

LA CIBERDELINCUENCIA EN ESPAÑA: UN ESTUDIO BASADO EN LAS ESTADÍSTICAS POLICIALES*

ANA ISABEL CEREZO DOMÍNGUEZ**
REMEDIOS GARCÍA CORNEJO

Recibido: 26.SEP.2019
Aprobado: 05.DIC.2019

SUMARIO

1. Introducción. 2. Evolución de los hechos conocidos. 3. Evolución de los hechos esclarecidos. 4. Evolución de las detenciones e investigados. 5. Evolución de la victimización. 6. Conclusiones. Bibliografía.

RESUMEN

El presente trabajo analiza con profundidad los datos publicados por el Portal Estadístico de Criminalidad del Ministerio del Interior sobre ciberdelincuencia desde el año 2011 al 2017. Los resultados muestran como estas actividades delictivas han tenido una tendencia constante al alza, llegándose a duplicar las denuncias durante los años abarcados en el análisis estadístico.

PALABRAS CLAVE: ciberdelincuencia, análisis longitudinal, estadísticas oficiales

ABSTRACT

The current study analyses deeply data published by “Portal Estadístico de Criminalidad” from the Ministry of Interior about cybercrime from 2011 to 2017. The results show how these criminal activities had a constantly upward trend, doubling the reports during the period analysed.

KEY WORDS: Cybercrime, longitudinal analysis, official data

* El presente trabajo forma parte de las actividades que se realizan por parte del Grupo de estudios en Nuevas tecnologías y Criminalidad (G-CrimTech) y del Observatorio de la Delincuencia (ODA) en el seno del Instituto andaluz interuniversitario de Andalucía (Sección Málaga). Y forma parte de las actividades llevadas a cabo por el proyecto denominado “Ayudas a las acciones de dinamización “Redes de Excelencia” proyecto: *Desarrollo de un modelo criminológico y empírico de la política criminal – Acrónimo EmpiriC –*”. Financiado por MCIU-AEI (Ref. DER2017-90552-REDT).

** Universidad de Málaga. Directora del Instituto Andaluz interuniversitario de Criminología, sección Málaga, aicerezo@uma.es

1. INTRODUCCIÓN

Desde que en la década de los 90 aparecieran las tecnologías de la información y la comunicación (en adelante, TIC), a través del surgimiento de la “*World Wide Web*”, se ha ido transformando el comportamiento humano a nivel mundial. El crecimiento imparable del uso de estas nuevas tecnologías ha favorecido la ampliación y la diversificación de los espacios y de las condiciones de comunicación social. En términos generales, podemos afirmar que hemos pasado a ser dependientes de las nuevas tecnologías y, al igual que nuestra forma de comunicación ha dado un salto evolutivo en estos últimos años, este importante cambio también se ve reflejado en nuevas formas de cometer delitos. Nadie puede negar que la utilización de las TIC conlleva un buen número de ventajas, ya que éstas se caracterizan por ofrecer respuestas rápidas, obteniéndose así recompensas inmediatas, pero también ocasionan una serie de riesgos, como ser víctima de delitos cibernéticos, delitos que afectan cada vez más a la sociedad actual.

Loredo y Ramírez (2013) afirman que el “*delito informático es el uso de cualquier sistema informático como medio o fin de un delito*”. Por su parte, en el preámbulo del Convenio sobre la Ciberdelincuencia de Budapest, aprobado por el Consejo de Europa el 23 de noviembre de 2001 y ratificado por España el 20 de mayo de 2010 (BOE, núm. 226/2010 de 17 de septiembre de 2010¹), se define la ciberdelincuencia como “*aquellos actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de los sistemas, redes y datos*”. En el artículo 1 del convenio se definen estos términos. Así, “*por sistema informático se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa*” y “*por datos informáticos se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función*”.

De este modo, la ciberdelincuencia engloba a todo delito en el que el objeto de la actividad delictiva son los propios sistemas informáticos o las TIC. Se trata por tanto de comportamientos delictivos dirigidos a tres objetivos: los dispositivos informáticos, los datos y la información informatizada. Podemos clasificar estos delitos del siguiente modo:

- a) Delitos de daños, sabotaje informático los ataques por virus sabotaje informático y ataques de denegación de servicios. Ejemplo de estos delitos

1 Disponible en: <https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf>

son los ataques por virus o el espionaje a sistemas informáticos de los Estados o empresas.

- b) Delitos de acceso sin autorización a datos, programas o sistemas informáticos.
- c) Delitos de descubrimiento y revelación de secretos, cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos.

Pero por ciberdelincuencia también podemos entender todo delito cometido a través del ordenador o la red, en los que la actividad delictiva se sirve para su ejecución de las ventajas que ofrecen las TIC, ejemplo de ello son la estafa informática, la pornografía infantil, el ciberacoso o los robos de identidad (IAM, 2015²).

