Smart Protection es el guardián de Google, Amazon o Facebook: así se gana su confianza para perseguir las infracciones de sus usuarios

Alberto R. Aguiar
10 dic. 2020 7:01h.

José Ignacio Carrillo, responsable de Enforcement de Smart Protection. Smart Protection

José Ignacio Carrillo es el responsable de Enforcement en Smart Protection, la startup española que seguriza contenidos para evitar emisiones o descargas piratas.

Él es el encargado de velar por la buena relación de la compañía con las

Explica cómo consigue con su trabajo que las plataformas acepten las demandas por contenido infractor o ilegal que lanza Smart Protection para su rápida retirada.

Descubre más historias en *Business Insider España.*

Las principales plataformas tecnológicas afrontan un problema: cada día sus usuarios suben millones de contenidos. **Y no todos son legales.**

Por ello, hay compañías como Smart Protection que se erigen como aliadas indispensables para ayudar que desde *marketplaces* como el de Amazon o eBay hasta redes sociales como Facebook o TikTok puedan ser seguras para marcas y contenidos.

La startup es una de las puntas de lanza del ecosistema tecnológico español: levantó hace poco 10 millones en una ronda de financiación. La firma se mueve con comodidad en un triángulo por el cual se la puede definir como una empresa de ciberseguridad, una legaltech o incluso una marketingtech.

La Europol quiere entrenar con este videojuego a los policías de toda Europa para que aprendan a reclamar datos de usuarios sospechosos a Google, Facebook o TikTok

---

Lo consiguen gracias a la variedad de productos que ofrecen: una plataforma en la nube que, conjugada con herramientas de **aprendizaje automático e**

o libros, o cualquier contenido que pueda poner en riesgo una marca, un producto o la reputación de cualquiera de sus clientes.

Trabajan con clientes del calibre de Warner Bros, Telefónica, RBA o Anagrama, entre muchos otros que no son públicos por razones de confidencialidad. Ya han conquistado un buen trozo del mercado internacional.

Y trabajan, irremediablemente, con todo tipo de plataformas: **Amazon, Twitch, Facebook, Google** y todos sus productos derivados.

Su plataforma y su compromiso, por supuesto, no pueden ser suficientes. Una firma como Smart Protection necesita una relación cercana y fluida con los gigantes tecnológicos, en las que los usuarios vuelcan todos sus datos y las marcas todos sus contenidos. De lo contrario, sería mucho más complicado que la startup española alcanzase el grado de eficacia del que presume.

> *El plan europeo para que Facebook, Twitter y YouTube se responsabilicen de lo que publican sus usuarios: multas millonarias por permitir contenidos ilegales, fraudulentos o que fomenten el odio*

Para eso está José Ignacio Carrillo. Carrillo es el responsable de *Enforcement* en Smart Protection. Salvaguarda que la firma tenga **una estrecha relación** con plataformas como Google o Facebook.

Pero tras el éxito de Carrillo y Smart Protection, hay una pregunta que se torna inevitable: **¿cómo lo consiguen?** ¿Por qué hay recordados casos de cuerpos

Hace unas semanas, la Europol anunciaba el lanzamiento de una suerte de videojuego corporativo con el que pretendían formar a agentes de todo el continente para que sepan cómo hay que relacionarse y solicitar información a estas tecnológicas. Pero, ¿pueden realmente mejorar esa colaboración?

Carrillo da algunas pistas en esta entrevista con *Business Insider España*.

"Hay que ser muy bueno en lo que uno hace"

"Las plataformas **son las primeras interesadas** en que no haya productos ilícitos o contenidos infractores en sus servicios", reconoce Carrillo nada más empezar a conversar. Con la abundante cantidad de material nuevo que se sube cada día, cada minuto, a una red social, es muy difícil plantear que las compañías tecnológicas puedan hacer una moderación efectiva de todo.

"Por eso necesitan la ayuda de un tercero, en este caso nosotros, que le vamos avisando de los contenidos infractores". La colaboración es diligente y fluida, ya que las redes con las que colabora Smart Protection certifican la eficacia de sus informes.

Por eso, acudir a Smart Protection puede ser mucho más eficaz que un solo usuario individual denunciando un contenido ilícito en una plataforma como YouTube, por ejemplo. "Ellas [las plataformas] prefieren, por decirlo de algún modo, que **hablemos entre abogados**", reconoce Carrillo.

