Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Artigo de pesquisa

Larissa Maria Melo Ambrozio de Assis[1]
ORCiD 0009-0000-0681-2147

PARÂMETROS LEGAIS PARA O USO ESTATAL DE FERRAMENTAS TECNOLÓGICAS POTENCIALMENTE INTRUSIVAS PARA FINS DE SEGURANÇA

https://doi.org/10.58960/rbi.2025.20.274

Assis, Larissa Maria Melo Ambrozio de. 2025. "Parâmetros legais para o uso estatal de ferramentas tecnológicas potencialmente intrusivas para fins de segurança." *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.274. https://doi.org/10.58960/rbi.2025.20.274.

Recebido em 09/04/2025
Aprovado em 22/04/2025
Publicado em 24/04/2025

1 Pesquisadora associada ao Núcleo de Pesquisa em Inteligência (NUPI) da Escola de Inteligência (ESINT). Integrante da Rede LideraGOV do Poder Executivo Federal. Graduada em Direito pelo Centro Universirario de Brasília (UniCEUB), mestre em Direito pelo UniCEUB, com intercâmbio pela Universidad Nacional del Litoral (Argentina) e doutora em Direito pela Universidade de Brasília (UnB) com intercâmbio na Law School da Cornell University (EUA).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

PARÂMETROS LEGAIS PARA O USO ESTATAL DE FERRAMENTAS TECNOLÓGICAS POTENCIALMENTE INTRUSIVAS PARA FINS DE SEGURANÇA

Resumo

Este artigo trata da problemática dos parâmetros para o uso de ferramenta tecnológica potencialmente intrusiva (FTPI) para fins de manutenção da segurança da sociedade e do Estado e da segurança pública. O estudo parte do recorte dos direitos fundamentais afetados pelo uso de FTPIs definido na audiência pública nº 39 do Supremo Tribunal Federal. O direito à segurança da sociedade e do Estado, a construção do conceito do direito à segurança e sua relação com o uso de ferramentas tecnológicas são analisados com o objetivo de distinguir a atividade de inteligência da atividade repressiva estatal. Em sequência, aborda-se sobre o controle e a *accountability* desses ramos de atuação estatal e propõe-se parâmetros para o uso de FTPIs adequados a essas finalidades.

Palavras-chave: ferramentas tecnológicas, inteligência, sistema repressivo, segurança da sociedade e do Estado, segurança pública.

LEGAL FRAMEWORK FOR STATE USE OF POTENTIALLY INTRUSIVE TECHNOLOGICAL TOOLS FOR SECURITY PURPOSES

Abstract

This article addresses the issue of establishing parameters for the use of potentially intrusive technological tools (PITTs) for the purpose of maintaining the security of society and the State and public security. The study is based on the framework of fundamental rights affected by the use of PITTs, as defined during the 39th Public Hearing of the Brazilian Supreme Federal Court. It analyzes the right to security, the development of the concept of the right to security, and its relationship with the use of technological tools, with the aim of distinguishing intelligence from State repressive activities. Subsequently, the article discusses the control and accountability mechanisms applicable to these areas of State action and proposes parameters for the use of PITTs.

Keywords*: technological tools, intelligence, repressive system, social and state security, public safety.*

PARÁMETROS LEGALES PARA EL USO ESTATAL DE HERRAMIENTAS TECNOLÓGICAS POTENCIALMENTE INTRUSIVAS CON FINES DE SEGURIDAD

Resumen

Este artículo aborda la problemática de los parámetros para el uso de herramientas tecnológicas potencialmente intrusivas (HTPIs) por parte del Estado, con la finalidad de preservar la seguridad de la sociedad e del Estado y la seguridad pública. El estudio analiza los derechos fundamentales afectados por el uso de las HTPIs, conforme la audiencia pública nº 39 del STF. Se examina el derecho a la seguridad, la construcción de su concepto y su relación con el uso de herramientas tecnológicas, con el objetivo de distinguir la actividad de inteligencia de la actividad represiva estatal. Posteriormente, se abordan los mecanismos de control y accountability aplicables a estos ámbitos de actuación estatal, y se proponen parámetros para el uso de las HTPIs.

Palabras clave*: herramientas tecnológicas, inteligencia, sistema represivo, seguridad de la sociedad y del Estado, seguridad pública.*

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Introdução

Na atual Era Digital, direitos fundamentais dos cidadãos são constantemente colocados em risco no domínio cibernético tanto pela atuação de atores privados quanto públicos. Neste artigo discutiremos sobre a atuação do Estado, mais especificamente sobre os parâmetros para o uso de ferramenta tecnológica potencialmente intrusiva (FTPI) para fins de manutenção da segurança da sociedade e do Estado e da segurança pública, consideradas as finalidades estatais de atuação preventiva e repressiva.

O uso de ferramentas tecnológicas é crescente desde a revolução industrial, com especial escalada a partir da *Advanced Research Projects Agency Network* (ARPANET), na década de 1960, base para o desenvolvimento da internet nos anos 70 e 80 e, posteriormente, o seu uso civil. Porém, desde a criação e proliferação de tecnologias há a discussão sobre a vigilância global dos usuários (McLuhan e Powers 1992).

O caso Edward Snowden, em 2013, reforçou o debate sobre a vigilância estatal massiva da população a partir do uso de FTPIs.[1] O contínuo avanço tecnológico desde então torna imprescindível aprofundar o debate sobre quem vigia a atuação estatal e sobre a necessidade de transparência[2], controle e *accountability*[3] para o uso desses recursos (Cole 2014).

Esse debate ganhou densidade e dimensão no Brasil a partir da ADPF nº 1.143 (Brasil 2024b), que busca questionar as balizas para o uso de *spywares,* de

1 Vale ressaltar que essas ações foram realizadas com base no *USA PATRIOT Act*, que ampliou os poderes de vigilância externa e investigação das autoridades norte-americanas, permitindo o monitoramento de comunicações e outras atividades com o objetivo de combater o terrorismo.

2 A transparência não foi arrolada aqui porque dentro do emprego de ferramentas tecnológicas intrusivas, seja para fins de prevenção ou repressão, o sigilo é a regra, até mesmo para garantir o menor dano aos direitos à privacidade, intimidade, dos dados e da vida privada afetados pela ação estatal. Acredita-se que o parâmetro da transparência importa para a compreensão da limitação de liberdades individuais quando da análise dos estudos técnicos preliminares realizados para aquisição dessas ferramentas e do cumprimento da legislação que assegura a proteção de dados pessoais, dentre outras garantias fundamentais, e as implicações para a soberania digital do país. Apesar da relevância dessa análise, o enfoque desse estudo é centrado na perspectiva da autorização para o uso dessas ferramentas, de acordo com a motivação estatal de atuação preventiva ou repressiva. Sobre o debate de cibersegurança e soberania digital, uma referência relevante é a obra de Luca Belli e outros (2023).

3 Uso o termo *accountability* ao invés de responsabilidade pela intenção de considerar o dever de prestação de contas, de transparência, de controle e de fiscalização, enquanto um conjunto de práticas que envolvem a responsabilização de gestores e instituições por suas ações (IFAC 2001). Para o debate sobre a tradução do termo para português, confira Pinho e Sacramento (2009).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Imsi Catchers, e de dispositivos que rastreiam a localização de um alvo específico através da rede celular.[4] A ação, assim, reabriu o debate brasileiro, por meio da audiência pública, para o uso de FTPIs, sobretudo o seu uso sem critérios legais específicos que permitam o controle e a *accountability*.

Essa discussão não é exclusiva ao Brasil. O relatório da ONU sobre privacidade na era digital indica justamente esse problema e concluiu por três tendências notáveis relacionadas ao papel dos Estados na salvaguarda e promoção do direito à privacidade: a atenção ao abuso generalizado de ferramentas intrusivas de hackeamento; ao seu papel fundamental de criptografia robusta para garantir o exercício do direito à privacidade e de outros direitos; e ao monitoramento generalizado dos espaços públicos (ONU 2022).

As FTPIs, quando utilizadas pelo Estado, devem atender a finalidades específicas porque podem afetar direitos fundamentais[5]. Nesse ponto, o direito à segurança, enquanto direito fundamental previsto no *caput* do art. 5º da Constituição Federal (CF), é destacado como principal fator de motivação para o uso dessas ferramentas. Contudo, os fundamentos da Constituição, a efetivação dos objetivos do País e a proteção dos princípios das relações internacionais, previstos nos arts. 1º a 4º da CF[6], igualmente podem motivar o uso das FTPIs.

