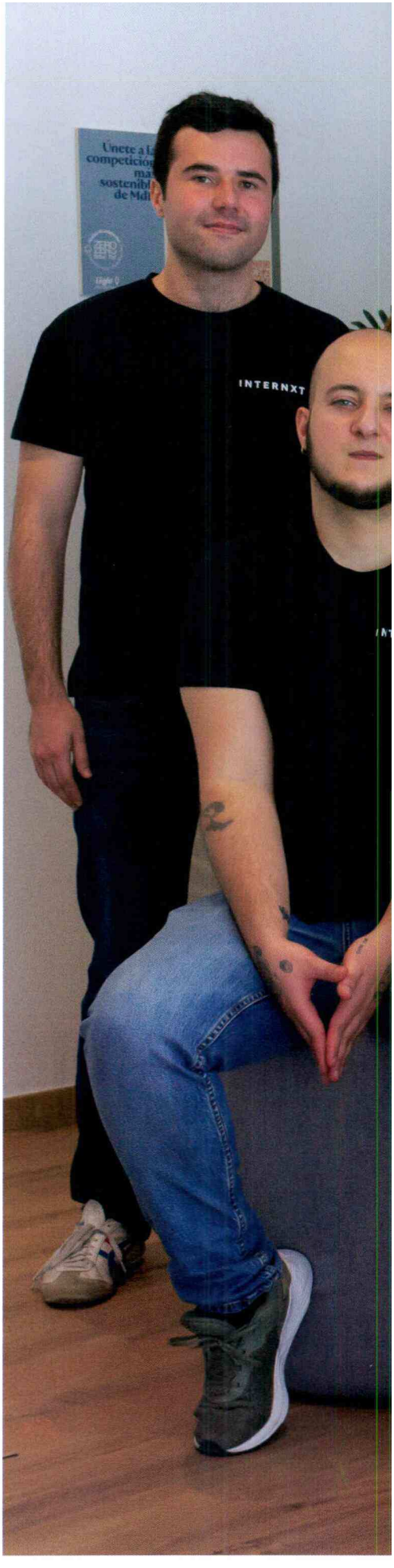
CIBERSEGURIDAD, un desafío del que no escapa nadie

Los datos son el activo más codiciado en la red, tanto por las empresas como por los ciberdelincuentes

POR **ANA DELGADO** @anadelgadoam



Casos de ciberataques tan notorios como los sufridos por instituciones de la talla de Iberdrola o el Servicio Público de Empleo (SEPE) o, más recientemente, escándalos como el caso Pegasus, ponen de manifiesto la importancia de tomarse en serio la ciberseguridad. Se equivoca quien piense que esto no va con él.

A mayor digitalización, mayor vulnerabilidad, un problema que atañe a todos y que corresponde solucionar a la ciberseguridad. Hablamos de un sector muy transversal, un habilitador que todo desarrollo tecnológico debe tener ya en cuenta desde la base.

Existen estudios que afirman que la ciberdelincuencia mueve ya más dinero que el narcotráfico o la pornografía en el mundo, con la particularidad añadida de que, en este tipo de delitos, la capacidad de hacer daño es más fácil que la de defenderse. Cualquier organización mal intencionada podría contratar a bajo coste los servicios de un *hacker* y hacerse con los datos sensibles para extorsionar a una empresa a cambio de un rescate.

Pero tampoco hace falta apuntar tan alto. El Incibe (Instituto Nacional de Ciberseguridad) gestionó el año pasado 109.126 incidentes de ciberseguridad, 90.168 de los cuales corresponden a ciudadanos y a empresas. En cuanto a su tipología, el 29,88% fueron *malware*, un *software* malicioso diseñado para infiltrarse en un dispositivo sin el conocimiento del usuario, muchas veces a través de descargas de aplicaciones o enlaces incluidos en un *email*.

La Comunitat, referente

Pionera en esta materia es la Comunitat Valenciana destacando entre las más avanzadas del país al disponer, desde el año 2007, de la Unidad de Ciberseguridad (CSIRT-CV), un servicio que atiende a todas las administraciones e instituciones públicas valencianas, puesto en valor como modelo de éxito en numerosas ocasiones.

El CSIRT-CV consiguió frenar y gestionar durante el año 2021 un total de 1.428 incidencias vinculadas a ciberataques, entre las que destacan 373 campañas de *phishing* detectadas en las 72 intervenciones relacionadas con suplantaciones de identidad, o siete intervenciones relacionadas con *ransomware* el tipo de ciberataque que sufrió el Hospital General Universitario de Valencia en plena pandemia.

Concienciadas de los riesgos que corren al dejar brechas abiertas, instituciones y empresas se apresuran a implementar medidas de ciberseguridad, au-

El equipo de Internxt con su fundador Fran Villalba (al fondo, en el centro).

mentando los recursos a tal fin. En esta línea, el Gobierno de la nación aprobó una inversión de 224 millones de euros en compra pública innovadora en materia de ciberseguridad.

