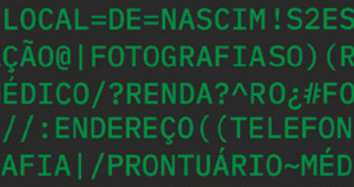
As práticas de Inteligência de Fontes Abertas (OSINT) são amigas ou inimigas dos direitos humanos?

ARTIGO 19

PRÁTICAS DE INTELIGÊNCIA DE FONTES ABERTAS (OSINT) SÃO AMIGAS OU INIMIGAS DOS DIREITOS HUMANOS?



AS PRÁTICAS DE INTELIGÊNCIA DE FONTES ABERTAS (OSINT) SÃO AMIGAS OU INIMIGAS DOS DIREITOS HUMANOS?

REALIZAÇÃO
ARTIGO 19 Brasil e América do Sul

DIRETORIA EXECUTIVA
Paulo José Lara e Raísa Cetra

DIRETORIA FINANCEIRA
Walquiria Moreira

CONSELHO ADMINISTRATIVO
Bianca Santana
Lucia Nader
Luís Eduardo Regules
Malak Poppovic (Presidente do Conselho)
Marcos Rolim
Rodolfo Avelino

CONSELHO FISCAL
Dirlene da Silva
Marcos Fuchs
Mário Rogério Bento

SUPERVISÃO DA PUBLICAÇÃO
Luana Almeida
Paulo José Lara

COORDENAÇÃO DE PESQUISA
Júlia Rocha
Paulo José Lara
Raquel da Cruz Lima

PESQUISA
Brenda Cunha
Jade Alves
Marília Papaléo Gagliardi
Rafaela Cavalcanti de Alcântara
Taynara Lira

TEXTO
André Boselli
Marília Papaléo Gagliardi

REVISÃO TEXTUAL
Larissa Fontana

PROJETO GRÁFICO
E DIAGRAMAÇÃO
Luan Freitas

ILUSTRAÇÃO
Filipe Moura

EDITORAÇÃO
Romulo Santana Osthues

_
Esta pesquisa foi possível graças ao projeto *Latin America Internet Freedom*, realizado com o suporte do Bureau of Democracy, Human Rights, and Labor (DRL).

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

As práticas de inteligência de fontes abertas (OSINT) são amigas ou inimigas dos direitos humanos? [livro eletrônico] / [coordenação Júlia Rocha, Paulo José Lara, Raquel da Cruz Lima ; ilustração Filipe Moura ; texto André Boselli, Marília Papaléo Gagliardi]. -- 1. ed. -- São Paulo : ARTIGO 19, 2023.
PDF

Vários colaboradores.
Bibliografia.
ISBN 978-65-89389-37-8

1. Direito à privacidade - Brasil 2. Direitos humanos 3. Inovação tecnológica 4. Proteção de dados pessoais 5. Proteção de dados - Direito - Brasil 6. Proteção de dados - Leis e legislação I. Rocha, Júlia. II. Lara, Paulo José. III. Lima, Raquel da Cruz. IV. Moura, Filipe. V. Boselli, André. VI. Gagliardi, Marília Papaléo.

23-171914 CDU-342.721(81)

Índices para catálogo sistemático:

1. Brasil : Lei Geral de Proteção de Dados : Direito à privacidade 342.721(81)

Aline Graziele Benitez - Bibliotecária - CRB-1/3129

Use este QR code para acessar nossas outras publicações

– Sumário

<pág. 07/> Apresentação

<pág. 09/> 1. O que é OSINT e quais são seus riscos e possíveis benefícios?

<pág. 13/> 2. Por que e como foi feita a pesquisa?

<pág. 17/> 3. Normas aplicáveis às práticas de OSINT

<pág. 19/> 3.1. Leis que protegem dados pessoais

<pág. 20/> 3.2. O que diz a LGPD?

<pág. 22/> 3.3. Normas sobre atividade de inteligência

<pág. 25/> 4. Análise de decisões judiciais e administrativas

<pág. 26/> 4.1. Decisões judiciais

<pág. 28/> 4.2. Decisões administrativas

<pág. 29/> 4.3. Debates jurídicos

<pág. 31/> 5. Respostas de órgãos de Estado
<pág. 33/> 5.1. Resultados

<pág. 37/> 6. O que dizem as empresas e outras pessoas jurídicas

<pág. 39/> 7. Respostas de profissionais que usam OSINT e de especialistas no tema

<pág. 43/> Conclusões

<pág. 45/> Apêndice - Perguntas feitas aos órgãos de Estado

<pág. 47/> Notas

– Apresentação

A ARTIGO 19 é uma organização internacional de direitos humanos, fundada em Londres, em 1987, cujo foco de atuação é a proteção e a promoção dos direitos à liberdade de expressão e ao acesso à informação pública, previstos pelo artigo 19 da Declaração Universal dos Direitos Humanos. No Brasil desde 2007, a ARTIGO 19 vem atuando na proteção de comunicadores e comunicadoras e de defensores e defensoras de direitos humanos; no combate às violações dos direitos de protesto e de participação; na defesa das liberdades de imprensa, artística e de ensino, assim como do direito da população à informação; e na garantia dos direitos digitais.

O programa de Direitos Digitais da organização trabalha com a intersecção entre tecnologia, direitos humanos e liberdade de expressão, e atua com formação, advocacy, pesquisa e implementação de soluções para a construção de uma internet mais democrática e diversa, menos desigual e concentrada, que permita a concretização do exercício das manifestações e expressões também nas redes digitais. Entre os muitos temas trabalhados pela ARTIGO 19 nos últimos anos, citamos as discussões e contribuições para a aprovação da Lei Geral de Proteção de Dados Pessoais (LGPD), a pesquisa e a implementação de Redes Comunitárias, o desenvolvimento de estudos, debates e políticas sobre a desinformação online, a atuação no campo das tecnologias do voto e da democracia digital e outras várias ações no campo do combate à vigilância em massa.