Para tanto, trataremos do tema em quatro partes. Primeiro traremos alguns esclarecimentos sobre as FTPIs destacadas na ADPF nº 1.143 e no debate da audiência pública nº 39 do Supremo Tribunal Federal (STF), particularmente sobre como elas podem afetar um determinado rol de direitos fundamentais. Em segundo, abordaremos o dever estatal de prover o direito à segurança da sociedade e do Estado, onde buscaremos compreender a construção do conceito do direito à segurança e sua relação com o uso de ferramentas tecnológicas. Em terceiro, trataremos de compreender as distinções entre a inteligência e o aparato punitivo estatal em suas finalidades de atuação

4 Em sua peça inicial, o Ministério Público Federal (MPF) não se manifesta contrário ao uso dessas ferramentas, mas reclama a omissão de parâmetros para o uso e considera a necessidade de controle judicial prévio. Na audiência pública, por exemplo, o MPF defendeu o uso de *spywares* contra estrangeiros pela inteligência (Brasil 2024).

5 Consideramos aqui o conceito de direitos fundamentais de Robert Alexy (1993), pelo qual esses direitos são normas de ordem constitucional que se distinguem por seu caráter de princípio, ou seja, um mandamento de otimização.

6 Vale ressaltar, ainda, que a motivação para relativizar tais direitos, seja pela finalidade estatal de prevenção ou repressão, não se limita aos dispositivos aqui elencados. O Estado pode, por exemplo, motivar sua atuação na proteção da ordem econômica, o que envolve também previsões do art. 170 a 181 da CF.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

para concretização do direito à segurança, com o objetivo de compreender as necessidades específicas de controle e a *accountability* desses ramos de atuação estatal. Tais bases nos serviram para propormos, ao final, alguns parâmetros mínimos de uso de FTPIs pelo Estado.

Como ferramentas potencialmente intrusivas podem afetar direitos fundamentais?

Ferramentas tecnológicas de comunicação facilitam a difusão e o acesso à informação, por meio de redes e de dispositivos eletrônicos[7]. No contexto da ADPF nº 1.143 (Brasil 2024b), há uma preocupação com a capacidade intrusiva dessas ferramentas, ou seja, de acesso aos dispositivos eletrônicos pessoais de determinado indivíduo, contra sua vontade[8], o que gera impacto para uma série de direitos fundamentais.

De acordo com a petição inicial da ADPF nº 1.143, o caráter intrusivo dessas ferramentas é definido por sua capacidade de proporcionar o monitoramento de aparelhos digitais de comunicação pessoal de forma remota. É importante compreendermos que se trata de algo diferente da ferramenta tecnológica ser invasiva, o que significa que ela subverte a forma de funcionamento do sistema para acessar o dispositivo por manipular a informação e comprometer a integridade do dispositivo eletrônico (Schneier 2018).

Para melhor compreensão de como FTPIs interferem nos direitos fundamentais, voltaremos nossa análise para o debate da audiência pública da ADPF nº 1.143, que destacou três FTPIs: *spywares*; *International Mobile Subscriber Number (Imsi) Catchers* e ferramentas de geolocalização[9].

7 Dispositivos eletrônicos funcionam a partir de uma arquitetura de infraestrutura de hardware, software e de telecomunicações, que são a base para manter sistemas de informação acessíveis aos usuários com características de flexibilidade, escalabilidade, confiabilidade, disponibilidade e desempenho (Tanenbaum e Bos 2016).

8 Em relação ao acesso de dispositivos eletrônicos é essencial considerar a ação do próprio usuário do dispositivo eletrônico rastreado. O usuário pode ter consentido com o acesso da FTPI de maneira intencional ou por omissão. É preciso conferir, também, se o usuário registrou o não consentimento de forma expressa e seu dispositivo, ainda assim, foi acessado contra sua vontade.

9 Ferramentas de geolocalização consistem em tecnologias que permitem identificar a posição geográfica de dispositivos eletrônicos, utilizando coordenadas geográficas (latitude e longitude) obtidas através de sinais de satélite, redes de internet ou radiofrequência.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Spywares

Mais que ferramentas intrusivas, *spywares*[10] são invasivos por serem capazes de monitorar e registrar uma variedade de atividades do usuário, como hábitos de navegação, teclas pressionadas, credenciais de sistemas, informações pessoais e outras atividades online.

Um exemplo de *software* empregado como *spyware* é o *Pegasus*, com capacidade altamente invasiva, permitindo acesso ilimitado a um dispositivo por padrão, deixando poucos ou nenhum vestígio, e tornando difícil para os usuários saberem quais dados foram capturados. O *Pegasus*, em específico, permite o monitoramento das teclas, de todas as comunicações de um telefone (textos, e-mails, pesquisas na web), assim como de chamadas telefônicas, de localização e de acesso ao microfone e à câmera do dispositivo eletrônico[11].

Outro *spyware* de impacto expressivo é o *TriangleDB*, que possui a capacidade, também, de manipular arquivos e processos em curso pelo dispositivo eletrônico infectado, extrair dados de certificado, identidades digitais e outras credenciais, além de transmitir a localização precisa do equipamento[12].

Spywares, portanto, são instrumentos invasivos que podem viabilizar a violação dos direitos fundamentais à intimidade, à vida privada, à inviolabilidade do sigilo das comunicações pessoais e de dados, nos termos do art. 5º, incisos X, XII e LXXIX da CF.

Quando pensamos a finalidade punitiva estatal, a capacidade de manipulação de arquivos e processos nos dispositivos eletrônicos permite o uso indevido para criar provas de condutas delitivas falsas contra indivíduos, razão pela qual se soma, potencialmente, à violação de direitos fundamentais ao devi-

10 Segundo o Glossário de Segurança da Informação publicado pelo Governo Federal, *spywares* "são um tipo de malware. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware" (Brasil 2021b). Vale considerarmos também o conceito apresentado pelo *National Institute of Standards and Technology* (NIST), segundo o qual *spyware* é "*[s]oftware that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code*" (NIST s.d.).

11 A ferramenta é desenvolvida pelo NSO Group, que afirma só fornecê-la para governos autorizados a auxiliá-los no combate ao terrorismo e ao crime, além de exigir dos clientes que utilizem os seus produtos apenas para investigações criminais e de segurança nacional (Kirchgaessner *et al.* 2021).

12 Para saber mais sobre o TriangleDB confira as publicações da Kaspersky (2023).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

do processo legal para ser privado da liberdade, ao contraditório e à ampla defesa, assim como do direito à inadmissibilidade do uso de provas ilícitas, da presunção de inocência e de não ser submetido à identificação criminal, salvo nos casos previstos em Lei, conforme dispõe o art. 5º, incisos LIV, LV, LVI, LVII e LVIII da CF.

Imsi Catchers

Imsi Catchers são utilizados para localizar dispositivos eletrônicos móveis (celulares), sem capacidade para captar o conteúdo da comunicação desses dispositivos. Basicamente, esses recursos concedem, dentre outros, o acesso a metadados[13] que fornecem a localização aproximada do dispositivo, o que permite monitoramento da localização de um indivíduo que porta o aparelho celular (Broek, Roel e Ruiter 2015).

Essas tecnologias possuem diversas variantes, que podem ser empregadas de forma "passiva", que se limita a capturar o identificador do celular, ou "ativa", quando a ferramenta testa se o dispositivo está ativo. Todavia, essas FTPIs só acessam metadados, sem capacidade intrusiva de acessar o teor da comunicação. Assim, mesmo que a ferramenta consiga dizer que o dispositivo se comunica com outro, não consegue acessar o conteúdo dessa comunicação.

Os *Imsi Catchers* possuem aplicações legítimas pela inteligência, como a detecção de redes móveis clandestinas, ou até mesmo como um instrumento de contrainteligência ao identificar que alguma rede de telefonia celular esteja sendo monitorada em alguma localidade específica (Sampaio 2023).

Essas FTPIs, portanto, não possuem potencial de violar o sigilo das comunicações pessoais e de dados. O uso repetitivo de *Imsi Catchers* pode fornecer conhecimento de hábitos de localização, por exemplo, o que podemos considerar, eventualmente, como uma relativização de direitos à intimidade, à vida privada, à privacidade.

Quanto à finalidade punitiva estatal, essas ferramentas não realizam qualquer ação invasiva, com acesso intrusivo somente aos metadados. Dessa forma, elas não detêm capacidade lesiva de, teoricamente, serem utilizadas para promover uma instrução probatória eivada de vícios por violação de direitos

13 Os metadados possuem diversos conceitos, mas podemos considerá-los como dados que descrevem outros dados (Arakaki e Arakaki 2020). No caso dos metadados registrados da comunicação de dispositivos eletrônicos, esses metadados são como um envelope do processo comunicacional que registra dados como a identificação do usuário, a localização, o tipo de mensagem, a rede utilizada, o horário, a duração.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

fundamentais ao devido processo legal para ser privado da liberdade, ao contraditório e à ampla defesa, assim como do direito à inadmissibilidade do uso de provas ilícitas, da presunção de inocência e de não ser submetido à identificação criminal, salvo nos casos previstos em Lei.

