El fraude online y la biometría como respuesta de confianza

La cada día mayor digitalización de la sociedad ha transformado nuestro modo de trabajar, estudiar, relacionarnos y, como no, adquirir y contratar productos y servicios de cualquier tipo, todo ello con Internet como común denominador.

Un escenario que se aceleraba sin duda con la pandemia y en el que las ventajas son múltiples (inmediatez, comodidad o globalidad, entre otras) pero que también conlleva riesgos. De hecho, según el Instituto Nacional de Ciberseguridad (INCIBE), de los casi 110.000 incidentes de ciberseguridad registrados en España el año pasado, un 28,6% fueron intentos de fraude, entendido como el uso de tecnologías y servicios por usuarios no autorizados, mediante suplantación de identidad u otros engaños económicos. Más de 90.000 ciudadanos y empresas fueron afectados por estos delitos.

“Los problemas que tenemos en el mundo digital no son nuevos, aunque hay gente que piensa que sí. Son los mismos que tenemos en el mundo físico. Lo único nuevo es que ahora todo es más inmediato, hay miles de operaciones por segundo…”, afirma **Raúl Sánchez Reíllo, del Grupo Universitario de Tecnologías de Identificación (GUTI) UC3M** y uno de los mayores referentes en biometría.

Y es que, sin duda, el fraude y el engaño siempre han existido, pero como señalábamos, la entrada en juego de la banca online, el comercio electrónico y los pagos en Internet no han hecho sino derivar esta clase de delitos hacia el mundo cibernético, en el que las fronteras diluidas y las complejidades derivadas de los avances de los ciberdelincuentes dificultan enormemente la investigación policial y la positiva resolución de estos incidentes.

Ante esta situación, se hace imperativo dotar de confianza a la parte más básica de todos estos campos y negocios online, un desafío en el que, incluso, es necesario repensar algo tan básico como los contratos.

Ese es precisamente el campo de estudio de **Natalia Mato**, investigadora del **Departamento de Derecho Privado** de la UC3M y líder del proyecto "Optimización de la transparencia en los contratos online" de la Fundación Ramón Areces, que, en este nuevo mundo online, trata de “garantizar que los procesos de contratación online de consumo sean transparentes para el consumidor y eficientes para los empresarios”.

Una transparencia que, pese a la multitud de normas que existen tanto a nivel nacional como europeo, no siempre se da. “Trabajamos para proponer un diseño del proceso de contratación online que sea óptimo en términos de garantías para el consumidor pero también eficiente para la marca o empresa. Que cumpla con todos los requisitos legales, que resulte comprensible y transparente para el usuario

y que, al mismo tiempo, beneficie a la empresa, porque genere una mayor sensación de confianza/seguridad en el usuario que va a contratar un producto o servicio con ellos".

Un reto en el que, además de la información que se proporciona, también es necesario analizar el modo en el que está dispuesta esa información en la propia página web, con qué lenguaje o con qué colores e iconos, etc. "Son los llamados "patrones oscuros", diseños pensados precisamente para dirigirnos a donde ellos quieren que vayamos, por ejemplo, situando la casilla en la que das el consentimiento o no a que utilicen tus datos personales lo más abajo posible de la web. De hecho ya hay estudios que señalan que este tipo de patrones oscuros pueden hacer que se duplique por ejemplo el número de consentimientos que obtiene una página web determinada y esto también habría que controlarlo de algún modo", apunta Natalia Mato.

Pero la lista de los riesgos que conlleva el mundo online no se queda ahí. Es necesario tener en cuenta también el negocio paralelo que determinadas marca o proveedores hacen precisamente con esos datos que el consumidor "consiente" en que se almacenen y exploten, "generalmente porque no entiende lo que le están diciendo o por la "fatiga" que le supone leer la excesiva información que muchas veces encuentra", recalca Mato.

"Es que muchas veces, por ejemplo, tu solo quieres leer el periódico y para ello debes responder que sí o que no a más de 15 cuestiones de lo más variopintas, pero sobre todo, que no entiendes, conceptos que no conoces… Y acabas diciendo a todo que sí. Y es que al final, en el mundo online lo que debemos tener claro es que si algo es gratuito es porque el producto eres tú, es decir, tu información", coincide Raúl Sánchez Reíllo.

Otro punto oscuro de las transacciones online lo encontramos en la responsabilidad de la calidad de los productos que adquirimos, especialmente, cuando el consumidor realiza esa compra en los llamados marketplaces como pueden ser Aliexpress o Amazon.

Ese es el objeto de la investigación que en este caso realiza **Isabel Antón, del Grupo ACCURSIO de Derecho Privado de la UC3M.**

"Uno de los aspectos de nuestro estudio sobre "Infracción de un derecho de marca en plataformas de e-commerce: la actuación de la plataforma y el impacto en su responsabilidad" ha sido en relación con la responsabilidad de esas plataformas que no sólo facilitan los aspectos técnicos para que terceros (normalmente pequeños empresarios, minoristas) vendan productos a través de dichas plataformas, sino que también participan en todo el proceso de logística y distribución. Por un lado, son un intermediario que permite que otros vendan productos en su plataforma, pero al mismo tiempo, tienen un papel muy activo, almacenando, empaquetando y enviando productos de terceros que quieren vender a través de su plataforma", explica Isabel Antón.

