademais, a própria aprovação do nome do Diretor-Geral da ABIN também ficou a cargo do Senado Federal.

Com esse panorama, é possível afirmar que os mecanismos de controle e fiscalização da ABIN se assemelham a dos órgãos estrangeiros congêneres de inteligência. Em países como Reino Unido, Estados Unidos, Canadá, Austrália, Nova Zelândia, Alemanha e França, como já destacamos em capítulo próprio, o controle da atividade de inteligência é exercido pelas Casas Legislativas individualmente ou pelo Parlamento. Há, também, uma cadeia hierárquica de comando e autorização e a fiscalização interna da atuação é exercida, comumente, por outros órgãos assemelhados aos que existem no Brasil.

Tome-se, como exemplo, o Reino Unido e os Estados Unidos, países com forte atuação na área de inteligência. No Reino Unido, o *Justice and Security Act* estabelece que o controle externo da Comunidade de Inteligência, o que engloba as sete agências e departamentos, compete a um colegiado composto por 9 membros da Câmara dos Comuns e da Câmara dos Lordes. Isto é, uma comissão mista, como se dá no Brasil. Nos Estados Unidos, há a fiscalização exercida pelo Senado, através do *United States Senate Select Committee on Intelligence*, e pela Câmara dos Representantes, via o *Permanent Select Committee*.

Assim, levando-se em conta o comparativo com 3 importantes parâmetros de estrutura de serviços de inteligência, verifica-se que o modelo brasileiro, da ABIN, não se afasta do que é praticado internacionalmente.

[1]Com a alteração promovida pelo Decreto n° 11.327/2023, a ABIN passou a ser órgão integrante da Casa Civil e não mais do Gabinete de Segurança Institucional, ficando, portanto, subordinada ao Ministro Chefe daquela Pasta.

10 CONCLUSÃO

À luz dos elementos de pesquisa destacados no texto, é possível concluir que a ABIN pode se utilizar da geolocalização em tempo real como técnica operacional voltada a identificar a localização de determinado indivíduo.

Ao longo do presente estudo foram elencados pontos que reforçam o raciocínio a que se chega nesta conclusão.

Em um estudo comparativo com diversos países, como Estados Unidos, Reino Unido, Canadá, Austrália, Nova Zelândia, Alemanha e França não foi possível identificar diferenças representativas nos aspectos formais de legislação, cadeia de autorização e controle das técnicas operacionais em relação ao Brasil. Ao revés, em grande parte desses países, há um crescente e forte uso de técnicas operacionais com utilização de tecnologia para obtenção de informações através de inteligência de comunicações (interceptação de comunicações de maneira geral), de imagens (por drones, satélites, balões), de sinais (ondas eletromagnéticas), assinaturas eletromagnéticas (*fingerprints* de armas, dispositivos, tecnologias e capacidades), telemetria e fotográfica. Todo esse aparato significa uma vigilância em massa, isto é, irrestrita, capaz de alcançar todos os indivíduos, inclusive brasileiros.

No universo de países pesquisados, à exceção da Nova Zelândia, constata-se que a legislação não oferece um detalhamento das técnicas operacionais passíveis de serem utilizadas pelos serviços de inteligência. Essa política legislativa é resultado da natureza dos serviços de inteligência que buscam restringir e manter sob sigilo suas capacidades de operação e coleta de dados e informações. Merece destaque, nesse particular, a Alemanha, país que é utilizado como referência pelo Brasil no contexto do direito à privacidade e em outras legislações. O Tribunal Constitucional Alemão se manifestou pela necessidade de aprimoramento da legislação referente aos serviços de inteligência, mas considerou que atendia à natureza da atividade que se editassem normas complementares sigilosas de detalhamento das ações. Ou seja, o princípio da legalidade se encontrava observado mesmo que as técnicas operacionais não estivessem detalhadas em lei.

O que se observa, pelos dados de pesquisa alcançados, é que a possibilidade da utilização da geolocalização em tempo real por serviços de inteligência dos Estados Unidos, Reino Unido, Canadá, Austrália, Nova Zelândia, Alemanha e França é tema ultrapassado. Não há qualquer questionamento quanto a essa possibilidade, inclusive por entidades de defesa do direito à privacidade. Mais ainda, os Tribunais Superiores nesses países têm considerado até a vigilância em massa como uma forma legítima de obtenção de informações para enfrentamento de fenômenos como o terrorismo e extremismo. A própria Corte Europeia de Direitos Humanos reconheceu que era essencial a vigilância em massa para proteger a segurança nacional no Reino Unido, devendo-se, no entanto, avaliar o uso com parâmetros, razoabilidade e proporcionalidade.

No Brasil, à exemplo do que aconteceu em outros países, a Lei 9.883/99, que criou a Agência Brasileira de Inteligência, lançou bases para o uso de técnicas operacionais, que devem encontrar limites na Constituição Federal e, sobretudo, observar os direitos e garantias individuais. A inexistência, no entanto, de detalhamento em lei das técnicas operacionais, não retira da ABIN a capacidade de uso de meios sigilosos para coleta e busca de dados e informações para o cumprimento de sua missão legal, como ocorre com outros serviços de inteligência.

O sistema de autorização do uso de técnicas operacionais e os mecanismos de controle da atividade de inteligência no Brasil não são diferentes em sua essência dos encontrados nos países pesquisados. Sob o ponto de vista hierárquico, o Brasil conta com um Ministro de Estado, que supervisiona a atividade, e um Chefe do serviço de inteligência, um Diretor-Geral, que é aprovado pelo Senado Federal. O controle externo se opera por meio de uma Comissão Mista de Senadores e Deputados, que tem poderes fiscalizatórios condizentes com os encontrados em comitês parlamentares de controle da atividade de inteligência em outros países.