Estas ventajas, a las que hacíamos referencia anteriormente, son debidas a las propias características específicas de la ciberdelincuencia, tales como el anonimato y la posibilidad del ciberdelincuente de acceder a personas y equipos informáticos de todo el mundo. Ello conlleva que en muchas ocasiones los delitos crucen fronteras y esto dificulte la persecución de dicha actividad (CEREZO *et al.*, 2007, MIRÓ, 2011 y ROCA, 2014). A todas estas ventajas se debe añadir la falta de concienciación sobre seguridad informática que poseen los usuarios de estas tecnologías, de tal modo que los ciberdelinquentes pueden encontrar con facilidad en la red las herramientas necesarias para realizar dichas conductas delictivas. Para la comisión de determinados delitos informáticos no es necesario disponer de muchos conocimientos y, en caso de que sean necesarios, es posible contratar estos servicios³ (ROCA, 2014).

Dicha ciberdelincuencia es el foco de atención de muchas investigaciones desde hace años, debido a que cada vez predominan más los nativos digitales. Se estima que la delincuencia informática tiene un coste mundial de 114 mil millones de dólares anuales, más de dos tercios de la población ha sido víctima *on-line* de alguna vez en su vida y 14 personas son víctimas de la delincuencia informática cada segundo (FLORES *et al.*, 2014).

El objetivo principal de este artículo es conocer la evolución de estos delitos en los últimos 7 años en nuestro país. Para llevar a cabo este análisis longitudinal se han utilizado los datos que publica anualmente el Ministerio del Interior a través de la web del Portal Estadístico de Criminalidad⁴, en la cual se pueden encontrar

2 Disponible en: <http://www.juntadeandalucia.es/iam/catalogo/doc/iam/2015/143528391.pdf>

3 Se han incrementado los denominados “empresarios individuales del delito”. Se trata de ciberdelinquentes que venden sus servicios a grupos de crimen organizado.

4 Disponible en: <https://estadisticasdecriminalidad.ses.mir.es/>

datos sobre hechos de índole delictiva y, entre ellos, concretamente sobre la cibercriminalidad. También se debe señalar que todos los datos a los que se hará referencia más adelante provienen de las Fuerzas y Cuerpos de Seguridad del Estado, de la Policía Foral de Navarra y de policías locales que proporcionan sus datos al Sistema Estadístico de Criminalidad. Lamentablemente, quedan excluidos los datos que proceden de la Ertzaintza y de los Mossos d'Esquadra.

De cara al análisis longitudinal que aquí se presenta haremos una distinción entre la cibercriminalidad económica, esto es, aquella que persigue un fin lucrativo y es ocasionada normalmente por organizaciones delictivas y la cibercriminalidad social, que correspondería a aquellos delitos perpetrados por individuos que persiguen ocasionar un daño moral o psicológico a las víctimas (MIRÓ, 2012).

Somos conscientes de las limitaciones y sesgos de los datos que aquí se muestran. Al igual que ocurre con cualquier tipo de delito, en la ciberdelincuencia también existe una cifra negra. En primer lugar, se trata de datos procedentes del Ministerio del Interior y, como bien señala Montiel (2016), en las estadísticas oficiales no se recogen aquellos hechos que no tienen la suficiente gravedad, aunque sean constitutivos de delitos, por tratarse de delitos con ausencia de pruebas para la imputación o debido a la reticencia a denunciar por parte de la víctima. En el estudio de Dominie et al. (2013, citado en Van de Weijer et al., 2019), se muestra que sólo el 13,4% de la muestra había denunciado el delito cibernético. Otro ejemplo lo encontramos en el estudio de Van de Weijer et al. (2019), quien analiza los datos de cuatro oleadas de una encuesta holandesa con una muestra de 97.186 víctimas, en el que mostró que estas víctimas denunciaron con menos frecuencia que en los delitos tradicionales.

A estas limitaciones hay que añadir las dificultades técnicas y jurídicas para esclarecer y condenar por este tipo de delitos (RAYÓN y GÓMEZ, 2014). Asimismo, los datos también pueden estar sesgados por las denuncias falsas, es decir, aquellas denuncias que, tras la investigación pertinente, se han podido constatar que en realidad el delito no se ha llegado a ocasionar.

2. EVOLUCIÓN DE LOS HECHOS CONOCIDOS

El presente trabajo se estructura en base a la presentación de los datos estadísticos por parte de los informes policiales, esto es, hechos conocidos, hechos esclarecidos, detenciones e investigaciones y victimizaciones.

Los datos que se muestran en el gráfico 1 señalan la evolución de las infracciones penales relacionadas con la ciberdelincuencia entre los años 2011 y 2017.

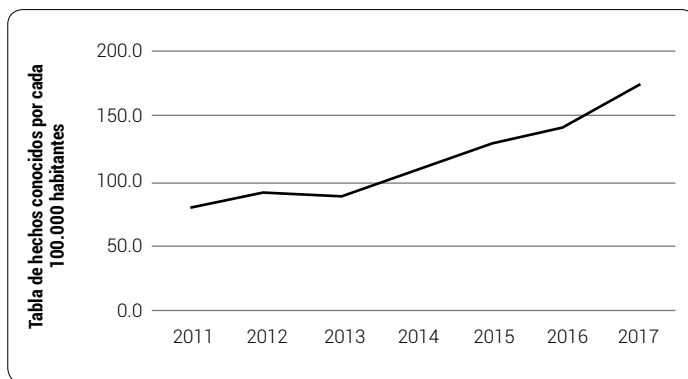


Gráfico 1. Evolución de los hechos conocidos en Ciberdelincuencia entre los años 2011 y 2017.
Fuente: elaboración propia a partir de los datos del Portal Estadístico de Criminalidad.