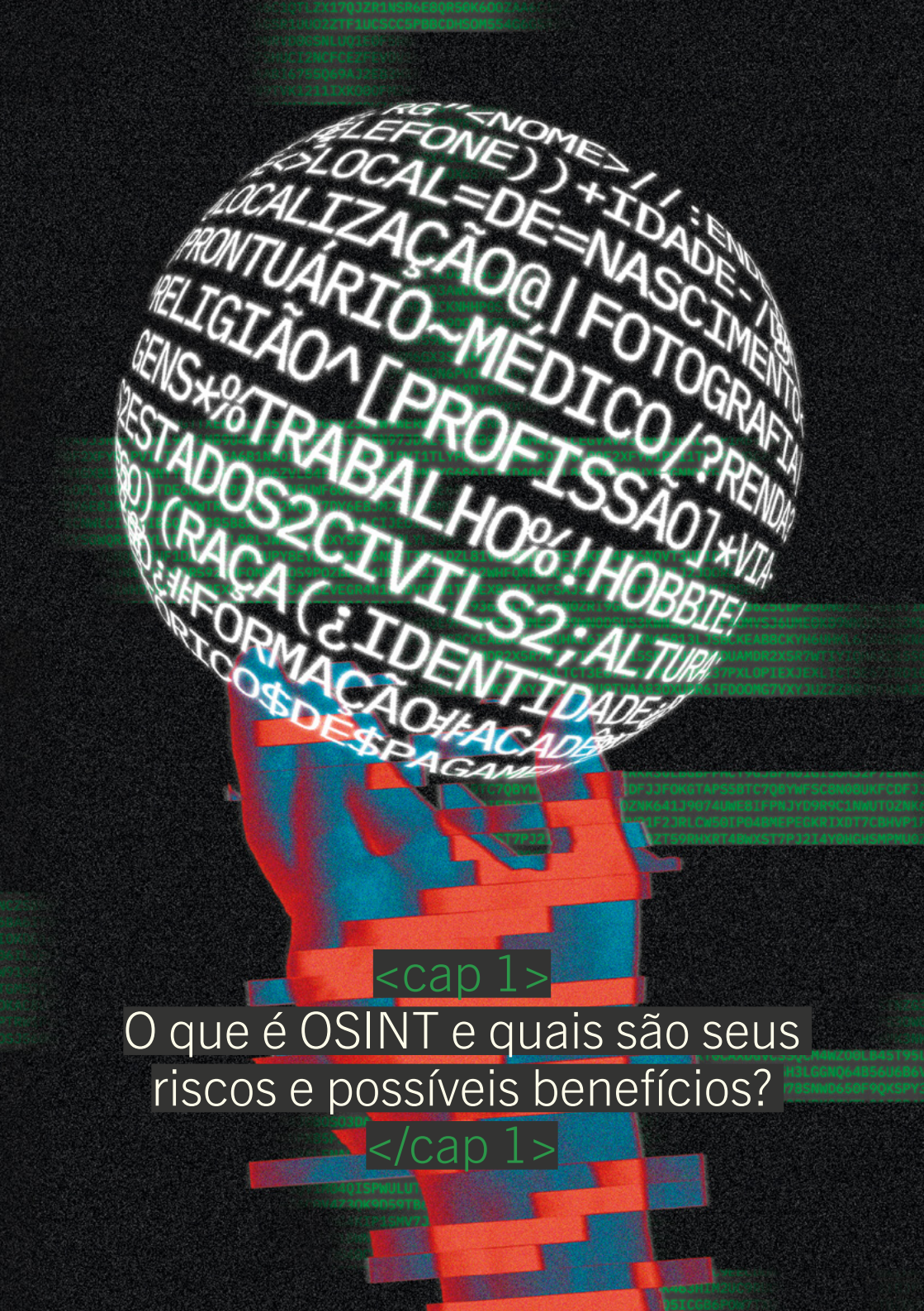
As chamadas práticas de "Inteligência de Fontes Abertas" (OSINT, do inglês *Open Source Intelligence*) consistem na coleta, na análise e no tratamento, para fins de inteligência, de dados disponíveis publicamente na internet. Respeitados direitos e salvaguardas, esse tipo de prática pode ser muito frutífero em algumas situações, como no auxílio à formulação de políticas públicas ou em investigações jornalísticas. No entanto, boa parte das iniciativas de OSINT é projetada para fins de

segurança pública, o que pode implicar excesso de vigilância e monitoramento por parte de agentes públicos e privados, colocando em risco uma série de direitos humanos.

Além disso, no Brasil, não existem normas que tratem diretamente do assunto, o que potencializa os riscos de que práticas de OSINT sejam manejadas sem transparência, representando uma ameaça a valores democráticos fundamentais, como a liberdade de expressão, a privacidade e o direito de reunião.

Foi justamente para identificar o atual cenário de uso de fontes abertas para fins de inteligência no País e entender como o manejo dessa prática pode impactar os direitos humanos que a ARTIGO 19 fez uma pesquisa sobre o assunto, que apresenta uma análise das principais normas aplicáveis à proteção de dados pessoais e à atividade de inteligência; um levantamento de decisões judiciais e administrativas que começam a tratar dessa questão; a submissão de perguntas a órgãos de Estado e empresas que atuam na área; e entrevistas com profissionais que trabalham com OSINT e com especialistas do tema.

A pesquisa foi feita no segundo semestre de 2022 e faz parte do projeto *Latin America Internet Freedom*, promovido pelo Bureau of Democracy, Human Rights, and Labor (DRL). A íntegra do material que resultou nesta publicação está com a ARTIGO 19 e pode ser solicitada por quem se interessar pelo assunto. Além do Brasil, a pesquisa foi desenvolvida também na América Central, pela ARTIGO 19 México; na Argentina, pelo Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE); e na Colômbia, pela Fundación Karisma.


<cap 1>
O que é OSINT e quais são seus riscos e possíveis benefícios?
</cap 1>

Open Source Intelligence (OSINT) – em português, "Inteligência de Fontes Abertas" – é a coleta, a análise e o tratamento de dados disponíveis publicamente na internet para fins de inteligência. Essas informações são consideradas "abertas" porque podem ser acessadas livremente, sem a necessidade de pagamento para sua obtenção ou de utilização de algum método ilícito para acessá-las (como a invasão de sistemas protegidos).

Alguns pontos importantes sobre o uso de OSINT

</> A coleta de dados, em diferentes fontes na internet, quando sistematizados e organizados, pode revelar informações valiosas sobre o comportamento de indivíduos ou grupos;

</> Com essa prática, é possível traçar perfis, identificar necessidades e demandas de determinados segmentos da população ou, ainda, auxiliar na prestação de serviços públicos e privados;

</> Esse método também é usado em investigações jornalísticas, o que permite a produção de conteúdo de relevante interesse público, ajudando a concretizar o direito de acesso à informação;

</> Essas informações públicas podem ser acessadas, por exemplo, por meio de buscadores de internet, como Google, Bing, Yahoo ou outro serviço do tipo;

</> As práticas de OSINT também podem ser utilizadas para fins específicos, por exemplo, em investigações jornalísticas sobre as pessoas que participaram dos atos golpistas de 8 de janeiro de 2023; ou para fins mais amplos, com o uso de softwares que coletam e processam em larga escala uma série de informações de fontes públicas;

</> Embora essas informações possam ter sido inseridas pelas próprias pessoas (em sites, fóruns, blogs ou redes sociais), também podem ter chegado à web por meio de terceiros, sem que a pessoa saiba ou concorde com a inserção de seus dados;

</> Nem sempre as pessoas sabem que suas informações, livremente espalhadas pelas redes, de forma consciente ou não, podem ser agrupadas e analisadas para um determinado fim;

</> **Um grande número das iniciativas de OSINT são projetadas para fins de segurança e podem implicar excesso de vigilância e monitoramento por parte de agentes públicos e privados, com risco de violação de direitos humanos;**

</> Ou seja, práticas de OSINT podem ser usadas para fins ilegítimos, como perseguição de opositores políticos, violação da privacidade e investigações criminais ilegais;

</> A situação se torna mais preocupante porque não existe uma regulamentação específica sobre o tema no Brasil, tampouco uma delimitação dos usos e finalidades admitidos – muito embora essa prática já esteja sendo plenamente aplicada, muitas vezes sem transparência por parte de quem a utiliza. Entretanto, existem algumas normas relativas à proteção de dados pessoais e à atividade de inteligência que podem ser aplicadas às iniciativas de OSINT;

</> Também é preciso considerar que, mesmo diante da ausência de normas que disciplinem especificamente o assunto, o emprego de práticas de OSINT deve respeitar as balizas estabelecidas pela Constituição Federal e os parâmetros internacionais de direitos humanos.

<cap 2>

Por que e como foi feita a pesquisa?

</cap 2>

A pesquisa contempla uma análise das principais normas aplicáveis à proteção de dados pessoais e à atividade de inteligência; um levantamento de decisões judiciais e administrativas que começam a tratar dessa questão; a submissão de perguntas a órgãos de Estado e empresas que atuam na área; e entrevistas com profissionais que trabalham com OSINT e com especialistas no tema.

Como as práticas de OSINT podem impactar os direitos humanos no Brasil?

PARA RESPONDER A ESSA PERGUNTA, A ARTIGO 19 DESENVOLVEU UM ESTUDO QUALITATIVO E EXPLORATÓRIO PARA DETECTAR

</> Quais normas do ordenamento jurídico brasileiro são aplicáveis a esse tipo de iniciativa (considerando que não existe no País uma regulamentação específica sobre o tema);

</> Como decisões judiciais e administrativas têm interpretado a questão;

</> Se órgãos do Estado brasileiro, especialmente os que atuam direta ou indiretamente na área de segurança pública, valem-se de práticas de OSINT e, caso isso aconteça, como é feito e com quais objetivos;

</> Quais empresas atuam nesse segmento no País e como esses serviços são realizados;

</> De que modo as práticas de OSINT são utilizadas por profissionais que as empregam em suas atividades (como jornalistas e integrantes de organizações da sociedade civil) e quais avaliações especialistas de OSINT têm feito sobre o assunto.