Sob outra vertente, no campo legislativo, avaliando o arcabouço legal, a análise da Lei Geral de Proteção de Dados permitiu atestar a sua inaplicabilidade em quase sua totalidade nas hipóteses de tratamento de dados que envolvam a defesa nacional e a segurança do Estado.

Assim, com mais ênfase, observa-se que a geolocalização em tempo real de um indivíduo deve ter como limitação ao seu uso o direito à privacidade e à proteção de dados, ambas com previsão constitucional. Essa assertiva não restou desnaturada com o exame de decisões do Supremo Tribunal Federal e Superior Tribunal de Justiça que se debruçam sobre aspectos do compartilhamento de dados entre órgãos públicos e privacidade.

Da mesma forma, quando é examinada a evolução do direito à privacidade, verifica-se um crescente discurso de reprovabilidade no acesso do Estado a dados pessoais dos indivíduos. Ao se realizar, todavia, um cotejo da finalidade da captação de dados pelas empresas de tecnologia em comparação com a coleta levada a efeito pelo Estado, com finalidade de interesse público, demonstra-se a desproporção do volume de dados acumulados por empresas privadas, sem a efetiva concordância do indivíduo e controle estatal. Esse movimento resultou no enfraquecimento e incapacidade do Estado em lidar com a aptidão e habilidade das *big techs* em reunir e processar grande volume de dados dos cidadãos. Tanto assim, que em grande parte dos processos punitivos instaurados pela ANPD o sujeito passivo é um ente estatal. Deve-se registrar, porém, que, recentemente, tem se detectado iniciativas que visam limitar e controlar a atuação das empresas de tecnologia, como no estado americano de Utah e na Europa.

No exame da atividade em si, não há que se confundir a geolocalização em tempo real com a geolocalização estática. A geolocalização estática tem sido deferida pelo Poder Judiciário em processos criminais e visa detectar quais indivíduos estariam presentes em determinado local em um intervalo de tempo, quais palavras essas pessoas teriam pesquisado em serviços de busca na internet, quais aplicativos utilizaram e assim por diante. A geolocalização estática esquadrinha os dados e rastros deixados pelos indivíduos no uso da internet, acessando aspectos da privacidade e intimidade de um universo de pessoas, inclusive e na

sua maioria, daqueles que não estão envolvidos no cometimento do crime. O objetivo é obter indícios e vestígios que resultem na determinação de autoria de um crime. A geolocalização em tempo real, por sua vez, visa à captação unicamente da localização da pessoa.

Nesse sentido, examinou-se o uso da campana e da vigilância física, técnicas assemelhadas, que se traduzem apenas na observação de pessoas ou ambientes, utilizadas pelas polícias judiciárias e inteligência. Conforme posicionamento do Superior Tribunal de Justiça esses mecanismos de monitoramento não ferem o direito à privacidade. Por meio da vigilância ou campana é possível constatar a localização e trajeto de um indivíduo, bem como seu contato com outras pessoas, se levava consigo objetos, se buscava camuflar sua identidade, se apresentando com roupas e outros aspectos comportamentais que mereceriam um destaque ou alerta. A geolocalização em tempo real, por sua vez, é capaz de determinar apenas a localização da pessoa em tempo real. Assim, a possibilidade de obtenção de dados pessoais de um indivíduo por meio de uma vigilância física é muito superior do que se utilizada a geolocalização em tempo real. Em outros termos, a vigilância física seria mais invasiva à privacidade do que o seu correspondente eletrônico.

E, por fim, há um raciocínio lógico que leva à conclusão atingida, se à ABIN é autorizada o uso da técnica operacional vigilância, caracterizada pela observação em ambiente público de pessoas e locais, que permite visualizar outras circunstâncias além da localização do indivíduo, não parece razoável negar o uso de ferramenta eletrônica que lhe indicará apenas a localização da pessoa.

10.1 TRABALHOS FUTUROS

A complexidade do tema desenvolvido permite que alguns pontos suscitados no presente estudo sejam aprofundados em outro trabalho.

Apesar da robusta conclusão acerca da possibilidade da realização de vigilância por meio de geolocalização em tempo real pela Agência Brasileira de Inteligência, não se ingressou, detidamente, na análise da competência, na estrutura da ABIN, para autorizar a ação de vigilância, no papel do Ministro de Estado que supervisiona as atividades de inteligência ou, ainda, da Comissão Mista de Controle das Atividades de Inteligência, em relação às técnicas de inteligência.

REFERÊNCIAS BIBLIOGRÁFICAS

1 AMÉRICA, E. U. *FISA Amendments Act*. 2017. Disponível em: <https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf>. Acesso em 19 maio 2023.

2 UNIDO, R. *Investigatory Powers Act 2016*. 2016. Disponível em: <https://www.legislation.gov.uk/ukpga/2016/25/contents>. Acesso em 02 set 2022.

3 CANADÁ. *Canadian Security Intelligence Service Act R.S.C., 1985, c. C-23*. 1985. Disponível em: <https://laws-lois.justice.gc.ca/eng/acts/c-23/>. Acesso em 19 set 2022.

4 AUSTRÁLIA. *Telecommunications Interception and Access Act 1979*. 1979. Disponível em: <https://www.legislation.gov.au/Details/C2022C00170>. Acesso em 21 set 2022.

5 ZELÂNDIA, N. *Intelligence and Security Act 2017*. 2017. Disponível em: <https://www.legislation.govt.nz/act/public/2017/0010/latest/whole.html#DLM6920823>. Acesso em 25 set 2022.

6 ALEMANHA. *Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG) - Lei do Serviço Federal de Inteligência (Lei BND - BNDG)*. 1990. Disponível em: <https://www.gesetze-im-internet.de/bndg/BNDG.pdf>. Acesso em 18 out 2022.

