REVISTA JURÍDICA DA FA7 FA7 LAW REVIEW
PERIÓDICO CIENTÍFICO DO PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO DA UNI7

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

Programas de intrusão digital e monitoramento eletrônico: desafios e possibilidades à segurança pública e persecução penal

Pedro Henrique Hermes
Universidade de Santa Cruz do Sul (UNISC)
pedrohermes.1@hotmail.com

Rogério Gesta Leal
Universidade de Santa Cruz do Sul (UNISC)
gestaleal@gmail.com

Resumo

O presente artigo tem por problema de pesquisa: quais são os limites jurídicos para o uso de programas de intrusão digital e monitoramento eletrônico à luz do ordenamento jurídico brasileiro, especialmente no que tange à Ação de Descumprimento de Preceito Fundamental nº.1143? Utilizou-se o método de abordagem dedutivo e de procedimento o monográfico. Diante da ascensão tecnológica, denota-se crescente uso de mecanismos de intrusão digital para fins de segurança pública, ensejando a necessidade de padrões protetivos mínimos. Denota-se que a discussão judicial ou legislativa deve ser pautada pelo (i) dever do Estado em exercitar, com eficiência, suas obrigações no campo da segurança pública e persecução penal, observando o devido processo legal (constitucional e infraconstitucional), (ii) os direitos individuais de privacidade e intimidade da pessoa humana.

Palavras-chave

Intrusão Digital. Monitoramento Eletrônico. Persecução Penal. Segurança Pública.

1. Introdução

A realidade digital é marcante em diversas facetas da sociedade. Essas transformações vêm se mostrando presentes nas empresas, governos e cotidiano das pessoas. No âmbito da segurança pública não se tem mostrado cenário diferente, uma vez que surgem diversos desafios no que toca à prevenção de crimes, instrumentos de combate e videomonitoramento, exigindo-se do Estado a regulamentação e criação de parâmetros protetivos mínimos.

Assim como na realidade física, no mundo digital tem surgido inéditas formas de lesões a interesses privados e públicos, que vem culminando na criminalização de condutas desde o terrorismo, a pedofilia, o bullying, piratarias, racismos, xenofobias, furtos, dentre outros. Esse fator tem se alastrado tanto que os órgãos de segurança pública e privada em todo o mundo tem desenvolvido estratégias e treinamento para o seu enfrentamento, a despeito de que a legislação no ponto ainda seja deficitária, nomeadamente no Brasil.

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

O tema ganha especial relevância no Brasil, dado o julgamento em trâmite no Supremo Tribunal Federal (STF), que analisa a constitucionalidade do uso de determinadas ferramentas de intrusão digital por autoridades públicas. A Procuradoria-Geral da República protocolou Ação de Descumprimento de Preceito Fundamental nº.1143, sob relatoria do Min. Cristiano Zanin, postulando que (i) o Supremo Tribunal Federal reconhecesse a omissão do Congresso Nacional por não regulamentar o uso de ferramentas de monitoramento intrusivo e secreto de aparelhos de comunicação pessoal (celulares, tablets) por órgãos e agentes públicos; e que (ii) a Corte estabelecesse regras provisórias para proteger direitos fundamentais à intimidade, privacidade e inviolabilidade do sigilo destas comunicações, e de dados, até o surgimento de regulação própria pelo Parlamento.

Diante desse cenário, o presente artigo objetiva responder ao seguinte problema de pesquisa: quais são os limites jurídicos para o uso de programas de intrusão digital e monitoramento eletrônico à luz do ordenamento jurídico brasileiro, especialmente no que tange à Ação de Descumprimento de Preceito Fundamental nº.1143? Para responder a essa problemática, utilizar-se-á o método dedutivo, partindo das questões relacionadas aos desafios da segurança pública e persecução penal na era digital, chegando-se à questão concreta dos programas de videomonitoramento. Como método de procedimento, foi utilizado o método monográfico.

Nomeadamente em face da relevância temática, busca-se analisar em que medida se faz necessária legislação tópica da matéria a ser constituída pelo Congresso Nacional, e a partir de que premissas teóricas e pragmáticas isto deve ocorrer, inclusive pela via judicial. Nesse sentido, observa-se que marcos regulatórios são importantes na espécie, principalmente por se tratar de direitos fundamentais em face da liberdade. Todavia, a partir do reconhecimento dos objetivos e desafios que a realidade do mundo da vida – física e virtual – impõem, levando em conta a experiência já consolidada pelos tribunais no particular, constata-se importante equilibrar e buscar sinergias entre as temáticas.

2. Desafios contemporâneos à segurança pública no Brasil: perspectivas a partir das tecnologias digitais

A segurança pública não é de a muito conferida como perspectiva de direito fundamental ou ao menos os trabalhos e pesquisas nesse sentido remontam a pouco menos de duas décadas no Brasil. Apesar de sua previsão constitucional no Brasil, essencialmente nos artigos 5º, enquanto direito fundamental individual, e artigo 6º,

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

enquanto direito fundamental social, o debate de sua definição vem sendo desenvolvido.

A segurança pública é direito individual, na medida em que consagra a possibilidade subjetiva de tutela da pessoa, mas também se consagra como direito fundamental social, porquanto garante a possibilidade de tutela coletiva, difusa, entre outros. Assim, esse direito não assume, logo, uma feição coletiva ou individual, haja vista

> *Com relação aos fundamentos constitucionais da segurança, é possível fazermos referência àquelas duas perspectivas já referidas, de um lado, a que lhe outorga a condição de interesse coletivo, e, de outro, a que lhe reconhece a condição de direito fundamental individual. Estas posições, todavia, não são irreconciliáveis, e devem estar associadas, e isto porque as dimensões individuais e coletivas/sociais das relações humanas, hoje e cada vez mais, contam com intersecções integracionistas, basta vermos o que ocorre nas chamadas redes sociais (Facebook, Instagram, WhatsApp, YouTube, Twitter, LinkedIn, Pinterest, Google+); tudo e todos estão interligados (Leal, 2020, p. 354).*

Com a ampliação do uso de equipamentos informáticos e tecnológicos, denota-se que os desafios à segurança pública e persecução penal se ampliam. Pode-se visualizar dois fatores: (i) o uso de novos mecanismos de prevenção e repreensão; (ii) configuração de novas práticas delituosas ou reconfiguração de práticas já conhecidas. Os órgãos de segurança pública, por sua vez, passaram a adotar novas ferramentas digitais para monitoramento, inteligência e combate à criminalidade. Sistemas de reconhecimento facial, análise preditiva de crimes e softwares de intrusão digital tornaram-se cada vez mais comuns no aparelho tecnológico do Estado. No Brasil, esta regulamentação ainda é incipiente, necessitando cautela e criação de parâmetros protetivos e regulatórios em face do uso de tecnologias.

É em nome da segurança pública contra atos de terrorismo e de criminalidade organizada que vários governos têm desenvolvido programas de vigilância de seus cidadãos ao redor do mundo. iniciativas governamentais – isoladas ou em colaboração global – para acessar dados e informações privados e públicos, de pessoas físicas e jurídicas, em nome da segurança preventiva e curativa, sem qualquer informação e prestação de contas àqueles que são atingidos por suas políticas (Kukso, 2019).