Esta publicação apresenta a síntese de um material mais extenso. Quem tiver interesse em acessar a pesquisa na íntegra pode solicitá-la pelo email abaixo:

comunicacao@artigo19.org

PARA COLHER INFORMAÇÕES QUE RESPONDAM A ESSES TÓPICOS, REALIZAMOS, RESPECTIVAMENTE, AS SEGUINTES AÇÕES

</> Pesquisa de dispositivos constitucionais, legais e infralegais relacionados à proteção de dados pessoais e às atividades de inteligência na área de segurança pública;

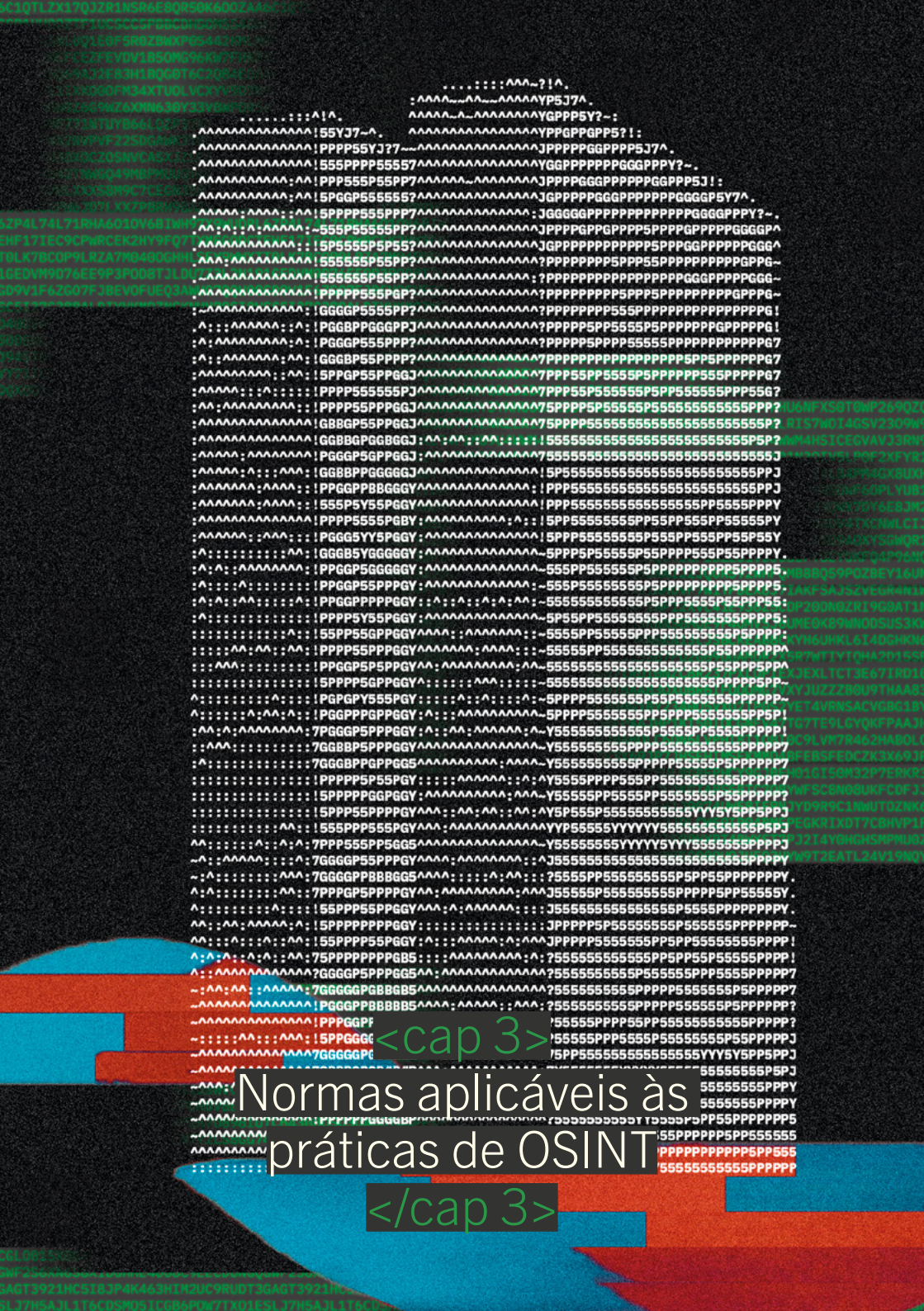
</> Pesquisa jurisprudencial no Supremo Tribunal Federal (STF), no Superior Tribunal de Justiça (STJ), Tribunais Regionais Federais (TRFs) e, na esfera administrativa, no Tribunal de Contas da União (TCU);

</> Envio de questionários a 19 órgãos da administração pública sobre o uso de inteligência de fontes abertas para fins de inteligência na área de segurança, junto à realização de pedidos formais respaldados pela Lei de Acesso à Informação (LAI), que regulamenta o direito constitucional de acesso às informações públicas;

<?> A relação completa dos órgãos que foram objeto da pesquisa estão na seção "Respostas de órgãos de Estado".

</> Envio de questionários às principais empresas e pessoas jurídicas que oferecem serviços de OSINT no Brasil, além da análise de seus respectivos sites;

</> Submissão de roteiros de perguntas às pessoas entrevistadas.


<cap 3>
Normas aplicáveis às práticas de OSINT
</cap 3>

No Brasil, não há leis, dispositivos infralegais ou regulamentações que disciplinem especificamente o uso de dados de fontes abertas para fins de inteligência. No entanto, existem leis e portarias que tratam da proteção de dados pessoais, além de normas que abordam a atividade de inteligência para fins de segurança pública.

3.1. Leis que protegem dados pessoais

O emprego de práticas de OSINT só é possível por meio da análise sistêmica de informações abertas. Como muitas delas são dados pessoais, seu tratamento deve respeitar as normas criadas para preservar a privacidade e a intimidade das pessoas por trás desses dados.

No Brasil, a proteção de dados pessoais foi reconhecida como um direito fundamental em 2022 e está prevista no art. 5º, inciso LXXIX, da Constituição Federal.

Além disso, algumas leis também dispõem sobre o tratamento de dados pessoais. As principais são:

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS[1] (LEI 13.709/2018)[2]

MARCO CIVIL DA INTERNET (LEI 12.965/2014)[3]

LEI DE ACESSO À INFORMAÇÃO (LEI 12.527/2011)[4]

LEI DO CADASTRO POSITIVO (LEI 12.414/2011)[5]

CÓDIGO DE PROTEÇÃO E DEFESA DO CONSUMIDOR (LEI 8.078/1990)[6]

Segundo a Lei Geral de Proteção de Dados Pessoais (LGPD), considera-se tratamento de dados pessoais "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".[7]

As normas que tratam de dados pessoais exigem transparência para a sua utilização. É necessário que as pessoas saibam a finalidade do uso das suas informações disponibilizadas online.

3.2. O que diz a LGPD?

A Lei Geral de Proteção de Dados determina como as informações pessoais podem ser coletadas e tratadas, estabelecendo parâmetros para evitar o uso indevido desses dados e prevendo responsabilidades para empresas e para o poder público em caso de descumprimento das exigências legais.

Apesar de não tratar especificamente de inteligência de fontes abertas, a lei prevê que "o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização".[8]

Mas a LGPD não se aplica integralmente ao tratamento de dados pessoais realizados para os seguintes fins:

- </> **De segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais;**
- </> **Jornalísticos e artísticos;**
- </> **Acadêmicos.**

No entanto, isso não significa que, nessas hipóteses, os dados podem ser tratados de qualquer maneira. Por exemplo, quanto às atividades de inteligência relacionadas à segurança e à defesa nacional, o Supremo Tribunal Federal entende que "é imprescindível

que a colheita de dados, a produção de informações e o respectivo compartilhamento entre os órgãos [...] se opere com estrita vinculação ao interesse público, observância aos valores democráticos e respeito aos direitos e garantias fundamentais".[9]

Além disso, nessas hipóteses de tratamento de dados pessoais realizados por órgãos de segurança pública e defesa, a própria LGPD prevê que o devido processo legal, os princípios gerais de proteção e os direitos do titular devem ser observados.

