

DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

DOCTRINA E PRÁTICA EM DEBATE < VOL.3 >

FRANCISCO BRITO CRUZ (ED.) / NATHALIE FRAGOSO (ED.) / AGATHA ROSA
/ ALCIDES PERON / ANDRÉ NICOLITT / ANTÔNIO MAGALHÃES GOMES FILHO
/ ANTONIO SANTORO / CLARICE TAVARES / CLEOPAS ISAÍAS SANTOS /
DIEGO COLETTI OLIVA / EMANUEL QUEIROZ RANGEL / EVANILDA GODOI /
FERNANDA DOMINGOS / FLÁVIA MITRI / GERALDO PRADO / JACQUELINE
DE SOUZA ABREU / KATERINA HADJIMATHEOU / MARCOS CÉSAR ALVAREZ
/ MARGARET HU / NORMA SUELI BONACCORSO / SAMYR BÉLICHE VALE

INTERNETLAB
pesquisa em direito e tecnologia

SÃO PAULO, 2020

InternetLab é uma organização sem fins lucrativos dedicada à produção de pesquisa acadêmica aplicada com impacto em políticas públicas de tecnologia e Internet no Brasil.

Citação sugerida

BRITO CRUZ, Francisco; FRAGOSO, Nathalie (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. III. São Paulo. InternetLab, 2020.

Este trabalho está licenciado sob uma licença Creative Commons CC BY-NC-SA 4.0 BR. Esta licença permite que outros remixem, adaptem e criem obras derivadas sobre a obra original, desde que com fins não comerciais e contanto que atribuam crédito aos autores e licenciem as novas criações sob os mesmos parâmetros. Toda nova obra feita a partir desta deverá ser licenciada com a mesma licença, de modo que qualquer obra derivada, por natureza, não poderá ser usada para fins comerciais.

Avenida Ipiranga 344 cj 11B | 01046-010 | São Paulo | SP | Brasil

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA

www.internetlab.org.br

Dados Internacionais de Catalogação na Publicação (CIP) (Câmara Brasileira do Livro, SP, Brasil)

Direitos fundamentais e processo penal na era digital / Francisco Brito Cruz, Nathalie Fragoso [editores] -- 1. ed. -- São Paulo: InternetLab, 2020. -- (Doutrina e prática em debate; 3)

Vários autores.

Bibliografia.

ISBN 978-65-88385-06-7

1. Direito processual penal **2.** Direitos fundamentais **3.** Processo penal **4.** Tecnologia e direito **5.** Tecnologias da informação e comunicação **I.** Cruz, Francisco. **II.** Fragoso, Nathalie. **III.** Série.