Embora haja avanços com a Lei nº 9.296/1996 (que autorizou, mediante critérios, medida judicial de interceptação do fluxo de comunicações telefônicas e em

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

sistemas de informática e telemática, no curso de investigação criminal e instrução processual penal); Lei nº12.965/2014 (Marco Civil da Internet - MCI, protegendo os mesmos bens jurídicos); e Lei nº13.709/2018 (Lei Geral de Proteção de Dados – LGPD, tutelando da mesma forma tais bens, mas ressalvando o tratamento de dados pessoais para fins de segurança pública, de defesa nacional, de segurança do Estado, de investigação e de repressão a infrações penais), ainda há que se avançar na regulação normativa dos temas relacionados à intrusão digital. A discussão ficou notória com o uso da ferramenta de espionagem digital chamada Pegasus, criada pela empresa israelense NSO Group. O mecanismo é utilizado para grampear smartphones, computadores e redes de comunicação e gestão de dados de forma global, em nome da promoção da segurança da democracia e dos povos democráticos.

Nesse sentido, a ADPF nº. 1143 nomeadamente objetiva discutir a temática sob o âmbito judicial, buscando delimitar parâmetros para o uso destes mecanismos. O argumento central da ação proposta pelo Ministério Público Federal é o de que o Congresso Nacional se mostrou omisso parcialmente em dar efetividade plena e conferir proteção eficaz aos ditames do art.5º, X e XII, da Constituição Federal de 1988 – CF/88, condizentes à inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, e do sigilo de suas correspondências e comunicações, salvo nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. Daí porque a PGR pretende ver reconhecida a omissão parcial do Congresso Nacional no que tange:

> *à edição de norma regulamentadora do uso, por órgãos e agentes públicos, de programas de intrusão virtual e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal – smartphones, tablets e dispositivos eletrônicos similares – para dar efetividade aos mandamentos constitucionais de proteção estatal da intimidade e da vida privada, e de inviolabilidade do sigilo das comunicações pessoais e de dados (Brasil, 2023, p. 23).*

Os recursos tecnológicos utilizados se valem, via de regra, de software com códigos fechados, impossibilitando níveis de transparência e visibilidade dos elementos constitutivos neurais de suas operações, inviabilizando controles sociais, políticos e jurídicos mais eficazes. Trata-se do fenômeno da opacidade das tecnologias digitais – que não será objeto de aprofundamento e debate.

Os fenômenos criminais hoje se encontram marcados por tensionalidades e complexidades diversos, tanto no âmbito físico como virtual, ameaçando a segurança

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

de nações inteiras (terrorismo, tráfico drogas, de armas, pessoas e órgãos), alcançando inclusive o Mercado – físico e virtual -, provocando danos individuais e coletivos, drenando recursos financeiros de consumidores menos avisados e atentos; a própria representação política e as eleições são atingidas – direta ou indiretamente – por comportamentos de duvidosa licitude.

O problema é que a cena do crime muda constantemente no ambiente virtual, e por isto, para cada tipo de crime que envolva recursos eletrônicos, medidas diferentes precisam ser implementadas para que se consiga reunir provas as mais amplas possíveis, nomeadamente digitais, sendo que os princípios básicos que se aplicam a delitos tradicionais também se aplicam a casos de crimes virtuais, o que implica a necessidade de as evidências serem sólidas e precisas, tudo passível de documentação, para que possam ser aceitas no tribunal.

Nos delitos que envolvem o uso de redes de computadores, denota-se que vem utilizando enorme quantidade de dados – valorosa parte à burla da lei, ensejando a necessidade de criação de mecanismos técnicos por parte dos órgãos de controle. De outro lado, os órgãos de segurança devem equilibrar a atividade e efetividade da persecução penal com o respeito aos direitos fundamentais individuais e sociais, com especial destaque à privacidade, intimidade, honra, imagem, dados pessoais, entre outros bem jurídicos por ventura capazes de ser atingidos.

O uso de avançadas tecnologias, como algoritmos de criptografia ou VPN para ocultar atividades criminosas, encontram ofertas as mais diversas em variados mercados ilícitos. sendo imperioso que os órgãos de segurança pública tenham mecanismos e protocolos de investigação e responsabilização a altura. Tais mecanismos, contudo, devem ser condizentes com o nível tecnológico capaz de inibir e reprimir as práticas delituosas, sobretudo sob o ambaro da lei e respeito aos direitos fundamentais. Recorda-se que os limites aos direitos fundamentais devem estar amparados em propósitos legítimos, sobretudo por se tratarem de instrumentos da liberdade (Sarlet, 2010). Nesse sentido, importante o avanço de novas ferramentas para auxiliar o Estado a lidar com inúmeros crimes através do uso de habilidades técnicas que permitem analisar dados e evidências relacionados aos delitos praticados (Casey, 2021).

O debate ganha maior profundeza quando contrastado com uma ativa vigilância, tão bem trazida por autores como Baumann. A capacidade de vigilância aumentou exponencialmente em quase todos os domínios institucionais – na segurança pública

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

não é diferente, transformando cumulativamente o nosso mundo sociotécnico e, no processo, colocando novos riscos políticos. Com já advertiu Haggerty (2021) a adoção em massa de vigilância carrega consigo o risco de formas draconianas de controle social. Ou seja, não apenas a vigilância infringirá as liberdades civis, mas que grupos combinarão e coordenarão tais dispositivos através de fronteiras institucionais, colocando-os a serviço de algumas das piores atrocidades imagináveis. Por conta destes elementos, foram consideradas necessárias medidas destinadas a detectar, por exemplo, membros de grupos do crime organizado através de comunicações (por exemplo, a Diretiva de Retenção de Dados) e medidas destinadas a reforçar a segurança das fronteiras e a controlar a circulação de pessoas e bens (por exemplo, passaportes biométricos, bilhetes de identidade e vistos) para combater o crime organizado. Trata-se de um amplo debate, posto que envolve atores públicos (Estado) e privados (Mercado), que este texto tangenciará.

No entanto, observa-se que o ambiente digital tem se tornado um amplo espaço para cometimento de crimes. Nesse sentido, a investigação de crimes, através da prática de vigilância, por operar com a lógica e práxis dos delitos físicos e tradicionais, por vezes, não tem instrumentos adequados; por vezes é engessada por procedimentos restringidos por Direitos Fundamentais Individuais (privacidade, intimidade, propriedade privada) (Cosatbile, 2005).

Entre as técnicas empregadas para a prática de crimes digitais, destacam-se o hackeamento de sistemas, a exploração de falhas de segurança para acesso remoto (superzapping), a coleta de informações residuais (scavenging) e o desvio de pequenas quantias de dinheiro de diversas contas (salemi slicing). O aumento do uso de redes sociais, webmail e aplicativos de comunicação criptografados também dificulta a responsabilização de infratores, tornando essencial o desenvolvimento de técnicas avançadas para obtenção de evidências eletrônicas. (Johnson, Post, 1996).

Os avanços tecnológicos e a erosão das fronteiras (que permitem a livre circulação de pessoas e bens), e a falta de controle e segurança nas fronteiras, não apenas criaram um conjunto de oportunidades para grupos do crime organizado se envolverem em atividades criminosas graves (por exemplo, tráfico de drogas e imigração ilegal) mas também dificultou a detecção dessa atividade. Por tais razões, as possiblidades de responsabilização por violações de normas jurídicas neste particular depende de investigações sofisticadas, que contem com adequados mecanismos de obtenção de evidências eletrônicas que não estão disponíveis publicamente.