7 FRANÇA. *Loi 2015-912. Code de sécurité interne - Lei 2015-912. Código de Segurança Interna*. 2015. Disponível em: <https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000025503132/2015-10-03/>. Acesso em 04 nov 2022.

8 BRASIL, R. F. d. *Agência Nacional de Telecomunicações. Acesso ao painel de dados de telefonia móvel*. 2023. Disponível em: <https://informacoes.anatel.gov.br/paineis/acessos/telefonia-movel>. Acesso em 19 maio 2023.

9 DONEDA, D. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJJL]*, v. 12, n. 2, p. 91–108, 2011.

10 JÚNIOR, T. S. F. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do estado. *Revista da Faculdade de Direito, Universidade de São Paulo*, v. 88, p. 439–459, 1993.

11 ALEXY, R. Teoria dos direitos fundamentais. tradução de virgílio afonso da silva. Malheiros, 2008.

12 MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, Faculdade de Direito de Vitória, v. 19, n. 3, p. 159–180, 2018.

13 BRANCO, P. G.; MENDES, G. F. Curso de direito constitucional - 15ª ed. *São Paulo: Saraiva Educação*, 2020.

14 MORAES, A. d. Constituição do brasil interpretada e legislação constitucional - 6ª ed. *São Paulo: Atlas*, 2006.

15 SARLET, I. W.; MARINONI, L. G.; MITIDIERO, D. *Curso de direito constitucional - 7ª ed*. [S.l.]: São Paulo: Saraiva Educação SA, 2018.

16 PALHARES, G. C.; SANTOS, A. S. D.; ARIENTE, E. A.; GOMES, J. D. O. A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. *Estudos Avançados*, São Paulo:SciELO Brasil, v. 34, p. 175–190, 2020.

17 BRASIL, R. F. d. *Lei nº 9.883 de 07 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN*. 1999. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9883.htm>. Acesso em 19 abr 2022.

18 KENT, S. *Strategic intelligence for American world policy*. [S.l.]: Princeton University Press, 2015. v. 2377.

19 BRASIL, R. F. d. *Decreto n° 8793/2016 - Política Nacional de Inteligência*. 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm>. Acesso em 19 abr 2022.

20 AMÉRICA, E. U. *Intelligence guide for first responders: What is intelligence?* 2013. Disponível em: <https://www.dni.gov/nctc/jcat/jcat_ctguide/intel_guide.html#intel>. Acesso em 11 nov 2021.

21 NATO, N. A. T. O. *Joint Intelligence, Surveillance and Reconnaissance*. 2013. Disponível em: <https://www.nato.int/cps/en/natohq/topics_111830.htm>. Acesso em 30 ago 2022.

22 BRASIL, R. F. d. *Doutrina Nacional de Inteligência*. 2020. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/Col3v5.pdf>. Acesso em 30 ago 2022.

23 CEPIK, M. Inteligência e políticas públicas: dinâmicas operacionais e condições de legitimação. *Security and Defense Studies Review*, v. 2, n. 2, p. 246–267, 2002.

24 BRASIL, R. F. d. *Cronologia de criação dos órgãos de inteligência e de estado no Brasil*. 2013. Disponível em: <https://www.gov.br/abin/pt-br/acesso-a-informacao/institucional/historico>. Acesso em 19 abr 2022.

25 BRASIL, R. F. d. *Decreto n° 14.503/2017 - Estratégia Nacional de Inteligência*. 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm>. Acesso em 26 abr 2022.

26 GONÇALVES, J. B. Atividade de inteligência e legislação correlata. rev. e atual. *Niterói: Impetus*, 2016.

27 ALVES, S. A matemática do gps. *Revista do professor de matemática*, v. 59, n. 1, 2006.

28 BRASIL, R. F. d. *Lei nº 12.965 de 23 de abril de 2014.Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil - Marco Civil da Internet*. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 01 fev 2023.

29 UNIDO, R. *High Court of Justice. Liberty vs Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs*. 2019. Disponível em: <https://www.judiciary.uk/wp-content/uploads/2019/07/Liberty-judgment-Final.pdf>. Acesso em 04 set 2022.

30 ECHR, E. C. o. H. R. *European Court of Human Rights. Big Brother Watch and Others vs. The United Kingdom*. 2005. Disponível em: <https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}>. Acesso em 19 maio 2023.

31 AMÉRICA, E. U. *The Intelligence Community: How the IC works*. 2022. Disponível em: <https://www.intelligence.gov/how-the-ic-works>. Acesso em 08 set 2022.

32 AMÉRICA, E. U. *Uniting and Strengthening America by Providing appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*. 2022. Disponível em: <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>. Acesso em 03 out 2022.

33 AMÉRICA, E. U. *Intelligence Reform and Terrorism Prevention Act of 2004*. 2004. Disponível em: <https://www.govinfo.gov/content/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf>. Acesso em 03 out 2022.

34 AMÉRICA, E. U. *H.R.3199 - USA PATRIOT Improvement and Reauthorization Act of 2005*. 2005. Disponível em: <https://www.congress.gov/bill/109th-congress/house-bill/3199>. Acesso em 04 out 2022.

35 AMÉRICA, E. U. *H.R.1962 - PATRIOT Sunsets Extension Act of 2011*. 2011. Disponível em: <https://www.congress.gov/bill/112th-congress/house-bill/1962/text>. Acesso em 04 out 2022.

36 AMÉRICA, E. U. *H. Rept. 113-452 - USA Freedom Act*. 2015. Disponível em: <https://www.congress.gov/congressional-report/113th-congress/house-report/452/1>. Acesso em 10 out 2022.

37 AMÉRICA, E. U. *Foreign Intelligence Surveillance Act of 1978 Amendments Act os 2008*. 1978. Disponível em: <https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf>. Acesso em 05 out 2022.

