El mercado negro de datos personales

Serie *Datos criminológicos, Nº 2*

Diciembre 2023

Instituto de Criminología y estudios sobre la violencia

ICEV – Instituto de Criminología y Estudios sobre la Violencia
Email: direccion@criminologia.pe
Web: www.criminologia.pe

Edición digital
Segunda edición, diciembre de 2023.

Imagen de portada: Canva
Diagramación: Ciudadanxs

Datos criminológicos es una serie de documentos de trabajo de divulgación dirigido por el Instituto de Criminología, con el objetivo de dar a conocer a la opinión pública, periodistas y tomadores de decisiones, datos clave sobre problemas asociados al delito y la violencia, en un lenguaje y formato comprensible por el público no especializado.

Citar como:

Instituto de Criminología y Estudios sobre la Violencia
El mercado negro de datos personales. Serie Datos criminológicos. N°02. Lima: ICEV. 2023
PRIVACIDAD / CRIMEN / MERCADO / PERÚ / CIBERSEGURIDAD / SEGURIDAD

El avance de la ciberdelincuencia

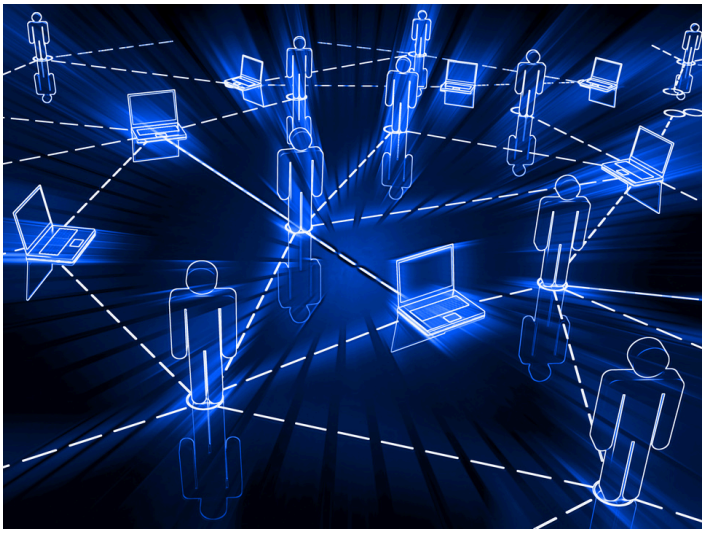
El constante avance de la tecnología, su uso masivo, y los altísimos niveles de interconexión, han generado un contexto en el que hay un dinámico flujo de información y datos personales circulando en diferentes sistemas. La delincuencia utiliza esos datos, adquiridos en el mercado negro, para generar prácticas criminales que van desde la extorsión, el fraude, la estafa y el hurto (además de una amplia modalidad de delitos sexuales on-line, y patrimoniales). En contraste, el Estado, en su lento desarrollo normativo, institucional, preventivo y persecutorio, no se acerca a la velocidad con la que evoluciona la delincuencia y el uso de TICs.

Cada mes, en Perú, se reportan más de 300 denuncias relacionadas con delitos informáticos, siendo los fraudes informáticos la categoría más frecuente. Los ciberdelincuentes emplean diversas modalidades, como la clonación de sitios web de entidades bancarias, compras ilícitas en línea y el uso de teléfonos móviles robados para ciberdelitos (El Peruano: 2023).