Atualmente, existem apenas propostas legislativas para regulamentar o tratamento de dados pessoais para fins de segurança do Estado, defesa nacional, segurança pública, investigação e repressão de infrações penais: um anteprojeto de lei, feito por uma comissão de juristas formada pela presidência da Câmara dos Deputados em 2020; e o projeto de lei 1.515/2022.[10]

Nas hipóteses compreendidas pela norma, a LGPD determina que o tratamento de dados pessoais deve respeitar alguns requisitos, como a concessão de consentimento por parte da pessoa titular das informações que serão utilizadas.

Esse consentimento é dispensado quando os dados são declaradamente tornados públicos pelo próprio titular. Ainda assim, seus direitos devem ser respeitados, bem como os princípios previstos pela lei para o trabalho com esses dados:

</> **Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados à pessoa titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;**

</> **Adequação: compatibilidade do tratamento dos dados com as finalidades informadas à pessoa titular, de acordo com o contexto do tratamento.**

Uma das hipóteses de uso de dados pessoais prevista pela LGPD se refere às atividades de tratamento e compartilhamento de dados entre órgãos públicos, realizadas pelo Estado e necessárias para a execução de políticas públicas.

Outra hipótese diz respeito ao uso de dados pessoais para a realização de estudos por órgãos de pesquisa, que deve garantir, sempre que possível, o tratamento dessas informações de forma anônima.

Apesar da atual inexistência de normas específicas sobre OSINT, já há iniciativas em andamento para a promoção do uso de dados de fontes abertas em estudos, investigações e pesquisas.

Exemplo disso é que o debate sobre o uso dessas informações já adentrou alguns órgãos estatais, como o Ministério Público Federal, que lançou, em 2019, um catálogo de fontes abertas;[11] o Instituto Brasileiro de Geografia e Estatística (IBGE); a seção de Dados Abertos do Ministério da Educação (MEC) e o Fundo de Educação Básica (Fundeb), que utilizam e disponibilizam informações de fontes abertas.

3.3. Normas sobre atividade de inteligência

Algumas normas que regem a atividade de inteligência no Brasil são:

</> **LEI 9.883/1999** - criou a Agência Brasileira de Inteligência (Abin). No texto, não há especificação do que significa o termo "dados", previsto na lei. "Inteligência" é definida como "a atividade que objetiva a obtenção, análise e disseminação de conhecimentos, dentro e fora do território nacional, sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado".[12] A lei também institui o Sistema Brasileiro de Inteligência (Sisbin), cuja missão é integrar as ações de planejamento e execução das atividades de inteligência do País, com o objetivo de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional.

</> **DECRETO 3.695/2000** - instituiu o Subsistema de Inteligência de Segurança Pública (Sisp), cuja função é oferecer aos governos federal e estaduais informações que amparem a tomada de decisões no âmbito da segurança pública.[13]

</> **RESOLUÇÃO 1/2009** - na qual a Secretaria Nacional de Segurança Pública (Senasp), órgão ligado ao Ministério da Justiça e Segurança Pública, regulamenta o Sisp e dispõe sobre o uso de informações, dados e seu respectivo tratamento estratégico. Não há definição do termo "dados".[14]

</> **A Política Nacional de Inteligência (PNI), fixada pelo Decreto 8.793/2016,** traz diretrizes sobre o uso e o compartilhamento de dados e sobre atividades de inteligência, no geral as associando à neutralização de ameaças à sociedade e ao Estado brasileiros. Não há definição do termo "dados".[15]

</> **LEI 13.675/2018** - institui o Sistema Único de Segurança Pública (Susp) e cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS). O Susp é composto por diversos órgãos de segurança pública do País, como todas as polícias do âmbito federal e estadual. A articulação entre esses órgãos, segundo a lei, deve contar com o compartilhamento de informações, inclusive com o Sisbin. Quanto à PNSPDS, a lei prevê que um dos seus objetivos é "fomentar a integração em ações estratégicas e operacionais, em atividades de inteligência de segurança pública" e "estimular o intercâmbio de informações de inteligência de segurança pública com instituições estrangeiras congêneres".[16]

</> **DECRETO 11.103/2022** - revogado em 2023,[17] disciplinava questões atreladas à Secretaria de Operações Integradas (Seopi).[18]

</> **DECRETO 11.348/2023** - regulamenta a Diretoria de Operações Integradas e de Inteligência e visa à integração e ao compartilhamento de dados e conhecimentos necessários à tomada de decisões administrativas e operacionais por parte da Secretaria Nacional de Segurança Pública. O decreto também prevê que o tratamento de dados pessoais é uma das competências do Ministério da Justiça e Segurança Pública (MJSP).[19]

A atividade de inteligência está, na maior parte dos casos, associada à segurança pública. Não há, no entanto, especificação sobre como os dados de fontes abertas podem ser usados para esse fim.

<cap 4>

Análise de decisões judiciais e administrativas

</cap 4>

Para avaliar como o Poder Judiciário e a Administração Pública estão interpretando casos relacionados ao uso de fontes abertas para fins de inteligência, mesmo inexistindo normas que disciplinem especificamente o assunto, foi feita uma pesquisa jurisprudencial em tribunais superiores e no Tribunal de Contas da União (TCU).

A pesquisa de jurisprudência realizada nesses tribunais usou as seguintes palavras e expressões:

- </> "inteligência em fontes abertas", "dados abertos", "fontes abertas", "dados públicos" e "banco de dados públicos";
- </> "OSINT", "Open Source Intelligence", "Fontes abertas", "Bancos de dados abertos".

4.1. Decisões judiciais

No geral, as buscas não encontraram correspondência exata com assuntos relacionados a OSINT. Por exemplo, muitas decisões encontradas se referem a dados de órgãos públicos, e não a informações pessoais disponibilizadas em bancos públicos. Entre as 2.914 decisões encontradas, apenas 31 dizem respeito a OSINT (pouco mais de 1% do total).

Apesar da falta de padronização de termos nas decisões judiciais, há o entendimento de que, mesmo para serviços de segurança e inteligência, o uso de dados pessoais deve obedecer a limites legais e constitucionais.

O "DOSSIÊ ANTIFASCISTA"

UM DOS CASOS MAIS IMPORTANTES SOBRE PARÂMETROS PARA USO DE OSINT FOI A DECISÃO DO STF NO JULGAMENTO DA ADPF 722[20] SOBRE O CHAMADO "DOSSIÊ ANTIFASCISTA", UM DOCUMENTO SIGILOSO QUE CONTINHA O MAPEAMENTO E A IDENTIFICAÇÃO DE 579 PESSOAS (A MAIORIA SERVIDORES PÚBLICOS DA ÁREA DE SEGURANÇA E PROFESSORES UNIVERSITÁRIOS) QUE FAZIAM OPOSIÇÃO AO GOVERNO DO ENTÃO PRESIDENTE JAIR BOLSONARO. O DOCUMENTO FOI ELABORADO PELA SECRETARIA DE OPERAÇÕES INTEGRADAS

(SEOPI)[21] DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA E CONTINHA INFORMAÇÕES FUNCIONAIS DOS SERVIDORES ALÉM DE DADOS RETIRADOS DE FONTES ABERTAS, COMO NOME, ENDEREÇO, FOTOGRAFIA, URL DE REDES SOCIAIS, ENTRE OUTROS. ESSE DOSSIÊ FOI COMPARTILHADO COM ÓRGÃOS PÚBLICOS DE SEGURANÇA, COMO A POLÍCIA FEDERAL, A POLÍCIA RODOVIÁRIA FEDERAL, A AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN), A FORÇA NACIONAL E ALGUNS CENTROS DE INTELIGÊNCIA VINCULADOS À PRÓPRIA SEOPI.