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

Conforme noticia a Comunidade Europeia, mais da metade de todas as investigações criminais que ocorrem na Europa exigem acesso a evidências eletrônicas transfronteiriças. Em dois terços dessas investigações há necessidade de obter evidências de provedores de serviços online com sede em outra jurisdição (European Commission, 2019. Esse elemento, no Brasil, por exemplo, já foi objeto de discussão por ocasião da ADC 51, acerca da obtenção de prova cujos servidores se encontram no exterior e a discussão sobre a jurisdição brasileira para sua competência.

Na Europa, conforme o relatório número de solicitações aos principais provedores de serviços online cresceu 84% no período entre 2013 e 2018. Estes tipos de dados são essenciais em investigações criminais para identificar pessoas – físicas e jurídicas - ou obter informações sobre suas atividades (European Commission, 2019).

Desde a década de 1990, a União Europeia, através da Diretiva 95/466/CE, a exigia que os Estados-Membros assegurassem a tutela dos direitos e da liberdade da pessoa física, em face do tratamento de dados pessoais. Por outro lado, a Diretiva 97/66/CE, dando maior efetividade aos princípios enunciados pela Diretiva anterior, abordou este tema no âmbito das telecomunicações, posteriormente aperfeiçoada pela Diretiva 2002/58/CE, regulamentando o tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrônicas. Com base na última Diretiva, os provedores de rede e serviços, em relação aos dados de tráfego e dados de localização gerados pelo uso de serviços de comunicação eletrônica, devem eliminá-los ou torna-los anônimos quando não forem mais necessários para os fins de transmissão de comunicações, exceto os necessários para o faturamento ou pagamento da interligação.

De outro lado, o Parlamento Europeu declarou, em 9 de março de 2004, que qualquer forma de vigilância em massa era injustificada, e que apenas medidas direcionadas eram justificáveis. Vigilância direcionada se refere a indivíduo específico (ou indivíduos), caso a caso, com base em suspeita razoável (ou causa provável). Este tipo de vigilância só era autorizado se incluísse adequadas garantias, tais como o requerimento de mandados de busca e outras ordens judiciais (European Parliament, 2004).

Um dos cenários de maior risco à privacidade é a emergência e os Estados de Exceção, fundados, por exemplo, nas questões de segurança pública, operadoras de restrições a esse direito fundamental. Leal (2020, p. 361) traz o exemplo do Estado de Urgência promovido na França a partir de ataques em Paris, no ano de 2015, sob o

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

fundamento da segurança pública e nacional, onde restou autorizada a promoção acesso a domicílios sem autorização judicial, devassando-se a privacidade do morador em nome de tais direitos.

Regulamentações posteriores, como a Diretiva 2006/24/CE, do Parlamento Europeu, e do Conselho de Europa, tratando da conservação de dados gerados ou tratados no âmbito dos provedores de serviços de internet, posteriores aos ataques terroristas de Londres e Madri, de 2005, implementaram situações amplas de monitoramento e vigilância social. Na sequência dos ataques com bombas em Madri, o Conselho da Europa emite a Declaração de Combate ao Terrorismo, adotando com urgência mecanismos preventivos de segurança pública como identidades biométricas, o que revela o surgimento de tendências a formatação de políticas de contraterrorismo seletivas.

Dworkin (2002) afirmar que, em tais cenários, a equação sensível não é entre nossa liberdade e nossa segurança em tempos de ameaça, mas entre nossa segurança e a liberdade deles; ou seja, as liberdades de pequenos grupos suspeitos, como muçulmanos adultos do sexo masculino. Nesta Declaração sobre o combate ao terrorismo, adotada em 25 de março de 2004, o Conselho Europeu instruiu o Conselho a examinar medidas para estabelecer regras sobre a retenção de dados de tráfego de comunicações por provedores de serviços (Brenner, 2006).

Cada vez mais a Comunidade Europeia entende que, devido ao aumento significativo das possibilidades oferecidas pelas comunicações eletrônicas e os dados relativos à utilização destas últimas constituem ferramenta particularmente importante e válida na prevenção, investigação, detecção e repressão de crimes, em particular do crime organizado (Brenner, 2006). O art.2º da Diretiva apresenta conceitos alargados dos temas tratados:

> *Para efeitos da presente diretiva, aplicam-se as seguintes definições:*
> *(a) dados: dados de tráfego e dados de localização, bem como dados relacionados necessários para identificar o assinante ou usuário;*
> *(b) usuário: qualquer pessoa singular ou coletiva que utilize serviços de comunicações eletrônicas de acesso público, para fins privados ou profissionais, sem necessariamente subscrever esse serviço;*
> *(c) serviço telefônico: chamadas telefônicas (incluindo chamadas de voz, correio de voz, conferências e transmissão de dados), serviços suplementares (incluindo reencaminhamento e transferência de chamadas), serviços de mensagens e multimidia (incluindo serviços de mensagens curtas e serviços de multimidia avançados);*

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

> *(d) identificador de utilizador: identificador único atribuído a indivíduo quando subscreve ou regista serviço de acesso à Internet, ou serviços de comunicações pela Internet;*
> *(e) rótulo de localização: significa a identidade da célula de onde se origina chamada móvel, ou na qual termina;*
> *(f) tentativa de chamada sem sucesso: chamada telefônica que foi completada com sucesso, mas não atendida, ou na qual houve intervenção da operadora de rede.*

A Convenção Europeia dos Direitos Humanos (CEDH), por sua vez, exige que qualquer interferência estatal na privacidade seja necessária e proporcional, seguindo critérios claros e justificados. Se observados os conjuntos legislativos sobre a temática, a questão da necessidade e proporcionalidade tem se mostrado a baliza aos desafios práticos acerca destes parâmetros de vigilância e efetividade penal.

Na Alemanha, desde 2016, vige lei de reforma dos poderes investigativos da agência para a segurança externa do país (BND), que prevê a possibilidade de interceptar comunicações telemáticas da internet de estrangeiros para fins de prevenção de potenciais e indiciários atos de terrorismo, introduzindo no ordenamento jurídico discutível diferenciação entre cidadãos tedescos e estrangeiros. Por sua vez, o Tribunal Constitucional Alemão decidiu que seriam necessários rígidos escrutínios de proporcionalidade à aplicação de várias disposições da lei federal sobre atividades de forças policiais – Bundeskriminalamtgesetz – BKAG -, que buscavam utilizar formas de vigilância oculta e o emprego de meios informáticos para adquirir dados remotos de investigados (Bundesverfassungsgericht, 2016).

De outro lado, em maio de 2021, a Corte Europeia dos Direitos Humanos – CEDH, com o julgamento do processo Big Brother Watch and Others v. the United Kingdom, envolvendo Grã Bretanha e Irlanda do Norte, por conta de violação do art.34, da Convenção à Proteção dos Direitos Humanos e Liberdades Fundamentais, decidiu que foi ilegal a finalidade e a magnitude dos programas de investigações operados pelo governo do Reino Unido que realizaram invasões de privacidade e intimidade pelo monitoramento e captação de comunicações eletrônicas indiscriminadas de milhares de pessoas, em nome da segurança nacional.

Nos Estados Unidos, a regulamentação da segurança e privacidade de dados segue um modelo setorial. Diferentes setores da economia, como saúde, finanças e telecomunicações, são regidos por normas específicas que estabelecem regras sobre a coleta, o armazenamento e o uso de informações pessoais – diferentemente do Brasil,

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

que adota padrões de normas gerais. Essas normas são estabelecidas tanto em nível federal quanto estadual, o que resulta em um sistema fragmentado, onde diferentes legislações podem se sobrepor ou variar conforme a jurisdição.