Algunos datos:

- Solo durante el 2022 “se registraron 2,382 denuncias por casos de fraude informático, convirtiéndolo en el delito informático más denunciado en el Perú a lo largo de 2022” (El Peruano: 2023).
- “Entre los años 2015 y 2019, el Poder Judicial condenó a 397 personas por la comisión de ciberdelitos previstos en la Ley de Delitos Informáticos” (DP: p.66), sin embargo, el subregistro es muy grande, pues, a pesar del carácter masivo de estos delitos, las denuncias representan solo el 2% de las registradas por el Ministerio Público en ese periodo (DP: p.66).
- El 2023 el Estado Peruano señaló los delitos que se han ampliado de manera más radical en nuestro país, entre ellos la extorsión y la ciberdelincuencia (“informáticos, estafas virtuales, y suplantaciones de identidad, entre otros que pueden afectar las finanzas de las víctimas” (Plataforma Digital Única del Estado Peruano. Dic, 23.)
- Asimismo, “la Unidad de Investigación Financiera del Perú (UIF), adscrita a la SBS, ha identificado los ciberdelitos como una amenaza emergente que agrava el lavado de activos en el país. El sector financiero sería el más afectado y la principal señal de alerta se relaciona con clientes que realizan operaciones frecuentes o significativas que no guardan correspondencia con su perfil económico” (DP: p.64)
- Hubo un cambio importante en la lógica de la ciberdelincuencia, pues “hasta hace poco, los ciberdelincuentes solían comunicarse directamente con la víctima para exigir un rescate de manera privada” (Andina: 2023), sin embargo, ahora utilizan la información privada tanto como mecanismo para realizar fraudes, estafas y extorsión, pero también como un bien para ser vendido en el mercado negro, “configurando una cuenta regresiva para la publicación de los datos robados”. La Policía señala que “esta tendencia continuará desarrollándose, porque es una táctica que beneficia a los ciberdelincuentes, ya sea que la víctima pague o no. Los datos a menudo se subastan, y la oferta de cierre a veces supera el rescate exigido” (Andina: 2023).

Vulnerabilidad de los sistemas informáticos del Estado



El Estado peruano posee diversos datos personales de la ciudadanía, tanto para el cumplimiento de sus funciones, como para la administración de los servicios públicos. Así, el Estado almacena información muy sensible, pero, no necesariamente sus sistemas de protección permiten tener siempre el debido cuidado. Solo en la última década, hubo cientos de vulneraciones a los servicios informáticos del Estado, que han implicado no solamente la penetración de sus bases de datos, vulneraciones en sus webs, sino también el hurto de información personal de la ciudadanía.

Es notorio que los sistemas de protección de las páginas web del Estado son limitados, y, también, que la protección de datos personales no ha sido eficaz. Las alertas de seguridad digital listan una enorme cantidad de casos que da cuenta de esta situación. Solo en el reporte del 2023 PCM señala 1) vulnerabilidades en "pfSense CE relacionadas con Cross-Site Scripting (XSS)" entre otras, las que "podrían haber sido utilizadas por posibles atacantes para interceptar comunicaciones o atacar servicios de red local" (PCM, 2023: p. 4); 2) vulnerabilidades críticas "de tipo deserialización de datos que no son de confianza (Path Traversal) y escritura fuera de límites en HPE vTeMIP", las que permitirían "a un atacante remoto corromper la memoria, desbordar la pila de memoria y realizar una denegación de servicio (DoS)" (PCM, 2023: 5); 3) vulnerabilidades críticas en "FortiMail de Fortinet Tipo de Ataque Explotación de vulnerabilidades conocidas Abreviatura EVC"; lo que "podría permitir a un atacante remoto no autenticado eludir el inicio de sesión de administrador a través de una solicitud HTTP maliciosa" (PCM, 2023: 6). Entre otras decenas de vulnerabilidades advertidas.

Casos de vulneración de los sistemas informáticos del Estado

Asimismo, hubo miles de vulneraciones a los sistemas informáticos del Estado. Los cientos de casos registrados son solo la punta del iceberg de un número no determinado de filtraciones, penetraciones, hurto de información, a diversas instituciones del Estado, que dan cuenta, no de casualidades o de vulneraciones ocasionales, sino del sistemático aprovechamiento de las debilidades digitales del sistema administrativo nacional, y del acceso de delincuentes cibernéticos a la información del Estado y a la data personal de la ciudadanía. Algunos de los casos más evidentes son los siguientes:

- Diciembre de 2023: "Tres tramitadores y tres funcionarios del Registro Nacional de Identidad y Estado Civil (Reniec) fueron detenidos tras ser acusados de cambiar la nacionalidad a ciudadanos extranjeros, por matar a procesados y resucitarlos con otra identidad, según reveló Cuarto Poder mediante un reportaje. (El Comercio, 2023)
- Junio de 2023: "En un preocupante episodio de violación de la privacidad, se ha descubierto una filtración masiva de datos personales de millones de ciudadanos peruanos. Estos datos fueron extraídos directamente de las bases de datos de (...) RENIEC (Registro Nacional de Identificación y Estado Civil), generando una situación de vulnerabilidad sin precedentes. Un grupo de Telegram y un bot conocido como @LEDER_DATA_BOT han sido identificados como los responsables de la distribución de esta información confidencial. (...) estos delincuentes cibernéticos exigen grandes sumas de dinero a cambio de proporcionar acceso a los datos filtrados". (Peru.gob.pe: 2023)
- Mayo de 2022: "Se detectó que delincuentes cibernéticos, a través de la Plataforma de Interoperabilidad del Estado Peruano (PIDE) (...) de la Presidencia del Consejo de Ministros, accedieron a las cuentas y claves de los usuarios de las instituciones públicas que cuentan con este servicio (RPP, 2022).
- Abril de 2022: Asbanc advirtió a PCM en varias ocasiones de "la comercialización de información altamente sensible que compromete los datos personales de un número considerable de personas (que) incluye el nombre, dirección, documento de identidad, datos de familiares, bienes, saldo deudor, huellas digitales, entre otros aspectos que pueden ser usados por estafadores" (RPP, 2022). Esta información habría sido hurtada a través de los servidores del Estado para ser difundida y vendida por delincuentes cibernéticos.

- Noviembre de 2020: “El viernes 13 de noviembre ocurrieron una serie de ataques cibernéticos contra el portal del Congreso peruano –así como contra otras páginas del Gobierno–, que dejaron la web del poder Legislativo inactiva durante varias horas”. (France24: 2020).
- Mayo de 2020: “Cerca de un millón de soles fueron robados por ciberdelincuentes, luego de haber hackeado el sistema del Registro Nacional de Identificación y Estado Civil (Reniec) para tener acceso a los datos personales de los beneficiarios del bono universal de 760 soles. Inicialmente, se informó que la web hackeada fue la del Ministerio de Desarrollo e Inclusión Social (Midis), pero la institución aclaró que fue el sistema de Reniec el afectado” (La República: 2020)
- Julio de 2018: “Entre octubre del año pasado y junio de este año, los nombres, apellidos, fecha de nacimiento, sexo y edad de todos los peruanos mayores de edad fueron accesibles y descargables a través de la página web de la ONPE. Un error informático en el formulario de inscripción de su Hackaton del año pasado, repetido en su más reciente versión, permitía a cualquier usuario de Internet descargar todos nuestros datos personales sin vulnerar ninguna medida de seguridad ni levantar ninguna alerta en ONPE”. (Hiperderecho: 2018)
- Julio de 2015: “El sitio web del Gobierno peruano www.peru.gob.pe fue hackeado este 28 de julio”. Se registró un ataque masivo a distintas páginas de entidades públicas con la consigna '#OpIndependencia' (Canal N: 2015)
- Junio de 2011. Hubo un ataque de varias horas al portal del Estado Peruano, las páginas del Ministerio de Economía, del Congreso de la República, de la Policía Nacional del Perú, de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y la de Servicios al Ciudadano y Empresas. Un grupo de hackers no identificados entró a los sistemas y se llevó información (OSIPTEL, 2011)

Las vulneraciones han sido muchas y los resultados han implicado la infiltración en bases de datos, hurto de información sensible y de datos personales de la ciudadanía. Tanto es así, que el propio Estado reconoció el problema y planteó una “Estrategia Nacional de Seguridad y Confianza Digital (ENSC)” para el periodo 2021-2026: “En este informe, se propone una estrategia para que el Estado Peruano ejecute el desarrollo (...) de una sociedad con confianza digital (...) para mitigar los riesgos digitales y brindar seguridad en los servicios digitales para los ciudadanos” (PCM: 2021); lo que, a todas luces, al día de hoy, no ha sido eficaz ni eficiente.

