Contribuições da Data Privacy Brasil para Supremo Tribunal Federal na ADPF 1143

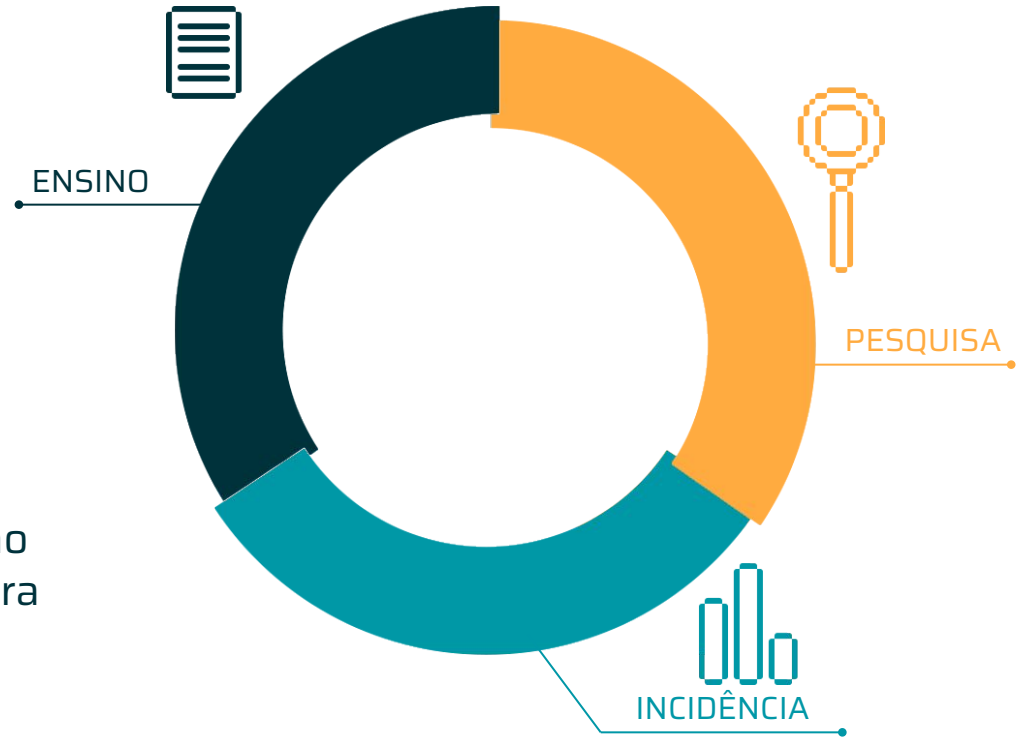
Pedro Saliba
Coordenador de Assimetrias e Poder

10/06/2024

DataPrivacyBR Research

Apresentação

A **Data Privacy Brasil** é uma organização que nasce da união entre uma escola e uma associação civil em prol da promoção da cultura de proteção de dados e direitos digitais no Brasil e no mundo.



Projeto sobre Tecnoautoritarismo (2020-2024)



O que é o tecnoautoritarismo? | What is techno-authoritarianism?

Data Privacy Brasil
5,73 mil inscritos

Inscrito 57 Compartilhar

Ilustração: Felipe Mayerle para o Intercept Brasil

INTERCEPT LANÇA BOLSAS PARA REPORTAGENS SOBRE TECNOAUTORITARISMO

Em parceria com a Associação Data Privacy Brasil de Pesquisa, queremos publicar histórias sobre como o uso de tecnologias por governos pode violar direitos

The Intercept Brasil
1 de fev de 2021, 13h35

Impacto constitucional

"O que significa o tecnoautoritarismo? Basicamente, é a utilização, cada vez mais massiva, em termos quantitativos e qualitativos, dos recursos das tecnologias de comunicação e tecnologias digitais para o controle, por parte do Estado, da sociedade. O tecnoautoritarismo não é um fenômeno típico somente de estados ditatoriais, mas é um fenômeno que está minando, de dentro para fora, as democracias"

(Ingo Wolfgang Sarlet, "Tecnoautoritarismo, democracia e direitos fundamentais", 2023)



O que aprendemos nos 4 anos de projeto?

- Caso **Pegasus/Harpia Tech**: há uma grande **confusão conceitual** entre *spywares* e *OSINTS* (“*Open Source Intelligence Softwares*”)
    - **Harpia**: software que permite cruzamento de mais de 5.000 pontos de dados que são extraídos da web (Telegram, IRC, blogs, conteúdos indexados) para identificação de um alvo e monitoramento persistente
    - Riscos à autodeterminação informativa e proteção de dados pessoais, tal com reconhecidos na **ADI 6387/2020**
- Caso **Abin/Denatran:** ilicitude na utilização secundária de dados que possuem contexto específico e que não podem ser utilizados para inteligência sem parâmetros constitucionais

O que aprendemos nos 4 anos de projeto?

- Caso **Excel/SEOPI/MJ**: criação de "zonas cinzentas" em devido processo, permitindo que autoridade administrativa (dedicada à segurança pública e inteligência) possa decidir casos de extração de dados sem decisão judicial

  - Atuação conjunta entre **Data Privacy Brasil, Conectas, Transparência Internacional, Artigo 19** e **Fórum Brasileiro de Segurança Pública**
  - Inquérito Civil nº 1.16.000.002757/2022-36
  - Tese da Data Privacy Brasil: uso de software de extração de dados de aparelhos celulares de suspeitos exige um **conjunto de freios e contrapesos** e arranjos institucionais de garantia de **necessidade, legalidade e proporcionalidade**

O que aprendemos nos 4 anos de projeto?

- Caso **FirstMile**: investigação científica em 2023 sobre técnica utilizada (exploração de vulnerabilidade em protocolo SS7 de telecomunicações)
    - Evidências de usos de soluções da Cognite em Myanmar e Sudão: acoplamento entre capacidades do software, monitoramento e prisões
    - Múltiplas violações de direitos fundamentais em razão do ***tipo de spyware*** utilizado
        - Violação às normas de privacidade do setor de telecomunicações (lei federal e Regulamento Geral dos Consumidores da Anatel)
        - Violação às normas constitucionais de privacidade, autodeterminação informativa e proteção de dados pessoais
        - Violação às normas constitucionais de livre associação e liberdades civis e políticas

tele.síntese
PORTAL DE TELECOM, INTERNET E TIC

PRIVACIDADE

Software invasor: 'Caso First Mile não deve ser visto como algo isolado', alerta Data Privacy

DA REDAÇÃO 20 DE OUTUBRO DE 2023 | 15:57

Para entidade, ferramentas de geolocalização como a que motivou investigação da PF é 'sintoma de um problema muito maior que precisa ser endereçado: a contenção do usos de softwares tecnoautoritários'

Iniciativa de

DEFESA DIGITAL

DataPrivacyBR Research

INTERNETLAB
pesquisa em direito e tecnologia

INTERMEDIÁRIO: apura

FABRICANTE: exterro

1 TECNOLOGIA

DERRUBADA DE CHAVES CRIPTOGRÁFICAS

- Busca de histórico de navegação de todos os navegadores e segmentação de por metadados categoria (conteúdo adulto, conversas, dark web, notícias, etc)
- Decriptação de arquivos, quebra de senhas; recuperação de senhas de **mais de 100 aplicações**
- Decriptação de discos de computador encriptados com a última versão do *McAfee Drive Encryption*

EXTRAÇÃO DE INFORMAÇÕES DE SEGUNDA ORDEM

- Unificação de banco de dados para armazenamento de provas
- Indexação, filtragem e ferramentas de pesquisa de resultados de dados armazenados
- Reconhecimento e detecção de imagens, incluindo faces e objetos
- Localização, manuseio e filtragem de dados, móveis, de rede, com segmentação entre dados e comunicações

OUTROS

- Coleta, processamento e análise de conjuntos de dados contendo arquivos do sistema Apple que estejam encriptados, comprimidos ou deletados
- Faz a decriptação de *FileVault* 2 do sistema de arquivos APFS (*Apple File System*)

INTERMEDIÁRIO: Cognyte

FABRICANTE: Cognyte

3 TECNOLOGIAS DIFERENTES

DERRUBADA DE CHAVES CRIPTOGRÁFICAS

- Interceptação de ligações e mensagens de texto
- Quebra de criptografia A5/1 e A5/2, com decodificador embutido

EXTRAÇÃO EM INFRAESTRUTURA

- Localização do dispositivo alvo com precisão, usando um dispositivo homing dedicado, sem desabilitar o alvo de se comunicar
- Extração de coordenadas GPS do celular do alvo em redes GSM e UMTS (3G)
- Coleta de tráfego GSM em "área ampla
- Identificação de "padrões suspeitos de comunicação" com base em localização, reconhecimento de fala, análise de relações ("links") e correlações entre textos
- Permite o monitoramento de até **10 mil donos de celulares** a cada 12 meses

OUTROS

- Ouvir, ler, editar, e redirecionar chamadas recebidas e realizadas, bem como mensagens de textos (criptografia A5/1 e A5/3)
- Ativar remotamente o microfone de um aparelho celular
- Identificar a presença do aparelho telefone do alvo
- Bloquear comunicações celular para neutralizar IEDs e mais
- Interceptação de SMS recebidos e enviados
- Permite múltiplos usuários analisarem chamadas ao mesmo tempo
- A tecnologia localizava aparelhos que utilizam as redes 2G, 3G e 4G. Através de falhas no protocolo Sistema de Sinalização Nº 7 (SS7), que deveriam ser compartilhados apenas entre as prestadoras de telecom para *rooming*
- Identificar a localização aproximada dos dispositivos, gerando alertas sobre a rotina de movimentação dos alvos de interesse

INTERMEDIÁRIO: Grupo TechBiz

FABRICANTE: exterro

1 TECNOLOGIA



DERRUBADA DE CHAVES CRIPTOGRÁFICAS

- Busca de histórico de navegação de todos os navegadores e segmentação de por metadados categoria (conteúdo adulto, conversas, dark web, notícias, etc)
- Decriptação de arquivos, quebra de senhas; recuperação de senhas de **mais de 100 aplicações**
- Decriptação de discos de computador encriptados com a última versão do *McAfee Drive Encryption*



EXTRAÇÃO DE INFORMAÇÕES DELETADAS

- Coleta, processamento e análise de conjuntos de dados contendo arquivos do sistema Apple que estejam encriptados, comprimidos ou deletados
- Faz a decriptação de *FileVault 2* do sistema de arquivos APFS (*Apple File System*)



EXTRAÇÃO DE SISTEMAS DE COMUNICAÇÃO EM NUVEM

- Recuperação de dados e comunicações de aplicativos com armazenamento em nuvem, como Whatsapp, Facebook, Instagram, Google, Twitter e outros
- Filtragem, marcação e visualização de conversas para mensagens individuais e chats completos



EXTRAÇÃO DE INFORMAÇÕES DE SEGUNDA ORDEM

- Unificação de banco de dados para armazenamento de provas; Indexação, filtragem e ferramentas de pesquisa de resultados de dados armazenados
- Reconhecimento e detecção de imagens, incluindo faces e objetos
- Localização, manuseio e filtragem de dados, móveis, de rede, com segmentação entre dados e comunicações

INTERMEDIÁRIO: apura

FABRICANTE: MSAB

7 TECNOLOGIAS DIFERENTES



DERRUBADA DE CHAVES CRIPTOGRÁFICAS

- Acesso e análise de dados em aplicações com criptografia forte, como Whatsapp, Whatsapp Business e Telegram e Signal. Compatível com dispositivos Android
- Possibilidade de acessar dados de celulares bloqueados
- Reconstrução de arquivos deletados



EXTRAÇÃO DE INFORMAÇÕES DELETADAS

- Clonagem de cartões SIM
- Leitura e clonagem de cartão SIM



EXTRAÇÃO EM DISPOSITIVOS

- Extração e cópia de dados de dispositivos digitais, incluindo cartões de memória SIM e SD
- Extração física de dados de dispositivos móveis
- Bypass e/ou recuperação de senhas
- Extração de dados de dispositivos digitais
- Extração lógica e física de dados de dispositivos móveis, incluindo dados deletados



EXTRAÇÃO DE SISTEMAS DE COMUNICAÇÃO EM NUVEM

- Extração de dados de aplicações com armazenamento em nuvem, como Facebook, Google, iCloud, Twitter e Snapchat. Inclui modalidade de extração automática, a partir de tokens de acesso a aplicações previamente extraídos com aparelho em mãos, e de extração manual, sem necessidade do aparelho estar presente, a partir de login e senha previamente acessados por outros meios

EXTRAÇÃO DE INFORMAÇÕES DE SEGUNDA ORDEM

- Adiciona recursos de visualização ao *XAMN Spotlight*, como análise a partir de geolocalização, de conversas em aplicações de mensageria e conexões entre diferentes usuários e dispositivos distintos
- Análise, filtragem, visualização e sistematicação de dados extraídos de dispositivos móveis, drones, tenologias vestíveis, de GPS, veículos, cartões SIM, cartões de memória e outras fontes

OUTROS

- Reconhecimento de conteúdos em imagens
- Suporte para extração e decodificação de dados de dispositivos "*non-standard*" ("*typically manufactured in Eastern Asia*")
- Identificação automática de "*pin-outs*"; Suporte para chpsets MediaTek, SpreadTrum, Coolsand e Infineon
- Extração de dados de dispositivos GPS

Spywares pela ótica jurídica

Spywares são programas de computador com capacidades intrusivas de extração de informações e invasão em dispositivos ou sistemas eletrônicos. Seu objetivo é explorar de falhas de segurança existentes para coleta de informações sobre seus alvos, que dificilmente conseguem identificar a invasão.