Como se puede comprobar, el número de infracciones ha ido en aumento, duplicándose en el año 2017 (174 casos por cada 100.000 habitantes) frente al año 2011 (80 casos por cada 100.000 habitantes). La posible explicación de este aumento concuerda con el aumento progresivo de la utilización de las TIC en la población española. El informe ofrecido por la Fundación Telefónica en el año 2018 (a partir de los datos de 2017) pone de relieve que ya existen más líneas móviles que habitantes en todo el planeta y, haciendo referencia a los usuarios de internet, señala que el 43,7% de la población entre 65 y 74 años hacen uso de ello, alcanzando esta cifra el 98% cuando se trata de los jóvenes. Otra posible explicación de este aumento está relacionada con la creciente incorporación de estos tipos penales en el Código penal y a una mayor persecución de los mismos, debido a la creación de unidades policiales y de guardia civil especializadas y dotadas de mayores recursos y conocimientos informáticos⁵.

Es necesario señalar que la web del Portal Estadístico de Criminalidad también ofrece los datos diferenciándolos por tipología delictiva, entre las cuales encontramos:

- *Fraude informático*. El artículo 248.2 castiga actualmente tres modalidades de estafa informática, a saber, la estafa bancaria, la fabricación,

5 Entre estas unidades se encuentran la Unidad Central de Ciberdelincuencia (conocida como UCC), perteneciente al Cuerpo Nacional de Policía, que a su vez se divide en tres brigadas: La Brigada de Investigación tecnológica, la Brigada de fraude informático y la Brigada de seguridad informática. Por su parte, se encuentra en funcionamiento desde hace varios años el Grupo de Delitos Telemáticos (conocido como GDT) perteneciente a la Guardia Civil. Además de estos grupos de investigación, existe el Instituto Nacional de Ciberseguridad (INCIBE), que trabaja para la prevención y la reacción sobre posibles incidentes de seguridad de la información.

introducción, posesión o facilitación de programas informáticos específicamente destinados a la comisión de estafas y las estafas con tarjetas de crédito, débito y cheques de viaje y otras estafas.

- *Amenazas y coacciones.* El Código penal castiga estos delitos en sus diversas modalidades. Mención especial merece el art. 172 ter, introducido en el Código penal por la LO 1/2015, que castiga el acoso persistente o *stalking*.
- *Falsificación informática.* Se entiende por tal la creación, manipulación o alteración de documentos o imágenes digitales (arts. 390 a 398 CP)
- *Acceso e interceptación ilícita.* Este grupo de delitos engloba el descubrimiento y revelación de secretos (arts. 197 a 201 CP, introducido en el Código penal por la LO 5/2010), haciendo especial mención al art. 197 bis y ter introducidos en el Código penal por la LO 5/2010. Del mismo modo, se incluyen en este grupo a los delitos de espionaje industrial (arts. 278 y 279 CP, recogidos entre los delitos relativos al mercado y a los consumidores)
- *Delitos contra el honor.* Incluye las calumnias (arts. 205 a 207 CP) y las injurias (arts. 208 a 210 CP).
- *Delitos sexuales.* En este grupo se incluyen delitos como el exhibicionismo (art. 185 CP), la provocación sexual (art. 186 CP), el acoso sexual (art. 184 CP), el abuso sexual sin penetración (arts. 181 y 182 CP), la prostitución, explotación sexual y corrupción de menores o personas con discapacidad necesitadas de especial protección (arts. 187 y 188 CP), la pornografía de menores (art. 189 CP) y el delito de contacto mediante la tecnología con menores de 16 años con fines sexuales (art. 183 ter CP introducido en el Código penal por la LO 1/2015). Se excluyen las agresiones sexuales y los abusos sexuales con penetración.
- *Interferencia en los datos y en el sistema.* Engloba daños y ataques informáticos (arts. 264, bis y ter, introducidos los dos últimos en el Código penal a partir de la LO 5/2010).
- *Contra la propiedad industrial/intelectual.* Como su propio nombre indica, engloba los delitos contra la propiedad intelectual (art. 270 a 272 CP) y aquellos delitos contra la propiedad industrial (art. 273 a 277 CP).

En el gráfico 2 se puede observar la incidencia de estos delitos. A lo largo de los años destaca de forma considerable el fraude informático, seguido en menor medida por las amenazas y coacciones sobre el resto de delitos, los cuales se mantienen con tasas muy similares y bajas. En solo siete años, las estafas *on-line* se han triplicado, pasando de 21.075 casos denunciados a 60.511, convirtiéndose en uno

de los delitos más comunes que se cometen en nuestro país por encima del tráfico de drogas (con un total de 12.958 hechos conocidos en el año 2017) y muy cerca de los robos con violencia (61.763 hechos conocidos también en 2017).