O SUPREMO TRIBUNAL FEDERAL DECLAROU ESSE TIPO DE DOSSIÊ "INCONSTITUCIONAL", CONSIDERANDO QUE O USO DA MÁQUINA PÚBLICA PARA A PRODUÇÃO E O COMPARTILHAMENTO DE INFORMAÇÕES DE SERVIDORES PARA INTERESSES PRIVADOS CARACTERIZA "DESVIO DE FINALIDADE" E "ABUSO DE PODER".[22]

A DECISÃO RESSALTOU QUE OS SERVIÇOS DE INTELIGÊNCIA TAMBÉM ESTÃO SUBMETIDOS AO PODER JUDICIÁRIO E QUE ESSAS ATIVIDADES DEVEM SER FEITAS DENTRO DOS LIMITES CONSTITUCIONAIS, LEGAIS E DEMOCRÁTICOS, NÃO SENDO ADMITIDO SEU USO PARA A PERSEGUIÇÃO DE OPOSITORES E O APARELHAMENTO POLÍTICO DO ESTADO.

Em relação ao conjunto das decisões analisadas que continham os termos "dados públicos", "fontes abertas" ou "bancos de dados públicos":

</> 80% tratam de fontes públicas, mas as definições desses termos, no geral, são vagas. Em algumas decisões, a expressão "fontes públicas" é usada como sinônimo de "base de dados disponíveis" e "elementos informativos colhidos em fontes abertas na internet";

</> Apenas em dois casos, que estão ligados a processos licitatórios e de inteligência, o termo "fontes abertas" é relacionado a mídias sociais, *deep web* e *dark web*, mas, em ambos os casos, os processos foram encerrados por motivos formais e o mérito sobre o uso desses dados não foi avaliado;

<?> *Deep web* é a expressão normalmente usada para se referir a endereços que não são indexados por mecanismos de busca, como Google, Yahoo e Bing. *Dark web* é uma parte da *deep web* na qual são realizadas atividades ilícitas, como a comercialização de substâncias proibidas, armas e mercadorias roubadas, e a disponibilização de conteúdos ilegais.

</> Apenas 12% das decisões tratam de "bancos de dados públicos", que foram vinculados à existência de informações disponíveis em diferentes fontes de acesso, mas sem nenhuma apuração sobre a possibilidade de o Estado lidar com esses dados para fins de inteligência;

</> Em apenas uma decisão, o termo "dados públicos" foi analisado como um tipo de registro ou banco de dados com informações "que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações". Nessa formulação, no entanto, não há uma vinculação ou uma especificação de dados públicos com dados pessoais.

4.2. Decisões administrativas

O TRIBUNAL DE CONTAS DA UNIÃO CHEGOU A SUSPENDER A COMPRA DE UM SISTEMA OSINT PELO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, POIS NÃO HAVIA TRANSPARÊNCIA SOBRE COMO OS DADOS PESSOAIS SERIAM TRATADOS.

As principais decisões encontradas nesse âmbito dizem respeito a um pregão eletrônico, realizado pela Secretaria de Gestão e Ensino em Segurança Pública do Ministério da Justiça e Segurança Pública (Segen/MJSP), para a compra de um sistema de "Solução de Inteligência em Fontes Abertas, Mídias Sociais, *Deep* e *Dark Web*" por um valor estimado de R$ 25,4 milhões. Em decisão cautelar (Acórdão 2.678/2021),[23] o TCU suspendeu o processo de aquisição, que já contava com uma empresa selecionada.

O caso chegou ao TCU por meio de representações de congressistas, do Ministério Público junto ao TCU e de uma denúncia feita por um cidadão cuja identidade não foi revelada. De acordo com a decisão, todos apontaram que o vereador Carlos Bolsonaro (Republicanos/RJ), filho do então presidente da República, "estaria intervindo nessas compras com o objetivo de aparelhar estruturas de inteligência no Ministério da Justiça e Segurança Pública e na Polícia Federal". O objetivo velado seria "produzir informações destinadas a pretensões particulares de dirigentes políticos, e não a assuntos de interesse nacional, o que poderia resultar na violação à privacidade dos cidadãos brasileiros".[24]

Segundo a decisão, as apurações indicaram que poderia haver "desvio de finalidade" no uso das informações produzidas pelo sistema. Havia "alto risco" relacionado ao acesso e ao manuseio de informações pessoais que, sem o devido controle, poderiam permitir a exposição de pessoas e seus dados, causando sérios prejuízos à sociedade.

Em outra decisão sobre o mesmo episódio (Acórdão 1.353/2022),[25] o TCU deu ciência do caso à Controladoria-Geral da União (CGU) para que esta avaliasse se deveria instaurar um processo administrativo disciplinar contra o administrador da empresa vencedora, já que ele pertenceria aos quadros da Abin, o que viola a proibição legal segundo a qual servidores públicos não podem participar da gerência ou da administração de empresas, constituindo conduta punível com demissão.

A decisão cautelar que havia determinado a suspensão da compra acabou sendo revogada, sob o entendimento de que não existia nos autos "qualquer elemento probatório da suposta intenção de se utilizar de maneira indevida as informações produzidas"[26] pela ferramenta. O caso foi encerrado em março de 2023.

4.3. Debates jurídicos

</> Pesquisas conduzidas em sites de temáticas jurídicas no Brasil, como ConJur; Jota, Jusbrasil e Migalhas, permitiram a análise de alguns casos que citaram OSINT ou fontes de dados abertas;

</> Um dos artigos encontrados menciona um software que, baseando-se em tweets, é capaz de prever a ocorrência de protestos com uma média de 75% de precisão;[27]

</> Outro caso da amostra se refere a fraudes de boletos bancários que utilizavam dados da vítima disponíveis em fontes abertas;[28]

</> Há também artigos sobre o uso de OSINT para investigação criminal em massa,[29] o uso dessas fontes em reações a ataques terroristas,[30] a origem de técnicas de OSINT,[31] a possibilidade de usar OSINT para a produção de provas digitais,[32] além de muitos artigos vinculando OSINT à segurança corporativa;[33]

- Entre os resultados da pesquisa, há, inclusive, a promoção de serviços de OSINT[34] e a divulgação de curso de capacitação sobre fontes de dados abertas para agentes do Ministério Público;[35]

- Apesar de o tema ser objeto de artigos em portais jurídicos, não foram identificados debates que tivessem como centro a necessidade de parametrização, por meio de legislação ou jurisprudência, do uso de fontes de dados abertas.

<cap 5>

Respostas de órgãos de Estado

</cap 5>

AINDA QUE EXISTAM POLÍTICAS INTERNAS SOBRE O TRATAMENTO DE DADOS PESSOAIS, EM NENHUM DOS ÓRGÃOS ANALISADOS, HÁ ALGUMA NORMA QUE REGULAMENTE O USO DE OSINT.

Em 2021, a informação da Polícia Militar de Minas Gerais de que a prisão de um jovem[36] foi possível a partir de um trabalho de monitoramento de redes sociais confirmou que a instituição emprega OSINT, apesar da falta de regulamentação da prática. O jovem foi preso por causa de uma publicação postada por ele no Twitter.

