# DOSSIER

MARTINIANO MALLAVIBARRENA MARTINEZ DE CASTRO

## CINCO GRANDES TENDENCIAS TECNOLÓGICAS DE LAS QUE ESTAR PENDIENTE EN CRIMINOLOGÍA (I)

Hay algo en lo que todos estaremos de acuerdo: las nuevas tecnologías han cambiado nuestras vidas en los últimos 10 años. Todos nosotros, en mayor o menor grado, utilizamos internet, teléfonos inteligentes o *tablets* (como el famoso iPAD de Apple) y hemos asumido que ver la televisión o hablar con otra persona distante ya no va ligado necesariamente a los "aparatos" correspondientes (TV y teléfono). Tener vida social, buscar todo tipo de información, compartir fotos con familiares y amigos o comprar viajes y libros tiene ahora un claro enfoque "digital" en la mayoría de las ocasiones (casi todos somos "*consumidores digitales*").

Mucho mas allá del ciberdelito (delincuencia de todo nivel cuyo campo de actuación es internet), las actividades criminales de todo tipo podrán ser poco a poco investigadas desde nuevos puntos de vista y con nuevas y poderosas herramientas.

En este artículo se revisan, a grandes rasgos, **cinco grandes paradigmas tecnológicos que**, en mi opinión al menos, están comenzando a transformar nuestras vidas y que de forma directa **tienen también impacto en la investigación criminal** a todos los niveles: inteligencia policial o militar, control de fraude, victimología, análisis de patrones de sospechosos, cálculos de zonas de mayor riesgo, perfilado psicológico, nuevas pruebas forenses digitales son algunos casos relevantes.

### 1) CUARTA GENERACIÓN MÓVIL (LTE)

La forma de vida de la mayoría de nosotros nos lleva a conectar nuestros ordenadores o teléfonos móviles "inteligentes" (Smartphones) a internet utilizando "conexiones móviles" (los conocidos como "pinchos" o "módems móviles" y, poco a poco, hemos dejado de quejarnos de la lentitud y problemas asociados a este tipo de comunicaciones. La actual tecnología se conoce como generación "3,5G" o "3,75G" que son términos que indican que son evoluciones de la original tercera generación móvil (técnicamente se utiliza el acrónimo UMTS para nombrar a este conjunto de tecnologías).

Un aspecto que no hay que olvidar es que estos pequeños "pinchos" que nos conectan con internet de forma cada vez mas eficiente se irán integrando poco a poco en un gran número de entornos donde ahora no tienen cabida: uno de los mas interesantes serán los coches que pasarán a estar "siempre conectados con internet". Cada uno de nuestros coches irán informando (como ahora hacen los vehículos de Fórmula 1) del estado de sus mecanismos, de los niveles de sus fluidos fundamentales y de sus futuras necesidades (pedirán cita en el taller cuando vean que alguna pieza está cerca del fallo o si el coche necesitará pronto una revisión completa, por ejemplo).

En estos próximos años comenzaremos a ver *flashes* de la conocida como 4G (o cuarta generación móvil, en algunos

**Martiniano Mallavibarrena Martinez de Castro**
Ingeniero técnico de telecomunicación | Máster en Dirección de Informática | Especialista en la aplicación de las TIC a la Criminología
MartyMBlog@gmail.com

escenarios denominada LTE o *Long-Term-Evolution* que es un concepto muy similar) que entre otros aspectos innovadores permitirá entregar velocidades de conexión alrededor de 100 Mbps (en las primeras conexiones ADSL en nuestros hogares, las velocidades era de 1 a 3 Mbps como comparación) y este rango de velocidades permitirá entre otras cosas el uso habitual de servicios en "modo nube" (ver apartado siguiente), el uso de servicios de vídeo en alta definición (retransmisiones de todo tipo incluyendo canales de TV pero también comunicaciones entre dos o mas personas como hemos visto tantas veces en el cine).