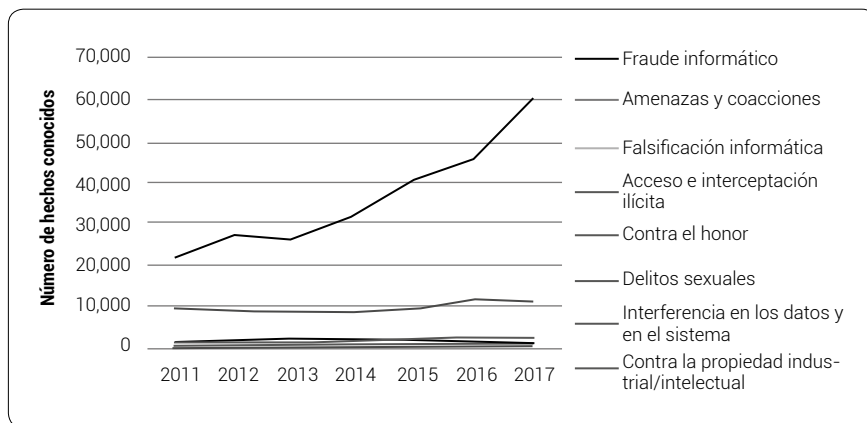


Gráfico 2. Evolución de los hechos conocidos en Cibercriminalidad entre los años 2011 y 2017 con distinción entre grupos penales. Fuente: elaboración propia a partir de los datos del Portal Estadístico de Criminalidad.

3. EVOLUCIÓN DE LOS HECHOS ESCLARECIDOS

De sumo interés nos parecen los datos que ofrece el Portal Estadístico en referencia a los hechos esclarecidos (Gráfico 3).

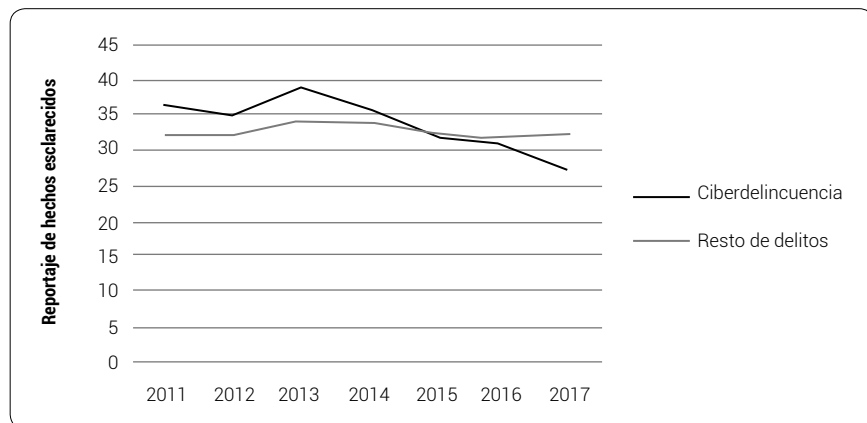


Gráfico 3. Evolución del porcentaje de hechos esclarecidos entre los años 2011 y 2017 en relación con los hechos conocidos. Fuente: elaboración propia a partir de los datos del Portal Estadístico de Criminalidad.

De todos los hechos conocidos en 2017, únicamente se esclarecieron el 27% de los delitos, mientras que en el año 2011 se esclarecieron un 36%. Esta tendencia a la baja se lleva observando desde el año 2013, en el que se esclarecieron el 38,6% de los hechos conocidos. Esta situación puede ser debida a que no siempre se dan las circunstancias para que todos los hechos conocidos lleguen a esclarecerse, debido a que no siempre se detiene al autor “in fraganti”, no se tiene una identificación plena de éste, no existe una confesión verificada o incluso, puede darse que, a partir de la investigación, se revele que no hubo infracción. A todo ello se suma el auge en la comisión de estos delitos frente a la falta de recursos y medios con los que se cuenta para su persecución, detección y esclarecimiento por parte de las Fuerzas y Cuerpos de Seguridad.

Al comparar las tasas de los hechos esclarecidos en ciberdelincuencia con la tasa de esclarecimiento en relación con el resto de hechos conocidos, se puede observar que ambos obtienen tasas muy similares, ya que se esclarecen alrededor del 30 y el 35% del resto de delitos.

Si atendemos a los grupos delictivos, observamos una situación muy diferente. En el gráfico 4 se puede observar que existen grupos delictivos que poseen un alto porcentaje de hechos esclarecidos, es el caso de los delitos contra la propiedad industrial e intelectual, de los delitos sexuales, de las amenazas y las coacciones y de los delitos contra el honor, encontrándose los datos entre el 50 y el 80 por ciento de esclarecimientos, mientras que el resto de las tipologías delictivas ofrecen tasas de esclarecimiento por debajo del 35 por ciento. Si atendemos a la clasificación inicialmente efectuada entre cibercriminalidad social y económica, podemos observar que son precisamente aquellos delitos clasificados como ciberdelincuencia social los que más se esclarecen frente a los denominados de ciberdelincuencia económica. Una posible explicación se encontraría en el *modus operandi* de estos delitos, ya que mientras los denominados sociales son cometidos por personas inexpertas en el manejo de las TIC, los de corte económico son delitos que necesitan de cierto conocimiento informático para ser ejecutados y, por consiguiente, seguramente más difíciles de esclarecer.