La venta de datos personales en la red

En los últimos años se ha desarrollado un mercado de venta de información privada, sobre todo en Internet. En los últimos diez años se ha determinado que esta práctica genera un severo problema para la seguridad de los países y de la ciudadanía (MIT: 2014) y se reporta un amplio y complejo mercado de venta en la Dark Web:

> “Nuestros datos personales tienen un gran valor en la red. Eso lo podemos confirmar si accedemos a la Dark Web y vemos cuentas de todo tipo a la venta. Los ciberdelincuentes constantemente lanzan ataques informáticos para robar información personal, contraseñas o simplemente provocar un mal funcionamiento en los sistemas”. (Redes Zone: 2022)

Lo cierto es que hay un flujo de datos personales sensibles que ciertas instituciones administran, por ejemplo, en el caso del sistema de salud o los datos que administran las empresas de telecomunicación. En contraste el Estado ha demostrado que no tiene capacidad ni para proteger sus propias bases de datos institucionales de ataques cibernéticos, y tampoco de proteger el flujo de información personal que resguardan las empresas. Se ha generado un "tráfico ilegal de datos personales" (La República: 2023) que no recibe ni la atención adecuada, ni la protección y seguridad que el Estado debería brindar.

> “El Fiscal Superior de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, Humberto Flores Cáceres, explicó que las técnicas más utilizadas por los delincuentes son la obtención de información por ingeniería social. Esta modalidad puede consistir en la compra de información estatal en mercados negros o el manejo de software para conseguir datos de tarjetas de crédito, tales como el código de seguridad y fecha de vencimiento, para efectuar consumos no reconocidos” (El Comercio: 2022).

OSIPTEL: su rol y debilidades para resguardar información personal

Las debilidades del Estado en torno a las capacidades para resguardar sus bases de datos y la información personal de la ciudadanía son claras. Esto no escapa a OSIPTEL (Organismo Supervisor de la Inversión Privada en Telecomunicaciones), entidad pública descentralizada adscrita a la PCM (Presidencia del Consejo de Ministros), que maneja vasta información privada de ciudadanos, y que reconoce que tiene limitaciones logísticas y operativas para proteger sus propios sistemas, pero también para la vigilancia de los miles de casos diarios asociados al uso de la telefonía en el país.

Si bien OSIPTEL ha publicado una política de protección de datos personales, esta no ofrece información puntual sobre medidas prácticas para resguardar nuestros datos (OSIPTEL: 2021).

- OSIPTEL tiene designada una Oficial de seguridad de la información, pero no hay claridad ni de cuantos miembros tiene su equipo, sus funciones, limitaciones; ni cuál es la brecha de capacidades para resguardar la información que actualmente tienen. Y si tendrían la capacidad para ampliar esas funciones.
- OSIPTEL reconoce debilidades en torno de los sistemas de protección de información personal, ciberseguridad o vigilancia en general. Es elocuente el párrafo: "el súbito giro hacia el uso de medios e interacciones virtuales ofreció oportunidades a la ciberdelincuencia." (OSIPTEL: 2023, p. 5)

Las amenazas a la seguridad cibernética y a la información personal de las operadoras de telefonía implican medidas concretas por parte del Estado. Sin embargo, es claro que hay una brecha de protección muy grande, y no se han desarrollado las capacidades para reducirla. Por el contrario, las amenazas parecen haber crecido, y las vulneraciones aumentado.