> "Pegasus e spywares semelhantes (por exemplo, Candiru, Predator) têm sido utilizados como ferramenta de *hacking* e de vigilância contra jornalistas, advogados, políticos e ativistas dos direitos humanos em vários Estados-membros do Conselho da Europa e noutros países. Dado o **nível de intrusão sem precedentes deste software**, que concede acesso remoto não autorizado ("*zero-click*") e irrestrito ao telemóvel e a todos os seus dados pessoais e privados, a sua utilização tem sérias implicações para os **direitos humanos fundamentais** das pessoas visadas e todos os seus contatos, incluindo o seu direito à privacidade e o seu direito à liberdade de expressão, bem como, de um modo mais geral, à liberdade dos meios de comunicação social e às instituições democráticas"
>
> (Conselho da Europa, *Relatório do Comitê de Assuntos Jurídicos e Direitos Humanos*, relator: Pieter Omtzigt, 2023, p. 26).

Como tipologias podem ajudar na construção jurídica



Spywares de exploração de infraestrutura apresentam múltiplas violações ao direito, incluindo as regras dos setores regulados, gerando violações não somente aos cidadãos mas também às empresas responsáveis pela preservação da integridade contextual dos dados (exemplo: telecomunicações)



Spywares de extração de sistemas de comunicação em nuvem apresentam múltiplas violações a direitos fundamentais do ponto de vista relacional. Os riscos são gerados não somente aos “alvos” mas toda a rede de relações sociais constituídas e mediadas pelas comunicações (exemplo: metadados de Telegram)

Como tipologias podem ajudar na construção jurídica



Spywares de extração de dispositivos apresentam riscos menores, pois é possível diminuir riscos a direitos fundamentais a partir de protocolos e procedimentos para uso correto por autoridades de investigação e respeito aos preceitos constitucionais de produção de provas digitais



Spywares de inferências e informações de segunda ordem apresentam riscos gravíssimos, pois produzem conhecimento capaz de revelar orientações políticas, associativas e relacionais, que são cruciais em uma democracia. É um abuso informática que atenta contra os valores constitucionais do *habeas data* e vai além do direito de proteção de dados pessoais.

Como tipologias podem ajudar na construção jurídica



Nas análises físicas as pessoas investigadas muitas vezes têm conhecimento da apreensão, cabendo maior controle da atividade estatal. Isso **não acontece nas invasões remotas**, quase indetectáveis. Por fim, as inferências produzidas adicionam uma camada adicional de inteligência, mas sua **falta de transparência pode levar a interpretações equivocadas**.

Contato



Pedro Saliba

Coordenador de Assimetrias e Poder

pedro.saliba@dataprivacybr.org

DataPrivacyBR Research



INTELIS

União dos Profissionais de Inteligência de Estado da ABIN

ADPF 1143 – AUDIÊNCIA PÚBLICA

HUGO ALBERTO LAZAR – Presidente da Intelis

10 de junho de 2024

INTELIS
União dos Profissionais de Inteligência de Estado da ABIN

Objetivos

- Esclarecer a atividade de Inteligência no Brasil
- Expressar perspectiva sobre as ferramentas da ADPF
- Apontar mecanismos de regulação da Atividade no mundo
- Apresentar proposta de mecanismo de controle judicial prévio

INTELIS
União dos Profissionais de Inteligência de Estado da ABIN

Atividade de Inteligência no século XXI





INTELIS
União dos Profissionais de Inteligência de Estado da ABIN





INTELIS
União dos Profissionais de Inteligência de Estado da ABIN







INTELIS
União dos Profissionais de Inteligência de Estado da ABIN









E a Agência Brasileira de Inteligência?



E a Agência Brasileira de Inteligência?



CartaCapital EDIÇÃO D

POLÍTICA

Abin alertou Segurança do DF sobre risco de invasão a prédios horas antes de atos terroristas

O aviso se dirigiu ao então secretário Anderson Torres, exonerado horas depois por Ibaneis Rocha

POR CARTACAPITAL

09.01.2023 18H06

E a Agência Brasileira de Inteligência?



CartaCapital

EDIÇÃO D

POLÍTICA

Abin alertou Segurança do DF sobre risco de invasão a p
de atos terroristas

O aviso se dirigiu ao então secretário A
por Ibaneis Rocha

POR CARTACAPITAL

09.01.2023 18H06

Geral

Servidores da Abin identificam ameaças aos atos democráticos de hoje

Informação é da Intelis, associação dos servidores da agência

Publicado em 08/01/2024 - 12:27 Por Alex Rodrigues - Repórter da Agência Brasil - Brasília

E a Agência Brasileira de Inteligência?

Giro

Informes da Abin destacam benefício da quarentena e citam subnotificação

de atos terroristas

O aviso se dirigiu ao então secretário A
por Ibaneis Rocha

POR CARTACAPITAL

09.01.2023 18H06

Servidores da Abin identificam ameaças aos atos democráticos de hoje

Informação é da Intelis, associação dos servidores da agência

Publicado em 08/01/2024 - 12:27 Por Alex Rodrigues – Repórter da Agência Brasil - Brasília

E a Agência Brasileira de Inteligência?

Giro

Informes da Abin destacam benefício da

Abin identifica financiadores de 103 ônibus para atos golpistas em relatório enviado à CPMI

PRF também informou que no dia 7 de janeiro 105 ônibus fretados chegaram em Brasília

Redação
Brasil de Fato | São Paulo (SP) | 21 de julho de 2023 às 10:19

E a Agência Brasileira de Inteligência?

Giro

Informes

Abin apontou participação de grupos neonazistas e de supremacistas brancos em movimentos golpistas durante eleições

Órgão de inteligência afirmou que as comunidades usavam 'narrativas de deslegitimação' das instituições para 'avançar teses extremistas violentas' e 'fomentar movimentos de insurreição armada'

Abin identi stas em relatório enviado à CPMI

PRF também informou que no dia 7 de janeiro 105 ônibus fretados chegaram em Brasília

Redação
Brasil de Fato | São Paulo (SP) | 21 de julho de 2023 às 10:19

E a Agência Brasileira de Inteligência?

Giro

Informes

Abin apontou participação de grupos neonazistas e de supremacistas brancos em movimentos golpistas durante eleições

Órgão de inteligência afirmou que as comunidades usavam 'narrativas de deslegitimação' das instituições para 'avançar teses extremistas violentas' e 'fomentar movimentos de insurreição armada'

Abin identi … stas em relatório enviado à CPMI

PRF também informou que no dia 7 de janeiro 105 ônibus fretados chegaram em Brasília

COOPERAÇÃO

ABIN participa de operação internacional de combate ao crime organizado na aviação

Em 7 de março, a ABIN participou de reunião para discutir os resultados da Operação Colibri, ação interagências realizada em janeiro

E a Agência Brasileira de Inteligência?

Giro

Abin apontou participação de grupos neonazistas e de supremacistas brancos em

Criptografia da urna eletrônica será feita pela Abin

Há 23 anos a agência atua no apoio à realização de eleições

POR ESTADÃO CONTEÚDO

23.08.2021 17H24

ção'

stas

Bra

ABIN participa de operação internacional de combate ao crime organizado na aviação

Em 7 de março, a ABIN participou de reunião para discutir os resultados da Operação Colibri, ação interagências realizada em janeiro

E a Agência Brasileira de Inteligência?

Giro

Abin apontou participação de grupos neonazistas e de supremacistas brancos em

ABIN apoia recuperação do acervo da Biblioteca Nacional após ataque hacker

Invasão deixou a instituição fora do ar e ameaçou destruir a totalidade do seu acervo virtual

feita pela Abin

stas

Há 23 anos a agência atua no apoio à realização de eleições

POR **ESTADÃO CONTEÚDO**

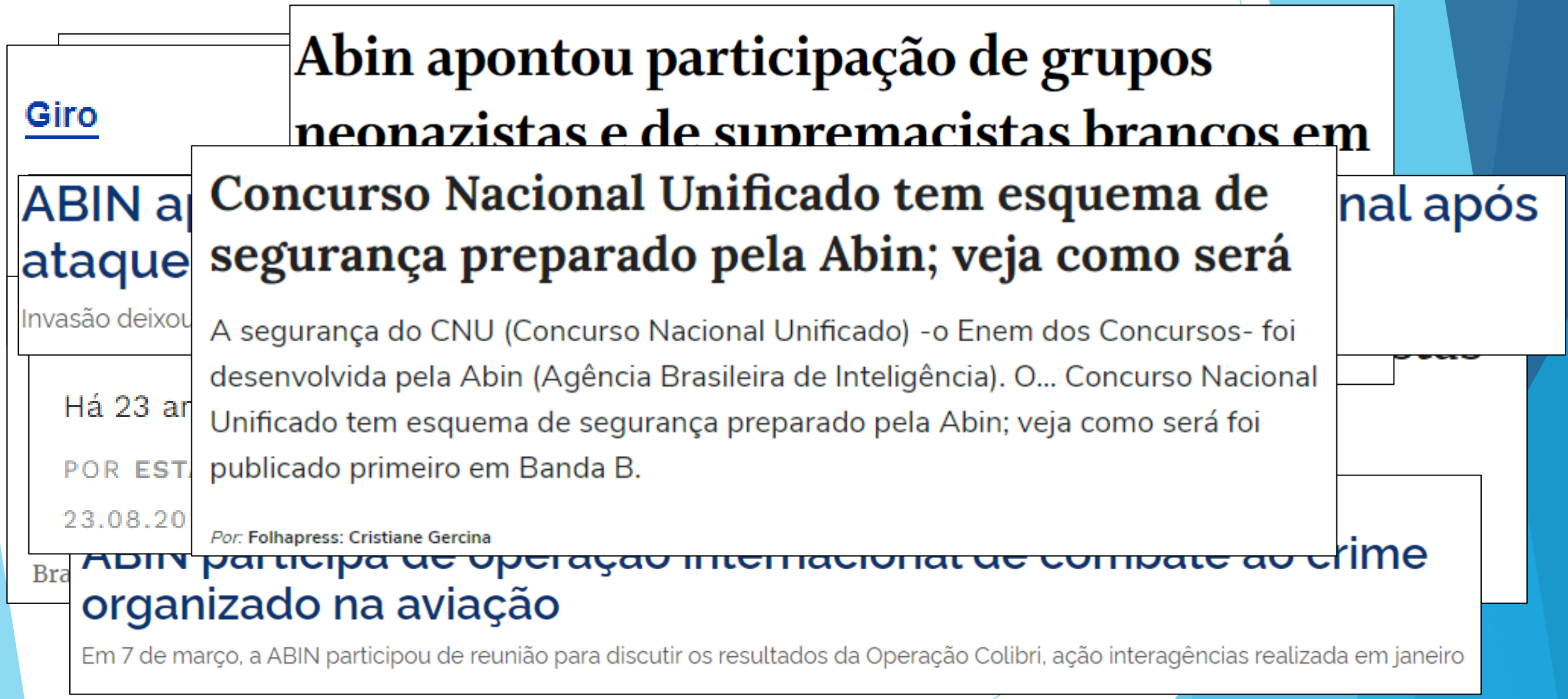
23.08.2021 17H24

Bra

ABIN participa de operação internacional de combate ao crime organizado na aviação

Em 7 de março, a ABIN participou de reunião para discutir os resultados da Operação Colibri, ação interagências realizada em janeiro

E a Agência Brasileira de Inteligência?



E a Agência Brasileira de Inteligência?



Abin identifica professor do Paraná suspeito de fazer apologia ao nazismo

Peterson Machado, investigado pro racismo e xenofobia, participava de grupos extremistas nas redes sociais e foi preso pela Polícia Civil nesta quinta-feira

POR CARTACAPITAL

19.04.2024 08H09

desenvolvida pela Abin (Agência Brasileira de Inteligência). O... Concurso Nacional Unificado tem esquema de segurança preparado pela Abin; veja como será foi publicado primeiro em Banda B.

Por: **Folhapress: Cristiane Gercina**

organizado na aviação

Em 7 de março, a ABIN participou de reunião para discutir os resultados da Operação Colibri, ação interagências realizada em janeiro

E a Agência Brasileira de Inteligência?



E a Agência Brasileira de Inteligência?

