Cartografías de la opacidad: spyware, contratación pública y fragmentación regulatoria en Argentina

CELS, Democracia en Red, Fundación Vía Libre, O.D.I.A.

Simposio LAVITS, 28/08/26

¿QUIÉNES SOMOS?

Modera: Beatriz Busaniche - Fundación Vía Libre

Margarita Trovato - Fundación Vía Libre
Manuel Tufró - CELS
Tomás Rausch - O.D.I.A.
Florencia Caffarone - Democracia en Red

Vía Libre CELS O.D.I.A. DEMOCRACIA EN RED

1. CONTEXTO . VIGILANCIA E INSTITUCIONALIDADES DÉBILES EN LA REGIÓN:

- Marcos regulatorios pobres sobre tecnologías de vigilancia, primacía de la excepcionalidad, institucionalidades débiles (historia de autoritarismos y vigilancia)
- Opacidad y uso de vigilancia frente al espacio cívico
- Interdependencia con actores corporativos y geopolíticos (vigilancia estatal + corporativa), en general mediante acuerdos que imponen restricciones sobre el control y la regulación.
- Desafíos en la protección de datos personales de la sociedad en general y de quienes ya fueron víctimas de vigilancia estatal (ej. Que no se reutilicen para entrenar sistemas).

→ normalización de la vigilancia masiva

1. CONTEXTO. FISCALIZAÇÃO E INSTITUIÇÕES FRACAS NA REGIÃO:

- Estruturas regulatórias deficientes em relação às tecnologias de vigilância, primazia do excepcionalismo, instituições frágeis (histórico de autoritarismo e vigilância)
- Opacidade e uso da vigilância contra o espaço cívico
- Interdependência com atores corporativos e geopolíticos (vigilância estatal + corporativa), geralmente por meio de acordos que impõem restrições ao controle e à regulamentação.
- Desafios na proteção dos dados pessoais da sociedade em geral e daqueles que já foram vítimas de vigilância estatal (por exemplo, que esses dados não sejam reutilizados para treinar sistemas).

→ normalização da vigilância em massa

1. CONTEXTO . EL AVANCE DEL ESTADO DE VIGILANCIA EN ARGENTINA Y LA COYUNTURA POLÍTICA ACTUAL:

- Marcos protectorios de datos personales débiles, pocos controles + acceso a información pública debilitada
- Marcos de vigilancia ampliados por decreto:
  - Reforma del Sistema de Inteligencia. Centralización de datos personales. Todo “encubierto” por definición.
  - Reforma de las FFSS con más facultades para vigilancia
  - Ciberpatrullaje + Unidad de IA Aplicada a la Seguridad (Resoluciones Ministerio de Seguridad)
- Blancos de vigilancia ilegales: opositores políticos, periodistas, activistas, ambientalistas, movimientos sociales, comunidades indígenas.
- Alineamiento geopolítico del gobierno actual. Lucha contra el terrorismo

¿Cómo y para qué podría usarse *spyware* en este contexto?

1. CONTEXTO. O AVANÇO DO ESTADO DE VIGILÂNCIA NA ARGENTINA E O PANORAMA POLÍTICO ATUAL:

- Estruturas fracas de proteção de dados pessoais, poucos controles + acesso à informação pública enfraquecido
- Estruturas de vigilância ampliadas por decreto:
    - Reforma do Sistema de Inteligência. Centralização de dados pessoais. Tudo “oculto” por definição.
    - Reforma das Forças de Segurança com mais poderes para vigilância
    - Patrulhamento cibernético + Unidade de IA Aplicada à Segurança (Resoluções do Ministério da Segurança)
- Alvos ilegais de vigilância: opositores políticos, jornalistas, ativistas, ambientalistas, movimentos sociais, comunidades indígenas.
- Alinhamento geopolítico do atual governo. Combate ao terrorismo

Como e para que o spyware poderia ser utilizado nesse contexto?

