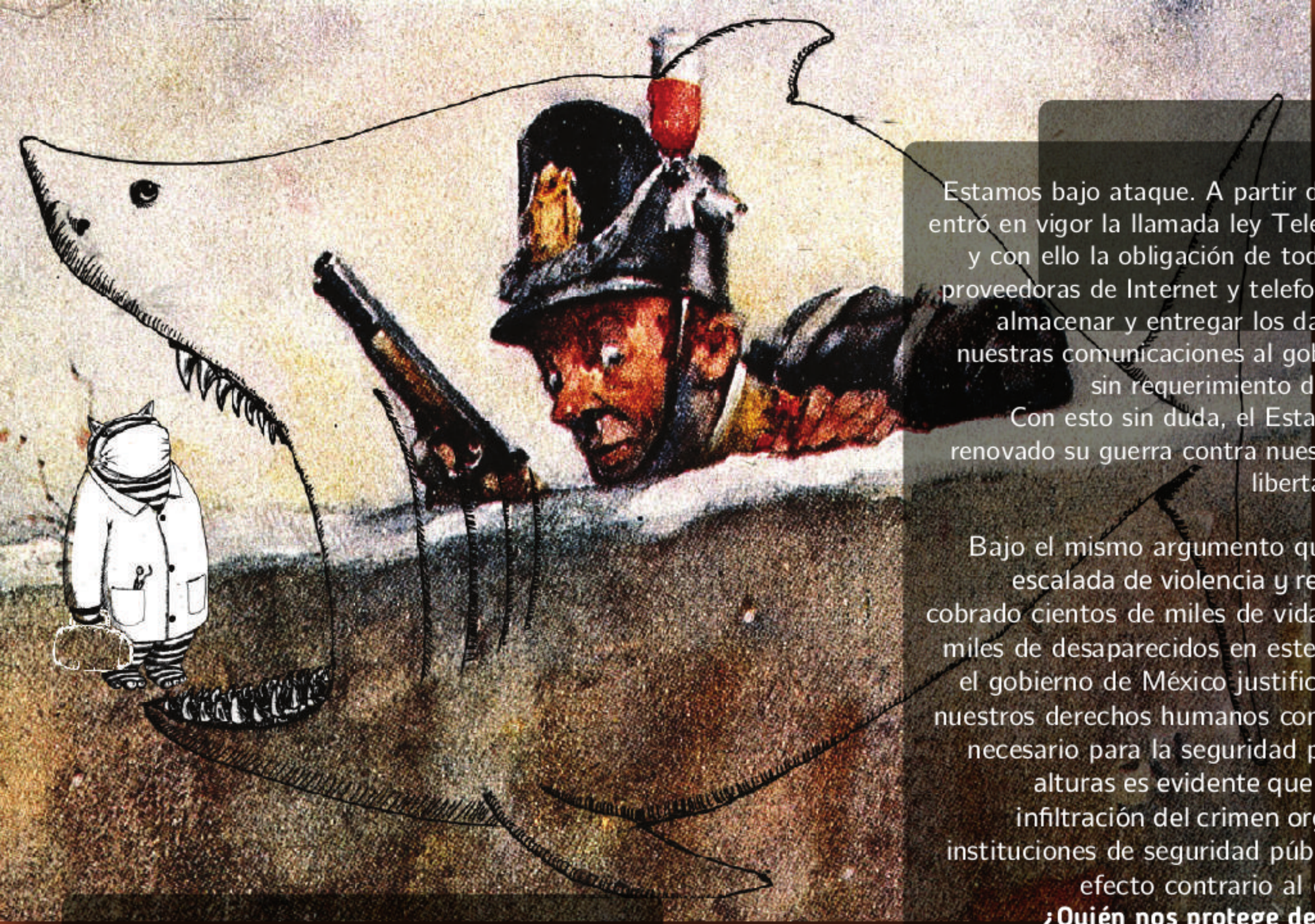

Estamos bajo ataque. A partir del 13 de agosto entró en vigor la llamada ley Telecom en México y con ello la obligación de todas las empresas proveedoras de Internet y telefonía de capturar, almacenar y entregar los datos sobre todas nuestras comunicaciones al gobierno mexicano sin requerimiento de orden judicial.
Con esto sin duda, el Estado mexicano ha renovado su guerra contra nuestra privacidad y libertad de expresión.