- LEI DE CRIAÇÃO DESATUALIZADA
- POLÍTICA NACIONAL DE INTELIGÊNCIA – AVANÇO TARDIO
- CONTROLE PARLAMENTAR INEFICIENTE
  - Comissão de Controle das Atividades de Inteligência
  - De 2019 a 2023 – apenas 15 reuniões
- INEXISTÊNCIA DE MECANISMO DE AUTORIZAÇÃO JUDICIAL PRÉVIA

INTELIS
União dos Profissionais de Inteligência de Estado da ABIN

Ferramentas intrusivas: *spywares*, *IMSI catchers* e geolocalizãção



Spywares

- PROGRAMA MALICIOSO PARA COLETAR INFORMAÇÕES E COMUNICAÇÕES PRIVADAS
- ATIVIDADE ESTATAL SEM REGULAÇÃO
- EXEMPLOS DE USO NA INTELIGÊNCIA DE ESTADO:
  - identificar rede de relacionamento de suspeitos de atentados contra instituições democráticas;
  - rastrear a infraestrutura empregada por grupos criminosos cibernéticos, com o fim de monitorar seus operadores e prevenir ataques; e
  - determinar se um agente responsável por operações sofisticadas de desinformação opera a mando de um ator estatal ou não-estatal adverso.

INTELIS
União dos Profissionais de Inteligência de Estado da ABIN

IMSI Catchers / cell-site simulator ("CSS")

- EQUIPAMENTOS QUE SIMULAM O COMPORTAMENTO DE UMA TORRE DE CELULAR PARA ATRAIR OS APARELHOS DE UMA DETERMINADA ÁREA
- TIPO ATIVO: VIOLA COMUNICAÇÕES E DADOS
- TIPO PASSIVO: APENAS CAPTURA IDENTIFICADOR DO CELULAR
- EXEMPLOS DE USO DO TIPO PASSIVO NA INTELIGÊNCIA DE ESTADO
  - determinar se um alvo, a exemplo de um suspeito de integrar organização terrorista ou extremista, encontra-se num certo local;
  - determinar se existem aparelhos de celular não permitidos numa área de segurança, como numa reunião de chefes de Estado; ou
  - determinar se existem pessoas suspeitas seguindo uma autoridade, por meio da captura dos identificadores de celulares que estão em volta da autoridade em questão em diferentes locais.

INTELIS
União dos Profissionais de Inteligência de Estado da ABIN

Ferramentas de geolocalização

- VIGILÂNCIA ELETRÔNICA ATRAVÉS DO RASTREAMENTO DE UM APARELHO CELULAR
- NÃO VIOLA INFORMAÇÕES OU COMUNICAÇÕES PRIVADAS
- EXEMPLOS DE USO NA INTELIGÊNCIA DE ESTADO
  - determinar os trajetos de um alvo, a exemplo de um suspeito de integrar organização terrorista ou extremista;
  - determinar se existem pessoas suspeitas seguindo uma autoridade, por meio dos locais por que esta circulou; e
  - monitorar locais de interesse de agentes de Inteligência clandestinos operando em solo brasileiro.

INTELIS
União dos Profissionais de Inteligência de Estado da ABIN

Serviços de Inteligência no mundo democrático



País	Interceptação de comunicações	Técnicas operacionais (previsão legal expressa)	Proteção ao profissional de Inteligência
México	Sim	Sim	Não indicado
Argentina	Sim	Não	Sim
Espanha	Sim	Sim	Sim
França	Sim	Sim	Sim
Noruega	Sim	Sim	Sim
Índia	Sim	Não indicado	Sim
África do Sul	Sim	Sim	Sim
Canadá	Sim	Sim	Sim
Alemanha	Sim	Sim	Sim
Itália	Sim	Sim	Sim

*Obs: nos casos "Não indicado", não foram encontradas referências aos tópicos propostos nas legislações ostensivas dos Serviços de Inteligência estrangeiros.

INTELIS
União dos Profissionais de Inteligência de Estado da ABIN

Necessário controle judicial prévio para a Inteligência



Mecanismo de autorização judicial prévia para a Inteligência de Estado

- EQUILÍBRIO ENTRE PRIVACIDADE E SEGURANÇA DO ESTADO E SOCIEDADE
- MECANISMOS DE CONTROLE DA ATIVIDADE SÃO AMBÍGUOS E INSUFICIENTES
- ESTADO ATUAL IMPLICA EM INSEGURANÇA PARA SOCIEDADE E PARA OS PROFISSIONAIS DE INTELIGÊNCIA
- PLEITO HISTÓRICO DOS SERVIDORES DA ABIN:
  - Juízo específico e especializado no brasil
  - Mecanismo legal para solicitação de autorização judicial
  - Capacidade postulatória da ABIN

INTELIS

União dos Profissionais de Inteligência de Estado da ABIN

https://intelis.org.br/

@intelis_abin

@Intelis_ABIN

A necessidade de regular o uso de programas de intrusão virtual e ferramentas de monitoramento secreto

A evolução tecnológica tem permitido o desenvolvimento de ferramentas cada vez mais sofisticadas para a vigilância e monitoramento remoto de dispositivos digitais. No entanto, o uso dessas tecnologias pelos órgãos públicos requer uma regulamentação cuidadosa para garantir os direitos fundamentais dos cidadãos.



Definição de programas de intrusão virtual remota e ferramentas de monitoramento secreto



Programas de Intrusão Virtual Remota

Esses programas permitem o acesso remoto e secreto a dispositivos digitais, possibilitando a coleta de informações e o controle de funcionalidades sem o conhecimento ou consentimento do usuário.



Ferramentas de Monitoramento Secreto

Trata-se de dispositivos e aplicativos invisíveis que capturam dados de comunicação, localização e atividades dos usuários sem sua ciência, invadindo sua privacidade.



Uso por Órgãos Públicos

Esses recursos são empregados por agências governamentais e forças de segurança para investigações e operações, mas seu uso inadequado pode violar direitos e liberdades individuais.

Aplicabilidade e finalidade do uso desses recursos pelos órgãos e agentes públicos

Combate ao crime

Os órgãos públicos poderão utilizar programas de intrusão virtual e ferramentas de monitoramento secreto para investigar e prevenir atividades criminosas, como crimes cibernéticos, terrorismo e corrupção.

Segurança nacional

Esses recursos também poderão ser empregados para proteger a integridade e a soberania do Estado, monitorando ameaças à segurança nacional, como espionagem e atos de sabotagem.

Inteligência estratégica

Os agentes públicos poderão utilizar essas ferramentas para coletar informações relevantes e subsidiar a tomada de decisões estratégicas pelos órgãos governamentais.

Princípios e diretrizes para o uso desses recursos

Legalidade e Proporcionalidade

O uso de programas de intrusão virtual remota e ferramentas de monitoramento secreto pelos órgãos e agentes públicos deve estar estritamente embasado em lei e seguir o princípio da proporcionalidade, com limites claros e justificáveis.

Transparência e Accountability

As ações de intrusão e monitoramento devem ser transparentes, com registro e prestação de contas detalhados sobre o uso desses recursos, submetidos a controle e fiscalização.

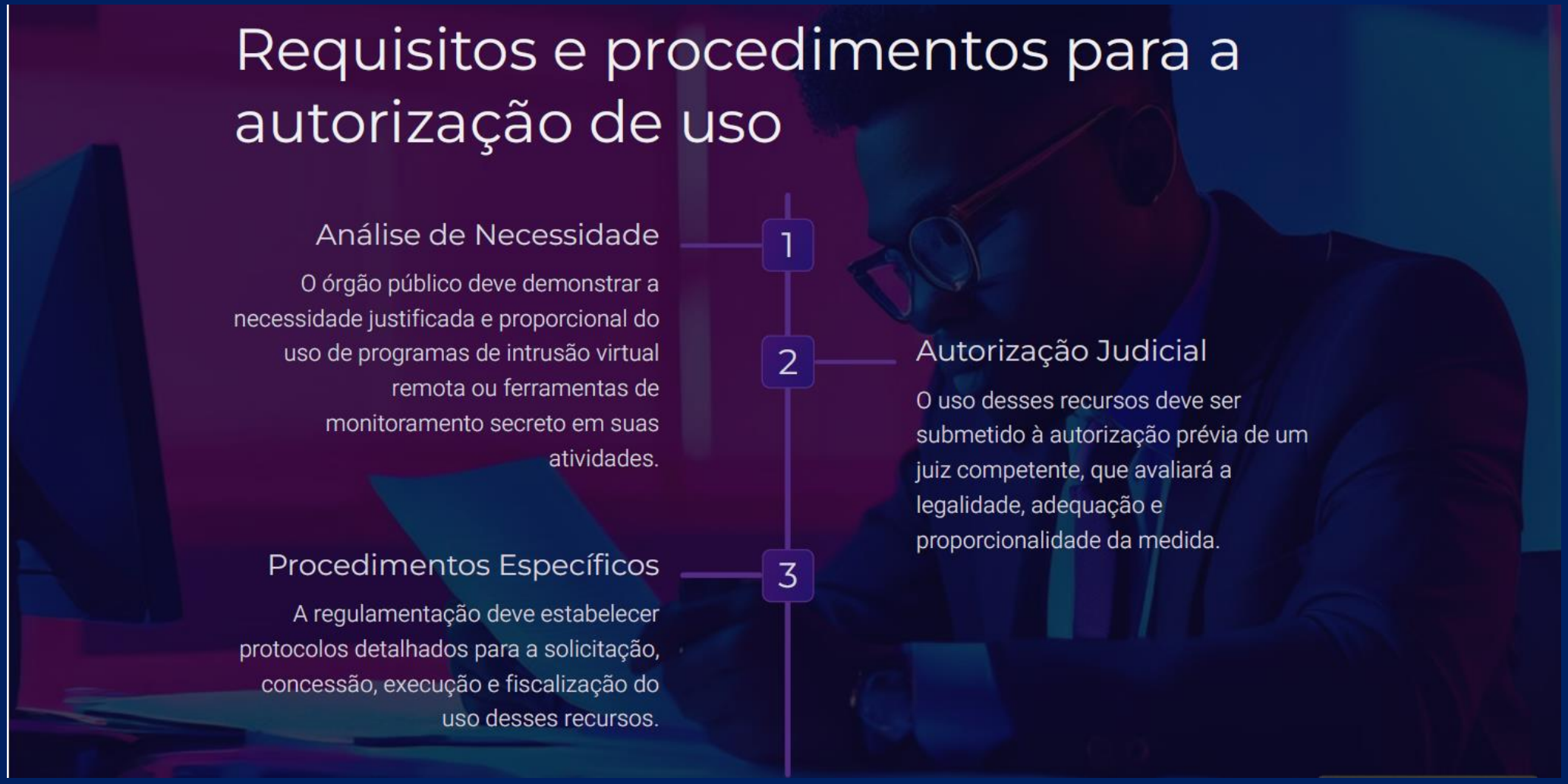
Respeito aos Direitos Individuais

O uso desses recursos deve assegurar a preservação dos direitos e garantias fundamentais, como privacidade, intimidade e livre exercício da comunicação.

Necessidade e Adequação

A utilização desses instrumentos deve estar limitada a situações excepcionais e demonstrada sua necessidade e adequação para o alcance de finalidades públicas legítimas.

Requisitos e procedimentos para a autorização de uso



1 Análise de Necessidade

O órgão público deve demonstrar a necessidade justificada e proporcional do uso de programas de intrusão virtual remota ou ferramentas de monitoramento secreto em suas atividades.

2 Autorização Judicial

O uso desses recursos deve ser submetido à autorização prévia de um juiz competente, que avaliará a legalidade, adequação e proporcionalidade da medida.

3 Procedimentos Específicos

A regulamentação deve estabelecer protocolos detalhados para a solicitação, concessão, execução e fiscalização do uso desses recursos.

Limites e salvaguardas para preservação de direitos e garantias individuais



Equilíbrio de Interesses

Deve-se estabelecer um equilíbrio entre os interesses de segurança pública e a proteção dos direitos e garantias individuais, como privacidade e liberdade de comunicação.



Requisitos Estritos

O uso desses recursos deve ser sujeito a requisitos estritos, como autorizações judiciais, supervisão de órgãos de controle e registro detalhado de cada ação.



Proteção de Dados

Deve-se garantir a proteção de dados pessoais e a preservação do sigilo das comunicações, com regras claras sobre acesso, armazenamento e descarte das informações coletadas.

Responsabilização e prestação de contas pelo uso indevido

1 **Responsabilização**

Os agentes públicos que utilizarem indevidamente os recursos de intrusão virtual e monitoramento secreto serão responsabilizados civil, penal e administrativamente pelos seus atos.

2 **Prestação de Contas**

Deverá haver mecanismos de prestação de contas periódica sobre o uso destes recursos, com relatórios detalhados e auditoria independente.

3 **Transparência**

As informações sobre o uso desses recursos, desde a autorização até os resultados obtidos, deverão ser publicadas de forma transparente, observando as devidas restrições de sigilo.

4 **Sansões**

Usos abusivos ou ilegais deverão resultar em sanções proporcionais, como advertências, suspensões, destituições de cargo e, em casos graves, responsabilização criminal.