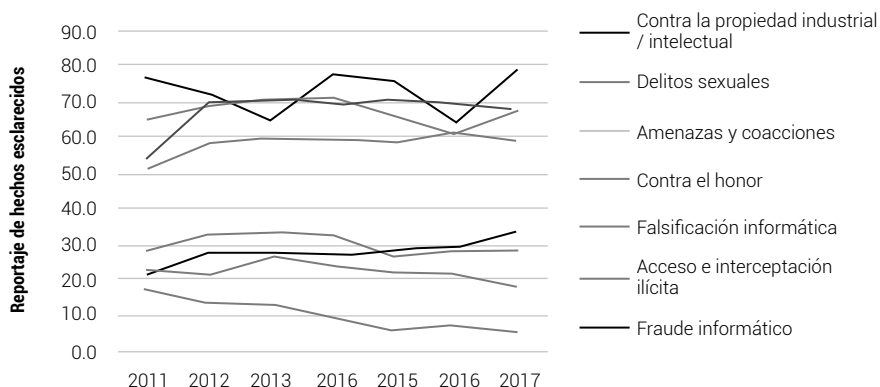


Gráfico 4. Evolución del porcentaje de hechos esclarecidos en Cibercriminalidad entre los años 2011 y 2017 con distinción entre grupos penales. Fuente: elaboración propia a partir de los datos del Portal Estadístico de Criminalidad.

4. EVOLUCIÓN DE LAS DETENCIONES E INVESTIGADOS

Desde el punto de vista del análisis de los datos, tanto de las detenciones e investigados como de la victimización, el Portal Estadístico ofrece datos más interesantes, ya que éstos vienen desglosados por sexo y por edad.

Comenzando por la evolución general, en el gráfico 5 se puede ver que las detenciones e investigaciones por cibercriminalidad se mantienen bastante estables a lo largo de los años, con un leve aumento en los años 2014 y 2015 y obteniendo su tasa más baja en el año 2016. Si se vuelve a comparar las detenciones e investigaciones de estos delitos con los delitos que más se cometen en nuestro país, como son el tráfico de drogas o los robos con violencia o intimidación, se puede comprobar que los datos de estos últimos triplican dichas detenciones, aunque es reseñable la disminución que ambos tipos de delitos están sufriendo, en lo que a las detenciones e investigaciones se refiere.

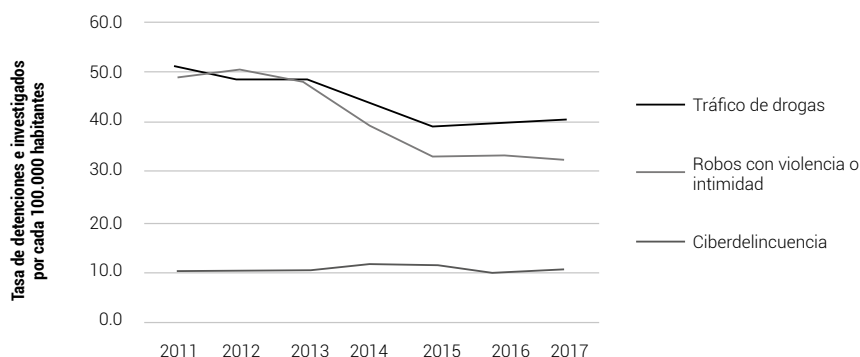


Gráfico 5. Evolución de las detenciones e investigados por Ciberdelincuencia, Tráfico de Drogas y Robos con Violencia o Intimidación entre los años 2011 y 2017. Fuente: elaboración propia a partir de los datos del Portal Estadístico de Criminalidad.

Asimismo, se ha calculado el porcentaje de detenciones e investigados en esas tres actividades ilícitas según los hechos conocidos en el año 2017. Los datos muestran que, del total de delitos que se conocen, sólo se detienen e investigan al 0,89% por tráfico de drogas, al 0,71% por robos con violencia e intimidación y al 0,23% por ciberdelincuencia⁶. Llama la atención que estas cifras sean tan dispares y que la tasa de detenciones de la ciberdelincuencia sea tan baja. Una posible explicación a este hecho puede ser que, aunque cada vez las unidades de investigación están más especializadas, las TIC siguen evolucionando a gran velocidad, complicando de esta forma las investigaciones llevadas a cabo. Todo ello es coherente además con la baja tasa de esclarecimiento que caracteriza a este tipo de delitos.

Si se analizan estas detenciones e investigados por sexo, estos resultados muestran el porcentaje de aquellos que pertenecen al sexo masculino es muy superior al femenino, siendo entre el 75-80% y el 20-25%, respectivamente.

Igualmente nos ha parecido interesante conocer si esa brecha de género se extrapola cuando atendemos a los datos de todos los delitos en general, lo que en efecto ocurre. El porcentaje de hombres detenidos e investigados (entre el 82 y el 85%) es muy superior al porcentaje de mujeres (entre el 14% y el 18%). Por todo ello, no se pueden establecer diferencias entre las acciones ilícitas cometidas *on-line* y los hechos delictivos en general, en lo que a personas detenidas e investigadas se refiere.