Entretanto, esse cenário sofreu uma mudança significativa após os atentados de 11 de setembro de 2001, quando o governo do então presidente George W. Bush aprovou o U.S. Patriot Act, uma legislação que ampliou substancialmente os poderes das agências de segurança pública e inteligência. Com a justificativa de combater o terrorismo, a lei trouxe novas prerrogativas para o monitoramento de cidadãos, empresas e estrangeiros em território norte-americano, permitindo invasões de privacidade sem a necessidade de autorização judicial prévia. Além disso, concedeu ao governo a capacidade de acessar registros financeiros, telefônicos e de comunicação eletrônica, bem como realizar buscas e apreensões em domicílios e propriedades sem notificação imediata aos investigados.

Paralelamente, a adoção de tecnologias de vigilância avançadas também se intensificou nesse período, bastando ver os relatos de diversos ativistas digitais (Snowden, 2019). Um dos sistemas amplamente utilizados foi o Carnivore. Esse programa era um sistema de monitoramento eletrônico desenvolvido pelo FBI que permitia a captura de dados de comunicações online diretamente dos provedores de internet. Ele funcionava a partir da identificação de palavras-chave específicas, interceptando e armazenando informações trocadas pelos usuários.

O período pós-11 de setembro, portanto, marcou uma transformação significativa na abordagem dos Estados Unidos em relação à segurança nacional, estabelecendo um novo paradigma de vigilância e controle estatal que se estendeu por décadas e continua influenciando políticas de privacidade e proteção de dados até os dias atuais.

O medo de ações terroristas desde o 11 de setembro de 2001 fomentou ainda mais o desenvolvimento de novos modelos de Estados de Inteligência, no qual as agências de inteligência não eram limitadas na coleta de informações privadas, não tinham o ônus de estabelecer a necessidade de tais informações além de uma dúvida razoável e podiam se envolver em atividades ilegais secretamente, e, portanto, sem responsabilidade política. Importante destacar as revelações feitas por Snowden sobre as políticas de vigilância secreta dos órgãos de segurança norte-americanos, como a National Security Agency – NSA (Snowden, 2019). Em nome da segurança nacional, realizaram-se operações globais de monitoramento de pessoas físicas e jurídicas

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

através de programas como o PRISM (visando acessar comunicações através de provedores de internet) (Snowden, 2019).

No mundo virtual inexistem fronteiras, e isto constitui característica muito atraente para quase todas as atividades criminais. Quando as autoridades tentam controlá-las encontram muitas dificuldades, a começar pelo fato de que este novo mundo costuma ofertar facilidades e estímulos para a consecução de muitos comportamentos potencial ou efetivamente criminosos, como o anonimato e as ferramentas de comunicação em tempo real com criptografia de ponta a ponta (signal, wickr, confide, telegram). Ou seja, o segredo da autoria virtual – quando ocorre – revela-se como chave estratégica e oportunidade excelente à realização de atos delinquentes, ou dissimulados, utilizando-se, por vezes, de formas jurídicas aparentemente lícitas (principalmente empresas de fachada que só existem para a prática de crimes).

De outro lado, fator que dificulta esta efetividade, em outros níveis de circulação de dados virtuais complexos e de difícil investigação, como os chamados deep web e dark web; o primeiro, identificado como a parte da rede cujo conteúdo não está disponível ou indexado nos principais mecanismos de pesquisa, sendo formada por milhões de páginas, com dimensão inimaginável e crescimento similar ao da Internet Visível. Por sua vez, a dark web refere-se as páginas não indexadas, que não seguem as regras do ICANN e não possuem nomes registrados no serviço de DNS. Essas páginas só podem ser acessadas com softwares específicos para navegação em ambientes criptografados e anônimos, como TOR, Invisible Internet Project (i2p) e FreeNet (Shimabukuro; Abreu e Silva, 2018). Embora haja infinidades de instrumentos de investigação, muitos deles se encontram em vazios normativos, objeto central da ADPF em discussão.

Por conta de todos estes elementos vistos até aqui, revela-se de importância destacada de marcos normativos claros e pontuais sobre estes temas, dando maior segurança tanto aos órgãos investigativos como à sociedade. O desafio de encontrar pontos de equilíbrio dentre os diversos interesses em jogo, dentre os quais, a exigência (até em face da natureza volátil e de difícil apreensão dos dados e informações virtuais) de que o Estado possa investigar de maneira eficiente. Também há a constante preocupação dos Estados Democráticos regularem os limites e possibilidades de acesso e gestão de dados e informações pessoais é fator importante na perspectiva de se evitar abusos de poder ou desvios de finalidade, tanto no sentido de dimensionar quando é possível tais ocorrências, e com base em que critérios de coleta,

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

armazenamento, uso e descarte, como dimensionar o tempo em que isto se dará, com os mecanismos de controle respectivos

3. Os programas de intrusão digital no Brasil: uma análise a partir da ADPF 1143

O tema da criminalidade física e virtual traz elementos identitários cada vez mais inéditos para inúmeros sistemas jurídicos globais. Esses problemas envolvem desafios de toda ordem, englobando desde protagonistas altamente qualificados em termos tecnológicos e comportamentais, até a complexa demarcação conceitual das ações típicas (criminalização) destes atores. Esses desafios geram dificuldades à delimitação de materialidades, autorias e culpabilidades, razões pelas quais os Estados têm procurado constituir, com certa lentidão, marcos normativos regulatórios destes temas no mesmo tempo em que eles estão a provocar danos de diversas naturezas. Veja-se que a identificação da autoria e da materialidade destas espécies de delitos envolvem a sofisticação de mecanismos investigativos para uma realidade complexa.

O mesmo ocorre no âmbito do devido processo legal necessário ao enfrentamento daqueles cenários, até em face dos cuidados para com direitos e garantias protegidos constitucional e infraconstitucionalmente, reclamando aperfeiçoamento permanente – tanto legislativo como jurisprudencial. Não é à toa que, autores como Bioni et al (2020) referem o surgimento do devido processo informacional, direito que regulamenta medidas legais e procedimentais para a forma com que dados pessoais serão tratados, investigações serão conduzidas, nomeadamente no ambiente digital, uma vez que impactam diretamente nas liberdades individuais e coletivas (Bioni et al, 2020). Veja-se que estes procedimentos se destacam a situações que envolvem a fragilização de direitos, nomeadamente no que tange à segurança pública. A ausência de algumas diretrizes mínimas que devem estar presentes nestes casos, especialmente pelo Estado, acarreta a fragilização de direitos, possibilitando concretos riscos à pessoa.

Salienta-se que a existência de previsões procedimentais, ainda mais em relação a atividades capitaneadas pelo Estado, especialmente nas questões de segurança, resguardam o devido processo legal, que, com a tecnologia, se tem conceituado como devido processo informacional, pois, assim "garante-se **contraditório e ampla defesa, o que ganha relevo ainda maior na seara penal, uma vez que as decisões ali tomadas impactam** um dos bens jurídicos cuja perda é de maior gravidade: a liberdade de locomoção" (Bioni et. Al. 2020, p. 9) [grifo do autor].

Com base em tais premissas, por exemplo, o STF, absolveu réu condenado pelo crime de roubo, tendo como prova tão somente o reconhecimento fotográfico feito,

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

inicialmente, por Whatsapp, sob o argumento de que o reconhecimento fotográfico, realizado na fase do inquérito policial, deve estar lastreado em outros elementos de prova que indiquem, com segurança, a autoria do fato, o que não ocorreu no caso (Brasil, 2022).