Mecanismos de Controle e Fiscalização do Uso de Recursos

Supervisão Independente

Será estabelecido um órgão independente de fiscalização, composto por especialistas em privacidade e direitos digitais, para monitorar o uso desses recursos pelos órgãos públicos.

Relatórios Periódicos

Os órgãos públicos deverão apresentar relatórios detalhados e periódicos sobre o uso desses recursos, incluindo informações sobre o número de autorizações, finalidades e resultados obtidos.

Auditorias Obrigatórias

Auditorias regulares e surpresa serão realizadas para verificar o cumprimento dos procedimentos e requisitos estabelecidos na regulamentação.

Transparência Pública

Os cidadãos terão acesso a informações sobre o uso desses recursos pelos órgãos públicos, respeitando as restrições necessárias para a preservação de investigações em andamento.

Penalidades e sanções para o uso abusivo ou ilegal



Sanções Administrativas

Os órgãos responsáveis poderão aplicar sanções administrativas como multas, suspensão de atividades e até mesmo o afastamento do servidor público envolvido no uso abusivo ou ilegal destes recursos.



Responsabilização Judicial

Em casos mais graves, o uso abusivo ou ilegal destes programas e ferramentas poderá ensejar responsabilização judicial, com a possibilidade de aplicação de penas de detenção e reparação de danos.



Proteção de Dados

Qualquer violação dos direitos e garantias individuais, como o vazamento ou uso indevido de dados pessoais, será severamente punida de acordo com a legislação de proteção de dados vigente.

Considerações finais e recomendações

Concluímos com uma visão geral das principais recomendações para a regulamentação do uso de programas de intrusão virtual remota e ferramentas de monitoramento secreto por órgãos e agentes públicos.

ABRAJI | MEDIA DEFENCE | tornavoz

CHARLENE NAGAE
Fundadora e Diretora-Executiva do Instituto Tornavoz

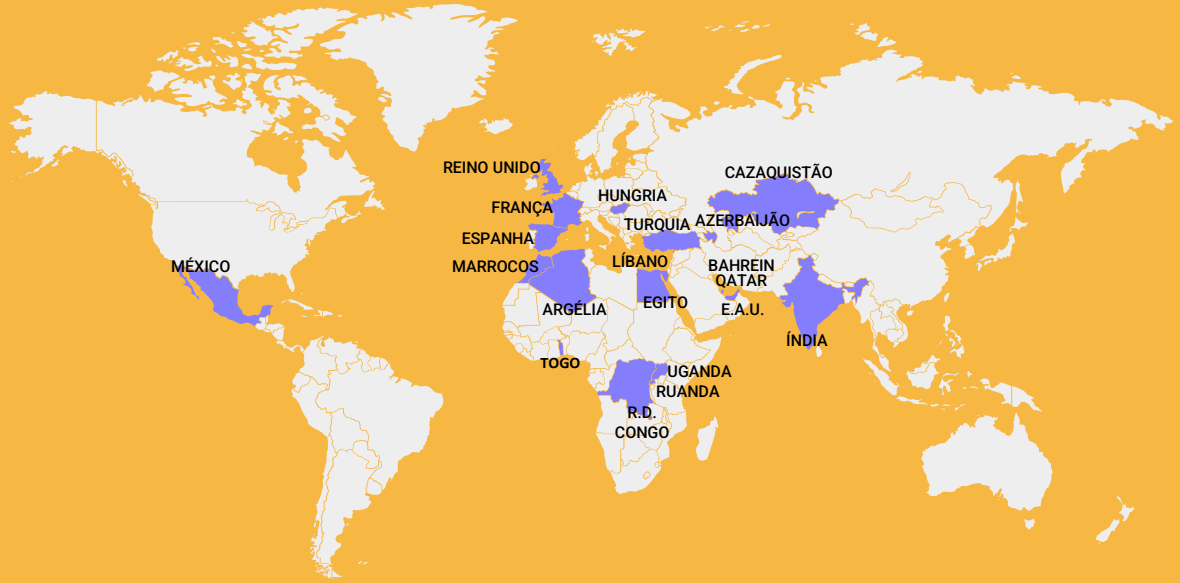
ADPF 1143

Audiência Pública

Junho de 2024

ABRAJI | MEDIA DEFENCE | tornavoz

Jornalistas: alvos preferenciais do Pegasus



180

jornalistas ao redor do mundo, foram selecionados como alvos por clientes da companhia israelense *NSO Group*, responsável pela comercialização do spyware *Pegasus*.*

Fonte: **Forbidden Stories** - 2021

Pegasus - América Latina



México

25 pessoas entre jornalistas e defensores de direitos humanos foram alvo do Pegasus

El Salvador

2/3 dos jornalistas do periódico ***El Faro*** tiveram seus celulares invadidos.



ABRAJI | MEDIA DEFENCE | tornavoz

Khadija Ismayilova

Azerbaijão

“Passei a noite toda pensando no que fiz com meu telefone. Me sinto culpada pelas mensagens que enviei. Me sinto culpada pelas fontes que me enviaram [informações] pensando que algumas formas de mensagens criptografadas são seguras e que não sabiam que meu telefone estava infectado. Os membros da minha família também foram vítimas. Minhas fontes foram vítimas, as pessoas com quem trabalhei, as pessoas que me contaram seus segredos íntimos foram vítimas.”

Além da jornalista, 90 números de sua lista de contatos também foram infectados com o Pegasus. Até mesmo o motorista de táxi que a atendia foi espionado.

Carmen Aristegui

México

“Foi um grande choque ver pessoas próximas a mim na lista. Tenho seis irmãos, mas pelo menos um deles, minha irmã, foi incluído no sistema. Minha assistente Sandra Nogales, que sabia tudo sobre mim - que tinha acesso à minha agenda, a todos os meus contatos, ao meu dia-a-dia, hora a hora - também foi inserida no sistema."

Carlos Dada

El Salvador

“Muitas das nossas fontes pararam completamente de falar com a gente (...) e isso é importante dizer, em termos jornalísticos. Em países como o meu, você depende das fontes cada vez mais, porque o governo impede o acesso a informações oficiais que normalmente são acessíveis ao público. Quando as fontes souberam que tínhamos sido infectados pelo Pegasus, as pessoas ficaram assustadas e pararam de falar, o que tornou o nosso trabalho muito mais difícil.”

Relatoria Especial sobre Liberdade de Expressão

Vigilância

"A vigilância cria incentivos para a autocensura e prejudica diretamente a capacidade dos jornalistas e defensores dos direitos humanos de conduzir investigações e construir e manter relacionamentos com fontes de informação"

"A mera possibilidade [de vigilância] serve para impedir que jornalistas deixem de cobrir temas sensíveis."

Papel do jornalismo

O Globo

Matéria jornalística revelou o uso do First Mile - software de vigilância da empresa israelense Cognyte - para monitoramento de jornalistas pela Abin

Papel do jornalismo

Revista Piauí

Em dezembro de 2023, a **Revista Piauí** revelou que, em abril de 2022, a seis meses das eleições, a Secretaria de Segurança Pública de Mato Grosso comprou o GI-2 da *Cognyte* por 4,67 milhão de reais.

Entre as justificativas para a compra estava o ***"combate de fake news, através da localização de aparelhos celulares suspeitos de criar ou disseminar [notícias falsas]"***.

Jornalistas MT

Celulares dos jornalistas apreendidos

Justificativa: apuração dos crimes de perseguição, calúnia e associação criminosa, que teriam sido praticados para atacar a reputação do governador Mauro Mendes.

Liminar proferida pela Ministra Cármen Lúcia na Reclamação 66.246 suspendeu a decisão que autorizou a busca e apreensão


ABRAJI
MEDIA
DEFENCE
tornavoz

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

UNINDO FORÇAS COM ESTADOS E O DISTRITO FEDERAL

ADPF 1143
Audiência Pública
Supremo Tribunal Federal

Victor Cravo
Consultor Jurídico junto ao MJSP
Doutor em Direito, Estado e Constituição (UnB)
Especialista em Regulação das Telecomunicações (Inatel)

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Roteiro

1. Suspensão Legítima do Sigilo das Comunicações
2. Ferramentas de Intrusão Virtual Remota e Monitoramento Secreto
3. Futuro da Suspensão Legítima do Sigilo das Comunicações

1. Suspensão Legítima do Sigilo das Comunicações

- **Constituição de 1988, art. 5º, XII**
  - inviolabilidade do sigilo das comunicações telefônicas
  - por ordem judicial
  - fins de investigação criminal ou instrução processual penal
    - => proibido para qualquer outro fim
    - => exceção para a decretação dos Estados de Defesa e de Sítio
  - na forma da lei

- **Lei nº 9.296, de 24 de julho de 1996**
  - interceptação de telecomunicações de qualquer natureza
    - fluxo de comunicações em sistemas de informática e telemática
    - apoio técnico e especializado das prestadoras de serviços de telecomunicações

- **Resolução da Anatel nº 738, de 21 de dezembro de 2020**
  - tecnologias necessárias à suspensão do sigilo devem integrar a plataforma da prestadora
  - Anatel deve estabelecer as condições técnicas específicas, observada a Constituição
    - constituído o Grupo Técnico de Suporte à Segurança Pública (GT-Seg)
    - SITTEL – Sistema de Investigação Telefônico e Telemático

2. Ferramentas de Intrusão Virtual Remota e Monitoramento Secreto

- Fornecidas por empresas privadas (nacionais e estrangeiras)

- Ao arrepio da legislação que disciplina a suspensão legítima do sigilo das comunicações

    - não são apoio às prestadoras de serviços de telecomunicações
        - Lei nº 9.296, de 24 de julho de 1996
        - Resolução da Anatel nº 738, de 21 de dezembro de 2020

    - exploram vulnerabilidades:
        - da rede pública de telecomunicações
        - dos sistemas operacionais dos aparelhos celulares

- A título exemplificativo:
    - First Mile
    - Pegasus

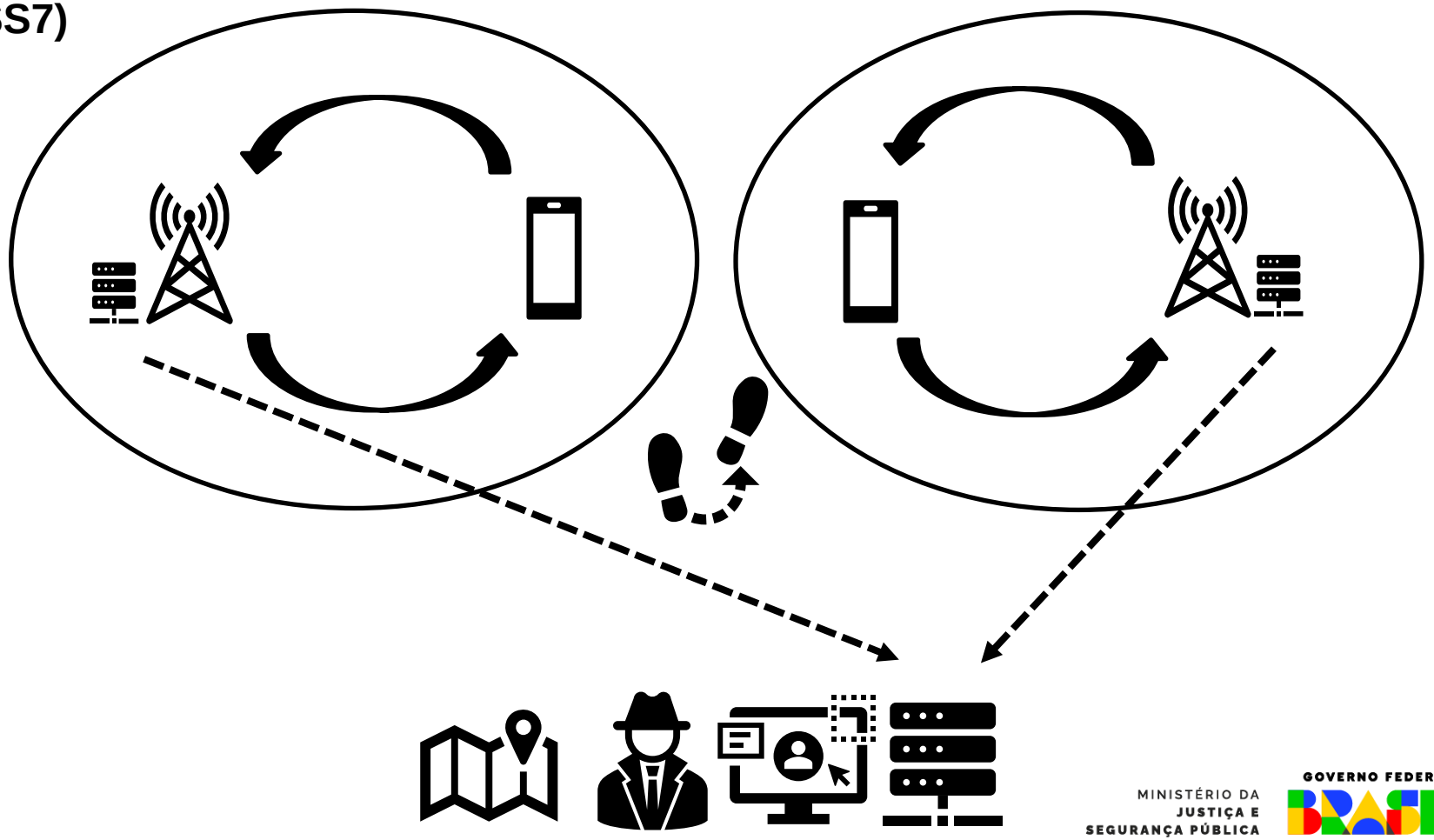
2. Exploração de Vulnerabilidades da Rede Pública de Telecomunicações (FirstMile)