La cuestión que la investigadora plantea en su investigación es qué sucede cuando esos productos que terceros quieren vender a través de su plataforma y que la misma se encarga de almacenar, empaquetar, enviar, hacer publicidad, etc. infringen derechos de marca o son directamente productos

falsos, ¿quién es el infractor? ¿El tercero que le ha dado los productos a la plataforma? ¿La propia plataforma porque su labor va más allá de la de un mero intermediario?

Y ella misma nos da la respuesta: “El Reglamento 2022/1925 sobre mercados digitales aprobado hace apenas unos meses cambia aspectos regulados en normativa anterior sobre la responsabilidad de las plataformas; veremos que sucede cuando se comience a aplicar a partir de mayo de 2023. Lo que está claro es que habrá cambios, sobre todo para las grandes plataformas de e-commerce ya que con este nuevo Reglamento la plataforma alberga unas obligaciones que antes no tenía en materias muy diversas: desde la publicidad, la protección de datos y también en relación con el comercio online. Obligaciones que van orientadas a que la plataforma tenga un papel mucho más activo cuando sabe que en su plataforma se están vendiendo productos que infringen derechos de marcas actúe y si no lo hace, pueda ser responsable por ello”.

Biometría, identidad digital y, sobre todo, educación

Este escenario de absoluto caos, como lo califica Raúl Sánchez Reíllo, obliga no solo a un nuevo marco legal sino también a identificar soluciones tecnológicas que permiten luchar contra el fraude online.

En ese sentido, encontramos las tecnologías biométricas como una respuesta proporcional que puede luchar contra ese fraude sin imponer excesivas fricciones a la experiencia de usuario. Pero hay más: abrir una cuenta solo con un *selfie*, entrar en un estadio acercando la cara a una cámara o comprobar la identidad de una persona en la frontera de un aeropuerto tan solo con sus rasgos faciales, todas ellas son algunas de las últimas aplicaciones desarrolladas a partir de biometría.

El uso de la identificación biométrica se impondrá en nuevos sectores como el inmobiliario **reconoce Manuel Ignacio Feliú Rey**, investigador del **Grupo de Derecho Inmobiliario, Registral y de la Edificación (DERINRE)**, en el que analiza el impacto en este sector de las nuevas tecnologías (Inteligencia Artificial, Internet de las cosas, Big Data, Blockchain...). Además, este grupo con foco internacional e interdisciplinar (formado por expertos en Derecho inmobiliario y arquitectos) cuenta con el Laboratorio de Derecho Inmobiliario y Tecnologías Inteligentes (LabDINTEC) como espacio de divulgación del conocimiento relacionado con el proceso edificatorio y las nuevas tecnologías con especial sensibilidad por la accesibilidad y combatir la brecha de género.

La biometría ha cambiado enormemente en la última década, con uno de los puntos fundamentales en este camino siendo la aparición de tecnologías de redes neuronales e inteligencia artificial. Además, cada vez más la industria tiene en cuenta la privacidad desde el diseño, la proporcionalidad y la posibilidad de que la persona afectada por él sea capaz de controlar sus datos en todo momento, solventando así las reticencias naturales de utilizar nuestro cuerpo como fuente misma de datos de manera consciente.

Y es esa evolución de la biometría el ámbito de la investigación de **Carmen Peláez-Moreno, del Grupo de Procesado Multimedia (GPM) de la UC3M**: “Si bien es cierto que los sistemas biométricos han aumentado su fiabilidad considerablemente gracias a los avances del aprendizaje profundo, los requisitos de fiabilidad suelen ser muy estrictos debido a que las aplicaciones en las que se suelen usar son muy sensibles. Las consecuencias de los errores, aunque sean muy reducidos, son muy graves y eso eleva los requisitos de robustez. Por otra parte, estos sistemas suelen experimentar una gran variabilidad de prestaciones entre personas debido tanto a factores intrínsecos (características específicas de cada persona) como extrínsecos (representatividad y cobertura de la diversidad que hacen las bases de datos disponibles)”, explica.

Por eso, señala Peláez-Moreno, “están cobrando fuerza los sistemas biométricos multimodales en los que se combinan varias modalidades para obtener mayor fiabilidad que pueden aportar también una mayor atención a la diversidad. En los proyectos EMPATÍA y SAPIENTIAE4Bindi nos concentramos en el reconocimiento de locutor con redes neuronales haciendo hincapié en la robustez de esos sistemas a condiciones de habla ruidosas, pero también a sus requisitos computacionales buscando soluciones que puedan ser implementadas en dispositivos portables”.

En ello trabaja **el grupo COSEC (Computer Security Group) UC3M**, que cuenta con dos investigadores, **Carmen Cámara y Pedro Peris-López,** dedicados a la implementación de soluciones biométricas en diferentes escenarios. “Algunos ejemplos son: diseño, implementación y verificación de protocolos de identificación y autenticación continúa basados en bioseñales (ECG, EEG, PPG, GSR, TEMP, etc.) o el diseño de mecanismos de protección de la privacidad en señales neuronales”, explican.