Este tipo de enfoques "4G" deben hacer que la criminalística preste mucha mas atención a las conexiones móviles en cualquiera de los múltiples escenarios que ahora se presentarán: conexiones por videoconferencia entre personas, grabaciones de fotos y vídeo que ahora se almacenarán directamente en "la nube" (ver el concepto de *Cloud computing* mas adelante), mensajes y datos que se generan en dispositivos móviles, etc.

Aquellos que siguen hablando de "pinchar teléfonos" se tendrán que replantear muchas cosas, entender algunas nuevas tecnologías y utilizar de forma adecuada diversos marcos regulatorios en función del contexto: en España el eje lo forman el Art. 18 CE (derecho a la intimidad y al secreto en las comunicaciones) en combinación con el Art. 579 de la LECr (posibilidad para el juez de ordenar una intervención telefónica si resulta adecuada al proceso). Se ha publicado diversos artículos analizando los escenarios actuales –la referencia [06] me parece muy completa– y la regulación internacional intentan proteger los derechos y libertades fundamentales en este tipo de actuaciones para evitar abusos por parte de los investigadores. Solo recordar que ahora puedes utilizar programas como Skype para tener conferencias telefónicas (incluso con imagen de vídeo simultánea) con tus contactos tanto desde tu teléfono móvil como desde, por ejemplo, tu televisor del salón. Es obvio que la "escucha telefónica" en estos casos no será igual a la actual por obvios aspectos tecnológicos pero es que tampoco lo será por aspectos básicos de concepto (¿puede un juez español ordenar "escuchar" una conversación en internet si los servidores no están en España?).

*"Aquellos que siguen hablando de "pinchar teléfonos" se tendrán que replantear muchas cosas, entender algunas nuevas tecnologías y utilizar de forma adecuada diversos marcos regulatorios."*

[**Casos de uso reales**] El uso de las posibilidades de las tecnologías móviles de cuarta generación no pasará desapercibida ni para los criminales ni para los investigadores:

- Uno de los principales organismos de standards de telecomunicación a nivel mundial, el *European Telecommunications Standards Institute* (ETSI) está trabajando [(1)] en nuevos usos de comunicaciones públicas seguras basadas en estas nuevas funcionalidades (que harán olvidar pronto a los sistemas de radio tradicionales).
- El especialista en tendencias criminales, Marc Goodman, nos relató como algunas grandes organizaciones del crimen organizado han creado sus propias redes de telecomunicación móvil (como se pudo comprobar [(2)] en 2011 en México). Es previsible que de igual forma, toda esta potencialidad tecnológica "en la palma" de la mano sea utilizada de forma recurrente para cometer

nuevas modalidades de cibercrimen y para apoyar la comisión de todo tipo de delitos, sobre todo en combinación con las tecnologías de *cloud computing* que se explican en el punto siguiente.

## 2) CLOUD COMPUTING

La "computación en la nube" (en inglés, *Cloud computing*) es un término que estamos escuchando con frecuencia en los últimos años y que refleja una manera innovadora de ofrecer recursos informáticos a los usuarios desde internet (se pueden tener escenarios *cloud* fuera de internet pero para el caso que nos ocupa, los descartaremos). Las características que hacen interesante el enfoque *cloud* son en esencia tres:

El usuario no tiene que adquirir equipos y casi siempre accede a los recursos desde cualquier tipo de dispositivo conectado a internet (puede conseguir mucha potencia con solo pagar por ello por el tiempo necesario).

Los recursos informáticos (espacio en disco, cuentas de correo electrónico, espacio para subir fotos o vídeos, etc.) parecen ser infinitos y siempre están disponibles con solo pedirlos.

El usuario se puede despreocupar de hacer mas copias de seguridad y si se le cobra por el servicio (muchos son gratuitos) se le cobra "por el uso" (no es tarifa plana, se abona por el consumo de los recursos consumidos en el periodo correspondiente).

Por todo ello, servicios como Gmail (el famoso correo electrónico de Google) o Dropbox (el nuevo "disco duro en internet") son cada vez mas utilizados por millones de personas en todo el planeta.

Es obvio señalar que los proveedores de estos servicios podrán estar en cualquier parte del planeta ya que podremos conectar con ellos a través de una internet cada vez más rápida (la distancia geográfica no se aplica en internet).