6 Estos datos se han obtenido del porcentaje de detenciones e investigados respecto al total de hechos conocidos, es decir, la suma de los hechos conocidos del resto de delitos junto con los hechos conocidos por ciberdelincuencia.

| | Hombres | Mujeres |
|--|---------|---------|
| Acceso e interceptación ilícita | 7,8% | 7,7% |
| Amenazas y coacciones | 25,1% | 21,3% |
| Contra el honor | 2,3% | 3% |
| Contra la propiedad industrial/intelectual | 2,1% | 1,8% |
| Delitos sexuales | 19,1% | 4,1% |
| Falsificación informática | 5,9% | 9,3% |
| Fraude informático | 37,1% | 52,6% |
| Interferencia en los datos y en el sistema | 0,6% | 0,2% |

Tabla 1. Porcentaje de hombres y mujeres detenidos e investigados según el grupo penal en el año 2017.
Fuente: elaboración propia a partir de los datos del Portal Estadístico de Criminalidad.

La siguiente pregunta que nos hacemos es si existen diferencias entre los delitos cibernéticos que comenten los hombres y los que cometen las mujeres. En la tabla 1 se muestran los datos de los delitos que cometen los hombres y las mujeres, respecto del total de las detenciones e investigados por sexo. El fraude informático es el grupo penal más cometido tanto por mujeres (52,6%) como por hombres (37,1%), seguido de las amenazas y coacciones (21,3% y 25,1%, respectivamente). Es en el tercer lugar donde encontramos una clara diferencia, mientras que para las mujeres el tercer grupo penal más cometido es el de falsificación informática (9,3%), para los hombres son los delitos sexuales (19,1%).

Otro aspecto interesante a analizar es la edad de los detenidos e investigados. En esta ocasión, los datos del gráfico 6 se muestran en términos relativos, es decir, están expresados en proporción al número de habitantes que había en esa franja de edad. Es destacable como, en el año 2013, el número de detenidos e investigados aumentaron en los grupos de 14 a 17 años y de 18 a 25 años, manteniendo una tasa estable desde entonces. En el resto de los grupos de edad, estas tasas se han mantenido estables durante todo el rango temporal estudiado. Además, se debe señalar que, desde 2013, destaca el grupo de 18 a 25 años, seguidos por el grupo de 14 a 17 y de 26 a 40 años, con tasas similares.

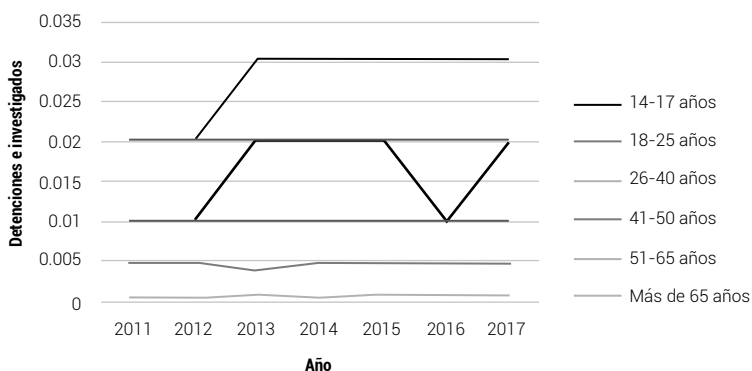


Gráfico 6. Evolución de las detenciones e investigados por ciberdelincuencia entre los años 2011 y 2017 diferenciado por grupos de edad.
Fuente: elaboración propia a partir de los datos del Portal Estadístico de Criminalidad.

Al igual que con la variable sexo, la variable edad también se ha comparado con las acciones ilícitas en general. Al igual que en los ciberdelitos, en el resto de delitos destacan las edades comprendidas entre los menores de edad y los adultos, es decir, entre los 14 y los 40 años, siendo más destacable, en el caso de todos los delitos el grupo de 18 a 30 años. Si llama la atención que, cuando se habla de delitos en general, se observa un descenso progresivo en las detenciones e investigados en los tres grupos de edad más destacados.

Por último, el gráfico 7 muestra las detenciones e investigaciones en base a la tipología delictiva y la edad, en términos relativos y únicamente del año 2017.

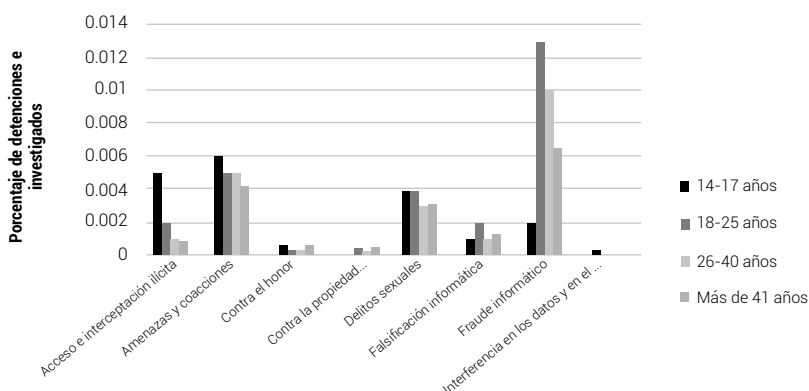


Gráfico 7. Detenciones e investigados por Ciberdelincuencia en el año 2017 según grupo penal y grupos de edad.
Fuente: elaboración propia a partir de los datos del Portal Estadístico de Criminalidad.