Para a pesquisa que resultou nesta publicação, esse episódio permite partir da hipótese de que órgãos públicos usam fontes abertas para fins de inteligência. Assim, foram submetidos questionários a 19 órgãos públicos (nem todos diretamente relacionados à área de segurança), com perguntas sobre a utilização desse tipo de ferramenta, bem como sobre os regramentos aplicados em seu uso.[37]

Os questionários foram enviados para as seguintes instituições:

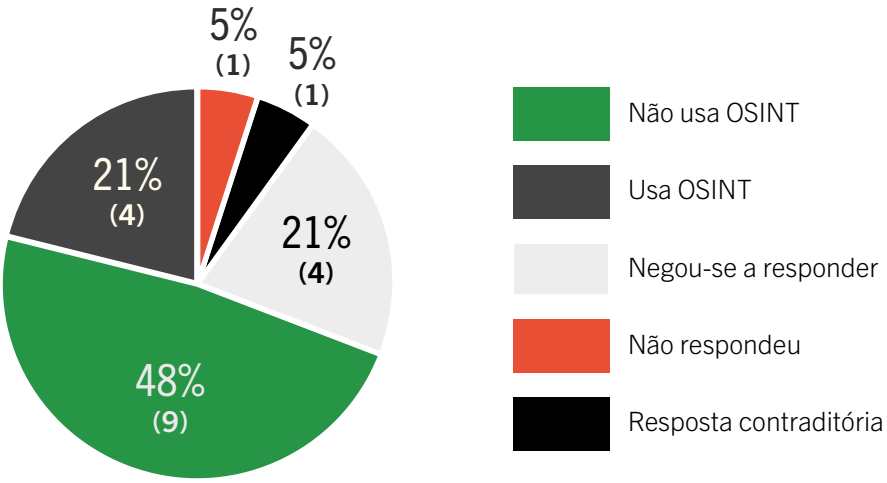
- [/] **Ministério da Defesa (MD)**
- [/] **Centro de Inteligência da Marinha do MD (CIM)**
- [/] **Ministério da Justiça e Segurança Pública (MJSP)**
- [/] **Secretaria de Operações Integradas do MJSP**
- [/] **Gabinete de Segurança Institucional (GSI)**
- [/] **Agência Brasileira de Inteligência do GSI (Abin)**
- [/] **Departamento de Polícia Federal (DPF)**
- [/] **Ministério Público Federal (MPF)**
- [/] **Conselho Nacional de Justiça (CNJ)**
- [/] **Ministério das Comunicações (MCom)**
- [/] **Ministério da Ciência, Tecnologia e Inovações (MCTI)**
- [/] **Ministério da Economia**
- [/] **Receita Federal do Brasil (RFB)**
- [/] **Procuradoria-Geral da Fazenda Nacional (PGFN)**
- [/] **Ministério da Cidadania**
- [/] **Secretaria Especial do Desenvolvimento Social (Ministério da Cidadania)**
- [/] **Tribunal de Contas da União (TCU)**
- [/] **Controladoria-Geral da União (CGU)**
- [/] **Instituto do Patrimônio Histórico e Artístico Nacional (Iphan)**

As perguntas consistiram em:

- Informar se, dentro da agência/órgão, existem setores que coletam dados pessoais de fontes abertas para prevenção e/ou investigação de crimes;
- Em caso positivo, indicar as regras, os regulamentos, as portarias ou os protocolos aplicados em tais atividades;
- Responder se já existem ou se há o planejamento de possíveis estudos, portarias, regulamentos, propostas de regulamentos, propostas de portarias ou documentos relacionados a coletas de dados pessoais de fontes abertas;
- Identificar se foram negociados e/ou assinados contratos com empresas privadas para coleta e análise de dados de fontes abertas e, em caso positivo, quais foram essas empresas.

5.1. Resultados

Respostas dos órgãos sobre uso de OSINT para prevenção e/ou investigação de crimes



<?>

Foram consideradas as nomenclaturas dos órgãos à época em que a pesquisa foi feita. Por exemplo, atualmente, o Ministério da Economia voltou a ser designado como Ministério da Fazenda, e o da Cidadania atende por Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome.

Entre todos os órgãos, quatro se recusaram a responder se usam ou se já usaram OSINT, sob o argumento de que essa informação é de acesso restrito porque poderia implicar riscos ou danos aos interesses da sociedade e do Estado. São eles:

[/] **Centro de Inteligência da Marinha (Ministério da Defesa)**

[/] **Gabinete de Segurança Institucional (GSI)**

[/] **Agência Brasileira de Inteligência (Gabinete de Segurança Institucional)**

[/] **Departamento de Polícia Federal**

Um órgão não respondeu ao questionário: **Receita Federal**. Quatro órgãos indicaram o uso de OSINT em atividades relacionadas à área criminal:

[/] **Ministério da Justiça e Segurança Pública (MJSP)**

[/] **Secretaria de Operações Integradas (Seopi), do MJSP**

[/] **Ministério Público Federal (MPF)**

[/] **Controladoria-Geral da União (CGU)**

O MJSP e a Seopi responderam que fazem "assessoramento estratégico" para subsidiar a ação de outros órgãos da área de segurança pública. As respostas não deixam de ser vagas, já que os órgãos também ressalvaram que não atuam em investigações criminais.

O MPF indicou que todos os setores da Secretaria de Perícia, Pesquisa e Análise (SPPEA) fazem coleta de dados pessoais de fontes abertas.

A CGU disse que a Diretoria de Pesquisas e Informações Estratégicas, ligada à Secretaria de Combate à Corrupção, usa dados obtidos de fontes abertas em "projetos específicos de ciência de dados".

Nove órgãos responderam que não usam ou usaram OSINT na prevenção ou na investigação de crimes:

[/] **Conselho Nacional de Justiça (CNJ)**

[/] **Ministério das Comunicações (MCom)**

[/] **Ministério da Ciência, Tecnologia e Inovação (MCTI)**

[/] **Ministério da Economia**

[/] **Procuradoria-Geral da Fazenda Nacional (PGFN)**

[/] **Ministério da Cidadania**

[/] **Secretaria Especial do Desenvolvimento Social (Ministério da Cidadania)**

[/] **Tribunal de Contas da União (TCU)**

[/] **Instituto do Patrimônio Histórico e Artístico Nacional (Iphan)**

A Secretaria Especial do Desenvolvimento Social, entretanto, informou que usa OSINT em atividades administrativas relacionadas à concessão de benefícios sociais.

Em um caso, as respostas foram contraditórias:

</> O Ministério da Defesa afirmou que não coleta dados pessoais em fontes abertas para fins de prevenção ou investigação de crimes. Mas, ao responder à questão sobre serviços prestados por terceiros, mencionou o uso de OSINT para a produção de informações que subsidiam o combate ao desmatamento e ao garimpo ilegal na Amazônia.

Nenhum órgão tem normas específicas para práticas de OSINT. No entanto, três deles indicaram a existência de diretrizes internas correlatas:

</> O MPF informou que observa sua Política de Privacidade e Proteção de Dados Pessoais[38] e um relatório com informações técnicas sobre os procedimentos adotados no recebimento e no tratamento de dados estruturados sob custódia da SPPEA;

</> A PGFN disse que o uso de dados é regido por sua Política de Governança e Gestão de Dados;

- O TCU indicou a existência do Programa de Dados Abertos do Tribunal de Contas da União, cujo objetivo é "promover a abertura de dados, em consonância com os princípios de dados abertos e com os princípios da publicidade, da transparência e da eficiência, visando ao aumento da disseminação de informações para a sociedade, ao incremento da participação social e à melhoria da qualidade dos dados disponibilizados".[39]

Dois órgãos responderam que contrataram serviços que usam dados abertos para outros fins:

- O Ministério da Defesa tinha um contrato para monitoramento de redes sociais e outro para prestação de serviços de apoio técnico à área de comunicação social, como clipping jornalístico (seleção de notícias publicadas por veículos de comunicação sobre um assunto de interesse específico, como o próprio ministério);

- O Ministério da Economia tinha dois contratos para coleta e/ou análise de dados de fontes abertas na área de comunicação social.

<cap 6>

O que dizem as empresas e outras pessoas jurídicas

</cap 6>

A pesquisa identificou empresas que potencialmente vendem serviços de OSINT, além de outras iniciativas que usam dados abertos em suas atividades, como organizações e projetos da sociedade civil. Ao todo, foram mapeadas 34 empresas ou iniciativas.

Em uma primeira etapa, para identificar as empresas que ofereceriam soluções OSINT, foram consideradas:

<1/> A participação em licitações cujo objeto se referia ao monitoramento de redes sociais;

<2/> O objeto social;

<3/> As informações fornecidas pelas próprias empresas em seus sites.

Após essa análise, chegou-se a 18 empresas que atuariam no setor, às quais foram enviados questionários. Duas delas retornaram o contato dos pesquisadores, informando que não lidam com dados de fontes abertas. As demais 16 simplesmente não responderam.