20-42487

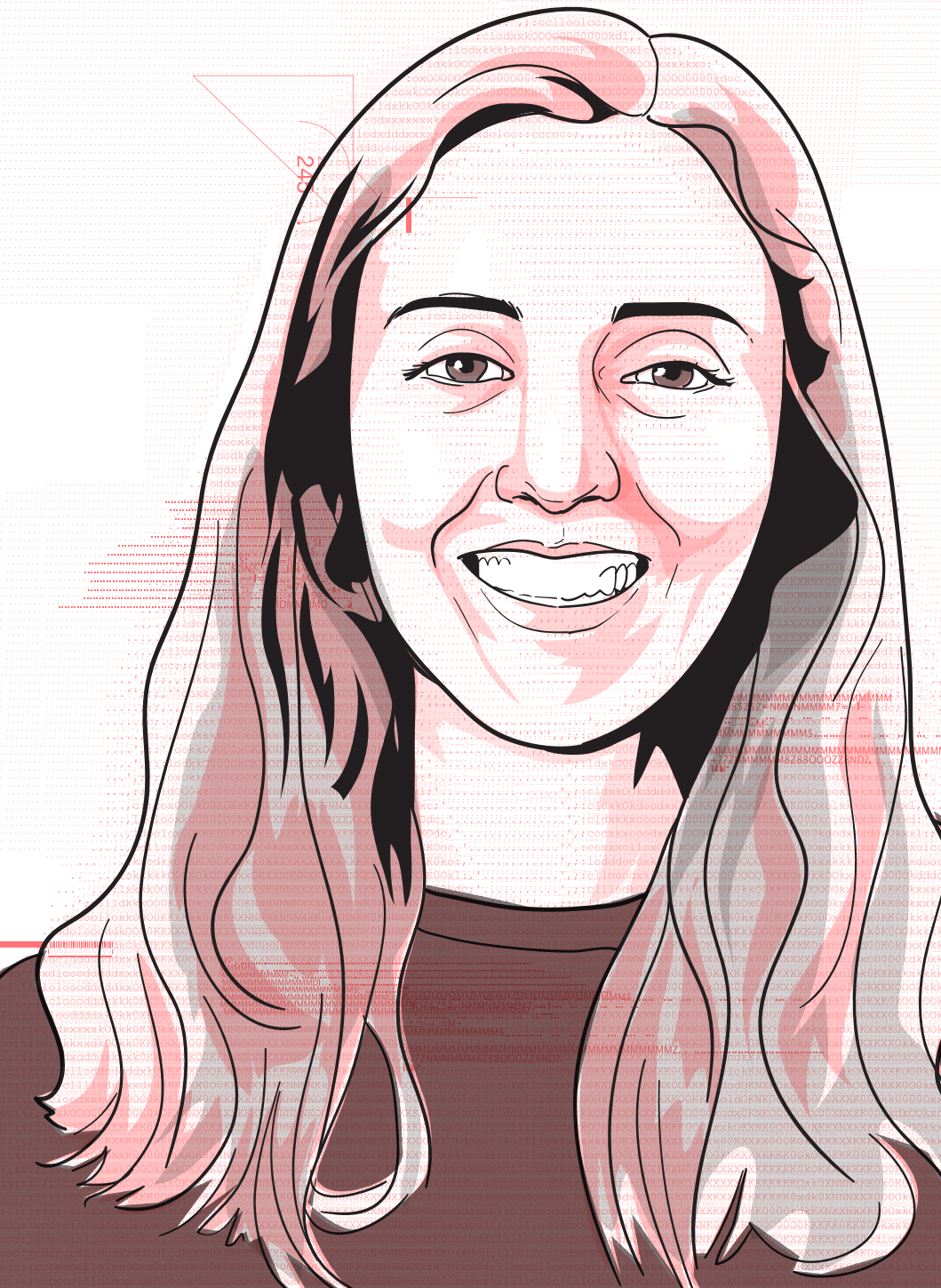
CDU-343.1:004

Índices para catálogo sistemático:

1. Direito e tecnologia : Direito processual penal

343.1:004

Maria Alice Ferreira - Bibliotecária - CRB-8/7964



09.

INFILTRAÇÕES
VIRTUAIS
NO DIREITO
BRASILEIRO:
MAPEANDO
O CENÁRIO

Jacqueline Abreu



A presente apresentação¹ oferece um panorama do quadro normativo hoje em vigor sobre o tema das infiltrações policiais virtuais no Brasil. Tentando mapear a discussão, partirei de uma concepção ampla de “infiltrações”. Para fins didáticos, esse tema pode ser dividido em três categorias, baseados em dois tipos de critério: (i) o elemento da interação: se a polícia está interagindo de alguma maneira com pessoas que estão sendo investigadas; e (ii) o elemento do espaço: em que tipo de espaço em que está ocorrendo a infiltração.

Então temos: (a) infiltrações que envolvem interação e se desenrolam tanto em fóruns públicos e privados, envolvendo um agente encoberto que assume a identidade falsa (o “agente infiltrado”); (b) infiltrações não interativas, em que a polícia não interage diretamente se comunicando com aqueles que está investigando, mas faz coleta de dados em uma fonte aberta para análise de informações (atividades de inteligência e investigação em fontes abertas); e (c) infiltrações não interativas por meio de invasão em um domínio privado (hacking estatal).