Desde la criminalística, una de las consecuencias mas directas de este fenómeno es que "la información estará en la nube" (que es la metáfora oficial para este uso de internet) y dejará de estarlo en los dispositivos que utilizamos las personas.

El registro del piso utilizado por un grupo terrorista o el domicilio de un presunto asesino en serie suele terminar ahora con el análisis forense del ordenador personal que los sospechosos suelen tener. Esta rutina que tantas veces hemos visto en las noticias, pasará ahora a un análisis forense en la "nube" de internet (posiblemente en lugares como Dropbox) y mucho mas concentrado en el teléfono móvil (habitual terminal de conexión al servicio en nube) que en el ordenador personal. En ambos casos y en la mayoría de ocasiones, los investigadores no encontrarán prueba "física" alguna en estos dispositivos.

Se deben desarrollar, por tanto, nuevos métodos de investigación en este tipo de entornos que tengan en cuenta su esquema de funcionamiento y el marco regulatorio asociado (no es lo mismo utilizar un servicio en "nube" en una empresa americana que europea, por ejemplo). De forma reciente, la "agenda [3] digital" de la Comisión Europea ha incluido diversos esfuerzos relativos a la normalización de este tipo de servicios sobre todo de cara a su posible uso por administraciones públicas de toda la Unión. Los aspectos aso-

***"El registro del piso utilizado por un grupo terrorista dará paso ahora al análisis forense en la "nube" de internet y se concentrará más en el teléfono móvil que en el ordenador personal."***

ciados a la clasificación de la privacidad de datos por su contenido y a su control asociado son notablemente más duros en España y en Europa que en otras zonas.

[**Casos de uso reales**] Es habitual encontrar escenarios de uso reales en ambos lados de la criminalística. Veamos algunos ejemplos recientes.

- El FBI y otras agencias están patrocinando el uso de una serie de buenas prácticas a la hora de utilizar tecnología cloud computing al almacenar datos sensibles. Con ello se quiere unificar el uso óptimo de este tipo de servicios por agencias policiales o de índole similar. El documento completo (de agosto 2012) está disponible en [03].
- Ya se ha creado el término Cloud forensics para determinar a aquellas labores de tipo forense que se deberán realizar en este tipo de entornos para desarrollar una investigación con el mismo espíritu que en los métodos tradicionales. En la referencia [04] podemos ver una de las obras mas recientes del Dr. Keyun Ruan (una de las grandes autoridades en esta reciente materia) que está liderando diversos trabajos de normalización y creación de standards. En ella se recogen las mejores prácticas a la hora de clasificar y procesar la información que pueda aparecer en este tipo de entornos de cara a que la "cadena de custodia" sea adecuada a los nuevos escenarios (y a las futuras regulaciones).

## REFERENCIAS


[01] GOSLING, GADDIS & VAZIRE. *Personality Impressions Based on Facebook Profiles*. 2007. Universidad de Texas.

[02] GOLBECK, ROBLES & TURNER. *Predicting Personality with Social Media*. 2011. Universidad de Maryland.

[03] FBI. *Recommendations for Implementation of Cloud Computing Solutions (Technical report)*. 2012. FBI.

[04] Ruan K. (2013) *Cybercrime and Cloud Forensics: Applications for Investigation Processes* (pp.1-348), IGI Global, December 2012, doi:10.4018/978-1-4666-2662-1'


(1) *http://www.etsi.org/plugtests/RCS-VOLTE/pres/PSCR%20-%20ETSI%20MSF%20GSMA%20RCS.pdf*

(2) *http://www.npr.org/2011/12/09/143442365/mexico-busts-drug-cartels-private-phone-networks*

(3) *http://europa.eu/rapid/press-release_IP-12-1025_en.htm*

**CONTINUARÁ EN QDC # 21:**

3) *SOCIAL MEDIA*;
4) INTERNET DE LAS COSAS (*SMART CITIES / BIG DATA*) Y
5) REALIDAD AUMENTADA.