Entre essas 16, apenas 8 têm políticas de privacidade delineadas em seus sites e nenhuma fornece informações sobre quais dados são coletados e agregados em seus serviços.

Dentre as demais pessoas jurídicas e iniciativas consideradas, nenhuma apresenta suas políticas de privacidade em seus sites.

O Serviço Federal de Processamento de Dados (Serpro), maior empresa pública brasileira na área de tecnologia, responsável por administrar bancos de dados da União, também foi consultada. Em resposta, afirmou que existem evidências de uso de OSINT "em protótipos e experimentos, geração de conhecimento e aplicação em provas de conceito, mas por iniciativas isoladas em ações específicas". Acrescentou ainda que, "para construção de algumas aplicações, painéis de informação, BI [*business intelligence*], o Serpro utiliza de algumas informações abertas, como dados do IBGE, Ipea etc." e que também são usadas informações de proposições legislativas do Congresso Nacional em experimentos.

<?> *Business intelligence* ("inteligência de negócios") se refere ao processo de coleta, organização, análise, compartilhamento e monitoramento de informações que oferecem suporte à gestão de negócios.

<cap 7>

Respostas de profissionais que usam OSINT e de especialistas no tema

</cap 7>

No total, foram entrevistadas oito pessoas:

- </> Cinco profissionais que usam OSINT em suas atividades (dois jornalistas e três integrantes de organizações da sociedade civil);
- </> Três especialistas.

Principais achados das entrevistas:

- </> Entre as pessoas entrevistadas, não foi constatada uma definição uniforme sobre o que são “fontes abertas”;
- </> Cinco delas as consideram informações cujo acesso dispensa procedimentos prévios, como pedidos formais, pagamento ou registro do solicitante;
- </> Para uma pessoa, mesmo que seja preciso um pedido formal a instituições, os dados ainda podem ser considerados públicos;
- </> Duas das pessoas entrevistadas entendem que, ainda que o acesso às informações seja pago ou dependa de exigências formais, elas podem ser consideradas de “fontes abertas”;
- </> Apesar da falta de definição uniforme, há consenso de que o uso de meios ilícitos para obtenção dos dados não constitui o conceito de “fontes abertas”;
- </> Muitas das atividades realizadas pelas pessoas envolvidas profissionalmente não poderiam ser feitas sem o uso de informações de fontes abertas;
- </> No entanto, algumas dessas atividades poderiam ser empreendidas sem o uso de dados pessoais, ou com dados anonimizados, desde que recortes quanto a elementos vinculados a território, gênero e etnia ainda possam ser aplicados. Em apenas um caso, o uso de dados pessoais é indispensável (por exemplo, na investigação jornalística sobre pessoas públicas);
- </> Para todas as pessoas entrevistadas, não existem normas que regulamentem o uso de OSINT no Brasil;
- </> Exceto em dois casos, as pessoas entrevistadas não tinham formação obrigatória em proteção de dados (apenas voluntária). Somente uma delas também tem formação específica em OSINT;

- Todas as pessoas entrevistadas dizem que estão submetidas a limites pessoais e/ou elaborados pelas instituições às quais estão vinculadas. Algumas delas também apontam a observância de limites éticos jornalísticos, do interesse público ou impostos pelas próprias bases de dados usadas (como as que advertem que as informações não podem ser usadas para fins comerciais);

- Foi ponderado que a OSINT pode ser usada por corporações e governos com diferentes finalidades. Segundo as entrevistadas, em determinados casos, a prática tem o potencial de expor pessoas;

- As pessoas entrevistadas avaliam que, na hipótese de uso e processamento de seus próprios dados por ferramentas OSINT, elas sentiriam sua privacidade violada, salvo (i) se a finalidade fosse de interesse público ou (ii) se a base usada fosse composta apenas por informações disponibilizadas voluntária e conscientemente pelo ou pela titular do dado;

- Em algumas entrevistas, aponta-se a existência de agentes que usam OSINT para traçar estratégias de mercado e para direcionar conteúdos publicitários;

- **Há o entendimento de que as práticas de OSINT, por si só, não violam a privacidade. Entretanto, isso pode ocorrer, a depender de como elas são empregadas e o que se pretende com seu uso (isto é, sua finalidade);**

- Também se considerou que a ausência de regulamentação do assunto pode ser entendida como estratégia para minimizar a responsabilização de quem atua no Estado por uso abusivo de OSINT;

- Em geral, atividades de inteligência na América do Sul se beneficiam dessa ausência de regulamentação e acabam investigando os chamados "inimigos internos", incorrendo, assim, em práticas autoritárias, ainda que em contextos democráticos;

- Também há o entendimento de que ferramentas de OSINT podem ser importantes para atividades de ativismo, advocacy e reivindicação de políticas públicas.

Existe a percepção de que, caso as pessoas saibam que seus dados podem ser vasculhados por práticas de OSINT, pode haver autocensura ou algum tipo de efeito inibidor da liberdade de expressão.

– Conclusão

A coleta, a sistematização e a análise de dados publicamente disponíveis na internet, quando operados dentro dos marcos constitucionais e de acordo com princípios de direitos humanos e transparência, podem gerar informações valiosas para a formulação de políticas públicas. O emprego de práticas de OSINT em outras atividades, como investigações jornalísticas e atividades de pesquisa, também pode resultar em conteúdos de relevante interesse social, contribuindo para concretizar o direito de acesso à informação.

Por outro lado, práticas de OSINT realizadas por órgãos estatais que atuam nas áreas de segurança pública, inteligência e defesa podem ser empregadas abusivamente na perseguição a opositores políticos, na violação da privacidade de cidadãs e cidadãos e em investigações criminais clandestinas. Ou seja, em vez de contribuir com o exercício de direitos humanos, essas práticas podem implicar violações de garantias fundamentais.

Foi justamente para identificar se e como as práticas de OSINT podem impactar os direitos humanos no Brasil que a ARTIGO 19 realizou esta pesquisa. A investigação analisou as principais normas aplicáveis e como tribunais e instâncias administrativas têm decidido casos relacionados a OSINT; questionou também vários órgãos de Estado sobre o uso de inteligência de fontes abertas para fins de inteligência na área de segurança; identificou e contatou ainda empresas que oferecem serviços de OSINT; e entrevistou, por fim, profissionais que usam OSINT em suas atividades e especialistas no tema.

A partir dos resultados obtidos nessas frentes de investigação, é possível tecer as seguintes conclusões:

- </> Não existe uma padronização conceitual nos campos técnico, normativo e jurisprudencial de termos atrelados a OSINT, como “dados públicos”, “fontes abertas” e “dados de fontes públicas”;
- </> O uso de fontes abertas para fins de inteligência já é feito no Brasil, tanto pelo setor público quanto privado;
- </> Não existe uma regulamentação sobre esses usos, que defina seus termos e determine suas finalidades, seu setor de aplicação e seus limites;

</> Existe risco aos direitos humanos quando se considera que, além da ausência de regulamentação, há especial falta de transparência quanto ao tratamento de dados feito para fins de segurança pública;

</> Não foram feitos debates sobre a possibilidade do uso de OSINT para segurança pública e persecução penal antes da sua implementação nesses setores;

</> O desconhecimento sobre o modo de uso de OSINT por agentes estatais, bem como sobre os limites desse uso, favorece o hipervigilantismo estatal, tal qual o caso do "dossiê antifascista" (citado no capítulo 5);

</> Esse uso imprudente e irrestrito de OSINT permite que pessoas sejam monitoradas e perseguidas em razão de seus posicionamentos e compromete o exercício das liberdades de expressão e de associação, o que é incompatível com o Estado Democrático de Direito;

</> O uso de OSINT pelo Estado e por empresas pode gerar autocensura, pois as pessoas, temendo que suas informações sejam usadas indevidamente (por exemplo, de maneira discriminatória ou para aplicação de alguma sanção ilegítima), podem evitar expor publicamente suas opiniões;

</> Quando existe transparência sobre o tratamento de dados, é possível avaliar o uso de OSINT como uma ferramenta para a promoção e a proteção de direitos humanos. Isso porque tais mecanismos podem ajudar a controlar e monitorar abusos cometidos pelo Estado ou falhas na prestação de serviços públicos;

</> Princípios e regras previstos pela Lei Geral de Proteção de Dados (LGPD) devem ser aplicados às práticas de OSINT implementadas pelo Estado, visando a conferir mais transparência às ações de órgãos e de agentes públicos, a contribuir para que usos abusivos e ilegítimos sejam evitados e a proteger direitos e garantias fundamentais. Também é importante que alguns pontos da LGPD sejam regulamentados, especialmente para que suas determinações tenham *enforcement*, isto é, sejam de fato observadas. Além disso, princípios constitucionais e parâmetros internacionais de direitos humanos tampouco podem deixar de ser observados.