Geolocalização

A geolocalização, por sua vez, não se confunde com comunicações privadas e pode ser usada para monitoramento de pessoas, tanto pelo uso do Serviço Móvel Pessoal (SMP), pelo *Global Positioning System* (GPS) ou por meio de "aplicativos".

A SMP é um serviço de telecomunicações de superfície, que permite a comunicação entre aparelhos móveis e aparelhos de diferentes estações, a partir de ondas de rádio que viabilizam a transmissão de dados e voz, inclusive com acesso à internet de banda larga para navegação via web, enviar e receber e-mails e usar aplicações que dependem do acesso à internet.

Para realizar essa transmissão entre os dispositivos são utilizadas Estações de Rádio Base (ERBs) e, a partir da triangulação dos dados de diferentes ERBs, é possível identificar a localização aproximada de um dispositivo[14].

O GPS pode ser entendido como um sistema de triangulação que usa sinais de rádio enviados por satélites artificiais. Receptores de GPS interpretam esses sinais e convertem as informações em coordenadas geográficas. Por meio dessa tecnologia, é possível precisar a localização de dispositivos, mesmo com serviços de *bluetooth*, *wi-fi* e telefonia desativados.

Por último, os aplicativos, popularmente conhecidos como Apps, são *softwares*, instalados em dispositivos eletrônicos, que oferecem soluções às necessidades dos usuários. Essas aplicações, vale destacar, permitem o compartilhamento da localização em tempo real, exigindo que o usuário disponibilize sua localização. Uma das razões para expansão do mercado de dados foi a perspectiva econômica do desenvolvimento de aplicações e serviços de tecnologia da informação, que viabilizaram a venda e "aluguel" de dados pessoais, no intento de reduzir custos para a transação dos empreendimentos tecnológicos (Varian 1996). Diversos Apps permitem o compar-

14 A Agência Nacional de Telecomunicações (Anatel) é a responsável por regular e controlar o acesso a dados da rede SMP. Sobre a regulamentação do SMP é importante conferir, ao menos, a Lei nº 9.472 – Lei Geral de Telecomunicações - LGT, de 16 de julho de 1997, a Resolução Anatel nº 477, de 7 de agosto de 2007, a Resolução Anatel nº 550, de 22 de novembro de 2010 e a Resolução Anatel nº 738, de 21 de dezembro de 2020.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

tilhamento da localização em tempo real, com a autorização concedida pelo usuário, o que é realizado utilizando tanto a geolocalização por GPS, como por SMP que permite a conexão com a internet.

Essas FTPIs de geolocalização não acessam dados ou comunicações, logo, não possuem essa capacidade lesiva. O uso delas permite georreferenciar pessoas a partir de seus dispositivos eletrônicos, o que pode relativizar direitos fundamentais à intimidade, à vida privada e à privacidade. Pelo entendimento dos Tribunais Superiores (Brasil 2020a; 2020c; Smanio 2021), entretanto, é constitucional e legal geolocalizar indivíduos por meio de FTPIs, face às necessidades estatais de assegurar outros direitos fundamentais, como a segurança[15]. A jurisprudência indica a necessidade de se observar critérios como o motivo e a motivação que explicite a proporcionalidade do uso de determinada FTPI que permita a geolocalização de um dispositivo.

Quando consideramos a finalidade punitiva estatal, o uso indevido desses recursos pode levar à violação do direito ao devido processo legal para ser privado da liberdade, ao contraditório e à ampla defesa, assim como do direito à inadmissibilidade do uso de provas ilícitas, da presunção de inocência e de não ser submetido à identificação criminal, salvo nos casos previstos em Lei.

Os direitos fundamentais em questão não são compreendidos como absolutos, visto que a esfera de proteção de um determinado direito leva à redução de outro direito igualmente protegido em nível constitucional (Andrade 1987). Assim, é necessário considerarmos a ponderação desses direitos, no caso concreto, para relativizar sua proteção de forma proporcional, dentro da concepção de colisão entre direitos fundamentais.

Quando pensamos o rol de direitos destacados em colisão, é necessário considerar a densidade desses direitos, visto que não são compreensíveis como dispositivos estáticos, mas como normas em sentido amplo de ordem principiológica por permitirem múltiplas facetas de interpretação de acordo com o caso concreto. Segundo Robert Alexy (1993, 105):

> [l]as contradicciones de normas en sentido amplio que tienen lugar dentro del ordenamiento jurídico son siempre colisiones de principios y las colisiones de principios se dan siempre dentro del ordenamiento jurídico. Esto pone claramente de manifiesto que el concepto de colisión de

15 É preciso considerarmos, inclusive, que o setor privado promoveu a geolocalização de pessoas por Apps durante a pandemia da COVID-19 e deixou a tecnologia à disposição dos órgãos e entidades públicas para fins de combate à disseminação do Coronavirus. A *startup* In Loco chegou a disponibilizar os dados estatísticos de geolocalização ao Estado de forma gratuita para essa finalidade de controle sanitário (ABES 2020).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

> principios presupone la validez de los principios que entran en colisión. Por ello, la referencia a la posibilidad de catalogar a los principios como inválidos no afecta el teorema de la colisión sino que simplemente revela uno de sus presupuestos.

Assim, não é possível a resolução da colisão de princípios constitucionais pela simples supressão de um em favor de outro, por não se tratar de dizer que um é válido e outro não. É preciso considerar o peso ou a importância relativa de cada princípio, com o objetivo de definir no caso concreto qual será limitado em face do outro.

A compreensão da colisão de direitos fundamentais exige uma visão estrutural, com o estudo dos conceitos desses direitos, sua influência no sistema jurídico e sua fundamentação. Isso requer tanto a compreensão da jurisprudência sobre tais direitos, como a reflexão sobre qual a decisão mais correta de limitação dos direitos fundamentais dentro do caso concreto, para formular parâmetros interpretativos-concretizadores específicos para a realidade de uma determinada coletividade (Alexy 1993).

O direito fundamental à segurança e sua relação com o uso de ferramentas tecnológicas

O direito à segurança e o dever estatal de assegurá-la são complexos e envolvem tanto as esferas de prevenção quanto as de repressão. De modo geral, vale considerar a segurança como um estado de normalidade, onde os demais direitos e deveres são usufruídos e cumpridos[16]. Desde o século XVIII, ao menos, a segurança é considerada como dever fundamental do Estado, enquanto principal ator e agente securitizador, previsto no art. 2º da Declaração de Direitos do Homem e do Cidadão de 1789[17].

Assegurar esse direito possui uma relação histórica com o uso de recursos tecnológicos. Para garantir o sigilo das comunicações, por exemplo, desde o século XVI, há o registro de diversas tecnologias como mensagens cifradas,

16 O exercício do poder punitivo estatal em prol de garantir o Estado de Direito não é o enfoque central do nosso debate. A compreensão da formação dessa faceta estatal, de prover o espaço do exercício de direitos e deveres, possui relação intrínseca com a compreensão do exercício do poder político, a formação do conceito de homem cidadão e de justiça. A construção do que se compreende como exercício do poder punitivo perpassa a literatura de Aristóteles, Platão, Jean Bodin, Thomas Hobbes, Nicolas Montesquieu, John Locke, Jean-Marie Constant, Jean-Jacques Rousseau, John Rawls, dentre outros.

17 Declaração dos Direitos do Homem e do Cidadão, 1789, art. 2º: "O objetivo de toda associação política é a conservação dos direitos naturais e imprescritíveis do homem. Esses direitos são a liberdade, a propriedade, a segurança e a resistência à opressão".

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

mensagens codificadas, criptografia e, já no século XIX, o telégrafo, entre outros[18].

É no curso da Segunda Guerra Mundial que se registra crescimento dos estudos de inteligência e da perspectiva da finalidade de prevenção. O discurso da segurança era proposto para proteger a sociedade de atentados contra o bem-estar social dos seus nacionais e de interferência nas suas decisões e interesses legítimos. As estruturas de inteligência dos Estados eram incipientes, mas até o final da Guerra Fria foram desenvolvidas metodologias e formas racionais de construir o conhecimento necessário para resguardar o que se compreendia por segurança (Buzan 1983; Herman 1996).

No período da Guerra Fria, a corrida armamentista impulsionou o desenvolvimento de tecnologias voltadas para a segurança, bem como a criação efetiva de agências de inteligência[19], no contexto de reconstrução e realinhamento necessários para o desenvolvimento e a segurança dos nacionais e para orientar as políticas públicas.

É nesse contexto, já nas décadas de 70 e 80, que a pauta da segurança começa a considerar questões sociais, econômicas e humanitária na compreensão do fenômeno da insegurança, em especial da criminalidade enquanto uma problemática interna de segurança, independente da pauta de segurança nas relações exteriores[20].