2. FACTORES DE RIESGO / FATORES DE RISCO

Condiciones estructurales que aumentan el riesgo de vulneraciones de derechos ligadas al uso de software intrusivo

- Las tecnologías de incorporan de manera express
- Federalismo: fragmentación regulatoria
- Federalismo: multiplicación de agencias, mayor dificultad para controlar
- Casos de descontrol de policías y servicios de inteligencia
- Debilidad del Estado frente a las empresas. Doble opacidad

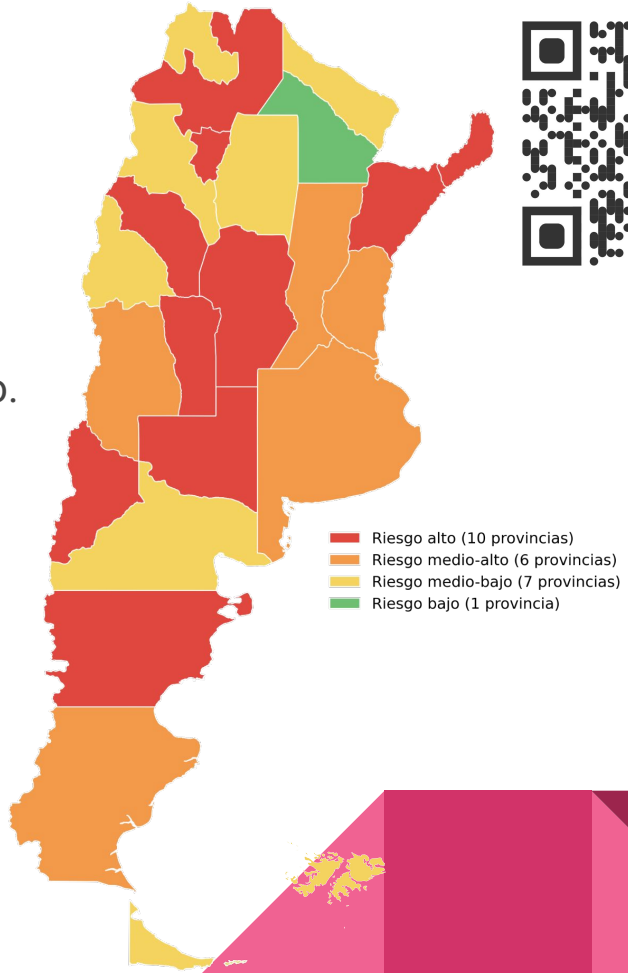
2. FATORES DE RISCO

Condições estruturais que aumentam o risco de violações de direitos ligadas ao uso de ferramentas intrusivas

- As tecnologias são incorporadas por via expressa
- O federalismo apresenta uma fragmentação regulatória
- O federalismo multiplica as agências, dificultando o controle
- Casos de uso descontrolado de capacidades de inteligência ou vigilância
- Fragilidade do Estado frente às empresas. Dupla opacidade.

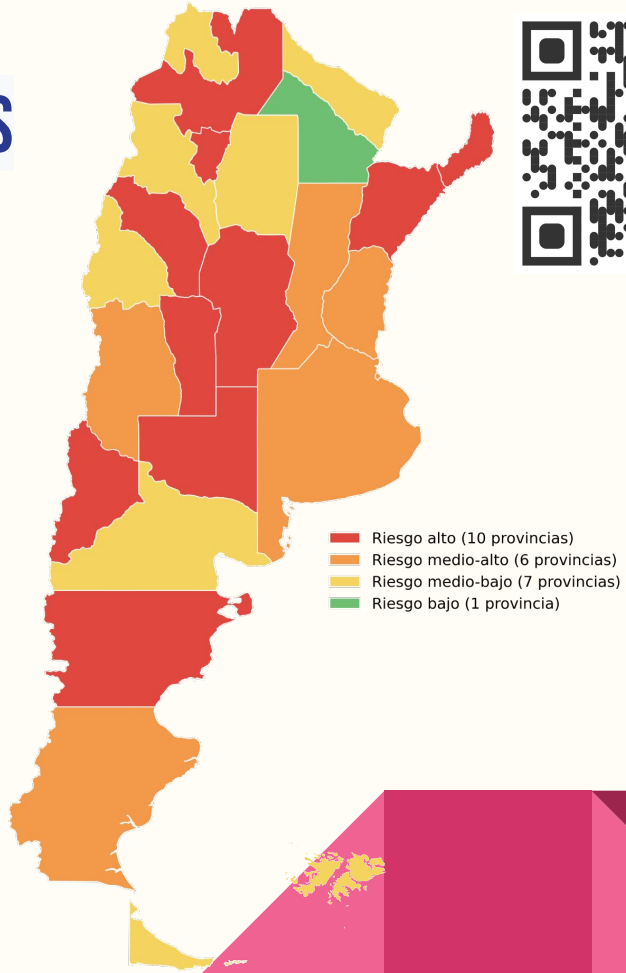
3. FEDERALISMO: UN PAÍS, 25 JURISDICCIONES.