38 AMÉRICA, E. U. *PUBLIC LAW 110-55: Protect America Act of 2007*. 2007. Disponível em: <https://www.intelligence.senate.gov/sites/default/files/laws/pl11055.pdf>. Acesso em 06 out 2022.

39 RUSBRIDGER, A. *The Snowden leaks and the public*. [S.l.]: NEW YORK REVIEW 1755 BROADWAY, 5TH FLOOR, NEW YORK, NY 10019 USA, 2013. 31–34 p.

40 AMÉRICA, E. U. *House of Representatives (H.R.) 5949 Enrolled Bill (ENR): FISA Amendments Act Reauthorization Act of 2012*. 2012. Disponível em: <https://www.intelligence.senate.gov/legislation/fisa-amendments-act-reauthorization-act-2012>. Acesso em 05 out 2022.

41 AMÉRICA, E. U. *Senate S. 2010: Extend the FISA Amendments Act of 2008 for 8 years, and for other*. 2017. Disponível em: <https://www.intelligence.senate.gov/legislation/fisa-amendments-reauthorization-act-2017>. Acesso em 10 out 2022.

42 AMÉRICA, E. U. *Supreme Court of the United States. No. 13-58: In Re Electronic Privacy Information Center, Petitioner*. 2013. Disponível em: <https://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/13-58.htm>. Acesso em 07 set 2022.

43 AMÉRICA, E. U. *Foreign intelligence surveillance court: Primary order*. 2013. Disponível em: <https://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf>. Acesso em 07 set 2022.

44 G1, G. N. *Portal G1: Suprema Corte rejeita apelação sobre programa americano de espionagem*. 2013. Disponível em: <https://g1.globo.com/mundo/noticia/2013/11/suprema-corte-rejeita-apelacao-sobre-programa-americano-de-espionagem.html>. Acesso em 14 set 2022.

45 AMÉRICA, E. U. *United States Senate Select Committee on Intelligence*. 2022. Disponível em: <https://www.intelligence.senate.gov>Acessoem11deout.2022.>. Acesso em 11 set 2022.

46 AMÉRICA, E. U. *Foreign intelligence surveillance court: Primary order*. 1976. Disponível em: <https://www.intelligence.senate.gov/sites/default/files/publications/94_comm_prt.pdf>. Acesso em 11 set 2022.

47 AMÉRICA, E. U. *The Intelligence Community: Oversight & Partners*. 2022. Disponível em: <https://www.intelligence.gov/how-the-ic-works#oversight>. Acesso em 14 out 2022.

48 AMÉRICA, E. U. *Senate 4503: Intelligence Authorization Act for Fiscal Year 2023*. 2022. Disponível em: <https://www.intelligence.senate.gov/legislation/intelligence-authorization-act-fiscal-year-2023-reported-july-12-2022>Acessoem11deout.2022.>. Acesso em 11 set 2022.

49 AMÉRICA, E. U. *The Permanent Select Committee on Intelligence*. 2022. Disponível em: <https://www.intelligence.house.gov>Acessoem11deout.2022.>. Acesso em 11 set 2022.

50 AMÉRICA, E. U. *Executive Order 12333–United States intelligence activities*. 1981. Disponível em: <http://www.archives.gov/federal-register/codification/executive-order/12333.html>. Acesso em 12 out 2022.

51 CANADÁ. *Supreme Court of Canada - Hassan Almrei v. Minister of Citizenship & Immigration, et al (30929)*. 2005. Disponível em: <https://www.scc-csc.ca/case-dossier/info/sum-som-eng.aspx?cas=30929>. Acesso em 16 set 2022.

52 CANADÁ. *SCC File Nº 34884: Harkat v Canada*. 2014. Disponível em: <https://www.scc-csc.ca/WebDocuments-DocumentsWeb/34884/FM020_Respondent_Mohamed-Harkat.pdf>. Acesso em 15 set 2022.

53 CANADÁ. *A Consolidation of The Constitution Acts (1867 to 1982)*. 1982. Disponível em: <https://laws-lois.justice.gc.ca/PDF/CONST_TRD.pdf>. Acesso em 16 set 2022.

54 CANADÁ. *Ontario Superior Court of Justice CRIMJ(P)299/14: R. v. Rogers Communication*. 2016. Disponível em: <https://ccla.org/wp-content/uploads/2021/06/R-v.-Rogers-and-Telus-Judgment-January-14-2016-1.pdf>. Acesso em 17 set 2022.

55 AUSTRÁLIA. *The Surveillance Devices Act 2004*. 2004. Disponível em: <https://www.legislation.gov.au/Details/C2022C00180>. Acesso em 21 set 2022.

56 AUSTRÁLIA. *Reform of Australia's electronic surveillance framework*. 2022. Disponível em: <https://www.oaic.gov.au/__data/assets/pdf_file/0015/12363/submission_Electronic_surveillance_framework_discussion_paper.pdf>. Acesso em 23 set 2022.

57 ZELÂNDIA, N. *Supreme Court of New Zealand (SC 125/2010): HAMED v R*. 2011. Disponível em: <https://www.courtsofnz.govt.nz/assets/cases/2011/sc-125-2010-omar-hamed-and-others-v-the-queen-redacted.pdf>. Acesso em 28 set 2022.

58 ZELÂNDIA, N. *Courts of New Zealand (SC CIV 19/2004): Attorney-General v Ahmed Zaoui, Inspector General of Intelligence and Security, and Human Rights Commissioner*. 2005. Disponível em: <https://www.courtsofnz.govt.nz/cases/attorney-general-v-ahmed-zaoui-inspector-general-of-intelligence-and-security-and-human-rights-commissioner>. Acesso em 29 set 2022.

59 ALEMANHA. *Bundesnachrichtendienst - BND (The Foreign Intelligence Service of Germany)*. 2022. Disponível em: <https://www.bnd.bund.de/EN/Home/home_node.html>. Acesso em 17 nov 2022.