No pós-Guerra Fria, os processos de redemocratização, a globalização, a

18 Desde o início, a atividade de inteligência promoveu de forma preventiva a proteção do conhecimento a partir da codificação de mensagens (Thompson e Padover 1965). O desenvolvimento da criptografia para proteger a informação é um dos marcos dessa finalidade, que inclusive é um dos destaques da ONU, ao apontar o uso de criptografia robusta como um dever do Estado (ONU 2022). Atualmente, no Brasil, compete ao órgão central do sistema de inteligência, por meio do Centro de Pesquisa para o Desenvolvimento da Segurança das Comunicações (CEPESC), promover e desenvolver esses algoritmos, que são empregados, inclusive, nas urnas eletrônicas desde 1996 (ABIN s.d.).

19 Os serviços de inteligência foram organizados e estruturados em diversos países — como Alemanha, França, Estados Unidos das Américas, Reino Unido, União Soviética, Itália, dentre outros — até a Segunda Guerra Mundial (Bobbio, Matteucci e Pasquino 2016, 1147-1148).

20 Vale ressaltar que até a década de 1980 predominava a visão tradicional, dentro de um paradigma realista de segurança centrado no Estado forte, encarregado de manter a sua própria segurança territorial e de sua população por meio de visões distintas de segurança e defesa. A Escola de Copenhague somou a perspectiva de que estudos de segurança devem abranger, além das ameaças militares, aquelas provenientes das áreas política, econômica, ambiental e social. A premissa da Escola de Copenhague é que as pautas de defesa e segurança são construídas a partir de um contexto político e social da interpretação intersubjetiva (Buzan 1983; Floyd 2007).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

abertura econômica, a redução das regulações do mercado financeiro e a abertura de fronteiras representaram mudanças expressivas que intensificaram a transformação na gestão de diversas temáticas, entre elas, a segurança. A Agenda para a Paz da ONU, de 1992, concretiza essa virada do tratamento da pauta de segurança ao reconhecer que o seu conceito relaciona-se com a instabilidade nos campos econômico, social, humanitário e ecológico (ONU 1992).

Nesse período se registra uma distinção concreta e estruturada entre as finalidades de prevenção e repressão da atuação estatal, em especial a partir dos processos de redemocratização, com o intento de aumentar as liberdades constitucionalmente asseguradas e delimitar o poder punitivo estatal (Buzan 1983; Herman 1996).

O conceito de segurança, dentro dessa perspectiva, também passou por uma expansão e novas ameaças e perspectivas relativas a atores não-estatais foram incluídas, em temas correlatos como a economia, as fronteiras, os recursos naturais, demográficos, energéticos, cibernética, entre outros. Essa mudança, por exemplo, é registrada na estrutura atual de inteligência brasileira, conforme é detalhado nos "Desafios de Inteligência - Edição 2025" (Brasil 2025).

Com a densidade dessas mudanças e a complexidade do tratamento de múltiplas facetas do direito à segurança, o uso de ferramentas tecnológicas, intrusivas ou não, passa a ser uma necessidade para a resposta estatal de concretização desse direito. O impacto das mudanças trazidas pela tecnologia à sociedade demanda uma mudança de como compreendemos o alcance dos direitos fundamentais.

Diferenças entre garantir a segurança da sociedade e do Estado e a segurança pública

Justamente pela complexidade associada ao conceito de direito à segurança, o emprego de ferramentas tecnológicas para sua concretização necessita ser considerado de forma distinta, de acordo com a finalidade preventiva ou repressiva estatal. Como destacamos inicialmente, a finalidade, enquanto propósito da norma, é essencial para definirmos como interpretá-la e aplicá-la (Maximiliano 2003; Ferraz Júnior 1980).

Nesse ponto, a finalidade estatal nos apresenta motivo e motivações distintas para justificar o emprego de FTPIs, razão pela qual nos é importante com-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

preender a diferença entre segurança da sociedade e do Estado e segurança pública e a relação dessas com as finalidades de prevenção e repressão. Isso porque elas exprimem o motivo da atuação estatal, o que reduz o espectro de motivação para o emprego de FTPIs.

Inteligência e a finalidade preventiva da segurança da sociedade e do Estado

A Segurança da sociedade e do Estado é direcionada a garantir a estabilidade e a soberania do Estado, protegendo-o de ameaças externas e internas, de forma a promover a segurança e o bem-estar dos cidadãos (Kent 1949; Platt 1974). Isso requer ações, inclusive sigilosas, direcionadas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o processo decisório nacional, assim como para permitir o adequado planejamento e proteção de conhecimentos sensíveis para as decisões e interesses nacionais legítimos.

Apesar de o texto constitucional não prever de forma explícita a inteligência, ao estabelecer o dever estatal de garantir a segurança e de resguardar a soberania nacional, dentre diversos outros deveres atribuídos ao Estado, há a consolidação implícita da atuação de um sistema de inteligência[21].

Essa expressão do direito à segurança – Segurança da sociedade e do Estado – encontra guarida constitucional no *caput* do art. 5º da CF, e regulação infraconstitucional, em especial, na Lei nº 9.883, de 7 de dezembro de 1999, que institui o Sistema Brasileiro de Inteligência e cria a Agência Brasileira de Inteligência como seu órgão central, com atribuições de promover a segurança da sociedade e do Estado e de fornecer os subsídios para o assessoramento estratégico do Presidente da República, o que inclui ações e operações de caráter sigiloso.

As ações estatais de inteligência brasileiras são direcionadas a prevenir o dano e promover oportunidades, ou seja, sempre na perspectiva preventiva e sob o enfoque estratégico para o adequado assessoramento ao processo decisório, que assegure os interesses nacionais legítimos e viabilize a pro-

21 De acordo com a teoria dos poderes implícitos, quando a Constituição concede uma função a determinado órgão ou instituição, também lhe confere, implicitamente, os meios necessários para a consecução das funções que lhe foram atribuídas. Dessa forma, implicitamente, é válido considerar que o texto constitucional abarca a atuação do sistema de inteligência, por estabelecer deveres aos órgãos e instituições que dependem da atuação de um sistema de inteligência. Sobre o reconhecimento da teoria dos poderes implícitos e a imprescindibilidade do serviço de inteligência, confira a jurisprudência do STF (Brasil 2007; 2021a; 2022).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

teção dos conhecimentos sensíveis.

Atualmente, no Brasil, o mapa de ameaças e oportunidades da atividade de inteligência é orientado em uma perspectiva do conceito de segurança pós-Guerra Fria, pela Política Nacional de Inteligência, dentre diversos outros marcos normativos[22], que estabelece:

> **Atividade de Inteligência:** 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. A atividade de Inteligência divide-se, fundamentalmente, em dois grandes ramos:
>
> **I – Inteligência:** atividade que objetiva produzir e difundir conhecimentos às autoridades competentes, relativos a fatos e situações que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e do Estado;
>
> **II – Contrainteligência:** atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado (Brasil 2016b).

A Estratégia Nacional de Inteligência complementa essa visão por indicar a seguinte finalidade da 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 (Brasil 2017a).

O sistema de inteligência existe, assim, para obter dados, processá-los e transformá-los em conhecimento. Para isso é necessário gerir diversos dados de fontes abertas, de bases governamentais de acesso restrito e também dados não acessíveis por outros meios.

22 Vide a Lei nº 11.776, de 17 de setembro de 2008, que dispõe sobre a estruturação do Plano de Carreiras e Cargos da Agência Brasileira de Inteligência - ABIN; o Decreto nº 11.693, de 6 de setembro de 2023, que dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência; Resolução nº 2, de 2013-CN, que dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI); o Decreto nº 8.793, de 29 de junho de 2016, que fixa a Política Nacional de Inteligência; o Decreto S/N, de 15 de dezembro de 2017, que aprova a Estratégia Nacional de Inteligência; e a Portaria GAB/DG/ABIN/CC/PR no 1.205, de 27 de novembro de 2023, que aprova a Doutrina da Atividade de Inteligência. Esses normativos e outros que ainda seguem necessários de regulamentação são essenciais pela atividade de inteligência fugir à regra da transparência de suas ações, pela necessidade de sigilo, eles possuem regras mais estritas de controle e de *accountability*.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

O compartilhamento de dados dentro do sistema foi debatido pelo STF na ADI nº 6.529 (Brasil 2021a), onde se estabeleceram diretrizes complementares para o fornecimento de dados à ABIN. Sobre os dados não acessíveis por outros meios, o uso de ferramentas tecnológicas, inclusive as intrusivas, é essencial para alcançar desses dados, com o intento de promover a segurança da sociedade e do Estado. Isso porque o cenário internacional demanda ações de inteligência e de contrainteligência para proteger os interesses nacionais legítimos e seus cidadãos no ciberespaço[23], sobretudo quando consideramos o ambiente cibernético como palco de conflito entre serviços de inteligência (Broeders 2024; Nussbaum 2017; Oosthoek e Doerr 2021; Ambros 2024).