Analizando el gráfico 7 se observan datos muy interesantes. Los menores de edad destacan en delitos como el acceso e interceptación ilícita, en amenazas y coacciones y en delitos contra el honor. El grupo de 18 a 25 años destaca en el fraude informático, seguido de las amenazas y coacciones (con una tasa similar al grupo de 26 a 40 años) y cometiendo en tercer lugar delitos sexuales (con una tasa semejante al grupo de menores de edad). Por último, aunque con tasas diferentes, el grupo de 26 a 40 años y de 41 a 50 años cometen más delitos de fraude informático, seguido de delitos de amenazas y coacciones y, en tercer lugar, delitos sexuales.

Hemos analizado asimismo los datos referidos a la evolución de las detenciones e investigaciones por ciberdelincuencia diferenciados por grupo de delitos. Al igual que ocurría cuando se analizaban los datos de hechos conocidos, los grupos penales que destacan entre las personas detenidas e investigadas son el fraude informático en primer lugar, seguido de las amenazas y coacciones. Hay que señalar que en ambos grupos penales se observaba un descenso desde el año 2015, siendo dicho descenso más notable en las amenazas y coacciones. Es destacable como el tercer grupo penal más común, los delitos sexuales, van incrementando su tasa paulatinamente. Con este tipo de actividad se debe tener especial cuidado, ya que es un asunto sensible, y esto lleva, en muchas ocasiones, a que la víctima no denuncie por diferentes motivos. Algunos de estos pueden ser la relación que una a la víctima con el victimario, que la conducta no se llegue a consumir o el sentimiento de vergüenza que pueda llegar a surgir en la víctima al contar determinado tipo de delito. Aun así, en relación con su incremento, se puede llegar a pensar a que la población es cada vez más consciente respecto a estos asuntos y poco a poco son más los que dan el paso de interponer la denuncia.

5. EVOLUCIÓN DE LA VICTIMIZACIÓN

Centrándonos finalmente en la víctima, los datos muestran una tendencia ascendente, duplicándose la cifra en el último año del que se obtienen datos (61,9 por cada 100.000 habitantes en 2011 y 133,8 por cada 100.000 habitantes en 2017). Si se atiende al sexo de estas víctimas, los datos muestran que son los hombres quienes sufren más estos delitos (34.019 hombres frente a 28.305 mujeres en el año 2017), aunque la diferencia no es tan elevada como en el caso de las detenciones. Aun así, en ambos sexos se observa una tendencia al alza a lo largo de los años, en el caso de los hombres, aumentan desde 20.125 víctimas en el año 2011 a 34.019 en 2017 y, en el caso de las mujeres, aumentan de 14.561 víctimas en el 2011 a 28.305 en 2017.

En lo que respecta a la edad de las víctimas, los datos muestran que son las personas de 26 a 40 años quienes más sufren las actividades ilícitas que se realizan a

través de las TIC. Tras ellas, se encuentran las personas de 41 a 50 años y, en tercer lugar, los de 51 a 65 años. En todos los grupos de edades se observa ese aumento con el paso de los años, aunque son las tres franjas ya comentadas, junto con los de 18 a 25 años, quienes sufren un aumento más destacado.

Para concluir este análisis de datos, los datos de victimización según los diferentes grupos penales, sexo y edad muestran resultados similares a los que se han visto con anterioridad, siendo el fraude informático y las amenazas y coacciones aquellos grupos con mayores tasas de victimización, siendo el primero de ellos el grupo con un crecimiento más significativo a lo largo de los años analizados. Aunque también es destacable el crecimiento en la victimización del grupo de acceso e interceptación ilícita detectado en el año 2016, con 4.547 víctimas.

En relación al sexo y la tipología penal de las víctimas, los datos del año 2017 muestran que los hombres son con más frecuencia víctimas de delitos tales como el fraude informático (71,3%) y las amenazas y coacciones (20%). La misma situación se encuentra cuando se observan los datos de las mujeres, quienes son víctimas de fraude informático en un 65,2% de los casos y un 20% de amenazas y coacciones.

Y, por último, cuando se revisan los datos de victimización por edad y por grupo penal se observa que se acentúa el fraude informático sobre el resto de delitos, seguido de las amenazas y coacciones. En estos dos grupos penales, los grupos de edad que destacan son el de 26 a 40 años, seguido del grupo de más de 41 años. No se debe pasar por alto datos como los que nos ofrece el grupo de delitos sexuales, en el que destacan por encima del resto de grupos el de menores de edad.

6. CONCLUSIONES

El incremento de los delitos denunciados y clasificados por el Ministerio del Interior como ciberdelincuencia es evidente en los últimos años. Esto puede deberse al aumento progresivo que existe con el uso de las tecnologías en todos los ámbitos, ya que, las TIC han ido evolucionando y modificándose, a la misma vez que los seres humanos hemos ido adaptándonos a ellas. Esto significa que, al igual que la sociedad en general se ha trasladado al mundo *on-line*, los delincuentes lo han hecho también.