60 ALEMANHA. *Julgamento Bvr 2835/2017.Tribunal Constitucional Alemão. BVerfG)*. 2020. Disponível em: <http://www.bverfg.de/e/rs20200519_1bvr283517.html>. Acesso em 25 out 2022.

61 ROJSZCZAK, M. Extraterritorial bulk surveillance after the german bnd act judgment. *European Constitutional Law Review*, Cambridge University Press, v. 17, n. 1, p. 53–77, 2021.

62 FRANÇA. *Decreto no 2017-1095 de 14 de junho de 2017 relativo ao Coordenador Nacional de Inteligência e Combate ao Terrorismo, à Coordenação Nacional de Inteligência e Combate ao Terrorismo e ao Centro Nacional de Contraterrorismo*. 2017. Disponível em: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000034938469/>. Acesso em 04 nov 2022.

63 FRANÇA. *Decreto no 2014-445 de 30 de abril de 2014 relativo às missões e organização da Direção-Geral da Segurança Interna*. 2014. Disponível em: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028887486/>. Acesso em 04 nov 2022.

64 FRANÇA. *Código de Defesa*. 2022. Disponível em: <https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071307/>. Acesso em 04 nov 2022.

65 FRANÇA. *La stratégie nationale du renseignement (Estratégia nacional de inteligência)*. 2019. Disponível em: <https://www.academie-renseignement.gouv.fr/files/piece_jointe_2_strategie_Nationale_du_Renseignement.pdf?_x_tr_sch=http&_x_tr_sl=fr&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em 04 nov 2022.

66 FRANÇA. *Decreto no 2014-833 de 24 de julho de 2014 relativo à inspeção dos serviços de inteligência*. 2014. Disponível em: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029290787/>. Acesso em 05 nov 2022.

67 FRANÇA. *LEI n ° 2007-1443 de 9 de outubro de 2007 sobre a criação de uma delegação parlamentar de inteligência (1)*. 2007. Disponível em: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000252177/>. Acesso em 05 nov 2022.

68 FRANÇA. *Decisão no 2015-722 DC de 26 de novembro de 2015. Lei relativa às medidas de vigilância das comunicações eletrônicas internacionais*. 2015. Disponível em: <https://www.conseil-constitutionnel.fr/decision/2015/2015722DC.htm>. Acesso em 07 nov 2022.

69 EUROPEIA, U. *Tratado da União Europeia (versão consolidada)*. 2016. Disponível em: <https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF>. Acesso em 30 out 2022.

70 BRASIL, R. F. d. *Lei nº 13.709 de 14 de agosto de 2018. Lein Geral de Proteção de Dados*. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 12 fev 2022.

71 EUROPEIA, U. *The Regulation (EU) 2016/679: General Data Protection Regulation (GDPR)*. 2016. Disponível em: <https://gdpr-info.eu/>. Acesso em 26 fev 2022.

72 G1, G. N. *Portal G1: Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades*. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em 26 fev 2022.

73 BRASIL, R. F. d. *Projeto de Lei 5276/2016: Dispõe sobre o Tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural*. 2016. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=Tramitacao-PL+5276/2016>. Acesso em 22 fev 2022.

74 BRASIL, R. F. d. *Supremo Tribunal Federal: Arguição de Descumprimento de Preceito Fundamental n° 695. Compartilhamento de dados pessoais pelo Serpro à ABIN*. 2020. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693>. Acesso em 12 mar 2022.

75 TJSP, T. d. J. d. S. P. *ACF no 15.997/2022 - Apelação Cível n° 1090663-42.2018.8.26.0100*. 2023. Disponível em: <http://esaj.tjsp.jus.br/cjsg/getArquivo.do?conversationId=&cdAcordao=16739524&cdForo=0&uuidCaptcha=sajcaptcha_dd7befad82614e61848cee120e386d4e&g-recaptcha-response=03AAYGu2ShWDnOVqirY6SsFCcS4sBd37baA8UeUp6UNy-sq6bCG34Qb93Q7PBicITUcf5nrR6wYYjl4F9M7qOaqhUPqmM9JBlkGYr8zPlilkMDLZGwXgyS-uZU1SfdYhs97Glkp6MbOh3QlC9e_

wKzEeSV2U-2TDDqMJM5ZT6H6mquqY15x1eDkl8Isq0Px3fJJKCmevfzlLOQGDRqknYGECxNNFFRXZi1QKeLPIo
rf9xmJwGqYLRC4BFTHo2gKjteB5zyH4Vft-UKGRbPXoAYEIZKQWeARhZHIUHj2BbDQ_
h8HS2u78Pqa_DSsQvyAXkPfPV6xJNfiD_4jrrO-wGFSb_
R2Z8h4armbdoIC0VBlGWyoQOQXRd0rLtABlAAyLuVUjQI4pmEAEnWOpG5Hpg6_
S-ebU6ScDkcP1k1ivXMbWWpJ7-g3wmGKPRzYlrlVpBrk6_CVXD6kJqGw2O5qSukiakMJhCmDy>.
Acesso em 18 jul 2023.

76 BRASIL, R. F. d. *Câmara dos Deputados. Anteprojeto de Lei Geral de Proteção de Dados Penal*. 2020. 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/DADOSAnteprojetocomissaoprotecaodadosseguranca persecucaoFINAL.pdf>. Acesso em 12 mar 2022.

77 ARGENTINA. *Lei n° 25.326, de 02 de novembro de 2000: Ley de Protección de Los Datos Personales - Lei de Proteção de Dados Pessoais*. 2000. Disponível em: <https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790>. Acesso em 13 fev 2022.