AGENTES INFILTRADOS

Quando pensamos em infiltrações policiais, é difícil não pensar no que é retratado em filmes como “Os Infiltrados” (2006) e “Infiltrado na Klan” (2018). Essa é a concepção mais clássica de “agente infiltrado”. É o policial que passa a se envolver com determinada pessoa ou grupo, que é alvo de investigação, e tenta ganhar a sua confiança, para que assim ele possa colher informações privilegiadas sobre aquele grupo, repassar para a polícia e permitir uma investigação apurada. Como existe esse elemento de conseguir a confiança do investigado (e até de tolerância a crimes presenciados), há também por isso um elemento de fraude – uma certa falsidade em que o Estado permite que a polícia se engaje nesses casos específicos em que haveria um interesse relevante para fins de investigação.

Esse tipo de infiltração é interativa e envolve todos os tipos de espaço. Se a polícia desenvolveu uma relação com as pessoas que ela está investigando, ela está se comunicando e colhendo informações tanto em fóruns públicos como em ambientes privados – incluindo nas comunicações de grupo na internet, WhatsApp etc. –, porque a pessoa faz parte daquele grupo agora, em termos de confiança.

O que a gente tem do quadro jurídico aqui? Desde 2006 há uma menção simples e genérica a esse tipo de infiltração policial no art. 53² da Lei de Drogas (Lei nº 11.343/2006) como procedimento investigatório disponível para investigar os crimes punidos por aquela lei. Nesse momento não existiu nenhum estabelecimento de critérios de regulamentação específica sobre quais são os parâmetros e qual é o rito.

Em 2013, veio a Lei das Organizações Criminosas (Lei nº 12.850/2013) com uma previsão semelhante no seu art. 10 e alguma regulamentação: é necessário que haja autorização judicial, indícios de que os alvos que estão sendo investigados por infração penal de organização criminosa e demonstração da necessidade desse tipo de prova. Também se impôs limite de seis meses (com possibilidade de renovação) e a elaboração de relatórios circunstanciado sobre tudo aquilo que é feito e apurado. Há ainda um regime de responsabilização por excessos (art. 13), caso o policial se engaje em algum tipo de crime, durante a infiltração, que seja entendido como excesso, além daquilo que ele deveria ter feito ou poderia ter feito para manter a sua identidade naquele grupo. Aos agentes são também resguardados certos direitos (art. 14), como o de fazer cessar a atuação infiltrada.

Por sua vez, em 2017, foi incluído o art. 190-A³ no Estatuto da Criança e do Adolescente (Lei nº 8.069/1990), que pela primeira vez faz uma menção explícita à infiltração de agentes de polícia *na internet*, como uma medida investigativa possí-

vel para todos os crimes lá elencados – a maioria relacionada a abuso infantil, sendo um deles também o art. 154-A do CP, o crime de invasão de dispositivos. Então, nesses casos, há previsão legal expressa de que um agente de polícia possa se engajar em infiltração virtual. Estão previstos os seguintes elementos: exigência de autorização judicial, delimitação do escopo do que se pode fazer, demonstração de necessidade, limitação temporal (nem tão limitada assim – dois anos), exigência de relatório circunstanciado e etc.

Um comentário pertinente a esse tipo de infiltrações é que, também por conta dessa redação da alteração do ECA com foco em infiltrações *na internet*, levanta-se a dúvida de se a infiltração policial prevista na Lei de Drogas e na Lei das Organizações Criminosas incluiria também autorização para infiltração *virtual* de agentes de polícia. Como pontuei, a categoria de infiltração aqui analisada se refere a infiltrações de agentes policiais em que há elemento de engajamento interativo, voltado a estabelecer relações de confiança, em qualquer tipo de fórum. Como apontei, me parece natural que agentes infiltrados *fisicamente* em grupos também exerçam essa infiltração pela internet – como extensão da mesma identidade falseada. A dúvida, portanto, era/é o quanto desse tipo de engajamento seria permitido através da criação de identidades falsas e estabelecimento de relações com investigados em fóruns quase-públicos (como redes sociais, em que é necessária a criação de perfil para acesso ou de autorização do administrador) ou privados (chats em aplicativos de mensagens) *unicamente ou preponderantemente online*, sem o contato presencial. Nesse aspecto, uma atualização legislativa recente foi trazida pela Lei nº 13.964/2019, que alterou a Lei das Organizações Criminosas para dispor explicitamente sobre infiltrações policiais virtuais (arts. 10-A a 10-D), estando disponível para “investigar os crimes previstos nesta Lei e a

eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas”.