Los trabajos realizados requieren técnicas avanzadas de procesamiento de señal, machine learning y aprendizaje profundo, así como sólidos conocimientos en el diseño y verificación de protocolos criptográficos. “Dos de los últimos proyectos dirigidos por estos investigadores en los que abordan estos conceptos son CARDIOSEC (dedicado a la ciberseguridad para Dispositivos Cardiacos Implantables junto a la Fundación BBVA) y CIOMET (centrado en Ciberseguridad, Salud, Infraestructura médica conectada, de la mano del Ministerio de Ciencia e Innovación.

En ese camino hacia la tecnología o tecnologías que mejor puedan ayudar a luchar contra el fraude online también se sitúa Raúl Sánchez Reíllo, que apunta que lo realmente importante es “forzar a que las herramientas que se utilicen sean herramientas validadas y certificadas; y si el fabricante o proveedor del servicio decide utilizar herramientas que no estén certificadas, que corra con todos los gastos que puedan darse si se produce un fraude”.

Así defiende los métodos de identificación oficiales, como el ¨wallet” de identificación digital europeo en el que se está trabajando o la revisión que se está realizando del EIDAS, el reglamento europeo de identificación digital.

“No sé si hay una solución perfecta pero sí sé que no hay una solución fácil y rápida. Y la clave está en la educación, en que seamos conscientes de los riesgos que corremos en el mundo online”, apunta en ese sentido y como conclusión Natalia Mato.

Algo en lo que también coincide Sánchez Reíllo: “Solo mediante educación la gente puede llegar a ser consciente de los riesgos que corre en lo que hace en su día a día. Y eso es muy importante porque incluso el más “paranoico” respecto a la seguridad online acaba eligiendo la comodidad y la rapidez. Por ejemplo, hay gente que piensa que el pago móvil es igual seguro que pagar con la tarjeta de crédito o débito e incluso gente que piensa que es más seguro ya que puedes perder la tarjeta y no darte cuenta, pero si pierdes el móvil sí, te das cuenta al instante. Pero nadie se plantea cómo se puede acceder a ese método de pago, si tienes que desbloquear la pantalla o no, qué método utilizas para desbloquearla y mucho menos que hay aplicaciones que entran en tu móvil y directamente utilizan tu medio de pago. La gente lo que quiere es con solo hacer click comprar o pagar algo. El primer mayor enemigo de la seguridad online, por desgracia, es el ciudadano y por eso los expertos (también en lo legal), frente a esta vulnerabilidad completa del ciudadano deben tratar de protegerlo, aunque eso muchas veces pase por hacerle las cosas más complicadas”.

Biomarcadores funcionales

El uso de la biometría en el campo de la ciberseguridad es una tendencia en auge en los últimos años, pero no podemos obviar su recorrido en el camino de la sanidad y nuestra propia calidad de vida. En ese sentido encontramos proyectos como el que lleva a cabo **María Durbán, investigadora del Departamento de Estadística de la Universidad Carlos III de Madrid.**

“Estoy trabajando en un proyecto cuyo objetivo es la predicción de la edad biológica como un marcador de envejecimiento alternativo a la edad cronológica. La edad biológica se refiere a la situación actual del sujeto en relación con su ciclo vital potencial”, explica la experta. “Podría definirse como el desgaste real de las energías producto del paso de los años. Tiene en cuenta los cambios físicos y biológicos que se van produciendo en las estructuras celulares, de tejidos, órganos y sistemas. Es solo cuestión de tiempo que, en medicina, la edad biológica (la edad real de nuestras células y órganos), sustituya a la edad cronológica y se vaya imponiendo como medidor de envejecimiento”.

El objetivo de proyecto es generar un algoritmo que calcule la edad biológica basado en biomarcadores sociales, culturales y económicos, biomarcadores de hábitos de vida, biomarcadores funcionales y de envejecimiento molecular y biomarcadores metabólicos y genéticos. “La edad biológica, una vez que se determine un algoritmo que de verdad se acerque a su cálculo real, de mayor exactitud, será sin duda el medidor del riesgo asociado a la naturaleza humana, como la salud, la dependencia y la predicción individualizada de la longevidad”, sentencia.

ODS implicados: 3, 5, 9, 16, 17

Más información de interés para innovar juntos:

Grupos de Investigación participantes en la validación de este reto:

- Grupo Universitario de Tecnologías de Identificación (GUTI)
- Computer Security Lab (COSEC)
- Grupo de Derecho Inmobiliario, Registral y de la Edificación (DERINRE)
- Grupo de Investigación en Responsabilidad Extracontractual
- Técnicas no Paramétricas y de Computación Intensiva en Estadística
- ACCURSIO de Derecho internacional privado
- Grupo de Procesado Multimedia

Startups y Spinoffs del programa de Incubación de la UC3M relacionadas:

- E-commerce: Twinny
- Uso de biomarcadores: Altum Sequencing