IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

ARTÍCULO

Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos[1]

Fernando Miró Llinares
Catedrático de Derecho Penal y Criminología de la Universidad Miguel Hernández de Elche

Fecha de presentación: julio de 2020
Fecha de aceptación: diciembre de 2020
Fecha de publicación: febrero de 2021

Resumen
Este trabajo aborda el impacto de la crisis de la COVID-19 en la cibercriminalidad, recopilando y valorando críticamente los estudios existentes y añadiendo análisis propios. Al respecto se plantea que, durante el confinamiento, más que un traslado de los delincuentes del espacio físico al ciberespacio, lo que ha existido es una adaptación de los cibercriminales a las nuevas oportunidades de delincuencia que surgían por el contexto de la COVID-19, así como un desplazamiento de las oportunidades al ciberespacio fruto del mayor tiempo y más actividades realizadas en internet, que podría haber derivado en un aumento de algunos ciberdelitos. Se argumenta que esta correlación negativa de tendencias, de reducción de la delincuencia en las calles y de aumento de la perpetrada en el ciberespacio, está directamente relacionada con el desplazamiento de actividades diarias derivada de la digitalización, que venía dándose desde hace décadas. La crisis de la COVID-19 aparece, así, más que como causante como aceleradora de tal proceso y se valora cómo incidirá ello en las tendencias del crimen en el futuro.

Palabras clave
cibercrimen, tendencias del crimen, desplazamiento, oportunidad delictiva, adaptación del cibercrimen

Tema
Criminología

1. Trabajo del proyecto «Criminología, evidencias empíricas y Política criminal». Referencia: DER2017-86204-R, financiado por la Agencia Estatal de Investigación (AEI)/Ministerio de Ciencia, Innovación y Universidades y la Unión Europea a través del Fondo Europeo de Desarrollo Regional-FEDER.

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Crime, cyberspace and Covid-19: (accelerated) displacement of opportunities and situational adaptation of cybercrime

Abstract

This paper addresses the impact of the Covid-19 crisis on cybercrime, gathering and critically evaluating the existing studies and adding some analyses of its own. The work suggests that during the lockdown, more than a shift of criminals from physical space to cyberspace, what has existed is, on the one hand, an adaptation of cybercriminals to the new opportunities for crime that were emerging in the context of Covid-19, and, on the other hand, a shift of opportunities to cyberspace as a result of the increased time and activities carried out on the Internet that could have effectively led to an increase in some cybercrimes. It is argued that this negative correlation of trends, of reduced crime on the streets and increased crime in cyberspace, is directly related to the shift in everyday activities resulting from digitisation, which has been taking place for decades. The Covid-19 crisis thus appears to be more than a cause but an accelerator of this process, and it is important to consider how this will affect future crime trends.

Keywords

cybercrime, crime trends, displacement, criminal opportunity, adaptation of cybercrime

Topic

Criminology

1. Tendencias del crimen y crisis de la COVID-19: el auténtico valor de los *outliers*

Dos modos antagónicos de afrontar, desde las ciencias sociales, el estudio de los diferentes impactos de la crisis sanitaria de la COVID-19 y el confinamiento social a ella ligado son, por un lado, el de medir y analizar desde ya, tratando de no desaprovechar el «experimento natural» que estamos viviendo y, por otro, el de rechazar cualquier análisis inmediato y apresurado esperando a tener más datos y una visión de conjunto del impacto para medir consecuencias y variables relacionadas con las mismas. Detrás de tales procederes, ambos defendibles, hay dos máximas compatibles entre sí y válidas para configurar una praxis de investigación racional en torno a estas cuestiones. Porque, si bien es claro que no podremos extraer conclusiones indiscutidas hasta más adelante y que será el paso del tiempo el que nos muestre en qué debiéramos fijarnos para comprender y comparar, también es cierto que «el grupo experimental» está «aconteciendo ahora» por lo que la oportunidad para recopilar información podría pasar, siendo este el momento de medir, recopilar y comenzar a comprobar si estamos fijándonos en lo que debemos.