O serviço de Inteligência estatal brasileiro serve, assim, para prover informações e conhecimentos essenciais[24] para a tomada de decisão em várias dimensões institucionais, em níveis estratégico, tático e operacional, com impactos positivos nas três esferas de poder, assim como para proteger as atividades do Estado contra tentativas de interferência estrangeira[25] que

23 O STF tem debatido a importância da segurança cibernética para a proteção de direitos fundamentais no julgamento da ADI nº 5527, Min. Relatora Rosa Webber e da ADPF nº 403, Min. Rel. As ações debatem a suspensão do funcionamento, por ordem judicial, de aplicações que fornecem proteção às comunicações (Whatsapp). Em seu voto, o Min. Rel Edson Fachin destacou sete premissas: "Primeira: o impacto tecnológico das mudanças porque passa a sociedade reclamam um permanente atualizar do alcance dos direitos e garantias fundamentais. Segunda: os direitos que as pessoas têm offline devem também devem ser protegidos online. Direitos digitais são direitos fundamentais. Terceira: a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. Quarta: a privacidade é o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública. Quinta: A liberdade de expressão tem primazia prima facie e constitui condição essencial ao pluralismo de ideias, vetor estruturante do sistema democrático de direito. Sexta: Na internet, a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões, o que geralmente ocorre por meio de comunicações online como o e-mail, mensagens de texto e outras interações. A criptografia, em especial, é um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública. Sétima: É contraditório que em nome da segurança pública deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas."

24 Vale compreendermos que quando falamos em informações e conhecimentos essenciais, não está inclusiva a divulgação de todo e qualquer dado. O profissional de inteligência processa os dados e possui dever de manter sigilo sobre dados a que obteve acesso, os quais não devem ser divulgados para fins de cumprimento da legislação vigente. Dessa forma, quando hipoteticamente um profissional da inteligência acessa dados que afetam a intimidade, a vida privada ou a privacidade de indivíduos, há o dever de não divulgação dessas esferas na medida em que não é relevante para formação do conhecimento necessário para o cumprimento de suas finalidades preventivas e de assessoramento estratégico. Há diversas decisões do STF (Brasil 2016a; 2024a) que tratam sobre o compartilhamento de dados e o dever de manutenção de sigilo dos servidores públicos que os acessam.

25 Sobre essas formas de ameaças estrangeiras, destacamos algumas estabelecidas na PNI,

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

comportam prejuízos ao país e ao bem-estar dos cidadãos.

Dentro da perspectiva de controle e *accountability*, a inteligência conta, atualmente, com o controle externo finalístico realizado *a posteriori,* conforme previsto no art. 6º da Lei nº 9.883, de 1999, pela Comissão Mista de Controle das Atividades de Inteligência (CCAI), do Congresso Nacional[26].

Ressalta-se que, até o momento, a inteligência não possui previsão legal de controle prévio judicial. Essa ausência normativa coaduna com a finalidade da atuação estatal de assegurar o direito à segurança da sociedade e do Estado, justamente por não afetar garantias penais e processuais penais e o direito à liberdade, conforme destacamos em seção anterior[27].

O emprego das FTPIs por esse controle requer que pensemos critérios que permitam ao controle ter a rastreabilidade e auditabilidade adequada para eventual responsabilização por violações de agentes públicos e do sistema de inteligência por suas ações.

Poder punitivo e a finalidade repressiva da segurança pública

Por sua vez, a segurança pública é uma reação formal ao crime, que abarca um conjunto de ações e políticas que o Estado realiza, a partir do seu poder coercitivo, para garantir a ordem pública e a proteção dos cidadãos. Isso envolve a atuação de órgãos e instituições que possuem atribuições de implementar a política criminal no intento de reduzir os índices de criminalidade e ampliar aos cidadãos o espaço efetivo de normalidade para o exercício de direitos e cumprimento de obrigações (Zaffaroni 2007; Zaffaroni *et al.* 2013).

A segurança pública é prevista no art. 144 da CF, que a determina como "*dever do Estado, direito e responsabilidade de todos [...]".* O caput do dis-

tais como espionagem, sabotagem, interferência externa, ações contrárias à Soberania Nacional e ataques cibernéticos.

26 Esse modelo é adotado por outros países, como Estados Unidos da América e Reino Unido. O Brasil, entretanto, ainda carece de maturidade no exercício desse controle pelo Poder Legislativo. Para conferir um estudo comparado de formas de controle da atividade de inteligência, confira Sampaio (2023; 2024e).

27 Vale considerarmos que a decisão do STF na ADI nº 6.529 (Brasil 2021a) ressalta que os órgãos e entidades do Sistema Brasileiro de Inteligência não podem compartilhar diretamente dados obtidos por meio de autorização judicial, justamente por estarem sob segredo de justiça. O debate, entretanto, não adentrou o mérito sobre como e com base em quais critérios a inteligência deve acessar dados que afetem o mapa de direitos fundamentais que possuem reserva de jurisdição para fins de persecução criminal.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

positivo ainda indica que ela *"[...] é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio*", a partir de um rol de órgãos e entidades. Podemos considerar que essa definição não explicita toda a complexidade da segurança pública, o que envolve, ainda, a atuação, além das forças policiais judiciárias, penais e militares previstas no rol do artigo, o Ministério Público, a Defensoria Pública, o sistema prisional e o Poder Judiciário.

As ações de segurança pública, por conseguinte, são direcionadas a reparar e reduzir os danos causados à ordem pública, dentro da perspectiva de controlar o crescimento da criminalidade e promover o ambiente de normalidade para o exercício do contrato social – exercício de direitos e cumprimento de obrigações pelos cidadãos. Tais ações, assim, possuem uma faceta precipuamente repressiva[28].

A estrutura punitiva estatal utiliza-se, principalmente, da polícia judiciária para construção da instrução probatória. Essa atividade é submetida ao controle externo do Ministério Público[29] e ao controle judicial[30], de acordo com a previsão legal de necessidade de autorização prévia para o emprego de determinadas técnicas e meios para obtenção de provas. É preciso considerarmos, nesse sentido, que os critérios para uso de FTPIs segue uma lógica inversa, devido ao controle externo para seu emprego envolver, muitas vezes, a autorização judicial prévia, o que não dispensa a necessidade de critérios de

28 Órgãos e entidades que possuem atuação de repressão estatal, por vezes, detêm competências que somam atuação preventiva. Ocasionalmente, essas ações são baseadas em informações de inteligência, mas isso não consiste, necessariamente, em atuação de inteligência em si. Por exemplo, as polícias militares possuem programas de policiamento ostensivo com o intento de permitir tanto uma atuação imediata de repressão em caso de necessidade, quanto de inibir práticas delitivas pela presença do aparato estatal. A definição dos locais de atuação, assim, pode decorrer de informações obtidas pelo sistema de inteligência, porém o policiamento ostensivo em si não representa uma ação de inteligência.

29 Lei Complementar nº 75, de 1993, art. 9º: "O Ministério Público da União exercerá o controle externo da atividade policial por meio de medidas judiciais e extrajudiciais podendo: I - ter livre ingresso em estabelecimentos policiais ou prisionais; II - ter acesso a quaisquer documentos relativos à atividade-fim policial; III - representar à autoridade competente pela adoção de providências para sanar a omissão indevida, ou para prevenir ou corrigir ilegalidade ou abuso de poder; IV - requisitar à autoridade competente para instauração de inquérito policial sobre a omissão ou fato ilícito ocorrido no exercício da atividade policial; V - promover a ação penal por abuso de poder."

30 O controle judicial decorre da previsão constitucional de reserva de jurisdição prevista nos incisos XI e XII do art. 5º da Constituição Federal: "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial" e "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

auditabilidade e rastreabilidade para eventual responsabilização por violações de agentes públicos e das estruturas estatais envolvidas por suas ações.

Problemáticas de controle e accountability relacionadas à apropriação do termo inteligência pelo aparato punitivo estatal

Como destacamos acima, a produção de conhecimento de inteligência assumiu funções delimitadas à finalidade preventiva, a partir da formação de uma metodologia de produção baseada no conceito amplo de segurança consagrado pela Agenda da Paz de 1992 (ONU 1992), que somou uma nova visão de como prover apoio às relações externas e de subsidiar o Estado em cenários de guerra e de paz (Buzan 1983; Herman 1996).

Já no final da Guerra Fria, a inteligência havia formado uma base doutrinária clássica, que consolidava essa mudança. Sherman Kent (1949, 3), nesse sentido, definiu inteligência como "conhecimento" indispensável para manutenção do bem-estar e da segurança, na perspectiva do Estado.