- Solo 12 de 25 jurisdicciones respondieron. Ninguna reportó protocolos o guías de buenas prácticas de uso.
- Dos de ellas reconocen la facultad legal pero dicen no haber adquirido software todavía. Una de ellas confirmó una interpretación institucional amplia, mientras que sólo una la negó expresamente.
- Cinco provincias con habilitación expresa ni siquiera respondieron, siendo las más opacas y riesgosas.
- Muchas respuestas mostraron confusión conceptual.



3. FEDERALISMO: UM PAÍS, 25 JURISDIÇÕES

- Apenas 12 das 25 jurisdições responderam. Nenhuma relatou protocolos ou diretrizes de boas práticas de uso.
- Duas delas reconhecem a prerrogativa legal, mas afirmam ainda não ter adquirido software. Uma delas confirmou uma interpretação institucional ampla, enquanto apenas uma a negou expressamente.
- Cinco províncias com autorização expressa sequer responderam, sendo as mais opacas e de maior risco.
- Muitas respostas demonstraram confusão conceitual



4. RECOMENDACIONES

Recomendaciones regulatorias orientada a fortalecer los mecanismos de control y rendición de cuentas frente al avance del spyware estatal, para cada etapa del ciclo de vida completo del spyware (adquisición, habilitación judicial, uso operativo, obtención y destrucción):

- ***Adquisición:*** *idoneidad técnica e idoneidad probatoria de la herramienta*
- ***Habilitación judicial:*** *validación técnica previa a la ejecución*
- ***Ejecución:*** *tratamiento diferenciado de material amparado por secreto profesional*
- ***Retención y destrucción:*** *revisión periódica de utilidad procesal*
- ***Supervisión:*** *informe anual de implementación y control*

Recomendações regulatórias destinadas a fortalecer os mecanismos de controle e prestação de contas diante do avanço do spyware estatal, para cada etapa do ciclo de vida completo do spyware (aquisição, autorização judicial, uso operacional, coleta e destruição):

- **Aquisição:** adequação técnica e adequação probatória da ferramenta
- **Autorização judicial**: validação técnica prévia à execução
- **Execução:** tratamento diferenciado do material protegido pelo sigilo profissional
- **Retenção e destruição**: revisão periódica da utilidade processual
- **Supervisão**: relatório anual de implementação e controle

4. RECOMENDACIONES / RECOMENDAÇÕES

El desafío regulatorio que plantea el spyware es construir un nuevo marco o regulatorio integral adecuado propio que parta del reconocimiento de su singularidad técnica y de sus consecuencias jurídicas específicas.

Las recomendaciones intentan traducir estos principios de gobernanza integral en exigencias institucionales concretas, organizadas justamente en torno al ciclo completo de vida del spyware.

O desafio regulatório que o spyware apresenta consiste em construir um novo marco regulatório abrangente e adequado, que parta do reconhecimento de sua singularidade técnica e de suas consequências jurídicas específicas.

As recomendações buscam traduzir esses princípios de governança abrangente em exigências institucionais concretas, organizadas justamente em torno de todo o ciclo de vida do spyware.

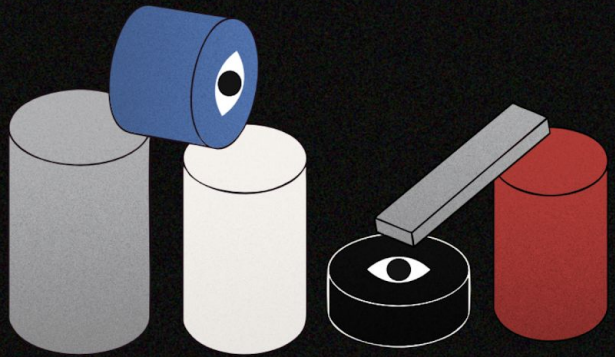
PUBLICACIONES

ALERTA SPYWARE

Uso judicial en argentina.
Situación normativa y de implementación
en las distintas jurisdicciones

Recomendaciones
para
regulación, control y
compras estatales

¡GRACIAS!



ALERTA SPYWARE