El estudio de las tendencias del crimen está acostumbrado a vivir en esa tensión[2]: cualquier variación en la línea esperada parece un cambio de tendencia e incita a análisis inmediatos, pero, a la vez, nos obliga a la calma, a la revisión sosegada de los factores que podrían estar detrás de tal desviación o de que parezca tal y no lo sea. En la representación de la evolución macro de la delincuencia, como sucede con otros fenómenos sociales, las curvas acostumbran a ser largas y más bien suaves, con descensos o ascensos no muy pronunciados y valores generalmente estables. Pero si algo hemos aprendido de esta crisis sanitaria fijándonos en la evolución de las curvas epidemiológicas, es que las tendencias pueden cambiar de forma drástica cuando surgen cambios sociales dramáticos[3]. En este sentido, para el estudio de las tendencias del crimen esta crisis puede resultar una distracción, dado que los datos que de ella surgirán supondrán un *outlier*, una observación claramente distante del resto de los datos. Es tan obvio que una intervención social tan masiva como fue la del confinamiento social durante la crisis de la COVID-19 afectará a las tendencias del crimen por la significativa reducción de la movilidad, que si nos centramos exclusivamente en la visualización comparada de las curvas a lo largo del tiempo difícilmente obtendremos nada que no sepamos. Pero los *outliers* son «un problema» si se pretende su inclusión junto al resto de datos. En cambio, los mismos constituyen un significativo indicio de algún problema estadístico o de alguna variable relevante que generalmente no tomamos en cuenta. Quizá lo que hay que hacer es centrarse en el *outlier*, aislarlo y comprender su relación con las variables que nos interesan.

A mi parecer la crisis del coronavirus es una oportunidad para profundizar en el impacto que tiene la movilidad cotidiana en las tendencias del crimen, en particular para tratar de comprender sus condicionantes e impactos en relación con otros cambios que están aconteciendo en nuestra vida y que son menos llamativos y estridentes pero que pueden ser determinantes a la hora de definir las curvas a largo plazo[4]. Uno de ellos es la irrupción de la tecnología digital y el impacto que la misma tiene, ha tenido y tendrá en la evolución de la delincuencia en los últimos treinta años[5]. En este sentido, la crisis de la COVID-19 ha precipitado, y exagerado en el tiempo, un cambio que venía produciéndose desde hace tiempo, como es el traslado de algunas actividades del espacio físico al ciberespacio. Y dado que ahora tenemos aislada la variable «movilidad» puede ser un buen momento para analizar cómo ello ha impactado a la delincuencia perpetrada en el ciberespacio.

2. Baumer, Velez y Rosenfeld (2018).
3. Según Rosenfeld (2018), el estudio de las tendencias de la delincuencia sigue dos caminos: las investigaciones sobre cambios lentos de los índices de delincuencia, y las investigaciones sobre cambios inesperados y abruptos como resultado de perturbaciones externas.
4. Stickle y Felson (2020) califican la crisis como un gran «experimento natural», una oportunidad para estudiar el funcionamiento ecológico del delito.
5. Véase Miró Llinares y Moneva (2019).

2. De las calles a las casas y de allí al ciberespacio: correlación negativa entre tendencias delictivas por la crisis de la COVID-19