El estudio longitudinal que aquí se presenta arroja resultados interesantes respecto a la ciberdelincuencia denunciada. En relación con los datos que se han analizado, es destacable el incremento producido en este tipo de hechos, sobre todo, desde el año 2013, siendo el fraude informático y las amenazas y coacciones aquellos más comunes. Desde ese mismo año, se observa una tendencia a la baja de los delitos esclarecidos en relación con los hechos conocidos, esclareciéndose sólo el 27% de delitos en el año 2017. Es sumamente interesante observar cómo la tasa de

esclarecimiento es distinta según el tipo de ciberdelito al que nos refiramos. De este modo, aquellos hechos delictivos clasificados como ciberdelitos sociales presentan una tasa de esclarecimiento mucho mayor a los delitos clasificados como ciberdelitos económicos.

La evolución de las detenciones e investigados a lo largo de los años analizados nos indica que su tasa es especialmente baja (4.912 en el año 2017) si se comparan con la tasa de hechos conocidos (81.307 en el año 2017). En cuanto al género, hay una gran brecha en relación con este aspecto, que se mantiene en todos los grupos penales, destacando especialmente en determinados delitos, como los delitos sexuales y aquellos delitos cometidos normalmente por hackers. Respecto a la edad, destacan los grupos de personas jóvenes: los de 18 a 25 años, de 14 a 17 años y de 26 a 40 años desde el año 2013.

En último lugar, se han analizado los datos de victimización. Entre ellos se encuentra que la evolución de la victimización presenta una tendencia ascendente, como no podía ser de otra forma al constatar el aumento de los hechos conocidos, llegando a duplicarse el número de víctimas en el año 2017. En los datos sobre víctimas también se encuentra una importante brecha de género, siendo los hombres quienes más sufren estos delitos, aunque se debe señalar que, en esta ocasión, la diferencia no es tan destacable como en las detenciones. Y, respecto a la edad, estas víctimas tienen comúnmente entre los 26 y los 40 años.

No nos cabe la menor duda de que nos encontramos ante delitos que van a continuar engrosando las cifras de delincuencia en nuestro país. Este tipo de delitos van a continuar aumentando, debido a la transformación digital de las compañías y empresas tanto públicas como privadas, al aumento de la población que utiliza las TIC para comunicarse e interactuar con otros, a las dificultades de persecución de los ciberdelinquentes por cuestiones relacionadas con la extraterritorialidad y con la sensación de impunidad.

BIBLIOGRAFÍA

- CEREZO, Ana Isabel / LÓPEZ, Javier / PATEL, Ahmed, “International cooperation to fight transnational cybercrime”, en Preenel, Bart (ed.) / Gritzalis, Stefanos (ed.) / Kokolakis, Spyros (ed.) / Tryfonas, Theo (ed.), *Digital Forensic and Incident Analysis*, Ed. IEEE Computer Society, USA, 2007, págs. 13-27.
- DOMENIE, Miranda / LEUKFELD, Rutger / VAN WILSEM, Johan / JANSSEN, Jurjen / STOL, Wouter, *Victimisation in a Digitised Society*, The Hague: Eleven International Publishing, 2013.

- FLORES, Emilio Javier / ASANZA, María Isabel / BERRONES, Marcelo, “Ciberdelincuencia un mal que afecta a la sociedad actual”, en *Contribuciones a las Ciencias Sociales*, septiembre 2014, págs. 1-14.
- FUNDACIÓN TELEFÓNICA. sociedad digital en España 2017. Madrid: Ariel, 2018. <https://www.fundaciontelefonica.com/artecultura/publicaciones-listado/pagina-item-publicaciones/itempubli/625/>
- INSTITUTO ANDALUZ DE LA MUJER, Protocolo de detección e intervención en la atención a víctimas de ciberdelincuencia de género. Sevilla: IAM, 2015. <http://www.juntadeandalucia.es/iam/catalogo/doc/iam/2015/143528391.pdf>
- MIRÓ, Fernando, “La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen”, en *Revista Electrónica de Ciencia Penal y Criminología*, N° 13, 2011, págs. 1-55.
- MIRÓ, Fernando, El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio, España/Madrid: editorial Marcial Pons, 2012.
- MONTIEL, Irene, “Cibercriminalidad social juvenil: la cifra negra”, en *IDP. Revista de Internet, Derecho y Política*, N° 22, 2016, págs. 108-120.
- LOREDO, Jesús Alberto / RAMÍREZ, Aurelio, “Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo”, en *Celerinet*, 2013, págs. 44-51.
- RAYÓN, María Concepción / GÓMEZ, José Antonio, “Cibercrimen: particularidades en su investigación y enjuiciamiento”, en *Anuario Jurídico y Económico Esculiarense*, XLVII, 2014, págs. 209-234.
- ROCA, José Luis, Cibercrimen y ciberterrorismo: ¿exageración mediática o realidad? Proyecto Fin de Grado, España/Madrid: Universidad Politécnica de Madrid, 2014.
- VAN DE WEIJER, Steve; Leukferldt, Rutger; Bernasco, Wim, “Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking”, en *European Journal of Criminology*, Vol. 16, N° 4, 2019, págs. 486-508.