Columnas & Opinión

Revista Pensamiento Penal
Sección Medios digitales y delitos informáticos
Vol. 2, núm. 3 – 2025, págs. 109–115
ISSN: 1853 – 4554

El fenómeno del *doxing*

Análisis e implicancias

Por Augusto Appolinari[1]

El uso del «*doxing*» ha crecido exponencialmente con el auge y la diversificación de las plataformas de redes sociales en las últimas décadas, junto con la facilidad de acceso a información personal en línea, convirtiéndose en un fenómeno significativo dentro de la cultura digital contemporánea.

*doxing – extorsión digital – derecho informático – delitos informáticos – nuevas tecnologías*

* * * * * *

a. Introducción

En los tiempos que transcurren, las nuevas tecnologías informáticas forman parte de nuestra vida cotidiana, estando presentes durante todo el día y en todo momento. Esta es la era de los *macrodatos*, dónde una enorme cantidad de datos personales se encuentran dispersos surcando la magnitud de internet.

Parafraseando al célebre sociólogo y filósofo Zygmunt Bauman, habitamos un mundo líquido y multicéntrico, un mundo en el que, a través de diversas redes de información, nos conecta con las realidades de otras personas, otros países, sus culturas y circunstancias, muchas veces descuidando nuestra propia situación, de la cual creemos tener el control y dónde esta misma realidad nos demuestra que lo tenemos menos de lo que creemos.

Las presentes líneas pretenden explorar las dinámicas del mundo digital, centrándose en una de las prácticas que las nuevas generaciones han adoptado como habitual, y que en muchos casos se utiliza como un «arma» de ingeniería social para realizar ataques digitales mediante las nuevas formas de comunicación. En este artículo nos referiremos al llamado «doxeo» o «doxing».

Este análisis busca abordar el origen de esta práctica, su metodología, uso actual y análisis, así como los peligros a los que todo internauta está expuesto y consideraciones necesarias para reforzar nuestra seguridad informática.

El uso del «doxing» ha crecido exponencialmente con el auge y la diversificación de las plataformas de redes sociales en las últimas décadas, junto con la facilidad de acceso a información personal en línea, convirtiéndose en un fenómeno significativo dentro de la cultura digital contemporánea.

[1] Abogado graduado de la Facultad de Derecho de la Universidad Nacional de Rosario. Adscripto de la cátedra de Sociología General y del Derecho de la Facultad de Derecho, Universidad Nacional de Rosario. Correo electrónico: augustoappolinari@gmail.com

b. ¿Qué es el doxing?

El término «doxing» proviene de la palabra inglesa «documents» (documentos), más precisamente de su acrónimo («docs», referida también como «dox»), su traducción «exponer dox» describe a la práctica de recopilar y publicar información personal sobre una persona sin su consentimiento, a menudo con la intención de acosarla o perjudicarla[2]. Esta situación se ha vuelto común con el apogeo de internet y la utilización masiva de redes sociales, donde mucha información personal puede ser fácilmente accesible.

El procedimiento comienza por parte de un *doxer* o *hacker* que recopila a partir de información identificadora básica de una persona en línea hasta información sensible, pasando desde su nombre real, dirección particular, lugar y domicilio de trabajo, números de teléfono personales, información de cuentas bancarias y/o tarjetas de crédito y otros datos financieros, correspondencia privada, antecedentes penales, fotos personales y cualquier otra información personal que pueda conseguirse en la red[3]. El paso posterior que el doxer o hacker realiza es divulgar al público esta información sin el consentimiento de la víctima. Previo a este paso, puede existir una instancia dónde el mismo doxer se comunique con la victima a los fines de extorsionarlo antes de la publicación de los datos recopilados.

Los agentes que utilizan el «doxing» generalmente emplean técnicas «OSINT» también conocidas como «*inteligencia de fuentes abiertas*» con la cual recopilan información a través de herramientas permitidas que contienen datos públicos no preservados. Entre los fines del doxing suelen podemos distinguir:

a) Divulgar online información de identificación personal y privada de una persona.

b) Revelar información anteriormente desconocida de una persona privada online.

c) Divulgar información a una persona privada online que podría ser perjudicial para su reputación y la de sus socios personales o profesionales[4].