Un ejemplo de predicción precipitada, aunque intuitivamente razonable y probablemente acertada, relacionada con el impacto de la crisis de la COVID-19 en el delito, es la del descenso general de la delincuencia urbana y el aumento de la cibercriminalidad y los delitos en el ámbito doméstico. Dentro de esa idea de «el delito, de las calles a internet», hay dos cuestiones que deben ser analizadas por separado: la primera, si realmente se pueden dar por ciertas las tendencias (inversas) hipotetizadas para los diferentes fenómenos delictivos; la segunda consiste en aclarar si se pueden relacionar de algún modo ambas tendencias. Y me refiero a que se relacionen entre sí en algún sentido distinto al de compartir los cambios de ambas idéntico origen etiológico: la existencia de una pandemia. Se trata, en definitiva, de analizar si la correlación (en un sentido de relación negativa) entre ambas tendencias tiene como causa algo que con la crisis del coronavirus se ha puesto especialmente de manifiesto pero que, en realidad, va más allá de ella y que en tiempos de «normalidad» también pueda acontecer. Antes de ello, sin embargo, hay que confirmar las tendencias o, cuanto menos, encontrar indicios de las mismas. Y no parece tan sencillo.

De momento ya existen algunas investigaciones que aportan evidencias sobre el impacto en el crimen del distanciamiento social adoptado tras la pandemia de la COVID-19. Los primeros estudios muestran tasas de criminalidad inferiores a las esperadas según los modelos de series temporales en varias modalidades de delincuencia urbana, si bien tales «descensos» muestran significativas variaciones según la modalidad delictiva y el lugar[6]. Menos datos hay sobre la evolución de la delincuencia perpetrada en el ámbito familiar, aunque los que hay parecen confirmar el incremento debido al aumento del contacto y la oportunidad[7].

Es posible que con el paso del tiempo dispongamos de mejor información sobre ambas tendencias. Es posible que no y que, existiera tal aumento o no, ello quede invisibilizado al no denunciarse. Algo similar sucede con la ciberdelincuencia. La predicción del incremento del cibercrimen también estaba presente en cualquier análisis sobre el impacto de la COVID-19 en la delincuencia[8]. Esto a veces se expresaba equívocamente como que los delincuentes se trasladaban de las calles a los ordenadores, obviando tanto la complejidad técnica de algunas formas delictivas perpetradas en internet (la gran mayoría no[9]) como que muchos delitos, especialmente los patrimoniales, tienen mucho más que ver con oportunidades surgidas que con «maldades planeadas» que permiten cambiar de un lugar a otro. Pero lo que siempre se expresaba es que el delito en internet crecería. Si todo está cerrado en las calles y todo, o casi, acontece en internet (el trabajo, el ocio, la compra de comida, el consumo de información sanitaria, etc.,) parece lógico pensar que también el delito vaya a acontecer allí. De este tipo fue el pronóstico de Europol, justo al comienzo de la crisis del

6. Diferentes trabajos muestran ya la evolución descendente de varios delitos en diferentes países en el período de confinamiento. Véase Payne y Morgan (2020). «COVID-19 and violent crime» [Payne, Morgan y Piquero (2020)]; Ashby, M. P. J. (2020); Hodgkinson y Andresen (2020); Mohler *et al.* (2020); Halford *et al.* (2020); Abrams (2020); Campedelli, Favarin, Aziani y Piquero (2020).
7. Piquero *et al.* (2020) muestran un incremento en las dos semanas posteriores al confinamiento y una disminución posterior, destacando la dificultad de determinar si el bloqueo fue la causa puesto que la violencia doméstica venía aumentando en Texas. El confinamiento muy probablemente reduce las posibilidades de denuncia dada la potencial vigilancia del agresor, señalan Bullinger, Carr y Packham (2020); Leslie y Wilson (2020); Bradbury Jones y Isham (2020). En España los casos activos en VioGén se han mantenido estables y el crecimiento acumulado de víctimas sigue la tendencia lineal creciente. Aumentaron las llamadas al 016: un 67% en abril de 2020, más (8.692) que en febrero de 2020 (5.194), y un 61% más que en abril de 2019 (5.396). Esto contrasta con las altas nuevas en (ATENPRO) para víctimas no convivientes, que bajaron (383 altas en abril de 2020, 889 en febrero de 2020 o 742 en abril de 2019). Véase: https://violenciagenero.igualdad.gob.es/violenciaEnCifras/boletines/boletinMensual/2020/docs/BE_Mensual_Abrl.pdf [Fecha de consulta: 10 de enero de 2021]. Detrás de estas cifras podría estar la mayor exposición a la violencia de género durante el confinamiento en el caso de convivencia con la pareja agresora y la reducción cuando no existe. En relación con los menores, los datos son escasos, si bien Pereda y Díaz-Faes (2020) señalan que el confinamiento habría atrapado a niños víctimas de agresiones domésticas en los hogares aislándoles de potenciales protectores e incrementando el estrés en hogares vulnerables y el riesgo de violencia.
8. Halford *et al.* (2020); Nikolovska, Johnson y Ekblom (2020).
9. Miró Llinares y Moneva (2020).