- **Sistema de Sinalização nº 7 (SS7)**

- protocolos de comunicações:
  - Estações Rádio Base - ERB
  - Dispositivos Móveis

- invasão obtém:
  - localização em tempo real
  - dado de tráfego:
    - IMSI (id. única / SIM Card)
      +
    - geolocalização da ERB
      =
    - dados de origem e destino



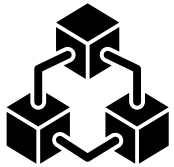


2. Exploração de Vulnerabilidades da Rede Pública de Telecomunicações (FirstMile)

- **Convenção de Budapeste**
  (Decreto nº 11.491, de 12 de abril de 2023)

- **dados cadastrais**

- **dados de tráfego**
  - de aparelhos interconectados
    - na cadeia de comunicação
      - origem
      - destino
      - caminho
      - hora
      - data
      - extensão
      - duração
      - tipo de serviço



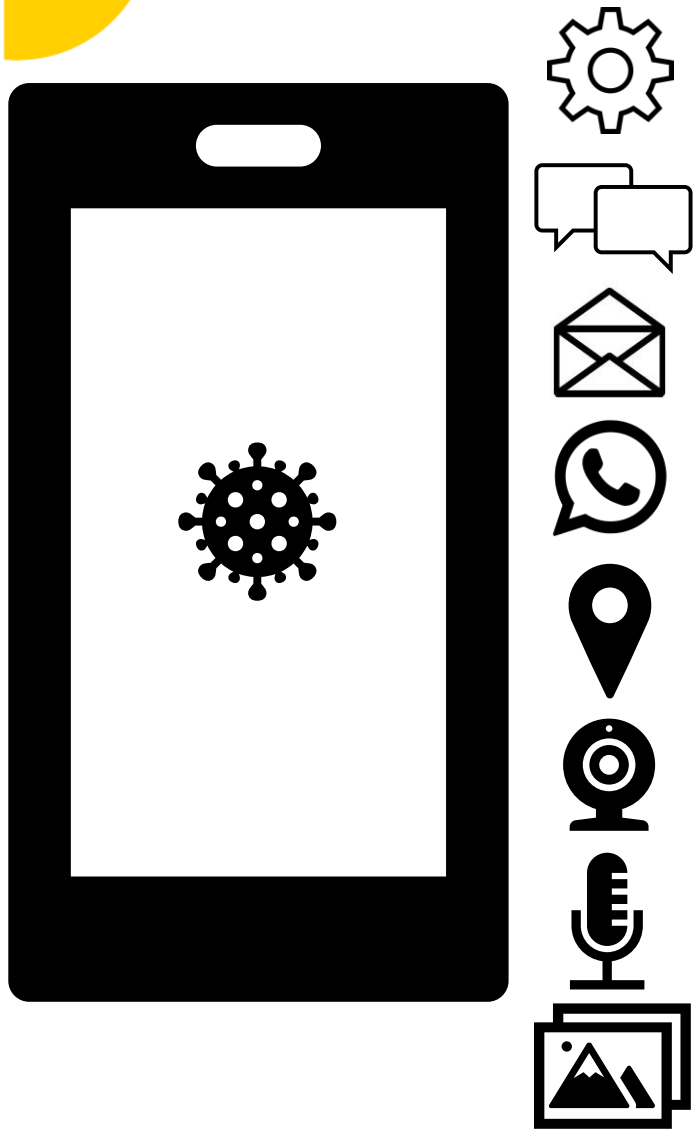


- Dados cadastrais => LGPD



- Dados de tráfego => sigilo das comunicações (CF)

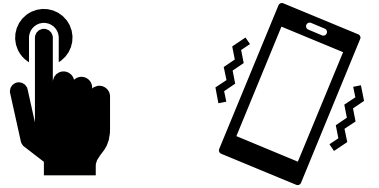
2. Exploração de Vulnerabilidades de Sistemas Operacionais de Dispositivos Móveis (Pegasus)



- Spyware: software malicioso com fins de espionagem



- Infecção do dispositivo
  - com clique
  - sem clique



3. Futuro da Suspensão Legítima do Sigilo das Comunicações

- **Suficiência do Quadro Legal vigente:**
  - -Constituição de 1988, art. 5º, XII
  - - Lei nº 9.296, de 24 de julho de 1996
  - - Resolução da Anatel nº 738, de 21 de dezembro de 2020
    - - tecnologias necessárias à suspensão do sigilo devem integrar a plataforma da prestadora

- **Continuidade do trabalho interinstitucional**
  - - por meio do Grupo Técnico de Suporte à Segurança Pública (GT-Seg)
    - - MJSP / Polícia Federal
    - - Polícias Civis
    - - Ministério Público
    - - Poder Judiciário / CNJ
      - => transparência
      - => accountability

Obrigado!

victor.cravo@mj.gov.br



POLÍCIA FEDERAL

Integridade • Inovação • Imparcialidade • Eficiência • Ética

Ministério da
Justiça e
Segurança Pública



Atividade de Inteligência Nacional

Vedação Constitucional

Interceptações telefônicas e telemáticas

- CF, art. 5º, inciso XII

  "... salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal"

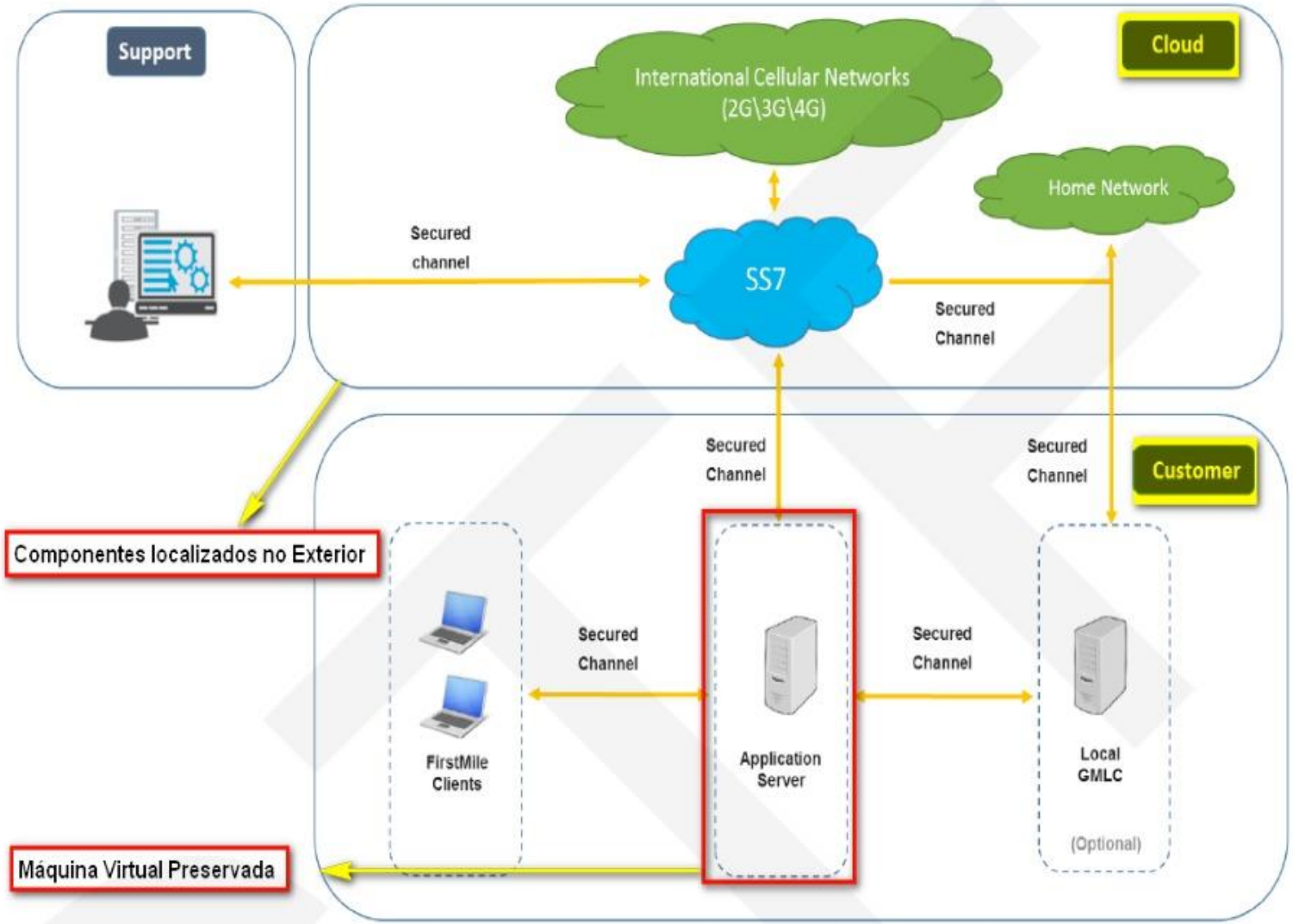
- Lei 9.296/96, arts. 1º, 7º, 8º e 10º - Trata das interceptações telefônicas, de informática ou telemática.
- Lei 12.850/2013 art. 3º, § 1º – Lei das Organizações Criminosas.
- Código Penal – art. 154-A – Invasão de Dispositivo Informático.
- Lei 13.869/19 arts. 25 e 28 – Lei de Abuso de Autoridade.

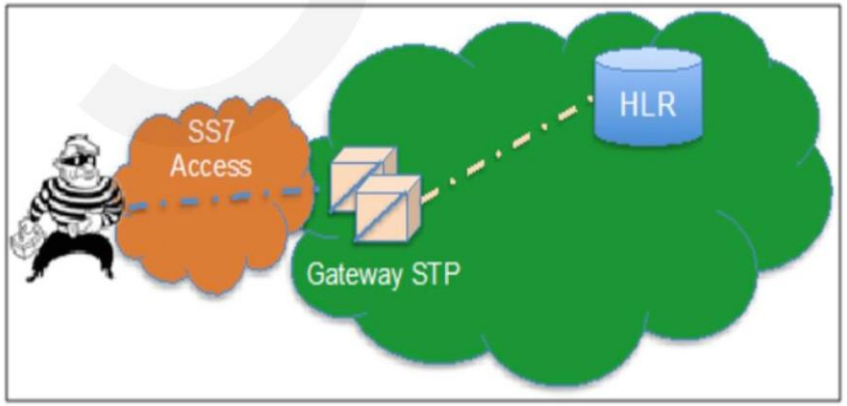
Vedação Legal

Infiltração

- Lei 12.850/13, art. 11

  "A infiltração de agentes de polícia em tarefas de investigação, representada pelo delegado de polícia ou requerida pelo Ministério Público, após manifestação técnica do delegado de polícia quando solicitada no curso de inquérito policial, será precedida de circunstanciada, motivada e sigilosa autorização judicial, que estabelecerá seus limites."





Ministério da
Justiça e
Segurança Pública

Obrigado!