78 COLÔMBIA. *Lei estatutária n° 1581, de 18 de outubro de 2012: Ley Estatutaria 1581 DE 2012: Disposiciones Generales para La Protección de Datos Personales - disposições gerais para a proteção de dados pessoais*. 2012. Disponível em: <http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html>. Acesso em 13 fev 2022.

79 RICA, C. *Lei n° 8968, de 07 de julho de 2011: Ley de Protección de La Persona Frente al Tratamiento de sus Datos Personales - Lei de Proteção da Pessoa contra o tratamento dos seus dados pessoais*. 2011. Disponível em: <http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989>. Acesso em 19 fev 2022.

80 PERU. *Lei n° 29733, de 03 de julho de 2011: Ley de Protección de Datos Personales - Lei de proteção de dados pessoais*. 2011. Disponível em: <https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733>. Acesso em 19 fev 2022.

81 MÉXICO. *Lei s/n°, de 26 de janeiro de 2017: Ley general de proteccíon de datos personales en posesión de sujetos obligados - Lei geral de de proteção de dados pessoais na posse de assuntos obrigados*. 2017. Disponível em: <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>. Acesso em 19 fev 2022.

82 PANAMÁ. *Lei n° 81, de 29 de março de 2019: Ley Sobre Proteccion de Datos Personales - Lei sobre proteção de dados pessoais*. 2019. Disponível em: <https://webcache.googleusercontent.com/search?q=cache:nNtzclv1Et4J:https://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2010/2019/2019_645_3008.pdf+&cd=9&hl=pt-BR&ct=clnk&gl=br>. Acesso em 19 fev 2022.

83 URUGUAI. *Lei n° 18331, de 18 de agosto de 2008: Proteccíon de Datos Personales y Acción de Habeas Data - Proteção de Dados Pessoais e Ação de Habeas Data*. 2008. Disponível em: <https://www.impo.com.uy/bases/leyes/18331-2008>. Acesso em 20 fev 2022.

84 DOMINICANA, R. *Lei n° 172, de 15 de dezembro de 2013: Ley Orgánica sobre Protección de Datos de Carácter Personal - Lei orgânica sobre proteção de Dados de caráter pessoal*. 2013. Disponível em: <https://indotel.gob.do/media/6200/ley_172_13.pdf>. Acesso em 20 fev 2022.

85 CHILE. *Lei n° 19.628, de 26 de agosto de 1999: Sobre Proteccion de La Vida Privada - Sobre proteção da vida privada*. 1999. Disponível em: <https://www.bcn.cl/leychile/navegar?idNorma=141599>. Acesso em 26 fev 2022.

86 CALIFÓRNIA, E. U. A. *Lei n° 375, de 29 de julho de 2018: Lei da Califórnia de Privacidade do Consumidor*. 2018. Disponível em: <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375>. Acesso em 26 fev 2022.

87 BRANDEIS, L.; WARREN, S. The right to privacy. *Harvard law review*, v. 4, n. 5, p. 193–220, 1890.

88 PROSSER, W. L. Privacy, 48. *California Law Review*, v. 383, 1960.

89 BLOUSTEIN, E. J. Privacy as an aspect of human dignity: An answer to dean prosser. *NYUL rev.*, HeinOnline, v. 39, p. 962, 1964.

90 ZANINI, L. E. D. A. et al. A tutela dos direitos da personalidade na alemanha. *Interfaces Científicas-Direito*, v. 8, n. 2, p. 266–283, 2020.

91 PINTO, P. C. C. d. M. A protecção da vida privada e a constituição. *Boletim da Faculdade de Direito da Universidade de Coimbra*, HeinOnline, v. 76, p. 153, 2000.

92 DONEDA, D. *Da privacidade à proteção de dados pessoais*. [S.l.]: Renovar Rio de Janeiro, 2006.

93 QUEIROZ, R. M. R.; PONCE, P. P. Tércio sampaio ferraz júnior e sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do estado: o que permanece e o que deve ser reconsiderado. *Internet & Sociedade, São Paulo*, n. 1, p. 64–90, 2020.

94 RODOTÀ, S. Privacy, libertà, dignità. In: *Ponencia presentada en la 26a Conferencia internacional sobre privacidad y protección de datos personales, Breslavia*. [S.l.: s.n.], 2004. p. 14–16.

95 ONU, O. N. U. Declaração universal dos direitos do homem. *Adoptada e proclamada pela Assembleia Geral das Nações Unidas, na sua Resolução 217ª (III) de*, v. 10, 2006.

96 EUROPE, E. C. o. H. R. C. o. Convenção europeia dos direitos do homem. *Conselho da Europa. Roma*, v. 4, 2017.

97 HUMANOS, C. A. S. D. Comissão interamericana de direitos humanos. *San José*, v. 22, 1969.

98 FRANÇA. *Code civil français - Código civil francês*. 2023. Disponível em: <https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070721>. Acesso em 13 mar 2023.

99 ESPANHOLA, C. *Constitución Española Junta de Castilla y León Junta de Castilla y León.[online]*. 1978. Disponível em: <https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugu%C3%A9s.pdf>. Acesso em 13 mar 2023.

100 PORTUGAL. *Constituição da República Portuguesa*. 1976. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em 13 mar 2023.

101 COLOMBO, C.; BERNI, D. L. M. Privacy no direito italiano: Tríade de decisões judiciais rumo a insights sobre limites conceituais, deslocamento geográfico e transparência do corpo eletrônico. *Revista IBERC*, v. 5, n. 1, p. 112–131, 2022.

102 BRASIL, R. F. d. *Lei nº 10.406 de 10 de janeiro de 2002. Institui o Código Civil*. 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em 20 maio 2023.

103 READS, E. *Google Tracks 39 Types of Private Data, the Highest Among Big Tech Companies*. 2022. Disponível em: <https://stockapps.com/blog/google-tracks-39-types-of-private-data-the-highest-among-big-tech-companies/>. Acesso em 03 abr 2023.