Essa mudança de paradigma na inteligência e a consolidação de sua metodologia e técnicas próprias para análise e produção de conhecimento levou, desde o começo desse debate, autores como Washington Platt (1974) a destacarem que inteligência servia a múltiplos setores enquanto uma ferramenta de análise e de produção de conhecimento.

Isso, porém, não torna essas áreas como próprias da inteligência. Diversos órgãos e instituições usam do nome inteligência em uma tentativa de empregar metodologias e técnicas que foram buscadas na inteligência, porém, isso não faz com que a atividade que já desempenhavam e exercem tenha se tornado atividade de inteligência no sentido estrito da atividade estatal de produzir conhecimento para a finalidade que destacamos: garantir a segurança em um sentido amplo, o que inclui o elemento do "bem-estar" destacado por Sherman Kent (1949).

Essa apropriação do termo inteligência por outras atividades estatais e até mesmo no setor privado é presente na atividade policial, o que em parte relaciona-se com a própria construção do que se compreende por direito à segurança. A relação intrínseca entre as finalidades de prevenção e repressão ao início da formação dos sistemas de inteligência leva, por vezes, a dificuldades de definição dos limites de atuação entre o aparato estatal de repressão e de inteligência (Andrade 2012).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Em emprego distinto desses parâmetros, o uso do termo inteligência pela estrutura policial, abarcando definições para "inteligência policial[31]", propicia uma série de confusões entre estruturas de aparato preventivo e repressivo. A Resolução nº 1 de 15 de julho de 2009, que regulamenta o Subsistema de Inteligência de Segurança Pública - SISP[32], por exemplo, define a inteligência policial como

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

A expressão "inteligência policial", por essa definição, atende à finalidade repressiva estatal, pela coleta, obtenção, processamento, análise e disseminação de informações e produtos gerados a partir do emprego de técnicas e meios de inteligência, por integrantes do sistema de persecução criminal, para fins de produção de provas de prática de contravenção ou crime.

A construção de provas para persecução criminal pela estrutura de inteligência é uma prática dissonante à proposta pós-redemocratização de delimitar o poder punitivo estatal para ampliar o exercício de liberdades individuais. Isso porque os espaços de controle e *accountability* das estruturas policiais de persecução criminal e de inteligência são estanques e diferentes, tal como abordado anteriormente, de acordo com essas finalidades estatais e do mapa de direitos fundamentais que atingem.

A confusão conceitual gera espaços em que a própria jurisprudência dos Tribunais Superiores permitiu, por vezes, que a atividade policial chamada de "inteligência policial" deixasse de ser submetida ao controle externo do Ministério Público.

Em 2020, por exemplo, o STF manteve decisão do Superior Tribunal de Justiça (STJ), no qual se definiu que a atividade de "inteligência policial" não se

31 Vale destacar recente proposta distinta de definição de inteligência policial que reduz a confusão entre atuação de investigação criminal e de inteligência, porém, ainda com a mistura do termo "policial", do Projeto de Lei nº 4.120/2024 da Câmara dos Deputados: "Atividade desenvolvida por policial que visa a produção de conhecimento ao processo de tomada de decisão policial, que envolve os processos de coleta, obtenção, análise e disseminação de informações e produtos gerados a partir do emprego de técnicas e meios de inteligência".

32 Vide Decreto nº 3.695, de 21 de dezembro de 2000, que cria o Subsistema de Inteligência de Segurança Pública, no âmbito do Sistema Brasileiro de Inteligência, e dá outras providências.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

submetia ao controle externo, porque não estaria no escopo da atividade-fim policial descrita no art. 144 da CF[33] (Brasil 2020b; 2018). Verifica-se, assim, uma confusão do que se considera como "inteligência policial" e "inteligência de Estado"[34].

É preciso pensar critérios de controle, de rastreabilidade e auditabilidade adequados para os campos da inteligência e do aparato punitivo estatal, justamente para evitar que ações de instrução probatória para fins criminais sejam realizadas inadequadamente por meio da inteligência, seja com ou sem o uso de FTPIs, em decorrência de os agentes públicos não compreenderem as diferenças de finalidade, motivo e motivação de atuação estatal para promover a segurança da sociedade e do Estado – pela inteligência – e para segurança pública – por meio dos órgãos e entidades que integram o aparato punitivo estatal.

Considerações finais

A regulamentação brasileira sobre o uso de meios e técnicas que possam restringir direitos fundamentais, sejam elas com uso de recursos tecnológicos ou não, é mais restritiva e direcionada ao sistema repressivo, com o objetivo de efetivar garantias penais e processuais penais[35].

A inteligência possui uma lacuna de compreensão de como operacionalizar sua atividade, em especial sobre o seu espectro distinto de impacto aos direitos fundamentais, por não afetar a liberdade individual e as garantias penais e processuais penais. O arcabouço normativo já existente reclama a observação dos limites de direitos fundamentais, todavia, carece de critérios específicos para o acompanhamento do controle externo sobre o uso de meios e técnicas que afetam direitos individuais, dentre elas as que empregam o uso de FTPIs.

Consideraremos aqui, ao menos, seis critérios para definição do uso de FTPI:

33 A fundamentação indica que o art. 129, inciso VII da Constituição restringe os poderes de controle externo do Ministério Público ao disposto no art. 9º da Lei Complementar nº 75, de 1993.

34 Vale ressaltar que STF e o STJ já decidiram anteriormente pela separação estrita dessas atividades, com a declaração de nulidade de provas produzidas a partir do aparato do sistema de inteligência. Nesse sentido, em 2019, o STF julgou HC (Brasil 2017b) impetrado contra RHC do STJ (Brasil 2017c).

35 A aplicação de técnicas e meios que visem à instrução probatória do processo penal, seja no código de processo penal ou em legislação específica, possui diversas limitações legais direcionadas para assegurar as garantias penais e processuais penais.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

motivo, motivação, finalidade, eficácia, eficiência e *accountability*.

1. O motivo decorre da própria compreensão de que o uso dessas ferramentas tecnológicas intrusivas pelo Estado decorre necessariamente em um ato administrativo, que requer motivo, ou seja, situação fática para o seu emprego adequado (C. Mello 1991; 2023).

2. A motivação relaciona-se com o motivo, por explicitar as razões pelas quais o fato demanda o uso de tais ferramentas. Todo ato da Administração Pública deve ser motivado, isso porque a ordem constitucional é de ampliar o exercício de direitos e liberdades, o que requer que o Estado deva agir por estrita permissão legal de restringir esse rol de direitos e liberdades individuais[36].

   A definição de concretização do direito à segurança muda de acordo com o contexto, logo, o ato de motivar é relevante para a compreensão do rol de direitos afetados e para a concretização do direito à segurança no caso concreto, seja pelo sistema de inteligência ou pelo aparato repressivo estatal.

   A delimitação do rol de direitos afetados é essencial para proporcionalidade do emprego da ferramenta no caso concreto. A motivação, assim, precisa evidenciar a necessidade do uso do recurso tecnológico, ao destacar que não é possível obter os dados, informações e conhecimentos necessários para concretizar o direito à segurança dentro da perspectiva preventiva da inteligência, ou de construção das provas necessárias para instrução probatória a partir dos indícios concretos demonstrados, para a finalidade repressiva do exercício punitivo do poder estatal.

3. Outro ponto relevante, para a proporcionalidade da medida, é considerar a eficácia da FTPI para alcançar o objetivo da ação. Isso porque a capacidade desse recurso de alcançar seu objetivo é o que justifica o seu emprego no grau específico em que afeta os direitos e liberdades individuais. Essa capacidade é relevante para definir, por exemplo, a necessidade de o controle ser exercido de forma prévia ou *a posteriori*, no intento de modular o uso da ferramenta e reduzir os danos.

36 Essa necessidade de o Estado motivar seus atos e de agir de forma restrita aos limites permitidos no ordenamento jurídico deriva do princípio da legalidade. Nesse sentido, Censo Antônio Bandeira de Mello (2023, 1-2) explica que "[...] o princípio da legalidade implica subordinação completa do administrador à lei. Todos os agentes públicos, desde o que lhe ocupe a cúspide até o mais modesto deles, devem ser instrumentos de fiel e dócil realização das finalidades normativas. Daí a impossibilidade seja de agirem sem lei que lhes sirva de supedâneo, seja de buscarem fins estranhos aos supostos na lei que invoquem para servir-lhes de calço. [...] O Texto Constitucional brasileiro, ao estabelecer, no art. 5.°, II, que 'ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei', e no art. 84, IV, que compete ao Presidente da República '(...) expedir decretos e regulamentos para sua fiel execução', deixa explícito e com explicitude inobjetável que o princípio da legalidade administrativa é, entre nós, adotado em sua plena extensão, pois, de um lado, proíbe restrições à liberdade individual que não estejam apoiadas em lei e, de outro lado, só admite edição de atos administrativos para cumprimento de lei, já que até mesmo os decretos e regulamentos presidenciais, que são os atos administrativos mais conspícuos, são propostos como simples instrumentos de execução de lei. 4. De outra parte, a exigência de que o ato sirva à fieldade o objetivo legal, sobre ser noção corrente, representa, como é óbvio, a simples afirmação de que a lei deve ser cumprida tal qual é; vale dizer, com obsequioso respeito à sua razão de existir, não se compreendendo que possa ser manipulada como simples pretexto para alcançar fins estranhos aos que visa prover, ainda quando não se trate de fins subalternos."