Si una compañía o un individuo denunciase por cuenta propia un contenido

recuerda el experto de Smart Protection, "en que alguien puede pensar que el contenido de un tercero infringe sus derechos y no lo hace, en realidad".

"Sin embargo, si tú haces un análisis previo legal y encima le mandas un gran volumen de contenido infractor a la plataforma, la plataforma está, por decirlo así, más dispuesta a colaborar contigo de primera mano".

Eso sí, "**hay que ser muy bueno en lo que haces**", reivindica José Ignacio, *head* de *Enforcement* en Smart Protection. "Si detecto 5 posibles infracciones y las remito a la plataforma en cuestión, tu contacto en la plataforma hará las comprobaciones. Si no son verdaderas infracciones, la próxima vez que envíes un reporte no te van a aceptar con tanta diligencia".

Cada red social es un mundo

Hace unas semanas Selva Orejón, CEO de onBRANDING, reconocía a *Business Insider España* que muchos de sus clientes están abandonando redes como Twitter **por la crispación que existe** en ella para acudir a otras algo más *naif* como TikTok, cuya popularidad se ha disparado este 2020.

La propia Orejón advertía de los riesgos que eso conlleva: TikTok ha crecido mucho en muy poco tiempo, pero en cuestiones de *compliance* todavía no cuenta con los mismos servicios que pueden brindar gigantes como Facebook o Google. O la propia Amazon, para la que su lucha contra falsificaciones es prioritaria, hasta el punto de que cuenta con su propia unidad contra falsificaciones.

manera, encontrar las infracciones que ocurren dentro de su plataforma y hay otras que lamentablemente no tienen esos recursos. O bien, porque son plataformas que están empezando ahora a funcionar o porque son plataformas que todavía no **pueden aplicar esa tecnología a nivel interno**", detalla Carrillo.

> *Ciberinvestigación, antihacking y hasta contraespionaje: la CEO de la primera firma española de analistas y detectives digitales explica cómo usan la tecnología*

"Al final, es un poco como la ciberseguridad. Cuando más grande eres, más inviertes en evitar accesos ilegales, en evitar que te roben contenidos", apunta. El experto **no considera que exista un fenómeno** de redes o plataformas "**rebeldes**", en sí.

En esencia, aunque cualquier usuario puede reportar contenidos en las grandes plataformas, el valor competitivo de Smart Protection reside en que cuenta con una herramienta que automatiza mucho el proceso y permite escalarlo de forma masiva. Mientras que una persona puede enviar varios reportes al día, el equipo de Smart Protection logra enviar miles en cuestión de horas.

Sin embargo, Carrillo se detiene en una idea: es esencial que firmas como Smart Protection o cualquier otra sigan confiando en abogados. Él es letrado especializado en Propiedad Intelectual. Pero hay conflicto de derecho, como en cualquier otro ámbito legal. "Tiene que haber **una figura que supervise todo el procedimiento".**

"Nosotros no podemos reportar cualquier cosa que nos encontremos en internet porque sea una cita: citar un fragmento de una obra en internet es legal".

"Hay que intentar entender a las propias plataformas", resume Carrillo. "Se persigue un equilibrio entre la libertad de expresión y evitar contenidos infractores. No se puede hacer un filtrado previo de todo lo que los usuarios suben a una red social porque **sería limitar la libertad de expresión".**

Descubre más sobre Alberto R. Aguiar. Conoce cómo trabajamos en Business Insider España.

LEER TAMBIÉN: Un hacker de Google demuestra que es posible robar fotos y datos de un iPhone 11 desde una habitación contigua solo con una Raspberry y dos adaptadores WiFi

LEER TAMBIÉN: La cadena de frío, esencial para la distribución de las vacunas del coronavirus, también está siendo amenazada por ciberdelincuentes

LEER TAMBIÉN: AstraZeneca, Johnson & Johnson y otras firmas que trabajan en vacunas contra el coronavirus han sido diana de cibercriminales norcoreanos

VER AHORA: José Miguel Aparicio, CEO de Audi España: "Los vehículos se van a transformar en plataformas de software que nos conectarán con nuestros clientes"