Ello ha provocado un movimiento de los ciberdelitos hacia los ciudadanos normales y corrientes, víctimas bastante más incautas y desprotegidas. Las redes sociales son un campo propicio para actuar. Dentro de lo que se conoce como ingeniería social, LinkedIn encabeza ahora la clasificación, al haber acaparado más de la mitad (52%) de los intentos de *phishing* durante el primer trimestre del año. Esta técnica consiste en ganarse la confianza de la víctima haciéndose pasar por una persona, empresa o servicio de confianza, para que comparta información confidencial como contraseñas, DNI o números de tarjetas de crédito.

Los datos privados son, pues, el activo más codiciado en el ciberespacio. Los ciudadanos tienen hoy más probabilidades de sufrir un fraude por internet que de un atraco en la calle, con el agravante de que el ataque puede proceder de cualquier lugar del mundo. El robo de información personal tiene siempre el mismo objetivo: la obtención de dinero. Tanto pueden venderse los datos a un tercero, como abrirse una cuenta bancaria con una identidad suplantada, hacer compras *online* o chantajear a una persona.

La red social LinkedIn encabeza la clasificación al haber acaparado más de la mitad (52%) de los intentos de *phishing*

Soluciones propias

Pero no son solo los delincuentes los que se interesan por acumular datos. Son también el alimento que nutre a toda la industria del marketing digital; la base del machine *learning*, el *big data* y la inteligencia artificial. Todos quieren saber cómo nos comportamos.

Para preservar la privacidad de los datos de los ciudadanos, la idea que tuvo el joven valenciano Fran Villalba Segarra fue crear una solución de almacenamiento en la nube cifrado de extremo a extremo. Esta permite al usuario ser poseedor de la única llave que da acceso a sus contenidos encriptados y fragmentados. A esto se dedican en Internxt.

Cuenta Villalba que lo que le empujó a crear la empresa fue el deseo «de recuperar la privacidad de los usuarios, creando una alternativa a Google, Amazon o cualquier otro navegador de uso masivo de las grandes tecnológicas. Internet está controlado por cuatro empresas que tienen toda la información y han sobrepasado el límite. Ofrecen servicios en apariencia gratuitos, pero que acaban teniendo un alto valor y que les permite recabar toda la información, muchísima más de la necesaria».

La startup fundada por Villalba en 2020 cuenta ya con más de 300.000 clientes en todo el mundo, un equipo de veintitrés personas y está valorada en 40 millones de euros. Entre sus inversores figuran nombres como los de Juan Roig —propietario del 10%—, la escuela de negocios Esade, The Venture City, Telefónica —a través de Wayra— o Balaji Srinivasan, antiguo CTO del *exchange* Coinbase.

Desde su creación, Internxt se ha posicionado como una de las startups con mayor proyección internacional en el ámbito

Josep Coll (centro), con sus socios de RepScan

tecnológico. También Monad, cofundada en San Francisco por el valenciano Christian García Almenar, se revela como otra startup muy prometedora en materia de ciberseguridad, en este caso con soluciones orientadas al mundo corporativo.

Piratería, injurias, calumnias...

Otro de los problemas que plantea la red es su enorme memoria. Internet ni olvida ni perdona, pero tampoco permite a los usuarios la opción de controlar lo que se dice de ellos, sea verdad o mentira. Si a alguien le da por difamar el nombre o la imagen digital de cualquier persona o empresa, tiene más posibilidades de ganar que el ultrajado. Se puede reclamar por vía judicial, obviamente, pero siempre que estemos dispuestos a adentrarnos en un proceso complejo, lento, costoso y de resultado incierto.

Pedro Durán, creador de La tienda del espía, es uno de los pocos que en España se atrevieron a denunciar a Google. Acusó a la tecnológica de «traficar con las marcas» e ignorar la protección del titular original a favor de los falsificadores que más invierten en Google Ads. El juicio no lo ganó, pero Durán está convencido de que fue «por ser una empresa pequeña y carecer de un equipo de abogados a la altura de los de Google».

Según la alicantina Luzentrum, «no llegarán a un 30 o 40% las empresas que cumplan la normativa de protección de datos»