INTELIGÊNCIA E INVESTIGAÇÃO EM FONTES ABERTAS

Há também um tipo de infiltração policial virtual que não é interativo com pessoas que se está investigando. O que se faz nesse tipo de infiltração é coletar e analisar comunicações e dados que estão disponíveis abertamente, em uma fonte aberta em fóruns públicos ou quase-públicos.

No final de 2018 saiu uma notícia de que a Polícia Civil de São Paulo faria algo chamado de *cerca eletrônica*⁴: uma raspagem dos dados disponíveis publicamente em redes sociais, a partir de recortes de publicações em regiões ou certas palavras chave, a pretexto de fazer “campana virtual” e até para começar investigações. Então, por exemplo, raspam-se todos os tuítes com a palavra “arma” ou “assalto” em São Paulo e aí se provoca o engajamento da Polícia Militar para certa área e/ou efetivamente começar uma investigação. Isso conversa bastante com a palestra da professora Margaret Hu na abertura do congresso, em que ela estava dizendo que hoje a polícia faz análise de big data.

O que temos aqui é um tipo de infiltração que consiste em uma **grande operação de coleta e análise de informações – inclusive pessoais. Coleta-se um grande volume de dados, que passa a ser analisado a partir de critérios definidos pela própria polícia e então se chega a quem e ao quê se vai investigar. Essa atividade envolve uma reversão da lógica do processo penal, que é partir não de um suspeito ou de um fato criminoso sobre os quais se quer produzir provas, mas de grandes volu-**

mes de dados para então chegar em um suspeito, então chegar em algum fato criminoso que você vai passar a investigar.

Esse tipo de atuação infiltrada é frequentemente associada com “campanas policiais” comuns, de policiamento ostensivo (como se faz na reportagem citada), para se pontuar que não precisa atender a requisitos materiais e formais específicos. De fato, esse tipo de atividade escapa de um regramento mais específico por duas razões: seu cunho preventivo (em detrimento de repressivo) e a afetação de dados pessoais (mas não propriamente de interesses de privacidade).

Quanto ao primeiro ponto, vale observar que esse é um tipo de infiltração virtual que é inserido principalmente em atividades de inteligência policial. Em outras palavras, não é uma atividade com ênfase investigativa propriamente dita, voltada à repressão de uma conduta criminosa. Quanto a atividades de “agentes de inteligência” – e ao modo como se contrastam com os agentes infiltrados da categoria anterior, vale mencionar uma distinção a que recorreu o STF em uma decisão recente da 2ª Turma (HC 147.837, de 26.02.2019, rel. Min. Gilmar Mendes): “a distinção entre agente infiltrado e agente de inteligência se dá em razão da finalidade e amplitude de investigação. Enquanto “agente de inteligência” tem uma função preventiva e genérica, buscando informações de fatos sociais relevantes ao governo, o “agente infiltrado” possui finalidades repressivas e investigativas, visando à obtenção de elementos probatórios relacionados a fatos supostamente criminosos e organizações criminosas específicas.”