104 GOOGLE, C. *Google: How our business works*. 2023. Disponível em: <https://about.google/intl/ALL_us/how-our-business-works/>. Acesso em 03 abr 2023.

105 ZUBOFF, S. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. *Rio de Janeiro: Intrínseca*, p. 585, 2020.

106 FORBES. *Por que a nova regra de privacidade da Apple fez as big techs perderem bilhões?* 2022. Disponível em: <https://forbes.com.br/forbes-tech/2022/02/por-que-a-nova-regra-de-privacidade-da-apple-fez-as-big-techs-perderem-bilhoes/>. Acesso em 03 abr 2023.

107 RODOTÀ, S.; MORAES, M. C. B. d.; DONEDA, D.; DONEDA, L. C. A vida na sociedade da vigilância: a privacidade hoje. In: *A vida na sociedade da vigilância: a privacidade hoje*. [S.l.: s.n.], 2008. p. 381–381.

108 HOBBES, T. *O Leviatã, tradução por João Paulo Monteiro e Maria Beatriz Nizza da Silva*. [S.l.]: LeBooks Editora, 2019.

109 LOCKE, J. *Segundo tratado sobre o governo civil e outros escritos. Ensaio sobre a origem, os limites e os fins verdadeiros do governo civil*. [S.l.]: BOD GmbH DE, 2019.

110 ROUSSEAU, J.-J. *Do contrato social ou princípios do direito político*. [S.l.]: BOD GmbH DE, 2017.

111 MELLO, C. A. B. D.; ANTÔNIO, C. *Curso de direito administrativo. 29ª ed*. [S.l.]: São Paulo: Malheiros Editores, 2011.

112 FILHO, J. d. S. C. Manual de direito administrativo. *São Paulo: Atlas*, v. 2, p. 50, 2012.

113 FILHO, M. J. *Curso de direito administrativo. 4ª ed*. [S.l.]: São Paulo: Saraiva, 2009.

114 CGU, C. G. U. *Relatório de consolidação dos resultados de avaliações realizadas pela Controladoria-Geral da União (CGU) acerca da execução do Auxílio Emergencial 2021 (AE 2021), instituído por meio da Medida Provisória (MP) no 1.039, de 18.03.2021*. 2021. Disponível em: <https://eaud.cgu.gov.br/relatorios/download/1162867>. Acesso em 05 abr 2023.

115 ANPD, A. N. P. D. *ANPD divulga lista de processos sancionatórios: A Autoridade divulga em transparência ativa a lista dos processos sancionatórios de empresas e órgãos públicos que aguardam conclusão*. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-sancionatorios>. Acesso em 06 abr 2023.

116 CASTRO, J. *Em palestra: Para Moraes, big techs devem ser equiparadas a empresas de comunicação*. 2023. Disponível em: <https://www.jota.info/stf/do-supremo/big-techs-nao-podem-fazer-a-politica-do-avestruz-diz-moraes-sobre-combate-a-fake-news-13032023>. Acesso em 06 abr 2023.

117 JURÍDICO, R. C. *Revista Consultor Jurídico - Combate à desinformação: Alexandre volta a defender responsabilização de plataformas digitais*. 2023. Disponível em: <https://www.conjur.com.br/2023-mar-31/alexandre-volta-defender-responsabilizacao-plataformas-digitais>. Acesso em 06 abr 2023.

118 EUROPA, P. E. *Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais)*. 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065>. Acesso em 01 maio 2023.

119 EUROPA, P. E. *Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho, de 14 de setembro de 2022, relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais)*. 2022. Disponível em: <https://eur-lex.europa.eu/eli/reg/2022/1925>. Acesso em 01 maio 2023.

120 MENDES, L. S. F. Autodeterminação informativa: a história de um conceito. *Pensar-Revista de Ciências Jurídicas*, v. 25, n. 4, 2020.

121 BRASIL, R. F. d. *Supremo Tribunal Federal: Arguição de Descumprimento de Preceito Fundamental n° 572. Compartilhamento dos Relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil com os órgãos de persecução penal para fins criminais*. 2020. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&queryString=uif%20compartilhamento%20RFB%20MP&sort=_score&sortBy=desc>. Acesso em 07 abr 2023.

122 BRASIL, R. F. d. *Supremo Tribunal Federal: Constitucionalidade do compartilhamento com o Ministério Público Eleitoral, para fins de apuração de irregularidades em doações eleitorais, dos dados fiscais de pessoas físicas e jurídicas obtidos com base em convênio firmado entre a Receita Federal e o Tribunal Superior Eleitoral, sem autorização prévia do Poder Judiciário*. 2019. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&pesquisa_inteiro_teor=false&sinonimo=true&plural=true&radicais=false&buscaExata=true&page=1&pageSize=250&queryString=compartilhamento%20de%20dados%201296829&sort=_score&sortBy=desc>. Acesso em 08 abr 2023.

123 BRASIL, R. F. d. *Supremo Tribunal Federal: ADI 6387/2020: Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o Instituto Brasileiro de Geografia e Estatística - IBGE*. 2020. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur436273/false>. Acesso em 07 abr 2023.

124 BRASIL, R. F. d. *Supremo Tribunal Federal: ADI 4924/2022: Contra a Lei estadual 17.107/2012, que instituiu multa por trote e acionamento indevido dos serviços telefônicos de atendimento a emergências envolvendo remoções ou resgates, combate a incêndios, ocorrências policiais ou atendimento de desastres*. 2022. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4382183>. Acesso em 07 abr 2023.