— Apêndice

Perguntas feitas aos órgãos de Estado

QUESTÃO 1.1 Caso existam, dentro dessa agência/órgão, setores que coletem dados pessoais de fontes abertas* para a prevenção e/ou investigação de crimes, por favor, indicar em quais setores/departamentos desse órgão essa coleta ocorre.

*"Fontes abertas" devem ser entendidas como aquelas com acesso aberto (entendido como acesso livre, que não exige registro prévio) ou acesso semiaberto (entendido como exigindo registro prévio, que pode ser pago ou não pago). Para fins do presente pedido de acesso à informação, pedimos que sejam consideradas no conceito de "fontes abertas" informações em redes sociais acessadas por meio da Internet.

QUESTÃO 1.2 Caso existam, dentro dessa agência/órgão, setores que coletem dados pessoais de fontes abertas para a prevenção e/ou a investigação de crimes, por favor, indicar as regras, os regulamentos e/ou as portarias ou os protocolos que guiam e/ou são aplicados em tais atividades.

QUESTÃO 2 Caso seja realizado, dentro desse órgão/agência, a coleta de informações pessoais de fontes abertas para a prevenção e/ou investigação de crimes: 1. Informar se estudos, portarias, regulamentos, propostas de regulamentos, propostas de portarias ou documentos foram ou planejam ser conduzidos com a coleta de dados pessoais de fontes abertas; 2. Indicar quais seriam esses estudos e fornecer link ou arquivo correspondente(s).

QUESTÃO 3.1 Caso tenham sido negociados e/ou assinados contratos com empresas privadas para coleta e análise de dados de fontes abertas, favor indicar: 1. Com quais empresas e para quais propósitos os contratos foram assinados?

QUESTÃO 3.2 Caso tenham sido negociados e/ou assinados contratos com empresas privadas para coleta e análise de dados de fontes abertas, por favor, fornecer a(s) cópia(s) do(s) contrato(s) correspondente(s).

— Notas

<1/> Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

<2/> As sanções previstas pela LGPD passaram a valer a partir de agosto de 2021.

<3/> Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

<4/> Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

<5/> Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.

<6/> Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

<7/> Ver nota 1.

<8/> Ver nota 1.

<9/> Trecho da ação de Descumprimento de Preceito Fundamental (ADPF) 722, julgada pelo Supremo Tribunal Federal em maio de 2022. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15351694176&ext=.pdf.

<10/> Disponível em: https://www.camara.leg.br/propostas-legislativas/2326300.

<11/> Disponível em: http://bibliotecadigital.mpf.mp.br/bdmpf/handle/11549/188193.

<12/> Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9883.htm.

<13/> Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d3695.htm.

<14/> Disponível em: https://www.normasbrasil.com.br/norma/resolucao-1-2009_111521.html.

<15/> Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm.

<16/> Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm.

<17/> A Seopi foi instalada por decreto em 1º de janeiro de 2019 pelo então presidente Jair Bolsonaro. O decreto foi revogado pelo presidente Luiz Inácio Lula da Silva em 1º de janeiro de 2023.

<18/> Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11103.htm.

<19/> Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm.

<20/> Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=487103&ori=1.

<21/> Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15351694176&ext=.pdf.

<22/> Ver nota 21.

<23/> Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/ac%25C3%25B3rd%25C3%25A3o%25202678%252F2021/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0.

<24/> Ver nota 23.

<25/> Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/KEY:ACORDAO-COMPLETO-2528759/NUMACORDAOINT%20asc/0.

<26/> Ver nota 25.

<27/> Melo, Henrique B. O Twitter como um recurso de segurança pública. *Jusbrasil*, 2019. Disponível em: https://www.jusbrasil.com.br/artigos/o-twitter-como-um-recurso-de-seguranca-publica/779019901.

<28/> Vieira, Danilo P. de C.; Rahman, Kássia S. B. A responsabilidade dos bancos em meio a fraudes em boletos bancários. *Migalhas*, 7 de abril de 2022. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/363347/a-responsabilidade-dos-bancos-em-meio-a-fraudes-em-boletos-bancarios.

<29/> Rosa, Alexandre M. da; Mendes, José. O poderio das armas matemáticas de investigação criminal em massa. *Conjur*, 5 de novembro de 2021. Disponível em: https://www.conjur.com.br/2021-nov-05/limite-penal-poderio-armas-matematicas-investigacao-criminal-massa.

<30/> Zanatta, Rafael A. F. Contraterrorismo e o legado do 11 de Setembro: um olhar crítico. *Jota*, 19 de setembro de 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/contraterrorismo-e-o-legado-do-11-de-setembro-um-olhar-critico-13092021.

<31/> Oliveira, Pedro C. Surgimento do OSINT: como a análise de notícias na Segunda Guerra influenciou a busca em fontes abertas. *Jusbrasil*, 2022. Disponível em: https://www.jusbrasil.com.br/artigos/surgimento-do-osint-como-a-analise-de-noticias-na-segunda-guerra-influenciou-a-busca-em-fontes-abertas/1626297241.

<32/> A produção de provas digitais e a tecnologia. *Jusbrasil*, 2021. Disponível em: https://www.jusbrasil.com.br/artigos/a-producao-de-provas-digitais-e-a-tecnologia/1385267128.

<33/> Clamer, Roberto. Informação: Riscos para a segurança corporativa. *Jusbrasil*, 2016. Disponível em: https://www.jusbrasil.com.br/artigos/informacao-riscos-para-a-seguranca-corporativa/413236321.

<34/> Oliveira, Pedro C. Da ideia até o IPO: 4 situações em que a Due Diligence pode ajudar sua startup. *Jusbrasil*, 2022. Disponível em: https://pedrocesaroliveira.jusbrasil.com.br/artigos/1620550689/da-ideia-ate-o-ipo-4-situacoes-em-que-a-due-diligence-pode-ajudar-sua-startup.

<35/> MPF/RS receberá curso "Cibersegurança: Ferramentas para Aplicação da Lei e Investigação". *Jusbrasil*, 2018. Disponível em: https://mpf.jusbrasil.com.br/noticias/680186794/mpf-rs-recebera-curso-ciberseguranca-ferramentas-para-aplicacao-da-lei-e-investigacao.

<36/> Disponível em: https://istoe.com.br/mg-jovem-e-preso-em-uberlandia-apos-publicacao-contra-bolsonaro-no-twitter.

<37/> A íntegra do questionário pode ser lida na seção de apêndices deste documento.

<38/> Disponível em: http://bibliotecadigital.mpf.mp.br/bdmpf/bitstream/handle/11549/243996/PT_PGR_MPF_2022_661.pdf?sequence=1&isAllowed=ycidade%20e%20Prote%C3%A7%C3%A3o%20de%20Dados%20Pessoaise%20Prote%C3%A7%C3%A3o%20de%20Dados%20Pessoais.

<39/> Disponível em: https://pesquisa.apps.tcu.gov.br/documento/ato-normativo/Portaria%2520139%252F2018/%2520/score%2520desc/0/%2520.


ARTIGO 19
DEFENDENDO A LIBERDADE DE EXPRESSÃO E INFORMAÇÃO