Em questões de direito material, no Brasil, a Lei nº12.737/2012 inovou – mesmo que de forma tímida – na criação do tipo penal de invasão de dispositivo informático (art.154-A, do Código Penal). Apelidada de Lei Carolina Dieckmann, tipifica como crimes infrações relacionadas ao meio eletrônico, como invadir computadores, violar dados de usuários ou derrubar sites, prevendo como crime a invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Os casos envolvendo criminalidade virtual, todavia, em muitas oportunidades, referem-se a delitos que já contam com proteção normativa vigente em termos do bem jurídico material tutelado, os quais são defraudados de modo virtual, como os casos de insultar a honra de alguém (calúnia artigo138, do CP); espalhar boatos eletrônicos sobre pessoas (difamação, artigo 139, do CP); insultar pessoas considerando suas características e atribuindo apelidos grosseiros (injúria, artigo 140, do CP); ameaçar alguém (ameaça, artigo 147, do CP); utilizar dados da conta bancária de outrem para desvio ou saque de dinheiro (furto, artigo 155); explicitar, em redes sociais ou em e-mails, de forma depreciativa, manifestações preconceituosas sobre raças, religiões e etnias (preconceito ou discriminação, artigo 20, da Lei nº7.716/89); enviar e, ou, trocar fotos de crianças nuas (pedofilia, artigo 247, da Lei nº8.069/90).

O cenário demonstra que tais delitos só aumentam através de comunicações em tempo real realizadas por aplicativos de mensagens instantâneas como o whatsapp, protegidos por criptografia de ponta a ponta que dificulta a apuração sobre as responsabilidades, o que evidencia ainda mais a necessidade de que investigações policiais e a persecução penal propriamente dita se valham, quando necessário e na forma da lei, de instrumentos de monitoramento intrusivo e secreto de aparelhos de comunicação pessoal (celulares, tablets).

Com a expansão incontrolada da informação e dos mecanismos de comunicação tecnológica, como o emprego difuso das redes sociais para múltiplas atividades, que vão desde as relações pessoais de amizade e afetivas até as relações de

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

trabalho, comércio, acadêmicas, etc., tem imposto a constituição de gestão e análise de dados a todo tempo, por muitos setores da vida cotidiana, inclusive para os campos Direito Penal e Processual Penal, eis que elementos uteis à investigação e conservação de provas – até com esquemas de segurança e segredo imensos – em formatos digitais (estamos falando de computadores pessoais, servidores de empresas, banco de dados em nuvens, pens drives) (La Muscatella, 2013). Cada vez mais especialistas forenses de rede são chamados para investigar estes tipos de crimes, o que envolve inúmeras coletas de provas (primárias, secundárias e mesmo ações de busca). Estas coletas primárias se destinam à obtenção de dados de livre acesso, envolvendo documentos públicos, fatos noticiados pela imprensa física e virtual. Já as coletas secundárias alcançam dados protegidos, como bancários, de comunicação, fiscal. Por fim, as ações de busca visam a obtenção de dados negados, razão pela qual reclamam uso de ações de vigilância, técnicas operacionais de inteligência (cobertura, disfarce), tudo autorizado judicialmente (Couto, 2015).

É crescente o uso destes mecanismos de investigação em todos os setores. De outro lado, que relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos (Nações Unidas, 2022) altera que

> *(...) Embora supostamente sejam empregadas para combater o terrorismo e o crime, essas ferramentas de programas espiões têm sido frequentemente usadas por razões ilegítimas, inclusive para reprimir opiniões críticas ou dissidentes, e aqueles que as expressam, incluindo jornalistas, figuras políticas da oposição e defensores dos direitos humanos.*
> *7. Os recursos das ferramentas e serviços de spyware oferecidos no mercado global são espantosos. O Pegasus, por exemplo, uma vez instalado, concede acesso completo e irrestrito a todos os sensores e informações dos dispositivos infectados, transformando efetivamente a maioria dos smartphones em dispositivos de vigilância 24 horas, acessando câmera e microfone, dados de geolocalização, e-mails, mensagens, fotos e vídeos, assim como todas as aplicações. Permite ao intruso obter um quadro detalhado da vida das suas vítimas, os seus pensamentos, preferências, atividades profissionais, pensamento político, saúde, situação financeira e vida social e íntima. Enquanto muitas ferramentas de hackeamento exigem alguma ação por parte da vítima, como clicar em um link ou abrir um anexo de uma mensagem, o Pegasus é instalado de forma furtiva, por meio do chamado "ataque de zero clique". O software torna quase impossível que as vítimas evitem a infecção depois de terem sido alvejadas.*

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

A questão que se segue, a partir disto, é: qual das nossas liberdades estamos dispostos a sacrificar em nome da segurança pública? Observa-se STF já teve oportunidade de assentar, há mais tempo, que a proteção garantida no art.5º, XII, da CF/88, assegura a inviolabilidade da comunicação de dados, e não todos os dados propriamente ditos – como os armazenados em computadores ou nas nuvens.

Mas até neste tema as circunstâncias de alguns delitos podem implicar modulações decisionais em nome da urgência que flagrantes de atos criminosos graves impõem aos agentes de segurança pública – nomeadamente as polícias-, para os fins de assegurar a cadeia de custódia de provas, o que se evidencia na discussão que trava o STF no tema nº977, versando sobre: a aferição da licitude da prova produzida durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime.

Para Davis (2021), embora reconheça que melhorar a inteligência é crucial para prevenir futuros ataques terroristas, por exemplo, a coleta indiscriminada de grandes quantidades de informações, sem suspeita particular de irregularidades, interfere no devido processo legal, inibe a atividade política e corrói a privacidade. Para além disto, em termos de devido processo legal, aquela Diretiva concede às agências poderes em grande parte não controlados para conduzir vigilância mesmo quando não há base para suspeitar de atividade criminosa, autorizando a retenção de dados de todos os cidadãos antes de qualquer investigação, sendo que isto pode ocorrer sem a exigência de ordens judiciais (ou mandados de busca).

É neste quadro amplo de conjunturas que precisamos avaliar se as matrizes legislativas que temos são, ou não, suficientes para dar proteção eficiente e adequada aos bens jurídicos tutelados pelo art.5º, X e XII, da Constituição Federal de 1988. Diante desse cenário, observa-se que a percepção é negativa, nomeadamente quando se fala: (i) de programas de intrusão virtual remota, e (ii) de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal (smartphones, tablets e dispositivos eletrônicos similares), pois é a casuística dos Tribunais brasileiros que tem feito isto, não em caráter universal, mas tópico, a cada caso que avalia, por certo que em muito contribuindo na formatação de parâmetros regulatórios da matéria, eis que muitas destas abordagens tem sido feitas inclusive em sede de controle concentrado de constitucionalidade, como vimos.

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

Embora a previsão Lei nº9.296/1996, ao regulamentar a parte final do inciso XII, do art.5º, da CF/88, tratando das possibilidades de interceptações telefônicas ou telemáticas, e determinando que as concessionárias de telefonia e provedores de mensageria eletrônica providenciem o fornecimento de dados em face de ordem judicial expressa, não significa que se pode contemplar todas as outras formas de investigação e persecução penal – como ferramentas intrusivas e remotas de monitoramento e invasão de privacidade. A dinâmica espacial e temporal destas, que permite o acesso e a captação instantâneos de informações e dados os mais diversos, reclamando, portanto, protocolos de segurança e preservação de direitos mais sensíveis. Embora suas previsões, há que se conferir a tutela adequada e específica ao bem jurídico e meio de investigação.