- Por ejemplo, "la venta informal y ambulatoria de líneas de telefonía móvil (...) puso en riesgo los datos personales de los usuarios (...). Así quedó demostrado al revisar los registros de abonados remitidos al OSIPTEL por las empresas operadoras, en los que no solo se registraron inconsistencias, sino casos en los que tanto nombres como tipos y números de documentos no coincidieron con los datos oficiales del RENIEC." (OSIPTEL: 2023, p. 5).
- Los propios sistemas de protección de OSIPTEL adolecen de las limitaciones de que tiene el Estado peruano en general. Por ende, no se tienen garantías claras de que esta información quede a buen recaudo; por el contrario, estaría sometida a las vulneraciones de la ciberdelincuencia, y al uso de esos datos para fines ilegales.

Con la aprobación del Dictamen del Proyecto de Ley 3752-2022, “Ley de desarrollo de las funciones y facultades del (...) OSIPTEL, fortaleciendo las facultades de decomiso de bienes vinculados a la infracción administrativa y otros”, la Comisión de Defensa del Consumidor y Organismos Reguladores de Servicios Públicos del Congreso de la República busca generar el acceso de OSIPTEL a datos personales de millones de usuarios para “fiscalizar” líneas telefónicas.

> "Articulo 6-A. Datos personales para fines de fiscalización de los servicios públicos de telecomunicaciones. El Osiptel puede solicitar a las empresas operadoras, bajo los alcances del artículo 14 de la Ley 29733, Ley de protección de dates personales, la remisión de información de datos personales relacionada a la prestación de los servicios públicos de telecomunicaciones. La información requerida es remitida por las empresas operadoras a través de mecanismos informáticos automatizados (...) (Comisión de Defensa del Consumidor y Organismos Reguladores de Servicios Públicos del Congreso de la República: 2023, p.26)

Es decir que, el Congreso de la República pretende poner a disposición de OSIPTEL toda la data existente en empresas privadas de telecomunicaciones, actualmente resguardada por la normativa de la materia. En vista de los datos disponibles y de la situación de precariedad de la seguridad informática, la posibilidad de que el Estado (OSIPTEL Y PCM), tengan acceso y administren más información de la ciudadanía, pone en riesgo de filtración la información personal y sensible de los y las peruanas; y los pone a merced de la ciberdelincuencia, que ha demostrado que ha podido aprovechar las notorias deficiencias de seguridad de los sistemas informáticos del Estado para obtener data privada, delinquir y vulnerar derechos de las personas.