Bajo el mismo argumento que acompaña la escalada de violencia y represión que ha cobrado cientos de miles de vidas y decenas de miles de desaparecidos en este país, de nuevo el gobierno de México justifica la violación a nuestros derechos humanos como un sacrificio necesario para la seguridad pública. A estas alturas es evidente que la corrupción e infiltración del crimen organizado en las instituciones de seguridad pública produce un efecto contrario al discurso oficial.
¿Quién nos protege de los vigilantes?

Autodefensa Digital

Tomamos las herramientas

La ley Telecom obliga a las empresas de telecomunicaciones a almacenar los datos de nuestra actividad en Internet y teléfonos celulares por un periodo de dos años. Sin embargo la ley no especifica las condiciones bajo las cuales deben protegerse los datos personales almacenados contra fraude o robo, y no contempla una institución autónoma y confiable que audite el proceso de retención de estos datos. Se vuelve sumamente preocupante, dado el historial de filtraciones de datos personales de ciudadanxs en el mercado negro, como ha sucedido con el padrón electoral múltiples veces desde 2000 y la base de datos del registro Nacional de Usuarios de Telefonía Móvil (Renaut) en 2010, delitos que permanecen impunes.

Hagamos autodefensa digital. Hay que investigar y evaluar los riesgos de la comunicación digital y aprender a utilizar herramientas útiles para defender nuestra privacidad.

Ranch Electrónic
ranchoelectronico.org
Fray Juan de Torquemada 76,Col. Obrera, México, D.F.

Recomendaciones para la autodefensa digital

*** Respaldos seguros**
Asegurémonos de respaldar constantemente nuestra información importante, previendo eventuales fallas en los dispositivos electrónicos y discos. Sería el colmo que el Estado y las empresas privadas tengan copias de nuestra información y nosotros ya no.

*** Software libre**
Ayuda a evitar virus y software espía, que hacen más vulnerables a los sistemas privativos como Windows y OSX.

*** Contraseñas fuertes**
Una contraseña compuesta de 4 a 5 palabras sin relación evidente aumenta su fortaleza y no debe ser demasiado difícil de recordar. Cuidemos de no repetir la misma contraseña para diferentes cuentas ni compartirla con otrxs.

*** Seguridad física**
Cuidemos el acceso físico a nuestras computadoras y teléfonos, y seamos conscientes de cuáles datos sensibles portamos con nosotrxs cuando estamos en tránsito.

*** Discos cifrados**
Cifrar nuestros discos puede evitar el acceso indebido a nuestra información en caso de robo o extravío. Recomendamos el software Luks con Dm-crypt o Encfs para cifrar discos.

***Conexiones cifradas y navegación anónima**
U tilizar la red de Tor o conexiones tipo VPN a servidores proxies ubicados en otros países puede ayudarnos a evitar la retención de datos en territorio mexicano.

*** Comunicación cifrada**
Cifremos los contenidos de nuestros correos con el software GPG y nuestras sesiones de chat con OTR o Cryptocat. Para teléfonos celulares cifremos nuestra comunicación son software libre como TextSecure, RedPhone, Signal y Chatsecure.

*** Servicios/servidores seguros**
Procuremos utilizar servicios de correo, web y almacenamiento de datos hospedados en servidores administrados por colectivos y organizaciones comprometidxs a defender los derechos de sus usuarixs.

*** Navegando más seguro**
Utilicemos navegadores de software libre como Firefox y complementos contra la vigilancia como Https Everywhere, Privacy Badger y Ghostery.