De fato, a Lei das Interceptações Telefônicas traz importantes elementos passíveis de serem replicados em outras formas invasivas de investigação e persecução penal, dentre os quais, não se admitir o uso de meios como estes: (i) em situações nas quais inexistem indícios razoáveis de autoria ou participação em infração penal; (ii) quando a prova puder ser feita por outros meios disponíveis; (iii) quando não descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada. Por mais que alguns destes elementos tenha carga de subjetividade em termos de condições e possibilidades, eles podem servir de parâmetro para aferição de outros mecanismos investigatórios.

A partir do debate se que instaura na ADPF nº1143, é possível compatibilizarmos direitos fundamentais individuais de privacidade e intimidade com direitos fundamentais sociais envolvendo a segurança pública e responsabilidade penal. A segurança configura, neste âmbito, valor super primário, no sentido de que não se presta a balanceamentos, mas deve sempre ser garantida em face de sua natureza contratualista matricial, inexoravelmente vinculada a dignidade da vida humana, à incolumidade física, patrimonial e extra-patrimonial das pessoas, seu bem estar e qualidade de existência, ou seja, trata-se de direito fundamental indispensável à fruição de direitos os quais os indivíduos são titulares (Leal; Monte, 2023).

Por outro lado, como lembra Albrecht (2016, p. 55),

> *verifica-se na atualidade uma crescente tematização do que seria uma suposta tensão envolvendo a eficiência do processo penal e da política de segurança, de um lado, e a liberdade dos cidadãos, de outro. Os debates sobre essa relação conflituosa entre segurança, eficiência e*

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

> *liberdade vêm sendo marcados por um deslocamento da função atribuída ao Direito Penal, do qual se exigem mais e mais medidas garantidoras da segurança e pela ênfase dada a riscos excepcionais atribuídos à criminalidade organizada transnacional e, sobretudo, ao terrorismo internacional. Com isso, também o conceito de "segurança" ganha novos contornos, passando a ser entendido cada vez mais como segurança frente à criminalidade e sobretudo frente à violência, convergindo nos conceitos de "segurança interna" e "segurança externa".*

A segurança, em sentido amplo, constitui inexoravelmente pressuposto da liberdade; ou seja, não pode existir qualquer oposição entre esses dois valores, já que a liberdade apenas pode ser exercida se houver condições sociais básicas de segurança que permitam a fruição desse Direito. O que pode haver entre estes Direitos Fundamentais/vetores axiológicos, contingencialmente, são eventuais tensões localizadas, questões que precisam ser aferidas a partir de severos testes de proporcionalidade entre os escopos perseguidos e bens tutelados.

Ou seja, sinergias entre o bem-estar coletivo e individual são basilares e essenciais para se estabelecer os parâmetros normativos e modos de tutela do direito à segurança pública, nomeadamente os limites legislativos, evitando-se arbitrariedades e ações ilegais. Trata-se de fundamento do Estado de Direito, nomeadamente pela "la eliminación de la arbitrariedad en el ámbito de la actividad estatal que afecta a los ciudadanos" (Zagrebelski, 1992, p. 21). Nesse sentido, Frosini aponta importante lição acerca da segurança como elemento jurídico de preocupação constitucional:

> *Se storicamente l'espressione "diritto alla sicurezza" poteva essere ritenuta una figura semantica a carattere retorico, oggi mi sembra che goda di uno status giuridico in parte autonomo - come diritto a un'esistenza protetta, indispensabile al godimento di altri diritti di cui un soggetto è titolare - e in parte indiretto, nel senso che è complementare agli altri diritti, ovvero come istanza radicata nella nozione di benessere e di qualità della vita, collettiva e individuale. Pertanto, la sicurezza può qualificarsi come bene inscindibilmente legato alla vita, alla incolumità fisica, al benessere dell'uomo e alla qualità della sua esistenza, nonché alla dignità della persona. Da ciò ne deriva che la sua titolarità oltre che in capo allo Stato, nella forma di interesse a garantire una situazione di pace sociale, è riferibile a ciascun individuo come diritto a un'esistenza protetta, indispensabile al godimento degli altri diritti di cui è titolare in condizioni di sicurezza*

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

As propostas que a arguidas na ADPF nº1143 para os fins de balizar a utilização de ferramentas tecnológicas de invasão e monitoramento de pessoas físicas e jurídicas em investigações e processos criminais são relevantes. Constata-se que são passíveis de serem incorporadas em processo legislativo constituidor de norma especifica sobre o tema, mas é preciso compatibilizar tais sugestões com as propostas de Lei que o Congresso Nacional já está avaliando, envolvendo o tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública e de persecução penal, nomeadamente: (i) o anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal, elaborado pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados, de 26 de novembro de 2019; (ii) o PL nº1515/2022, apresentado ao Congresso Nacional pelo Deputado Federal Coronal Armando.

Acerca da LGPD-Penal, denota-se que as alíneas a e d do inciso III do artigo 4º da LGPD referem que a legislação em questão não é aplicável as atividades de segurança pública e de investigação e repressão a infrações penais, cuja regulamentação será de forma específica (Brasil, 2018). Surge, então, a iniciativa e necessidade de uma legislação própria que discipline a matéria, na busca de regulamentação das questões atinentes às investigações criminais, ações penais, prevenção de crimes. Leal acentua, da mesma forma, que a LGPD reservou espaço a uma legislação específica nessa matéria, referindo, porém a existência de outros desafios relacionadas ao tema:

> *Ao mesmo tempo, em seu art. 4º, inc. III, a norma autorizou a flexibilização daqueles direitos para os fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais, sendo que o tratamento de dados pessoais previsto neste inc. III será regido por legislação específica, "que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei". Por certo que aqui já temos outros desafios que é o de densificar materialmente – e no caso concreto – os níveis e possibilidades das medidas proporcionais e estritamente necessárias ao escopo da norma e diante de cenários os mais particulares existentes – como o da segurança da saúde pública na pandemia (Leal, 2020, p. 368).*

Destes documentos legais, igualmente é possível extrair princípios importantes para a regulamentação pretendida pela ADPF nº 1143, em especial, que o uso de

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

ferramentas invasivas da privacidade e intimidade de pessoas físicas e jurídicas para fins de investigação/persecução penal observem a:

a) Finalidade, que obriga a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Por certo que a autoridade que acessar e manejar os dados deverá ponderar – fundamentadamente – o tempo e modo oportunos para prestar tal informação, a fim de não comprometer as atividades de segurança pública e persecução penal levadas a cabo, mas ao mesmo tempo terá de tomar cautelas formais e materiais no sentido de evidenciar, a todo tempo em que estiver tratando daqueles dados, os propósitos assinalados, sob pena de caracterizar-se o desvios e abusos de autoridade ou outras irregularidades e ilícitos.
b) Adequação (pertinência e relevância do tratamento diante dos objetivos pretendidos e em face do contexto do tratamento);
c) Necessidade (limitação do tratamento ao mínimo necessário às finalidades demarcadas, observados os critérios de abrangência, pertinência e não excessividade em face das finalidades informadas);
d) Proporcionalidade (como compatibilidade do tratamento em face dos objetivos pretendidos).