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

4. A proporcionalidade da medida também possui relação com a eficiência, princípio inserido no art. 37, *caput* da CF. Enquanto expressão da concepção da "boa administração" do direito italiano, a eficiência procura os meios mais adequados para os resultados almejados pelo Estado, o que envolve necessariamente pensar os princípios da legalidade, da economicidade e da celeridade da medida empregada (O. Mello 2010; C. Mello 2015).

   A proporcionalidade do uso da FTPI, portanto, deve considerar a legalidade, a economicidade e a celeridade que ela projeta aos objetivos estatais. O sistema de inteligência, por exemplo, necessita considerar a celeridade em termos de cumprimento da sua finalidade, visto que a informação que deixa de ser ofertada em tempo oportuno não serve mais para o alcance dos resultados pretendidos.

5. A finalidade pode ser preventiva ou repressiva, o que vimos ter, ao menos no contexto atual de concretização do direito à segurança, uma relação intrínseca com a ação ser realizada pela inteligência ou pelos órgãos e instituições que integram o sistema repressivo estatal. Quando a finalidade do uso de tais ferramentas é realizada pelo aparato punitivo, a liberdade individual é afetada; logo, é preciso considerarmos critérios mais estritos de motivação para o ato, por afetar mais direitos fundamentais e ser necessário seguir o rol de garantias penais e processuais penais constitucionais. Por outro lado, quando o uso é realizado pelo sistema de inteligência, o rol de direitos atingidos é restrito aos direitos à intimidade, à vida privada, à inviolabilidade do sigilo das comunicações pessoais e de dados. Nesse ponto, não há o debate sobre o emprego de garantias penais e processuais penais, por não ser destinado à construção de provas que possam afetar a liberdade individual.

6. A *accountability*, por sua vez, soma ainda a perspectiva de capacidade de o Estado promover a prestação de contas, conceder transparência, controlar e responsabilizar ações que fujam ao escopo do motivo, da motivação e da finalidade delineadas. Isso requer estabelecer requisitos que permitam a rastreabilidade e auditabilidade do emprego de ferramentas tecnológicas intrusivas.

Concluímos, destarte, que o uso de tecnologias, sejam elas FTPIs ou não, potencializam a capacidade do Estado de restringir direitos e liberdades individuais. A concretização do direito à segurança, seja em sua faceta de segurança da sociedade e do Estado ou de segurança pública possui especificidades próprias que devem ser observadas para não legitimarmos práticas dissonantes ao regime democrático pelo uso indevido do aparato de inteligência para fins de subsidiar o aparato punitivo estatal. Ademais, para enfrentarmos a problemática de parâmetros para uso de FTPIs na concretização do direito à segurança da sociedade e do Estado e à segurança pública, é preciso considerarmos, ao menos, o motivo, a motivação, a eficácia, a eficiência, a finalidade e a *accountability* para permitir a adequada ponderação, no caso concreto, para a relativização dos demais direitos fundamentais potencialmente afetados.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Referências

ABIN (Agência Brasileira de Inteligência). s.d. *Tecnologia.* Acessado em 15 de outubro de 2024. https://www.gov.br/abin/pt-br/assuntos/tecnologia.

Alexy, Robert. 1993. *Teoria de los derechos fundamentales*. Madri (Espanha): Centro de Estudios Constitucionales.

Ambros, Christiano Cruz. 2024. "Guerra cognitiva e operações cibernéticas de influência: vieses cognitivos como tática de combate." *Revista Brasileira de Inteligência* 19: e2024.19.252. https://doi.org/10.58960/rbi.2024.19.252.

Andrade, Filipe Scarpelli. 2012. "Inteligência Policial: efeitos das distorções no entendimento e na aplicação." *Revista Brasileira de Ciências Policiais* 3 (2): 37-54.

Andrade, José Carlos Vieira de. 1987. *Os direitos fundamentais na Constituição portuguesa de 1976.* Coimbra (Portugal): Almedina.

Arakaki, Ana Carolina Simionato, e Felipe Augusto Arakaki. 2020. "Dados e metadados: conceitos e relações." *Ciência da Informação* 49 (3): 34-45.

ABES (Associação Brasileira de Empresas de Software). 2020. "In Loco adapta sua tecnologia de geolocalização para ajudar no combate à Covid-19." 12 de abril de 2020. https://abes.com.br/in-loco-adapta-sua-tecnologia-de-geolocalizacao-para-ajudar-no-combate-a-covid-19/.

Belli, Luca, Bruna Franqueira, Erica Bakonyi, Larissa Che, Natalia, Chang, Sofia Couto, Nina da Hora, e Walter B. Gaspar. 2023. *Cibersegurança: uma visão sistêmica ruma a uma proposta de marco regulatório para o Brasil digitalmente soberano.* Rio de Janeiro: FGV Direito Rio.

Bobbio, Norberto, Nicola Matteucci, e Gianfranco Pasquino. 2016. *Dicionário de Política.* Vol. 2. 2 vols. Brasília: Editora Universidade de Brasília.

Brasil. 2007. "Medida Cautelar em Mandado de Segurança (MC-MS) Nº 26.547, Min. Rel. Celso de Mello." Supremo Tribunal Federal, 9 de maio de 2007.
Brasil. 2016a. "Ação Direta de Inconstitucionalidade (ADI) nº 2390. Min. Rel. Dias Toffoli" Supremo Tribunal Federal, 21 de outubro de 2016.
Brasil. 2016b. *Política Nacional de Inteligência*. Gabinete de Segurança Institucional da Presidência da República. https://www.gov.br/abin/pt-br/centrais-de-conteudo/politica-nacional-de-inteligencia-1/politica-nacional-de-inteligencia.

Brasil. 2017a. *Estratégia Nacional de Inteligência*. Gabinete de Segurança Institucional da Presidência da República. https://www.gov.br/abin/pt-br/centrais-de-conteudo/politica-nacional-de-inteligencia-1/ENINT.pdf.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Brasil. 2017b. "Habeas Corpus (HC) Nº 147.837, Min. Rel. Gilmar Mendes." Supremo Tribunal Federal, 19 de setembro de 2017.

Brasil. 2017c. "Recurso Ordinário em Habeas Corpus (RHC) nº 57.023, Min. Rel. Min. Sebastião Reis Júnior." Superior Tribunal de Justiça, 16 de agosto de 2017.Brasil. 2018. "Recurso Especial (RESP) nº 1.439.165, Min. Rel. Min. Gurgel de Faria." Superior Tribunal de Justiça, 25 de outubro de 2018.

Brasil. 2020a. "Recurso em Mandado de Segurança (RMS) nº 62143, Min. Rel. Rogério Schietti Cruz." Superior Tribunal de Justiça, 8 de setembro de 2020.

Brasil. 2020b. "Recurso Extraordinário (RE) nº 1.271.855, Min. Rel. Roberto Barroso." Supremo Tribunal Federal, 1º de julho de 2020.

Brasil. 2020c. "Referendo na Medida Cautelar em Ação Direta de Inconstitucionalidade (Ref-MC-ADI) nº 6387, Min. Rel. Rosa Weber." Supremo Tribunal Federal, 12 de novembro de 2020.

Brasil. 2020d. "Habeas Corpus (HC) nº 168052, Min. Rel. Gilmar Mendes." *Habeas Corpus.* Supremo Tribunal Federal, 2 de dezembro de 2020.

Brasil. 2021a. "Ação Direta de Inconstitucionalidade (ADI) nº 6529, Min. Rel. Cármen Lúcia." Supremo Tribunal Federal, 22 de outubro de 2021.

Brasil. 2021b. "Portaria GSI/PR nº 93, de 18 de outubro de 2021." Gabinete de Segurança Institucional. Acessado em 10 de outubro de 2024. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/glossario-de-seguranca-da-informacao-1.

Brasil. 2022. "Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 772, Min. Rel. Edson Fachin." Supremo Tribunal Federal, 9 de junho de 2022.

Brasil. 2023. "O Ministério Público no controle externo da atividade policial: prerrogativas e limites segundo o STJ." Notícias, Superior Tribunal de Justiça, 26 de fevereiro de 2023. Acesso em 21 de outubro de 2024. https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/26022023-O-Ministerio-Publico-no-controle-externo-da-atividade-policial-prerrogativas-e-limites-segundo-o-STJ.aspx.