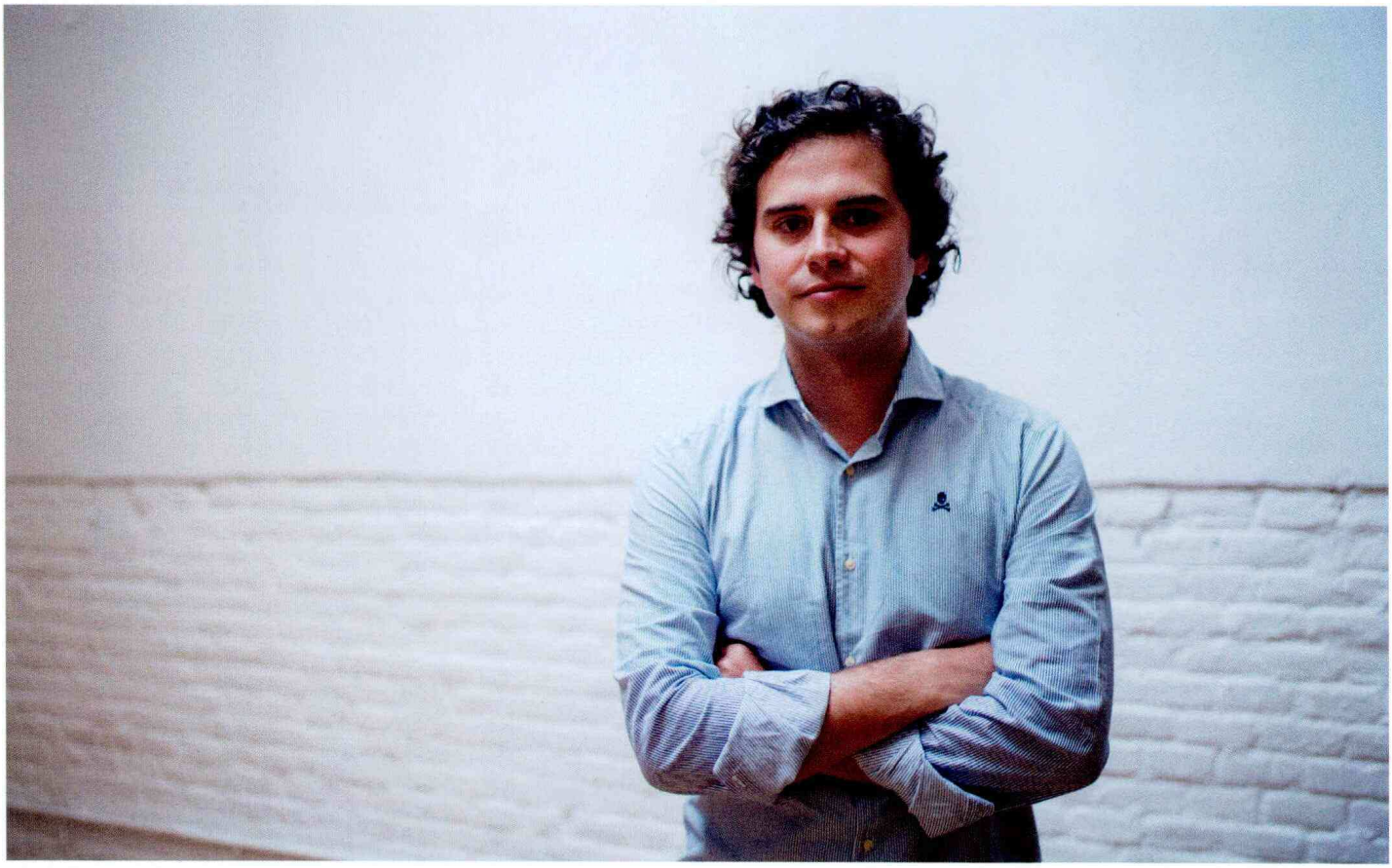
Para defender a las marcas de la piratería y las falsificaciones, creó Josep Coll la startup Red Points, hoy capitaneada por Laura Urquizu. Se trata de una plataforma que rastrea y elimina de la red a posibles falsificadores que venden imitaciones en nombre de la empresa original.

Tras abandonar la dirección de Red Points, Josep Coll ha fundado una nueva startup, RepScan, esta con el foco puesto en el derecho al olvido y en permitir a las personas eliminar de la red contenidos indeseados sobre ellos (fotografías, datos, vídeos o contenido falso). «Antes de RepScan, las personas no tenían el control sobre lo que acerca de ellos se decía o aparecía en Internet. Esto está pasando factura a muchas personas, tanto en su vida personal como profesional», dice Coll, quien añade que las mujeres suelen padecer más chantajes de este tipo que los hombres.

La obligación de las empresas

Hace más de tres años que todas las empresas españolas deberían haber adaptado sus espacios digitales al nuevo Reglamento General de Protección de Datos (RGPD) con amenaza de sanción por el uso incorrecto de los mismos. Son pues responsables de velar por la seguridad de los datos que recopilan. Las multas no son pequeñas, van desde 900 euros por una falta hasta el 4% de la facturación de la empresa con un máximo de 20 millones de euros.

Sin embargo, y según afirma Arroniz, responsable de la empresa alicantina Luzentrum, «no llegarán a un 30 o 40% las empresas españolas que cumplan con la normativa de la protección de datos». Ajustarse al cumplimiento de la ley serviría para demostrar la buena fe en el supuesto de que la empresa padeciese un ciberataque de sustracción de datos o suplantación de identidad.



Christian García Almenar, fundador de Monad. KIKE TABERNER