Referencias

1) OSIPTEL (2011). Anonymous atacó 6 webs del Gobierno Peruano. En: https://www.gob.pe/institucion/osiptel/noticias/179224-anonymous-ataco-6-webs-del-gobierno-peruano
2) Canal N (2015). Hackearon el sitio web del Gobierno peruano. En: https://canaln.pe/actualidad/hackearon-sitio-web-gobierno-peruano-n191446
3) Hiperderecho (2018). ONPE filtró los datos personales de millones de peruanos durante más de medio año. En: https://hiperderecho.org/2018/07/onpe-filtrado-datos-hackaton/
4) La República (2020): Ciberdelincuentes hackearon el sistema del bono universal y robaron casi un millón de soles. En: https://larepublica.pe/sociedad/2020/05/28/bono-universal-ciberdelincuentes-hackean-web-y-roban-cerca-de-un-millon-de-soles-destinado-a-familias-en-pobreza
5) France24 (2020). Anonymous se atribuye el hackeo al Congreso peruano, mientras la crisis en el país se agudiza. En: https://www.france24.com/es/am%C3%A9rica-latina/20201115-peru-crisis-anonymous-congreso-manuel-merino
6) Presidencia del Consejo de Ministros (2021). Estrategia Nacional de Seguridad y Confianza Digital. PCM: 2021. En: https://www.gob.pe/institucion/pcm/informes-publicaciones/1998221-estrategia-nacional-de-seguridad-y-confianza-digital
7) Presidencia del Consejo de Ministros (2023). Alerta integrada de seguridad digital N° 296-2023-CNSD. En: https://www.gob.pe/institucion/pcm/informes-publicaciones/4937165-alerta-integrada-de-seguridad-digital-n-296-2023-cnsd
8) RPP (2022). Reniec detectó que filtración de datos se dio a través de la Plataforma de Interoperabilidad del Estado. En: https://rpp.pe/politica/gobierno/reniec-detecto-que-filtracion-de-datos-se-dio-a-traves-de-la-plataforma-de-interoperabilidad-del-estado-noticia-1406677]
9) RPP (2022). Asbanc advierte a la PCM sobre una filtración de datos personales a través de plataformas del Estado. En: https://rpp.pe/politica/gobierno/asbanc-advierte-sobre-filtracion-de-datos-personales-que-ponen-en-riesgo-transacciones-bancarias-noticia-1406457
10) MIT Technology Review (2014). Así funciona la compra venta de tu información privada: En: https://www.technologyreview.es/s/4453/asi-funciona-la-compra-venta-de-tu-informacion-privada
11) La República (2023). ¿Qué datos personales pueden vender las empresas? En: https://larepublica.pe/datos-lr/respuestas/2023/01/27/venta-de-datos-personales-en-peru-cuales-son-los-datos-personales-puede-vender-empresa-atmp-382965]
12) Redes Zone (2022). Así compran y venden tus datos en la Dark Web. En: https://www.redeszone.net/noticias/seguridad/venta-cuentas-robadas-dark-web/
13) OSIPTEL (2021). Política de Protección de Datos en OSIPTEL. En: https://www.osiptel.gob.pe/informacion-institucional/nuestras-politicas-principios-y-metodologia-de-trabajo/politica-de-proteccion-de-datos-personales-del-sistema-automatizado-de-medicion-del-osiptel/]
14) OSIPTEL (2022). Informe de evaluación de implementación anual del PEI. OSIPTEL: 2022. En: https://www.osiptel.gob.pe/media/ajohyqxd/informe-eval-resultados-pei-2022.pdf
15) El Comercio (2022). Extorsión y ciberdelincuencia: recomendaciones para evitar ser víctima de estas modalidades de robo. En: https://elcomercio.pe/lima/policiales/extorsion-y-ciberdelincuencia-recomendaciones-para-evitar-ser-victima-de-estas-modalidades-de-robo-video-ministerio-publico-pnp-rmmn-noticia
16) Defensoría del Pueblo (2023). La Ciberdelincuencia en el Perú: Estrategia y Retos del Estado. En: https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf
17) Gob.pe (2023). ¿Cuáles son los delitos más comunes en el Perú? En: https://www.gob.pe/en/25482-cuales-son-los-delitos-mas-comunes-en-el-peru].
18) Andina (2023). Extorsión, fugas de datos y ramsomware son las principales amenazas para empresas. En: https://andina.pe/agencia/noticia-extorsion-fugas-datos-y-ransomware-son-las-principales-ciberamenazas-para-empresas-926551.aspx]
19) El Peruano (2023). ¡Cuidado con los fraudes informáticos! En: https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru]
20) El Comercio (2015). El mercado negro de datos privados en el Perú. En: https://cde.3.elcomercio.pe/doc/0/1/0/4/8/1048400.pdf}
21) Access Now (2022). Lo mejor y lo peor para 2022: Leyes de protección de datos a nivel global. En: https://www.accessnow.org/leyes-proteccion-datos-global/
22) Gob.pe (2023) LEDERDATA: Filtración masiva de datos de millones peruanos sacados de las bases de datos de (...) RENIEC. En: https://www.gob.pe/institucion/muninasca/noticias/779883-lederdata-filtracion-masiva-de-datos-de-millones-de-peruanos-sacados-de-las-bases-de-datos-de-la-reniec

El mercado negro de datos personales

Serie *Datos criminológicos, Nº 2*