O princípio da adequação, que também se pode associar a ideia de idoneidade, implica que toda a restrição aos direitos tutelados pelas leis de proteção de dados, em nome da investigação e persecução penal, seja idônea tão somente para o atendimento do escopo autorizado pela norma, exigindo-se que os meios empregados no particular se apresentem instrumentalmente adequados para alcançar o fim almejado. Já a necessidade deve ser entendida como indispensabilidade do acesso e manejo de dados para os fins sob comento, ou seja, que tais medidas se deem do modo menos restritivo possível aos direitos fundamentais consectários, evitando assim causar lesão dispensável a eles (certa proibição de excesso). E a proporcionalidade precisa ser compreendida de modo estrito, no sentido de que qualquer restrição aos direitos fundamentais dos titulares dos dados envolvidos deve ser justificada pela relevância da satisfação dos escopos perseguidos– legais e legítimos (Leal, 2014).

Esses fatores não são olvidados pela petição inicial da ADPF protocolada pela PGR, sobretudo quando implica deveres de fundamentação com base em dispositivos já vigentes:

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

> *O tipo de informação a ser disponibilizada direciona à autoridade requisitante um ônus agravado de fundamentação, o qual está implícito no referido art. 10 e decorre também da leitura sistemática do microssistema protetivo de dados e comunicações e de seus princípios reitores, dentro de um contexto em que envolvidos os direitos fundamentais e a preferência por meios investigativos que gerem menos riscos a terceiros não envolvidos no ilícito.*
> *Disso decorre que todo tratamento de dados há de ser regido pelos preceitos da adequação e da necessidade, o que significa ser compatível com as finalidades informadas ao titular e se limitar ao mínimo necessário para alcançá-las, abrangendo os dados pertinentes, proporcionais e não excessivos (art. 6º, II e III, da LGPD).*
> *Reforçam essa restrição os axiomas da segurança e da prevenção, que impõem o uso das medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, bem como a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VII e VIII, da LGPD) (Brasil, 2023).*

Mais adiante, a inicial ressalta o dever de fundamentação para decisões judiciais que relativizem a proteção legal, uma vez que é dever da autoridade "requerente se desincumbir de uma obrigação de fundamentação agravada, a fim de circunscrever a medida aos casos em que há efetiva necessidade e adequação, de modo a prevenir danos a terceiros e preservar sua segurança, sem que isso obste o cumprimento dos deveres constitucional e convencional de investigar e punir" (Brasil, 2023). Observa-se que a busca regulamentar é bem específica, que versa para que o Congresso Nacional

> *elabore normas primordialmente para regular o uso e controle das três principais ferramentas disponíveis no mercado : 1) spywares, como o Pegasus do NSO Group, que intercepta dados ao infectar um dos dispositivos envolvidos na comunicação; 2) Imsi Catchers, como o Pixcell (NSO Group) e o GI2 (Cognyte/Verint), que simulam estações rádio-base capturando dispositivos próximos; 3) dispositivos que rastreiam a localização de um alvo específico através da rede celular, como o First Mile (Cognyte/Verint) e o Landmark (NSO Group) (Brasil, 2023).*

Em síntese, as abordagens pretendidas com os atos normativos buscam justificar e permitir a observância do devido processo legal – agora sob as vestes de devido processo informacional. Embora o debate se iniciou pela via judicial, é na seara

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

legislativa que deve ganhar o seu espaço para ampla discussão em face dos direitos aqui discutidos.

4. Conclusão

À vista do exposto, observa-se que as conclusões devem versar muito mais sobre o caráter propositivo da presente pesquisa, que teve como problema: quais são os limites jurídicos para o uso de programas de intrusão digital e monitoramento eletrônico à luz do ordenamento jurídico brasileiro, especialmente no que tange à Ação de Descumprimento de Preceito Fundamental nº.1143?

Da presente pesquisa e das ferramentas investigatórias e legislativas disponíveis, constata-se que há problemas operacionais em demandas de investigação e persecução criminal que precisam ser sublinhados e observados por ocasião da estruturação das medidas legais.

Por mais que sistemas e modelos de tratamento dos dados acessados e armazenados por novas ferramentas virtuais de investigação criminal consigam constituir acervos de informações enormes, eventualmente será impossível avaliar a todos os dados acessados/coletados. Isso implica criar, normativamente, metodologias de abordagem e procedimentos destes dados/informações, com seus respectivos protocolos em termos de acesso, coleta, gestão e descarte, possibilitando inclusive o controle das seleções e filtros de uso destes dados pelas autoridades competentes.

Além disso, é preciso constituir regras claras sobre as políticas de segurança na mantença/custódia e disponibilização/destruição dos dados acessados e coletados. Igualmente, é fundamental protocolos e registros adequados das autorizações judiciais de acesso, coleta, gestão e descarte de dados para investigações e persecução penal (identificação das pessoas que usaram a ferramenta e da autoridade pública que permitiu/autorizou/determinou tal uso), assim como a execução destas medidas em toda a sua extensão e profundidade.

Importa neste âmbito a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei e autorização judicial. Veja-se que a informação plena – em tempo e modo oportunos – das pessoas físicas e jurídicas que foram atingidas por ferramentas virtuais e intrusivas de investigação/persecução criminal precisa ser garantida. Por outro lado, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, sob pena de responsabilização pelos danos decorrentes.

Sabe-se que determinadas investigações/processos criminais, em face de suas complexidades e sofisticações (principalmente em delitos econômicos, de corrupção, lavagem de dinheiro, tráfico de drogas, dentre outros), reclamam tempos diferidos de instrução e julgamento (notadamente em face de eventuais provas necessárias), não raro longos, eventualmente com múltiplas intercorrências e dificuldades. Em tais contextos, o uso de mecanismos invasivos (virtuais e físicos) de investigação/persecução penal envolvendo acesso e gestão de tratamento de dados poderá se prolongar, impondo-se a autorização judicial para tempo certo, aos que os acessam/manejam estes, contando com protocolos e instrumentos aptos a garantir suas integridades, sigilos possíveis e informação a quem de direito.

A ADPF nº1143, em verdade, está propiciando verdadeiros diálogos não coatados com máxima transparência entre os atores institucionais competentes e legítimos para tanto. Através de procedimentos que garantem a participação efetiva de múltiplas vozes republicanas e democráticas, provocam-se reciprocas sensibilizações e entendimentos voltados à constituição dos melhores argumentos normativos e regulatórios das matérias escrutinadas.

Ou seja, a ADPF nº1143 não está usurpando poderes e competências, mas se apresenta como lócus privilegiado de interlocuções emancipatórias entre sujeitos representantes lídimos da Sociedade, tendo como escopo demarcar, pela via de consensos, possibilidades ordenadoras de compatibilização entre (i) o dever do Estado em exercitar, com eficiência, suas obrigações no campo da segurança pública e persecução penal, observando o devido processo legal (constitucional e infraconstitucional), (ii) e os direitos individuais de privacidade e intimidade da pessoa humana.

Referências

ALBRECHT, Hans-Jörg. Direito Penal e Periculosidade: a política criminal entre prevenção, combate a perigos e retribuição de culpa. In: MACHADO, Marta R. de Assis; PÜSCHEL, Flavia Portella (org.). Reponsabilidade e Pena no Estado Democrático de Direito. São Paulo: FGV, 2016.

ALEXY, Robert. Teoría de los Derechos Fundamentales. Madrid: Centros de Estudios Constitucionales, 2000.