125 BRASIL, R. F. d. *Supremo Tribunal Federal: ADI 6529/2021: Vedação ao abuso de direito e ao desvio de finalidade. Obrigatoriedade de motivação do ato administrativo de solicitação de dados de inteligência aos órgãos do Sistema Brasileiro de IOnteligência - SISBIN*. 2021. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837>. Acesso em 07 abr 2023.

126 BRASIL, R. F. d. *Supremo Tribunal Federal: ADI 4739/2021: Conflita com a Constituição Federal - CF, considerada competência normativa reservada à União, lei estadual a versar fornecimento, à polícia judiciária, pelas empresas concessionárias de serviços de telecomunicação, de informação sobre a localização de aparelhos de telefonia móvel*. 2021. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4212219>. Acesso em 08 abr 2023.

127 BRASIL, R. F. d. *Supremo Tribunal Federal: ADI 5040/2021: Lei nº 6.336/2013 do Estado do Piauí. Prestadoras de servi;os de telefonia móvel. Obrigação de fornecimento de informações para fins de segurança pública*. 2021. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4461936>. Acesso em 20 maio 2023.

128 BRASIL, R. F. d. *Supremo Tribunal Federal: ADI 4401/2019: Lei nº 18.721/2010 do Estado de Minas Gerais, que dispõe sobre o fornecimento de informações por concessionária de telefonia fixa e móvel para fins de segurança pública*. 2019. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=3860438>. Acesso em 08 abr 2023.

129 RODOTÀ, S. *Tecnologie e diritti*. [S.l.]: Società editrice il Mulino, Spa, 2021.

130 SARMENTO, D. A ponderação de interesses na constituição federal de 1988. *Rio de Janeiro: Lumen Juris*, 2009.

131 BRANCO, P. G. G. *Juízo de ponderação na jurisdição constitucional*. [S.l.]: Brasília: Saraiva Educação SA, 2017.

132 BRASIL, R. F. d. *Supremo Tribunal Federal: ADI 3311/2022: Art. 3º, Caput e §§ 2º, 3º, 4º, 5º E 6º, da Lei nº 9.294/1996. Produtos fumígenos, derivados ou não do tabaco. Restrições à propaganda comercial. Advertências sanitárias nas embalagens*. 2022. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=2246660>. Acesso em 10 abr 2023.

133 BRASIL, R. F. d. *Supremo Tribunal Federal: ADI 4815/2015: Arts. 20 e 21 da Lei nº 10.406/2002 (Código Civil)*. 2015. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057>. Acesso em 10 abr 2023.

134 BRASIL, R. F. d. *Supremo Tribunal Federal: ARE 654432/2017: Vedação absoluta ao exercício do direito de greve aos servidores públicos integrantes das carreiras de segurança pública*. 2017. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4128634>. Acesso em 10 abr 2023.

135 DORNELAS, F. M. A proteção de dados pessoais na pandemia de covid-19: breves notas sobre "contact tracing apps" e o direito à privacidade na era da vigilância. *Jus Scriptum's International Journal of Law*, v. 6, n. 1, p. 79–101, 2021.

136 FARIAS, G. G. d. Vigilância movida a dados como mecanismo de combate à covid-19 e seus limites éticos envoltos na proteção de dados pessoais. *Caderno Virtual*, v. 2, n. 47, 2020.

137 SMANIO, G. M. A busca reversa por dados de localização na jurisprudência do superior tribunal de justiça: análise crítica do rms 61.302/rj. *Revista Brasileira de Ciências Policiais*, v. 12, n. 5, p. 49–76, 2021.

138 BRASIL, R. F. d. *Superior Tribunal de Justiça: RMS 62143/2020: Direito à privacidade e à intimidade. Identificação de usuários em determinada localização geográfica. Imposição que não indica pessoa individualizada. Ausência de ilegalidade ou de violação dos princípios e garantias constitucionais*. 2020. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201903182523&dt_publicacao=08/09/2020>. Acesso em 11 abr 2023.

139 MARQUES, J. G. P. d. S. *As modernas técnicas de investigação policial*. 2019. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-penal/as-modernas-tecnicas-de-investigacao-policial/>. Acesso em 20 maio 2023.

140 BRASIL, R. F. d. *Superior Tribunal de Justiça: HC 674031/2021: Direito Penal, Crimes Previstos na Legislação Extravagante, Crimes de Tráfico Ilícito e Uso Indevido de Drogas, Tráfico de Drogas e Condutas Afins.* 2020. Disponível em: <https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=202101857037&totalRegistrosPorPagina=40&aplicacao=processos.ea>. Acesso em 13 abr 2023.

141 HAGGERTY, K. D.; ERICSON, R. V. The surveillant assemblage. *The British journal of sociology*, Wiley Online Library, v. 51, n. 4, p. 605–622, 2000.

142 BENTHAM, J. *O panóptico[et al.]; organização de Tomaz Tadeu ; traduções de Guacira Lopes Louro, M. D. Magno, Tomaz Tadeu. – 2ª ed*. [S.l.]: Belo Horizonte: Autêntica, 2008.

143 BRASIL, R. F. d. *Projeto de Lei 3651/1997: Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências*. 1997. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=25586>. Acesso em 20 maio 2023.

144 BRASIL, R. F. d. *Resolução nº 2/2013-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*. 2013. Disponível em: <https://www2.camara.leg.br/legin/fed/rescon/2013/resolucao-2-22-novembro-2013-777449-norma-pl.html#:~:text=EMENTA%3A%20Disp%C3%B5e%20sobre%20a%20Comiss%C3%A3o,7%20de%20dezembro%20de%201999>. Acesso em 16 abr 2023.

145 BRASIL, R. F. d. *Relatório de atividades 2015: Comissão mista de controle das Atividades d Inteligência*. 2015. Disponível em: <http://legis.senado.leg.br/sdleg-getter/documento/download/801dc07e-afc7-4bbe-942b-84c41c17d471>. Acesso em 16 abr 2023.