Esta práctica se popularizó en la década de 1990 en comunidades en línea y foros, donde los usuarios comenzaban a «sacar» (o «doxear») información sobre otros, a menudo como una forma de acoso o venganza. La evolución de plataformas de redes hizo que ingresemos cada vez más datos a internet, aceptemos términos y condiciones, muchas veces sin siquiera leer, con lo cual, dejamos muchísimos rastros o *huellas digitales* en la red con cada registro.

Todos estos datos pueden ser utilizados de manera malintencionada por personas que buscan, a través de una conducta dolosa, extorsionar a un tercero recopilando los datos, exponiéndolos y/o viralizándolos, con el objetivo de que la víctima sufra de un «*linchamiento digital*».

En el último tiempo el doxing se ha convertido en una herramienta utilizada en las denominadas *«batallas culturales»*, ya que los hackers rivales realizan ataques de doxing contra quienes tienen opiniones opuestas a su ideología. Los doxers buscan intensificar el conflicto que tienen con personas en línea llevándolo al mundo real y revelando información sensible de sus adversarios[5].

La información recopilada puede emplearse de manera intimidatoria. El doxing no solo tiene que ver con la disponibilidad de la información, sino con cómo se utiliza para acosar o generar temor en la víctima. Por ejemplo, una persona que conoce el domicilio de una persona puede poner en riesgo su seguridad o la de su familia, quien tenga su número de celular o correo electrónico puede inundarlo con mensajes que dificulten y entorpezcan la comunicación con el círculo laboral e íntimo de la persona.

[2] Argentina.gob.ar. (2025).
[3] Kaspersky. (s. f.).
[4] Godino-Aldavez & Aldavez, 2024.
[5] Kaspersky. (s. f.).

También la información puede utilizarse en casos de suplantación de identidad, es decir, cualquier persona con determinación y tiempo puede construir un perfil detallado de alguien. Esto resulta aún más sencillo si la víctima ha dejado su información relativamente accesible en línea.

Las razones detrás del doxing son diversas. En algunos casos, quienes lo realizan pueden sentirse agredidos o insultados por la persona que eligen como blanco y, como represalia, deciden buscar venganza. También puede ocurrir que alguien conocido por expresar opiniones controvertidas ataque a una persona con posturas opuestas. No obstante, esto suele suceder principalmente en debates con posiciones extremadamente polarizadas, más que en desacuerdos políticos comunes[6].

Si bien, muchos de estos datos han sido ingresados por nosotros mismos, muchos otros pueden provenir de robos de bases de datos, filtraciones de seguridad o intromisión de personas que abusando de sus poderes o funciones que le permiten ingresar a base de datos, las cuales venden o utilizan en desmedro de terceros.

Sin importar la razón detrás del accionar, el propósito central del doxing es vulnerar la privacidad de las personas, lo que puede generarles incomodidad e incluso llevar a sufrir graves consecuencias.

c. ¿Nuestros datos personales están protegidos?

En nuestro país existen diversas normas que regulan nuestra información personal, siendo la más relevante, la ley No. 25.326 de protección de datos personales y su decreto reglamentario No. 1558/2001.

Es importante, como punto de partida, destacar en dicha ley, su segundo artículo distingue los conceptos de datos personales como aquella «información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables». y datos sensibles, como «datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual».

Todos estos datos, indistintamente, pero por preferencia de los doxers, aquellos datos sensibles, son el foco del objetivo de estos ataques recopilatorios, los cuales dejan en un estado de vulnerabilidad a la víctima, que queda expuesta ante el infinito público que puede tener una exposición en internet.

El inciso séptimo del artículo 4 de la mencionada ley hace referencia a que «[l]os datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados». Esto es muy importante, ya que ese dato que cumplió su función queda como parte de un residuo digital, el cual sigue merodeando el espectro de la red. Ahora bien, el incumplimiento de este inciso se da por parte de las corporaciones a las cuales el débito de este inciso interpela y en la mayoría de los casos, no lo cumplen.