Brasil. 2024a. "Ação Direta de Inconstitucionalidade (ADI) nº 7276, Min. Rel. Cármen Lúcia." Supremo Tribunal Federal, 19 de setembro de 2024.

Brasil. 2024b. "Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 1143, Min. Rel. Cristiano Zanin." Supremo Tribunal Federal.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Brasil. 2024c. "Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403, Min. Rel. Edson Fachin." Supremo Tribunal Federal, 11 de dezembro de 2024.

Brasil. 2024d. "Audiência pública n° 39 do Supremo Tribunal Federal: Regulação do uso de ferramentas de monitoramento secreto de aparelhos de comunicação pessoal." 4 de junho de 2024.

Brasil. 2024e. "Inteligência na democracia: desafios e perspectivas para a Agência Brasileira de Inteligência"". — Brasília: Abin, 2024. Acessado em 28 de dezembro de 2024. http://repositorio.enap.gov.br/handle/1/8217.

Brasil. 2025. *Desafios de Inteligência — Edição 2025*. Brasília: ABIN, 2024. Acessado em 5 de janeiro de 2025. http://repositorio.enap.gov.br/handle/1/8216.

Broeders, Dennis. 2024. "Cyber intelligence and international security. Breaking the legal and diplomatic silence?" *Intelligence and National Security* 39 (7): 1213–1229. https://doi.org/10.1080/02684527.2024.2398077.

Broek, Fabian van den, Roel Verdult e Joeiri de Ruiter. 2015. "Defeating IMSI Catchers." CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Nova Iorque (EUA): Association for Computing Machinery. 340-351. https://doi.org/10.1145/2810103.2813615.

Buzan, Barry. 1983. *People, States, and Fear: The National Security Problem in International Relations.* Brighton (Reino Unido): Wheatsheaf Book LTD.

Cellebrite. s.d. *Ufed.* Acesado em 1 de novembro de 2024. https://cellebrite.com/pt/cellebrite-ufed-pt/.

Cole, David. 2014. "Introduction: Watching the Watchers." em *Surveillance Nation: Critical Reflections on Privacy and its Threats. Articles from The Nation 1931-the Present*, por Richard Kreitner. Nova Iorque (EUA): The Nation.

Ferraz Júnior, Tércio Sampaio. 1980. *A Ciência do Direito.* São Paulo: Atlas.

Floyd, Rita. 2007. "Human Security and the Copenhagen School's Securitization Approach: Conceptualizing Human Security as a Securitizing Move." *Human Security Journal* 5 (37): 38-49.

Herman, Michael. 1996. *Intelligence power in peace and war.* Nova Iorque (EUA): Cambridge University Press.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

IFAC (International Federation of Accountants). 2001. *Governance in the Public Sector: a governing body perspective.* Nova Iorque (EUA): IFAC.

Kaspersky Team. 2023. "TriangleDB: the spyware implant of Operation Triangulation." 21 de junho. Acessado em 2 de outubro de 2024. https://www.kaspersky.com/blog/triangledb-mobile-apt/48471/.

Kent, Sherman. 1949. *Strategic Intelligence for American World Policy,* Princeton (EUA): Princeton University Press.

Kirchgaessner, Stephanie, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani e Michael Safi. 2021. "Revealed: leak uncovers global abuse of cyber-surveillance weapon." *The Guardian*, 18 de julho de 2021. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus.

Martins, Fernando Ramalho. 2006. "Controle: perspectivas de análise na teoria das organizações." *Cadernos EBAPE.BR* 4 (1). https://doi.org/10.1590/S1679-39512006000100008.

Maximiliano, Carlos. 2003. *Hermenêutica e aplicação do direito.* Rio de Janeiro: Forense.

McDowell, Mindi e Matt Lytle. 2019. "Recognizing and Avoiding Spyware." *CISA News*, 19 de novembro de 2009*.* https://www.cisa.gov/news-events/news/recognizing-and-avoiding-spyware.

McLuhan, Marshall, e Bruce R. Powers. 1992. *The Global Village: Transformations in World Life and Media in the 21st Century.* Oxford (Reino Unido): Oxford University Press.

Mello, Celso Antônio Bandeira de. 1991. *Elementos de Direito Administrativo.* São Paulo: Editora Revista dos Tribunais.

Mello, Celso Antônio Bandeira de. 2015. *Curso de Direito Administrativo.* São Paulo: Editora Malheiros.

Mello, Celso Antônio Bandeira de. 2023. "Legalidade, motivo e motivação do ato administrativo." *Revista de Direito Administrativo, Infraestrutura, Regulação e Compliance* 26: 429-442. https://doi.org/10.48143/RDAI.26.mello.

Mello, Oswaldo Aranha Bandeira de. 2010. *Princípios Gerais do Direito Administrativo.* Vol. 1. 3ª Edição. São Paulo: Malheiros Editores.

NIST (National Institute of Standards and Technology). s.d. "Spyware." *Computer Security Resource Center.* https://csrc.nist.gov/glossary/term/spyware#:~:text=Definitions%3A,a%20type%20of%20malicious%20code.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Nussbaum, Brian H. 2017. "Communicating Cyber Intelligence to Non-Technical Customers." *International Journal of Intelligence and CounterIntelligence* 30 (4): 743-764. https://doi.org/10.1080/08850607.2017.1297120.

Oosthoek, Kris, e Christian Doerr. 2021. "Cyber Threat Intelligence: A Product Without a Process?" *International Journal of Intelligence and CounterIntelligence* 34 (2): 300-315. https://doi.org/10.1080/08850607.2020.1780062.

ONU (Organização das Nações Unidas). 2022. *O Direito à Privacidade na Era Digital: Relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos.* Trad. Instituto de Referência em Internet e Sociedade (IRIS). Acessado em 5 de 2023. https://irisbh.com.br/wp-content/uploads/2022/12/O-direito-a-privacidade-na-era-digital-Relatorio-do-G.

ONU (Organização das Nações Unidas). 1992. *An agenda for peace: preventive diplomacy, peacemaking and peace-keeping: report of the Secretary-General pursuant to the statement adopted by the Summit Meeting of the Security Council on 31 January 1992 / Boutros Boutros-Ghali*. Acesso em 5 de outubro de 2021. https://digitallibrary.un.org/record/145749?ln=en&v=pdf.

Pinho, José Antonio Gomes de e Ana Rita Silva Sacramento. 2009. "Accountability: já podemos traduzi-la para o português?" *Revista Administração Pública* 43 (6): 1343-1368.

Platt, Washington. 1974. *Produção de Informações Estratégicas.* Rio de Janeiro: Biblioteca do Exército; Livraria Agir Editora.

Sampaio, Ricardo Ramos. 2023. *A possibilidade da realização de vigilância por meio de geolocalização em tempo real pela Agência Brasileira de Inteligência.* Dissertação de Mestrado Profissional. Brasília: Departamento de Engenharia Elétrica, Universidade de Brasília. Disponível em: http://repositorio.unb.br/handle/10482/47955.

Schneier, Bruce. 2018. *Click here to kill everybody: Security and Survival in a Hyper-connected World*. Nova Iorque (EUA) e Londres (Inglaterra): W.W. Norton & Company.

Smanio, Gianluca Martins. 2021. "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* 12 (5): 49-76. Disponível em: http://dspace.mj.gov.br/handle/1/7921.

Tanenbaum, Andrew S. e Hebert Bos. 2016. *Sistemas operacionais modernos.* 4ª Edição. São Paulo: Pearson Education do Brasil.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.274
ISSN 2595-4717

Thompson, James Westfall e Saul Padover. 1965. *Secret Diplomacy: espionage and Cryptography [1500-1815]*. 2ª Edição. Nova Iorque (EUA): Frederick Ungar Publishing CO.

Varian, Hal R. 1996. "Economic Aspects of Personal Privacy." em *Internet Policy and Economics: Challenges and Perspectives*, por William H. Lehr e Lorenzo Maria Pupillo. Massachusetts (EUA): Springer.

Walker, Jermaine. 2012. "Global Positioning System History." National Aeronautics and Space Administration (NASA). Acessado em 1º de outubro de 2024. https://www.nasa.gov/general/global-positioning-system-history/#:~:text=GPS%20has%20its%20origins%20in,US%20submarines%20carrying%20nuclear%20missiles.

Zaffaroni, Eugenio Raúl, Nilo Batista, Alejandro Alagia e Alejandro Slokar. 2013. *Direito Penal Brasileiro: Teoria Geral do Direito Penal.* 2 vols. Rio de Janeiro: Revan.

Zaffaroni, Eugenio Raúl. 2007. *O Inimigo no Direito Penal*. Rio de Janeiro: Revan.