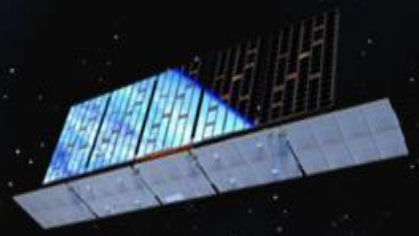
Rodrigo Morais Fernandes

Diretor de Inteligência Policial

dip@pf.gov.br

Ministério da
Justiça e
Segurança Pública

Audiência Pública no Supremo Tribunal Federal



Ten Cel Eng André Luiz Corrêa

Comando da Aeronáutica

FORÇA AÉREA BRASILEIRA
Asas que protegem o País

OBJETIVO

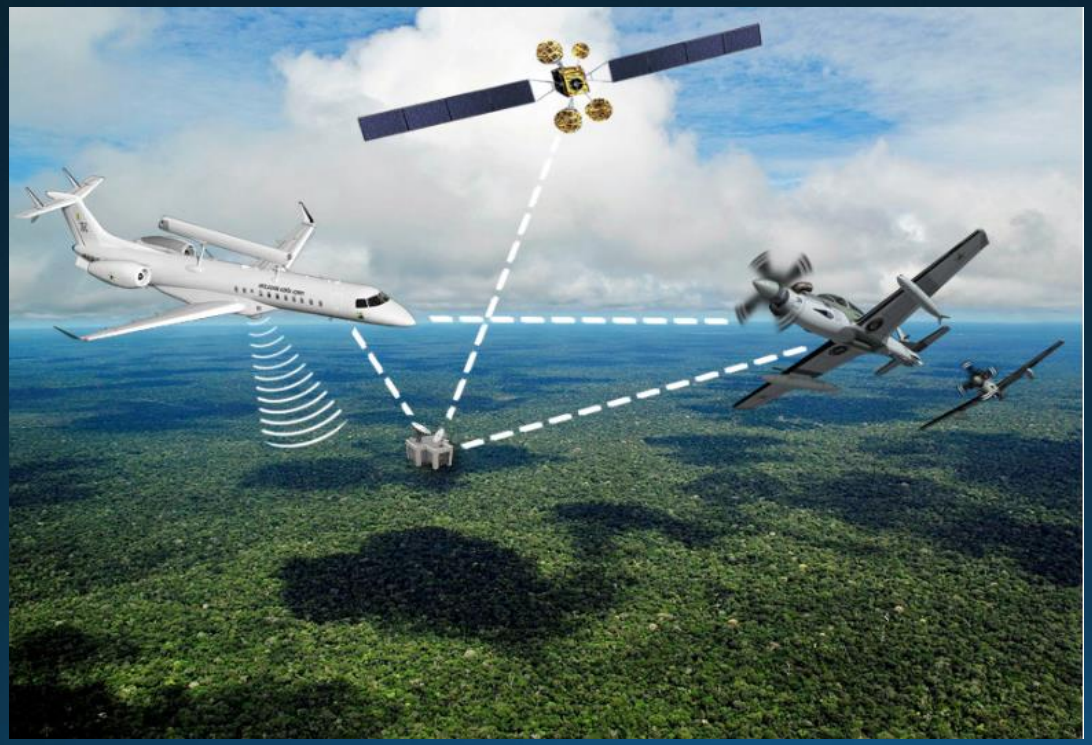


Demonstrar a necessidade do uso de ferramentas tecnológicas com vistas à segurança nacional

FORÇA AÉREA BRASILEIRA

MISSÃO

MANTER A SOBERANIA DO ESPAÇO AÉREO E INTEGRAR O TERRITÓRIO NACIONAL, COM VISTAS À DEFESA DA PÁTRIA.



FORÇA AÉREA BRASILEIRA
Asas que protegem o País

FORÇA AÉREA BRASILEIRA

ATRIBUIÇÕES SUBSIDIÁRIAS

As Leis Complementares nº 97, de 1999, nº 117, de 2004, e nº 136, de 2010, imputaram às Forças Armadas atribuições subsidiárias relacionadas a:

- desenvolvimento nacional e defesa civil;
- combate a delitos transfronteiriços e ambientais..

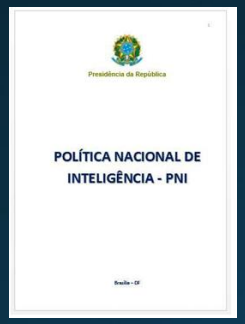




ATIVIDADE DE INTELIGÊNCIA

Produzir conhecimentos com oportunidade e credibilidade para assessorar no processo decisório e identificar fatos ou situações que possam resultar em ameaças ou riscos aos interesses da sociedade e do Estado.

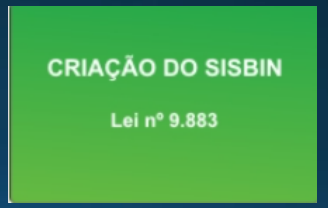












FORÇA AÉREA BRASILEIRA

CONTROLE E FISCALIZAÇÃO DA ATIVIDADE DE INTELIGÊNCIA

Lei nº 9.883 de 1999 e Resolução nº 2 de 2013-CN

Menu | SENADO FEDERAL | Acessibilidade | Fale com o Senado

Atividade Legislativa › Comissões

Buscar

Plenário | Comissões | Projetos e Matérias | Informações Legislativas | Legislação | Órgãos do Parlamento | Mais

Atividade Legislativa / Comissões / CCAI

CCAI Comissão Mista de Controle das Atividades de Inteligência



22/03/2024 - 18h03
IA precisa ser regulada, alerta Castells; Senado tem projetos

NOTÍCIAS

20/10/2023 - 16h56
Comissão repudia uso do aparato de inteligência estatal com fins políticos

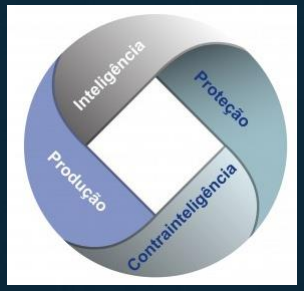
25/08/2023 - 12h39
CCAI deve votar audiência com Flávio Dino e novas informações sobre 8 de janeiro

27/04/2023 - 17h11
Comissão de Atividades de Inteligência dá posse a presidente e vice na terça

30/11/2022 - 11h52
Comissão da inteligência artificial entrega relatório na quinta

https://legis.senado.leg.br/comissoes/comissao?codcol=449

FORÇA AÉREA BRASILEIRA



ATIVIDADE DE INTELIGÊNCIA

(Assessorar na tomada de decisão, mitigar as ameaças)

x

INVESTIGAÇÃO POLICIAL

(Materialidade e culpabilidade)



FORÇA AÉREA BRASILEIRA
Asas que protegem o País

ATIVIDADE DE INTELIGÊNCIA NA FAB

O avanço tecnológico exige que a Força Aérea tenha **capacitação** e **prontidão** quanto ao uso de soluções tecnológicas de busca e de proteção do conhecimento para apoiar no Preparo e Emprego do Poder Aeroespacial.

Isso permite a **antecipação** e a **preparação** para uma situação de conflito ou beligerância.

Consequência contrária: **Surpresa**

FORÇA AÉREA BRASILEIRA
Asas que protegem o País

CUSTO DA FALHA



“Se não esperas o inesperado não o reconhecerás quando chegar”.

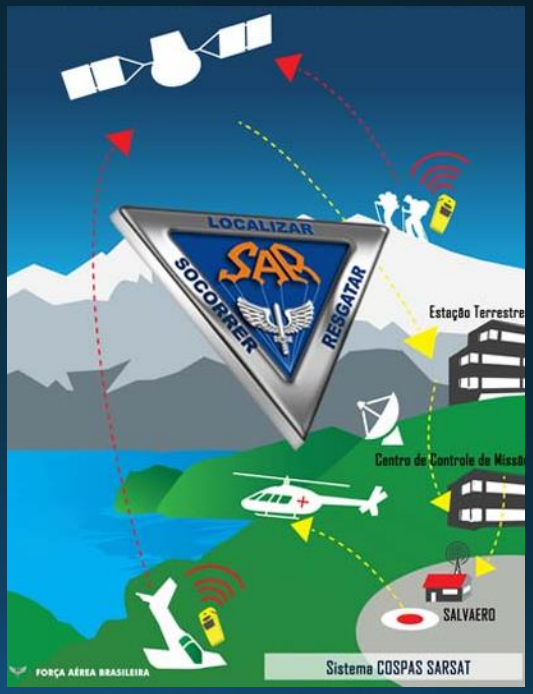
Heráclito

USO DUAL PARA CAPACITAÇÃO E PRONTIDÃO

Os programas e ferramentas tecnológicas podem ser empregados nas atribuições subsidiárias da Força Aérea e na Contrainteligência.

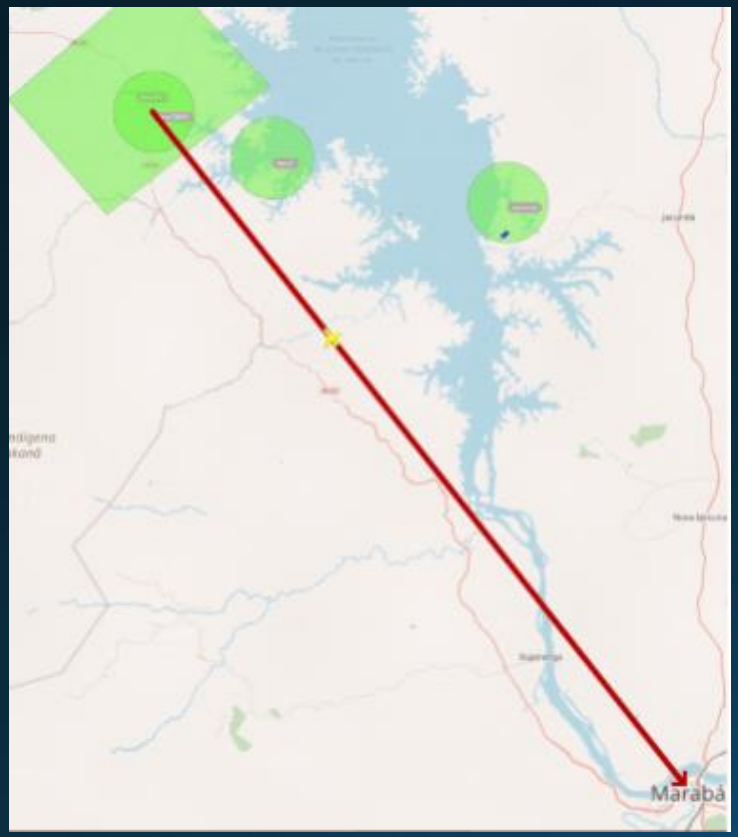


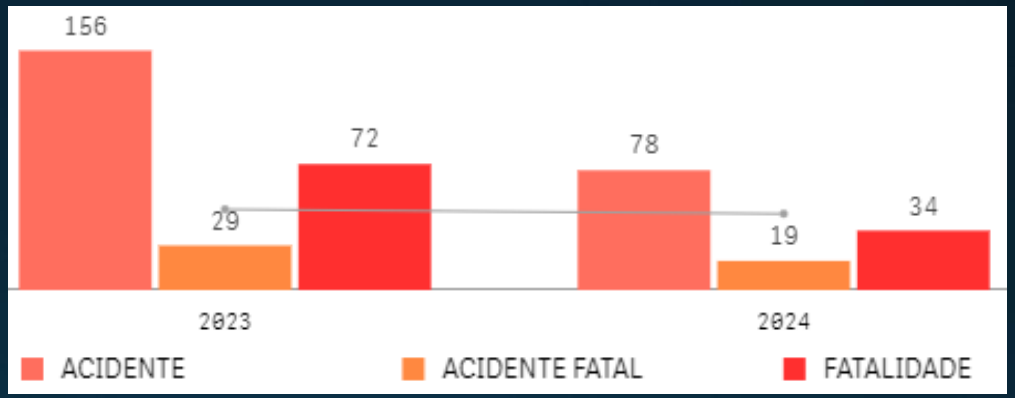




BUSCA E SALVAMENTO

CELULARES → Geolocalização de vítimas de acidentes aéreos.





Fonte: CENIPA



GEOLOCALIZAÇÃO



Fonte: https://www.cnnbrasil.com.br/nacional/geolocalizacao-de-celular-ajuda-a-encontrar-49-pessoas-desaparecidas-no-rs/

CONTRAINTELIGÊNCIA





Identificar e neutralizar ações de busca por informações estratégicas pela inteligência adversa.

FORÇA AÉREA BRASILEIRA
Asas que protegem o País

CONTRAINTELIGÊNCIA

TEMPEST

Computadores, cabos, telefones, sinais de rádio e sistemas operacionais emitem radiação eletromagnética (EMR) que pode ser usada por interceptadores para reconstruir dados inteligíveis.



CONTRAINTELIGÊNCIA





Identificar e neutralizar ações de busca por informações estratégicas do GRIPEN pela inteligência adversa.

FORÇA AÉREA BRASILEIRA
Asas que protegem o País

DESVIO DE FINALIDADE

O Comando da Aeronáutica é veementemente contrário à utilização indevida de ferramentas que violem os direitos fundamentais à intimidade e ao sigilo das comunicações, estabelecidos no art. 5º, X e XII, da Constituição Federal.

FORÇA AÉREA BRASILEIRA
Asas que protegem o País

DESVIO DE FINALIDADE

Art. 21. Tendo a CCAI apurado, em processo sigiloso, a prática de ilícitos civis ou penais por parte de pessoas ou órgãos responsáveis pela execução de atividades de inteligência, contrainteligência ou de salvaguarda de informações sigilosas, seja pela análise dos relatórios parcial e geral, seja pela apuração de denúncias de violação de direitos e garantias fundamentais, suas conclusões serão encaminhadas ao Ministério Público competente, conforme o caso, para que este promova a ação de responsabilidade civil ou criminal dos infratores.

Resolução nº 2 de 2013-CN

FORÇA AÉREA BRASILEIRA
Asas que protegem o País

CONCLUSÃO

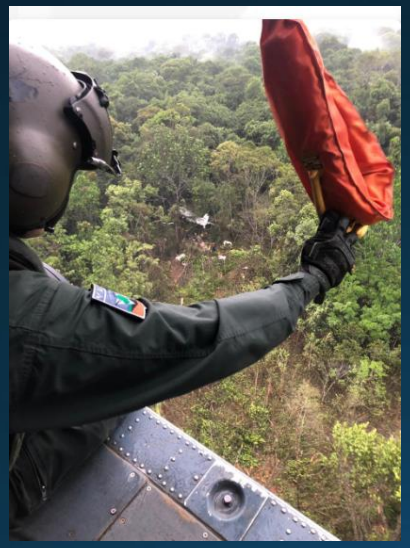
É fundamental o constante aperfeiçoamento da regulamentação, entretanto, a normativa atual é clara e proporcional de modo a garantir a legalidade e a proteção dos direitos individuais.