Es interesante destacar lo establecido en el primer inciso del artículo 5 «[e]l tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias».

Aquí el problema reside, que muchas veces, como mencionaba anteriormente, al momento de registrarnos en determinadas redes o servicios informáticos, firmamos y aceptamos un acuerdo de «términos y condiciones» que, a razón de sinceridad, pocas veces leemos, y que si lo hacemos probablemente nos sorprendamos de la cantidad de datos personales que se recopilan y autorizamos dicha recopilación. Ahí es cuando comienza el dilema moral, de si realmente necesitamos esa red, servicio, etc. y queda en nuestra consideración aceptar y seguir adelante (entendiendo las consecuencias) o descartar el registro. Lamentablemente no existe la posibilidad de negociar individualmente con la plataforma que se recopila, y que no.

[6] Kaspersky (s. f.).

Así mismo, el inciso 2c de dicho artículo excluye al consentimiento para recabar los siguientes datos «[s]e trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio».

Por su parte, los artículos 13 y 14 de la presente ley regulan tanto el derecho a la información como al acceso de los datos registrados. Disponen los artículos mencionados «[t]oda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables», «El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes».

En síntesis, toda persona, acreditando fehacientemente su identidad tiene derecho a exigir información sobre la existencia todo tipo de registros, sin importar si el banco de datos es público o privado.

Por su parte, el artículo 16 establece supuestos que garantizan el derecho de los titulares de datos personales a rectificar, actualizar, suprimir o someter a confidencialidad sus datos en un banco de datos, estableciendo también las obligaciones del responsable del tratamiento.

El mismo refleja el principio de *autodeterminación informativa*, eje central del derecho a la protección de datos, el cual consiste en la posibilidad que tiene el titular de los datos personales de controlar quienes serán destinatarios de dicha información y qué uso le darán, y se ejercita a través de los derechos de acceso, rectificación y cancelación[7].

por último, la ley 25.326 sistematiza, a partir del artículo 33 y subsiguientes, una herramienta efectiva a la hora de tutelar la protección de los datos personales y es la figura del *habeas data*, el cual significa «tiene sus datos» y lo que tiende a proteger es la privacidad o intimidad de las personas.

Dicha institución constituye una acción judicial que permite a cualquier persona proteger su derecho a la privacidad y al control sobre sus datos personales, y se encuentra amparado por el artículo 43 de la constitución nacional, además de la ley que analizamos.

Esta herramienta permite a los individuos acceder a la información, es decir, tomar conocimiento de sus datos personales asentados en bases de datos, qué datos personales están siendo recolectados, almacenados o tratados por bancos de datos públicos o privados. Admite rectificar o actualizar, corregir datos incorrectos, desactualizados o incompletos, suprimir o bloquear, y eliminar datos cuando su tratamiento sea ilegítimo o innecesario, salvo excepciones legales. Esta acción garantiza la autodeterminación informativa, protegiendo la intimidad de las personas y evitando abusos en el manejo de datos personales, clave en un contexto de creciente digitalización y recolección masiva de información[8].

d. ¿Qué es la extorsión digital?

Según expertos de ciberseguridad, la extorsión cibernética es una forma generalizada de delito cibernético en la que los cibercriminales

> chantajean digitalmente a organizaciones o personas para obtener lo que quieren. Los cibercriminales pueden amenazar con filtrar datos, lanzar ataques cibernéticos, deshabilitar operaciones, evitar que los usuarios accedan a los datos o destruir los datos robados si la víctima no paga algún tipo de rescate.

[7] Molina Quiroga, 2003.

[8] Fernandez Delpech, 2014.

La extorsión cibernética hace uso de numerosos métodos, uno de ellos, el doxing[9].

e. ¿Cómo protegernos del doxing?

De acuerdo a profesionales de seguridad informática, todos los usuarios están expuestos a ser víctimas de doxing, teniendo en cuenta la facilidad de la búsqueda de información en línea. Cualquier publicación hecha en un foro, participaciones en redes sociales, entre otras, se encuentra disponible de manera pública, como así también cualquier búsqueda que se realice en una base o registro público.