Como já se sinalizou, entretanto, uma atividade de inteligência pode se tornar uma atividade investigativa. A partir do momento em que há direcionamento para apuração de um fato concreto e finalidade repressiva, já se está diante de atividade com cunho investigativo. Na ausência do engajamento (interação para conquista de confiança), pode-se falar em

/ A ATIVIDADE
ENVOLVE A
REVERSÃO DA
LÓGICA DO
PROCESSO PENAL:
PARTIR DE GRANDES
VOLUMES DE DADOS
PARA CHEGAR A UM
SUSPEITO, A UM
FATO CRIMINOSO /

“agente disfarçado” – categoria que pressupõe atuação investigativa passiva e que não possui um regramento particular.⁵

Caso a atuação evolua para as características vistas na categoria anterior, atraindo-se o regramento aplicável (visto na categoria anterior). De fato, como decidiu o STF nesse caso, uma atividade de inteligência (de um policial militar), que começou para simplesmente obter informações para orientar as estratégias de atuação durante a Copa do Mundo e monitoramento de manifestações, logo passou a ser voltada a efetivamente investigar conduta de um grupo concreto de pessoas, estabelecendo-se relações de confiança com eles com o propósito de obter provas (para inquérito da Polícia Civil). Nesse sentido, a prova obtida e usada contra tais pessoas seria ilícita por não ter obedecido aos requisitos legais para infiltrações policiais.⁶

Quanto ao segundo ponto, cabe observar que a atividade de coleta e análise em si de informações em fontes abertas não é considerada invasiva de interesses de privacidade (que supõe interferência em âmbito privado) – sendo, na verdade, tratável sob a perspectiva da proteção de dados pessoais. Nesse sentido, não está sujeita a um regramento abrangente, que estabeleça balizas e salvaguardas nenhuma em termos de devido processo legal. Com efeito, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), além de ainda não estar em vigor, tem o âmbito de aplicação recortado: o seu art. 4º, III dispõe que não se aplica a tratamentos e operações para a segurança pública em investigações. O ponto aqui então é que nós precisamos avançar em uma discussão sobre uma legislação específica para esse assunto e finalmente criar uma autoridade nacional competente para a área.

HACKING


O terceiro tipo de infiltração a ser comentado é de tipo não interativo e envolve intrusão em domínio privado. Uma notí-

cia que ilustra esse tipo de medida, ou pelo menos a pretensão de executá-la, é essa: “PF quer instalar vírus em telefone grampeado para copiar informações.”⁷ Publicada em 2015, é interessante observar como ela é da mesma época em que o WhatsApp realmente ganhou popularidade. Demonstra como autoridades policiais passaram a se preocupar com o fato de que agora não conseguiam mais, com o mesmo tipo de efetividade, obter informações através de interceptações telefônicas. Nesse sentido, tentaram forçar empresas de telefonia a instalar vírus em telefones celulares, para assim conseguir acesso aos aplicativos que têm instalados naquele celular e inclusive aos dados dentro desses aplicativos, portanto, o Whatsapp e as mensagens etc. **Esse é um tipo de atuação policial que envolve um elemento de hacking (exploração de vulnerabilidades de computadores e sistemas, contaminando-os com programa malicioso).**⁸

Quais são os critérios e as balizas para esse tipo de diligência? Neste primeiro momento, a polícia dizia que uma ordem judicial baseada na Lei de Interceptações (Lei nº 9.296/96) era o suficiente. E, com base nessa tese, tentavam forçar as empresas a instalarem esse vírus espião.

Essa tese tem, entretanto, problemas e, para ilustrá-los, cabe mencionar uma decisão recente do STJ. Trata-se do RHC 99.735 (j. 12.12.2018, rel. Min. Laurita Vaz), que envolvia também o WhatsApp, mas não exatamente o uso de software espião. Nele, a autoridade policial apreendeu momentaneamente o celular de uma pessoa, fez o espelhamento pelo WhatsApp Web, com o QR Code. Assim, puxaram todas as mensagens para o computador e a seguir devolveram o celular para a pessoa, que seguiu em frente. A partir do que tinha obtido pelo WhatsApp Web, a polícia conseguiu ter acesso a diversas comunicações que estavam no histórico daquela pessoa, salvas ainda no celular dela.