É importante reconhecer e fortalecer a atuação da CCAI como órgão de Controle e Fiscalização externo para combater os desvios de finalidade quanto ao uso das ferramentas tecnológicas em prol da Atividade de Inteligência.

FORÇA AÉREA BRASILEIRA
Asas que protegem o País

CONCLUSÃO

A fixação de barreiras, mesmo que provisórias, pode comprometer a eficácia das missões constitucionais das Forças Armadas de produzir e proteger conhecimentos essenciais à segurança nacional, além de prejudicar missões de busca e salvamento e favorecer significativamente a atuação da Inteligência adversa.





FORÇA AÉREA BRASILEIRA
Asas que protegem o País

Fundação Instituto de Pesquisas Econômicas

Supremo Tribunal Federal
ADPF 1.143

Tema: regulamentação do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal

10 e 11 de junho de 2024



O debate dos problemas econômicos e sociais e a expansão do conhecimento econômico

Apresentação de estudos, solução e implantação

A formulação de políticas econômicas voltadas para o aumento do bem-estar

A produção de conhecimento e soluções de alto valor agregado

A formação complementar de profissionais de alto nível

Estudos e pesquisas de planejamento tributário

Quem é a FIPE?

fipe
Fundação Instituto de Pesquisas Econômicas

A Fundação Instituto de Pesquisas Econômicas é uma organização de direito privado, sem fins lucrativos, com mais de 40 anos, criada em 1973.

Entre seus objetivos está o apoio ao Departamento de Economia da Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo

Índices e Indicadores

Ensino

Projetos e Pesquisas

Como desenvolver inteligência analítica e proteger a privacidade do usuário ao mesmo tempo?

Políticas públicas para inovação tecnológica voltada para inteligência

Segurança da informação X Privacidade

Segurança da Informação

Prevenir o acesso não-autorizado e *hacking* de sistemas.

Prevenir invasão ou intrusão

Privacidade

Prevenir que dados pessoais não sejam usados para finalidades não desejáveis pelo indivíduo.
Exemplo:
- Dedução de fatos sensíveis a partir de outros;
- Identificação de um indivíduo entre uma população;
- Inferências sobre atributos sensíveis.

Prevenir o mau uso dos dados mesmo quando há acesso legítimo

A dia a dia de quem trabalha com dados

Práticas cotidianas que podem favorecer violações de segurança e privacidade

- Coleta de dados sensíveis
- Compartilhamento de dados entre instituições
- Desenvolvimento de inteligência artificial
- Desenvolvimento de funcionalidades tendo como base o hardware dos celulares

Fatos que impulsionaram pesquisas nos últimos 20 anos

Ananonimização insuficiente

- **Sweeney** - Re-identify anonymized medical records with public data-sets [1997]
- **AOL** - “Search Log - Thelma Arnold” [2006]
- **Netflix and IMDB** - “Movies Watched and Type of Person “ [2007]
- **MIT** - Gaydar project [2009]

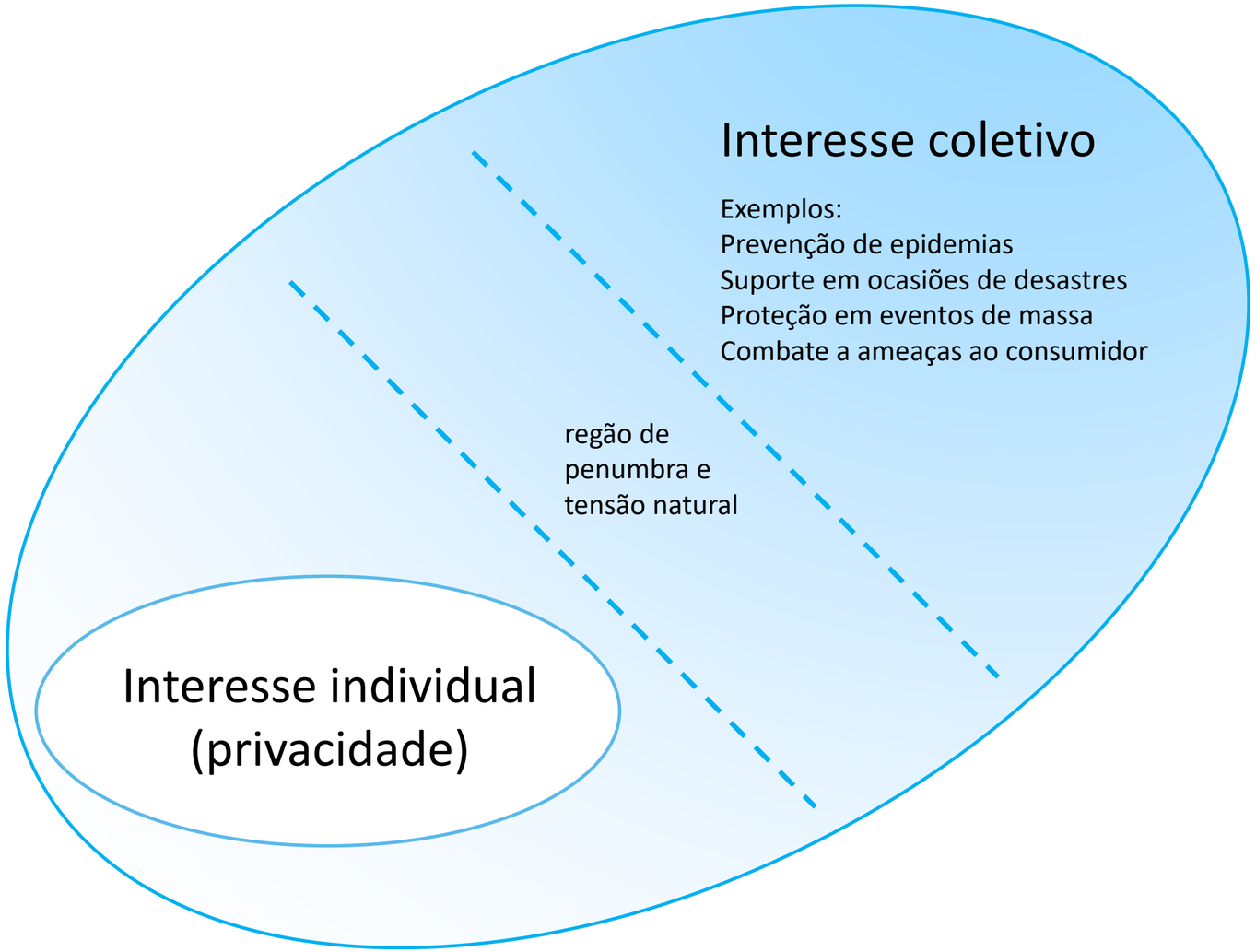
Engenharia reversa revela dados sensíveis

- **Target** - “Pregnancy” [2012]
- **Uber** - “Rides of Glory - One Night Stand “ [2012]

Uso dos dados para propósitos indevidos e não-autorizados

- **Facebook and Cambridge Analytica** [2018]

Um dilema natural amplificado pela tecnologia



Como a tecnologia pode ajudar a resolver esses problemas que ela criou?

Pesquisas enfocando descentralização do controle da informação individual

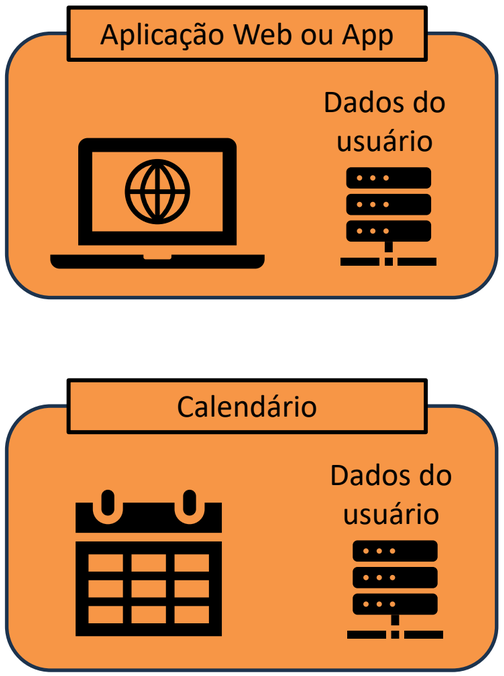
Quatro tecnologias emergentes que merecem atenção

WEB 3.0 arquitetura descentralizada para Web/Apps	Sempre que possível, permitir ao usuário controlar e armazenar seu próprio dado no ambiente digital
Differential Privacy	Sempre que um algoritmo for treinado, deve-se assegurar a privacidade dos indivíduos para que os resultados não gerem danos ou desigualdades aos usuários
Federated Learning	Treinar modelos de IA compartilhando a inteligência (pesos) sem compartilhar os dados (datasets)
Synthetic Data	Ao compartilhar dados entre entidades, gerar dados sintéticos

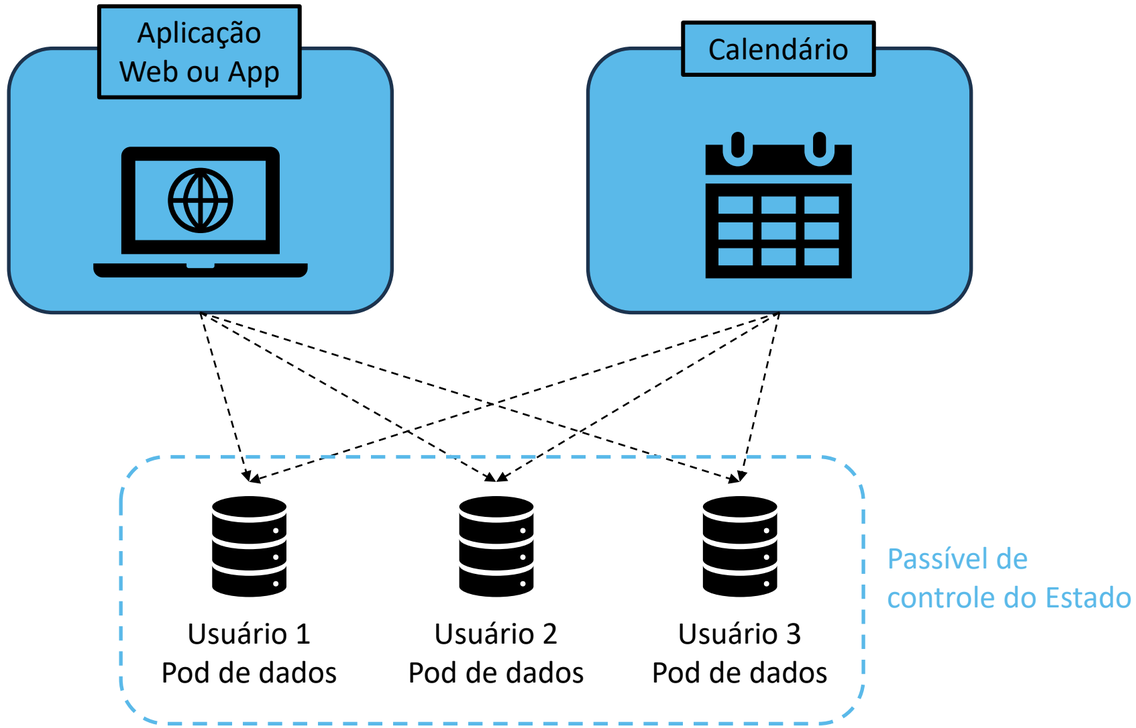
WEB 3.0: Arquitetura descentralizada para Web/Apps

Visa desacoplar os dados individuais das aplicações
Plataformas e ferramentas para habilitar apps descentralizados
A informação fica sob controle do indivíduo, e não do app (maior privacidade)

Web apps Centralizadores



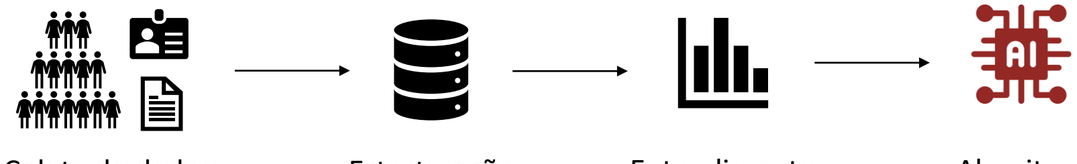
Web apps Descentralizados



Differential Privacy

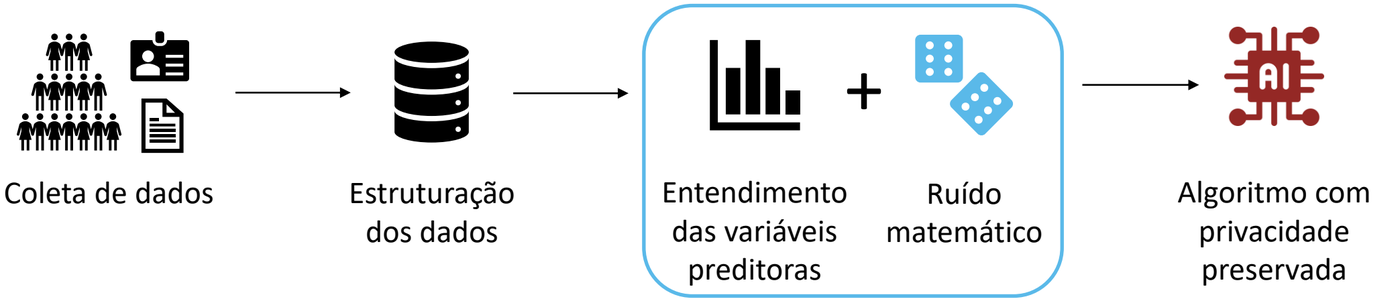
Permite criar algoritmos de inteligência artificial preservando a identidade do indivíduo.
Técnicas matemáticas e estatísticas que geram ruído nos bancos de dados.
A qualidade do algoritmo é preservada estatisticamente, sem revelar a identidade do indivíduo.
Dificulta inferências potencialmente danosas acerca de um determinado ruído.