Algunas de las recomendaciones para proteger la información son a través de las siguientes medidas:

a) manejo de VPN o red privada virtual: constituye en el cifrado de la conexión y su encriptación, antes de dirigir a la red pública, lo cual permite al usuario navegar de forma segura y anónima.
b) utilización de contraseñas seguras, las cuales deben ser renovadas periódicamente, así como también la adhesión a métodos de factores de doble autenticación.
c) uso de software antivirus y antimalware, como método de detección temprana de intromisiones no deseadas.
d) revisión de privacidad de redes sociales y de datos recopilados, evaluación de configuración y datos que requiere cada plataforma.
e) eliminación de perfiles obsoletos, aquellos perfiles de redes que el usuario ya no utiliza, siguen siendo visibles y contienen información personal, en caso de ser posible, la recomendación es de eliminarlos[10].

Todas estas acciones pueden completarse con una búsqueda de imagen inversa, es decir, controlar a través de un buscador de confianza todos los datos personales que se encuentran expuestos en internet, revisar que datos se encuentran en línea y reforzar la seguridad de las redes o sitios que contienen dichos datos.

f. Conclusiones

En nuestro país, el fenómeno del doxing ha cobrado relevancia en los últimos años, especialmente en el contexto de la creciente violencia digital y el acoso en línea a través de diversas plataformas. Actualmente no existen leyes en nuestro ordenamiento jurídico específicas que tipifiquen penalmente y aborden la problemática como tal, es por ello que este acto actualmente es denunciado bajo otras figuras dependiendo el grado de intromisión y exposición.

Teniendo en cuenta que tanto la legislación actual, como la actuación de los diversos operadores, son insuficientes para ofrecer una protección efectiva a las víctimas o para prevenir estos ataques, es imperiosa la necesidad de tomar las riendas y abordar la temática desde una perspectiva legal y educativa, la cual es fundamental para proteger a las potenciales víctimas y mitigar el impacto negativo que estas prácticas pueden tener en la sociedad.

La falta de una figura específica que contemple al doxing y sus consecuencias, además es un llamado de atención a nuestros legisladores, los cuales deben comenzar a debatir, para regular e implementar estrategias más robustas que incluyan educación sobre ciberseguridad y derechos digitales, tomando en consideración que esta problemática refleja un inconveniente aún más amplio de violencia digital y acoso en línea. Es menester poner cartas sobre la mesa, ya que serán más los casos avizorando el acelerado desarrollo de la sociedad de la información que habitamos.

[9] Keeper Security, 2024.
[10] Kaspersky. (s. f.)

g. Bibliografía

Argentina.gob.ar. (2025, junio). *¿Qué es el doxing y cómo podemos cuidarnos?* Ministerio de Justicia. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-doxing-y-como-podemos-cuidarnos (recuperado 27/10/2024)

Kaspersky. (s. f.). *Doxing: Definición y explicación.* Kaspersky. https://latam.kaspersky.com/resource-center/definitions/what-is-doxing (recuperado 27/10/2024)

Godino-Aldavez, F., & Aldavez, M. L. (2024). *Doxing: Avance de las nuevas tecnologías y su falta de regulación en el ordenamiento jurídico argentino.* Hammurabi. https://www.hammurabi.com.ar/godino-aldavez-doxing-avance-de-las-nuevas/ (recuperado 27/10/2024)

Molina Quiroga, E. (2003). *Protección de datos personales como derecho autónomo: Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material.* Sistema Argentino de Información Jurídica (SAIJ). http://www.saij.gob.ar/eduardo-molina-quiroga-proteccion-datos-personales-como-derecho-autonomo-principios-rectores-informes-solvencia-crediticia-uso-arbitrario-dano-moral-material-dacc030027-2003/123456789-0abc-defg7200-30ccanirtcod (recuperado 29/11/2024)

Fernandez Delpech, A. (2014). *Manual de derecho informático*. Abeledo Perrot.

Keeper Security. (2024, 15 enero). *What is cyber-extortion?* Keeper Security. https://www.keepersecurity.com/blog/es/2024/01/15/what-is-cyber-extortion/ (recuperado 27/10/2024)