ALEXY, Robert. The Construction of Constitutional Rights. In Law & ethics of Human Rights, Volume 4, Issue 1. Article 2. Berkeley: Berkeley Electronic Press, 2010.

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

ANZANELLO, Greta Moura e DEMUTTI, Thiago Bosak. Ferramentas de tecnologia da informação e de bussines intelligence aplicadas à investigação do crime de lavagem de dinheiro. In WENDT, Emerson e LOPES, Fábio Motta. Investigação Criminal – Provas. Porto Alegre: Livraria do Advogado, 2015.

ATERNO, Stefano. Data retention: problematiche giuridiche e prospettive europee. In CAJANI, Francesco e COSTABILE, Gerardo. Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea. Roma: UAE/IISFA, 2021.

BRASIL. Supremo Tribunal Federal. Recurso em Habeas Corpus nº206846, Segunda Turma, Relator Min. Gilmar Mendes. 2022.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº. 1143. 2023.

BRENNER, Susan W. Cybercrime, cyberterrorism and cyberwarfare. In Revue Internationale de Droit Pénal. V.77, 2006/3, pp.453/471, Disponível em: https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm. Acesso em: 26 mar. 2025.

BUNDESVERFASSUNGSGERICHT. Headnotes to the Judgment of the First Senate of 20 April 2016. Disponível em https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2016/04/rs20160420_1bvr096609en.html. Acesso em: 26 mar. 2025.

CAJANI, Francesco e COSTABILE, Gerardo. Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea. Roma: UAE/IISFA, 2021.

CASEY, Eoghan. Digital evidence and computer crime. New York: Elsevier, 2021.

COUTO, George Estefani de Souza. Inteligência policial judiciária e produção de prova. In WENDT, Emerson e LOPES, Fábio Motta. Investigação Criminal – Provas. Porto Alegre: Livraria do Advogado, 2015.

COSATBILE Gerardo. Scena criminis, documento informatico e formazione della prova penale. In Ciberspazio e Diritto, disponível no site http://www.altalex.com/documents/news/2005/04/27/scena-criminis-documento-informatico-e-formazione-della-prova-penale. Acesso em: 26 mar. 2025.

DAVIS, Howard. Human Rights and Civil Liberties. Cullompton: Willan Publishing, 2021.

DWORKIN, Ronald. The threat to patriotism. In CALHOUN, Craig; PRICE, Paul and TIMMER, Ashley. (eds). Understanding September 11. New York: The New Press, 2002

EUROPEAN COMMISSION. Recommendation for a Council Decision - authorizing the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

matters. Brussels, 5.2.2019 – COM (2019) 70. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52019PC0070. Acesso em: 30/03/2025.

EUROPEAN PARLIAMENT. European Parliament resolution on the first report on the implementation of the Data Protection Directive (95/46/EC). COM (2003) 265, 2004. Disponível em: http://www.europarl.europa.eu/omk. Acesso em: 26 mar. 2025.

FROSINI, Tommaso Edoardo. Il diritto costituzionale alla sicurezza. In Forum on line di Quaderni costituzionali, Disponível em: http://www.forumcostituzionale.it/wordpress/wp-content/uploads/pre_2006/440.pdf. Acesso em: 26 mar. 2025.

HAGGERTY, Kevin D. Ten thousand times larger – anticipating the expansion of surveillance. In GOOLD, Benjamin and NEYLAND, Daniel. New directions in surveillance and privacy. Devon/UK: Willan Publishing, 2019.

JOHNSON, David R.; POST, David. Law and Borders - the rise of law in cyberspace. In Stanford Law Review, V. 48, nº 5, may 1996.

KUKSO, Federico. Una historia de control. In El Atlas de la revolución digital – del sueño libertario al capitalismo de vigilancia. Buenos Aires: Capital Intelectual, 2019.

LA MUSCATELLA, Donato. La ricerca delle fonti di prova sulle reti di cloud computing: le nuove frontiere delle investigazioni digitali tra profili giuridici e questioni operative. In Rivista Ciberspazio e Diritto, Vol. 3, 2013.

LEAL, Rogerio Gesta e MONTE, Mario. Limites do direito fundamental de proteção de dados em face da instrução probatória no processo penal. In LEAL, Rogerio Gesta; GAVIÃO, Anizio Pires e DIAS, Handel Martins. Tutelas à Efetivação de Direitos Públicos Incondicionados, V.1. São Paulo: Ática, 2023.

LEAL. Rogério Gesta. Aspectos constitutivos da teoria da argumentação jurídica: a contribuição de Robert Alexy. In Revista de Investigações Constitucionais. Vol.1, nº2, maio/agosto de 2014. Curitiba: Núcleo de Investigações Constitucionais da UFPR, 2014.

LEAL, Rogério Gesta. Direito fundamental à proteção de dados em tempos de pandemia: necessárias equações entre segurança pública e privada. Revista Brasileira de Direitos Fundamentais & Justiça, Belo Horizonte, ano 14, n. 43, p. 357-374, jul./dez., 2020.

LIPTON, Eric; SANGER, David E. and SHANEDEC, Scot. The Perfect Weapon: how russian cyberpower invaded the U.S., publicado no The New York Times, edição de 13/12/2016, Disponível em https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html. Acesso em: 26 mar. 2025.

NAÇÕES UNIDAS (2022). O direito à privacidade na era digital: Relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos. Trad. DUTRA, Luíza, SANTARÉM, Paulo Renã da Silva. Genebra: ONU, 4.8.2022.

Submissão #1790
Submetido em: 29/04/2025
Aprovado em: 31/03/2026

SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10 ed. rev. atual. e ampl. Porto Alegre: Livraria do advogado, 2010.

SHIMABUKURO, Adriana e ABREU E SILVA, Melissa Garcia Blagitz de. Internet, Deep Web e Dark Web. In SILVA, Ângelo Roberto Ilha da. (org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado, 2018.

SNOWDEN, Edward. Permanent Record. New York: Metropolitan Books, 2019.

SHIMABUKURO, Adriana e ABREU E SILVA, Melissa Garcia Blagitz de. Internet, Deep Web e Dark Web. In SILVA, Ângelo Roberto Ilha da. (org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado, 2018.

ZAGREBELSKI, Gustavo. El derecho dúctil. Torino: Giulio Einaudi, 1992.

Digital intrusion and electronic monitoring programs: challenges and possibilities for public security and criminal prosecution

Abstract

The research problem of this article is: what are the legal limits for the use of digital intrusion and electronic monitoring programs in the light of the Brazilian legal system, especially with regard to the Action for Non-Compliance with a Fundamental Precept No. 1143? The deductive approach method and the monographic method of procedure were used. In the face of technological ascension, there is a growing use of digital intrusion mechanisms for public security purposes, giving rise to the need for minimum protective standards. It is noted that the judicial or legislative discussion must be guided by (i) the duty of the State to efficiently exercise its obligations in the field of public security and criminal prosecution, observing the due process of law (constitutional and infra-constitutional), (ii) the individual rights of privacy and intimacy of the human person.

Keywords

Criminal Prosecution. Digital Intrusion. Electronic Monitoring. Public Security.

Como citar

HERMES, P. H.; LEAL, R. G. Programas de intrusão digital e monitoramento eletrônico: desafios e possibilidades à segurança pública e persecução penal. **Revista Jurídica da FA7**, Fortaleza, v. 22, n. 1, p. 67-91, jan./abr. 2025.