Ao analisar a licitude da prova assim obtida, o STJ entendeu que havia características específicas aqui: esse tipo de medida (i) envolve um acesso aos dados armazenados historicamente, não só comunicações em tempo real; e (ii) implica a capacidade da polícia de deletar e editar mensagens, justamente porque ela tem a interface do próprio usuário. Essas duas características distinguem a medida de uma interceptação telefônica ou telemática tradicional – em que só se tem acesso a comunicações em tempo real, sem capacidade de intervir/editar. Seria uma medida que não comporta analogia com a Lei nº 9.296/96, e por isso esse tipo de prova, obtida dessa maneira, é ilegal até que seja passado algum tipo de legislação específica que aprove algo nesse sentido. Entendo que esse mesmo raciocínio se aplica a questões de hacking – não temos regramento específico para isso e, até termos, não é possível executar como meio lícito de obtenção de prova.

Então é esse o estado em que nós estamos. Existe um interesse de autoridades investigativas em autorizar isso, reconhecendo em lei. Foram propostas mudanças na Lei nº 9.296/96 nesse sentido no projeto de lei anticrime.⁹ Não foi, entretanto, acolhida a proposta nesse ponto. 

NOTAS

1. O presente texto se baseia em apresentação oral feita no painel “A atuação de agentes de investigação em redes sociais e aplicativos de mensagem” do III Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital, organizado pelo InternetLab em parceria com a FDUSP em agosto de 2019. A autora agradece aos organizadores e às organizadoras pelo convite e pela oportunidade de também registrar as reflexões por essa via. O texto foi revisto em junho de 2020, quando se fez pequenos ajustes para remover maiores oralidades e atualizar comentários.

2. Lei nº 11.343/2006, Art. 53: “Em qualquer fase da persecução criminal relativa aos crimes previstos nesta Lei, são permitidos, além dos previstos em lei, mediante autorização judicial e ouvido o Ministério Público, os seguintes procedimentos investigatórios: I - a infiltração por agentes de polícia, em tarefas de investigação, constituída pelos órgãos especializados pertinentes;”

3. Lei nº 8.069/1990, Art. 190-A, caput: “A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), obedecerá as seguintes regras: (Incluído pela Lei no 13.441, de 2017)”
4. Cerca eletrônica da polícia na internet ajuda a resolver crimes, *O Estado de São Paulo*, 10 de novembro de 2018, <https://bit.ly/2ZpiFLx>.
5. A Lei nº 13.964/2019 (Anticrime) faz menção da figura do agente policial disfarçado em alterações à Lei nº 10.826/2003 (arts. 17 e 18) e à Lei nº 11.343/2006 (art. 33), no sentido de que a venda de armas ou drogas para um agente policial disfarçado ainda caracterizaria crime quando haja “elementos probatórios razoáveis de conduta criminal preexistente”. Não há, entretanto, maior regulamentação da atuação em si. Para discussão sobre tal figura e como se diferencia de um agente *provocador*, ver LINS, C.; SOUZA, R.; CUNHA, R. (2020). “A nova figura do agente disfarçado”. In: Ministério Público Federal. *Inovações da Lei nº 13.964 de 24 de dezembro de 2019*. Brasília: MPF.
6. Para discussão sobre a decisão do STF, ver ROMÃO, L. (2019, dezembro). Agente Infiltrado e agente de Inteligência: distinções a partir de estudo de caso julgado pelo Supremo Tribunal Federal. *Revista Brasileira de Inteligência*. Brasília: Abin, n. 14.
7. Folha de São Paulo, 27 de abril de 2015, <https://bit.ly/2OyZybX>.
8. Para referência introdutória sobre o assunto, ver ABREU, J.; ANTONIALLI, D. (2017). E quando a polícia vira hacker? Blog do InternetLab. <https://bit.ly/3iX25dL>.
9. O PL 882/2019 chegou a contar com a proposta de inserir na Lei nº 9.296/1996 dispositivo que previa: “Art. 9º-A. A interceptação de comunicações em sistemas de informática e telemática poderá ocorrer por qualquer meio tecnológico disponível desde que assegurada a integridade da diligência e poderá incluir a apreensão do conteúdo de mensagens e arquivos eletrônicos já armazenado em caixas postais eletrônicas”.