Machine learning tradicional



Coleta de dados | Estruturação dos dados | Entendimento das variáveis preditoras | Algoritmo vulnerável à engenharia reversa

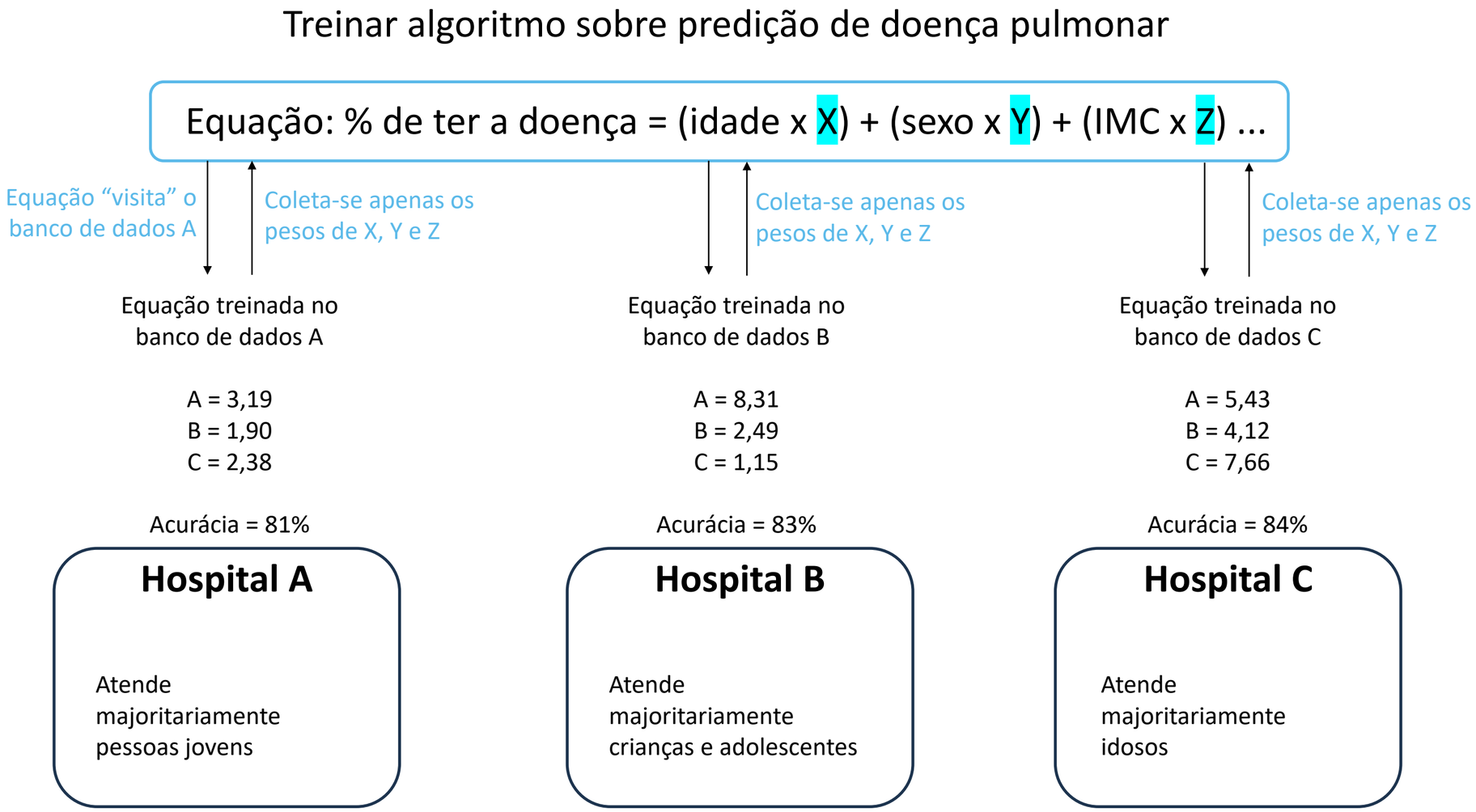
Machine learning com preservação da privacidade



Coleta de dados | Estruturação dos dados | Entendimento das variáveis preditoras | Ruído matemático | Algoritmo com privacidade preservada

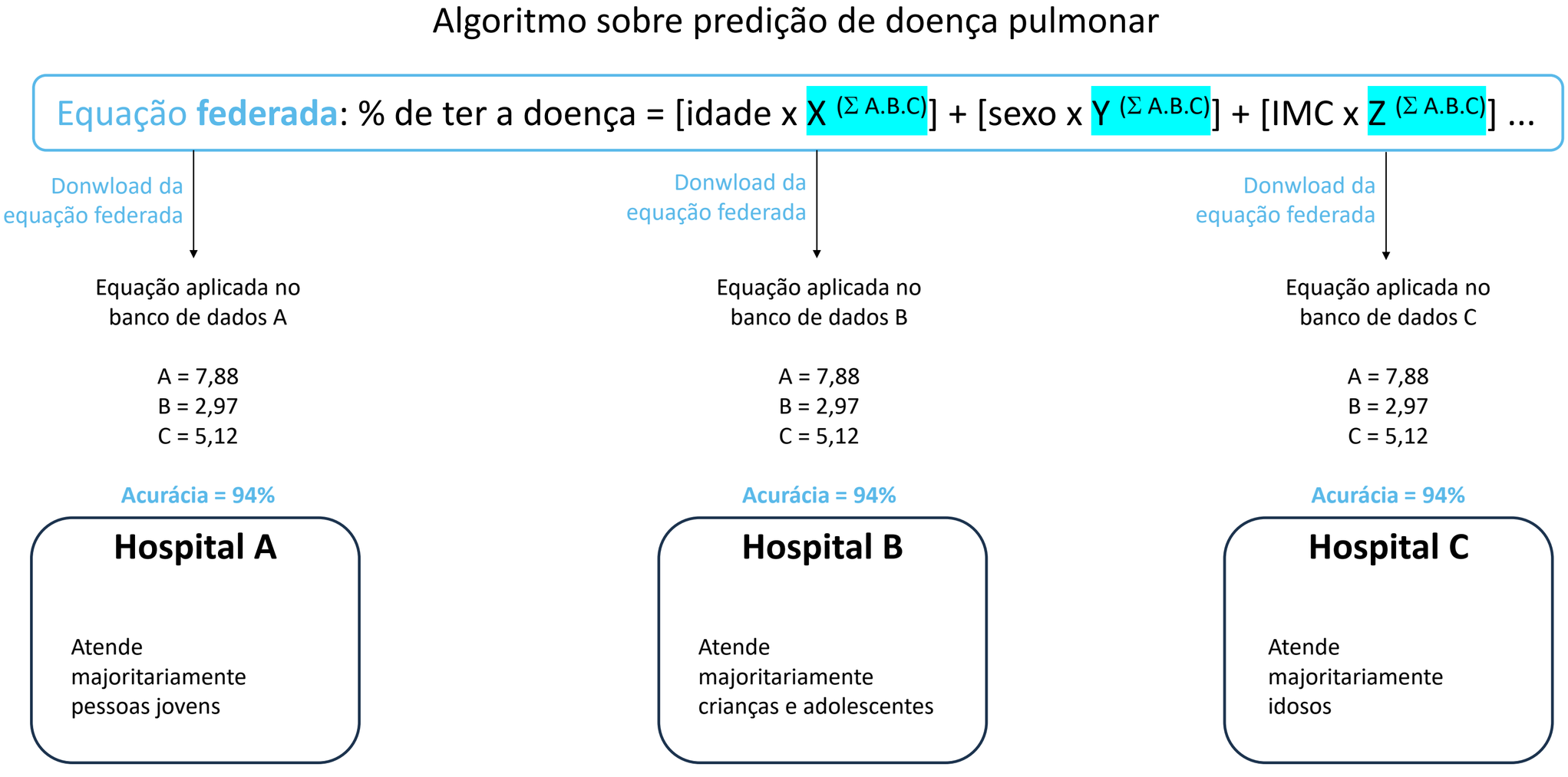
Federated Learning

Criar algoritmos de inteligência artificial com menos vieses, minimizando desigualdades sociais.
Permite compartilhar inteligências sem precisar compartilhar os bancos de dados.



Federated Learning

Criar algoritmos de inteligência artificial com menos vieses, minimizando desigualdades sociais.
Permite compartilhar inteligências sem precisar compartilhar os bancos de dados.



Dados sintéticos

Técnica matemática para gerar bancos de dados estatisticamente idênticos, sem dados sensíveis.
Especialmente útil para transmitir bases de dados de uma instituição para outra.
Permite criar algoritmos de IA sem dados individuai.

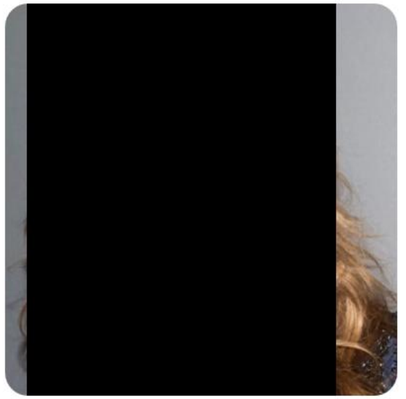
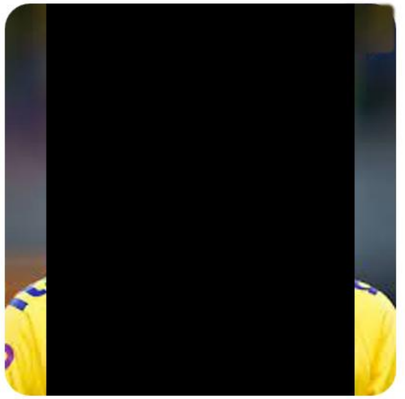
Pouca anonimização
Com engenharia reversa é possível inferir.






Anonimização excessiva
Praticamente destrói características do banco de dados e o torna inútil para gerar inteligência.



Dados sintéticos

Técnica matemática para gerar bancos de dados estatisticamente idênticos, sem dados sensíveis.
Especialmente útil para transmitir bases de dados de uma instituição para outra.
Permite criar algoritmos de IA sem dados individuai.



Uso de dados sintéticos
Cria ruídos controlados no banco de dados, mantendo as propriedades estatísticas (ex: perfil sociodemográfico), mas descaracterizando os indivíduos

Imagens geradas em https://generated.photos/anonymizer

Conclusões

Existem interesses coletivos legítimos que demandam coleta passiva de informações a partir dos celulares.

É muito difícil um produto tecnológico nascer isento de vulnerabilidade. As correções vêm com o uso e reportes.

Existem novas tecnologias de combate às violações de privacidade, especialmente no desenvolvimento de I.A.'s.

Uso disseminado dessas técnicas protegem o cidadão e dificultam a prática criminosa.

É preciso incentivar a inovação tecnológica que emprega essas boas práticas.

Recomendações para o debate

O Brasil precisa de mais pesquisas em tecnologias de descentralização de informações.

Evoluir na normatização sobre melhores práticas de desenvolvimento tecnológico, com inclusão de práticas que gerem maior proteção à privacidade como padrão de qualidade mínimo ("Inmetro dos softwares").

Uma ideia: um "Gov-ware" para celulares que permite a intrusão legal, programada e monitorada para fins investigativos e previstos em lei, com fiscalização por um conselho nacional com representação social.

Regulamentar o acesso aos softwares intrusivos, com fiscalização e punição de abusos.

Thiago Pavin
thiago.pavin@fipe.org.br

Fundação Instituto de Pesquisas Econômicas

Avenida Corifeu de Azevedo Marques, 5.677

São Paulo – SP - Brasil

(11) 3767-1700 / 3767-1770 / 3814-3379

www.fipe.org.br