coronavirus, expresado en la idea de que «*the number of cyber-attacks is significant and expected to increase further*», y apoyado en dos argumentos: en la constatación de que estaban empezando a usarse referencias a la COVID-19 para actividades fraudulentas en internet; y en que el incremento de la actividad en internet fruto del mayor tiempo en casa, la adopción del teletrabajo y la conexión entre ordenadores personales y de empresa, incrementaría las oportunidades delictivas allí[10]. Es necesario diferenciar ambos presupuestos. La constatación de que estaban empezando a aflorar ciberataques en webs, archivos descargables o correos tematizados con nombres como COVID-19, coronavirus o demás, ni indicaba un aumento de la cibercriminalidad ni puede considerarse un argumento etiológico en sí mismo. Tal declaración consistía en la descripción de una adaptación de los cibercriminales al nuevo contexto de oportunidad que ofrece el ciberespacio más que en una predicción sobre un incremento en el delito perpetrado. Puede ser que haya más criminales o más conductas delictivas en el ciberespacio, pero también puede ser que no, y desde luego eso no queda probado porque a raíz de la crisis de la COVID-19 se incrementaran las páginas web fraudulentas que usaban tales términos clave[11].

La hipótesis de que el mayor uso de los servicios de internet, debido al mayor tiempo en casa, derivará en un incremento de la cibercriminalidad se fundamenta en la relación entre cotidianeidad, oportunidad y delincuencia: si es en internet donde pasan tiempo será allí donde surjan las oportunidades que interaccionarán con sus motivaciones delictivas; y lo mismo se podría decir para las víctimas, que será en el ciberespacio donde converjan con quienes les ataquen[12]. Una de las consecuencias del confinamiento fue la reducción de la movilidad y el aumento del tiempo en casa, y ello ha conllevado tanto un mayor uso general de internet como la realización de actividades nuevas en el ciberespacio para un gran número de usuarios. Tanto Apple[13] como Google[14] han ofrecido datos sobre los cambios en la movilidad de sus usuarios, en los que se muestra una reducción sensible de la movilidad a partir de la entrada en vigor del estado de alarma (véanse gráficos 1 y 2).

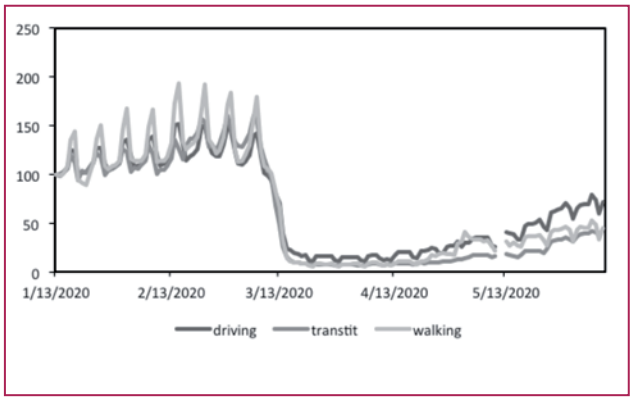

Gráfico 1. Gráfico de los porcentajes de cambios en la movilidad según el medio de transporte. Elaboración propia a partir de los datos ofrecidos por Apple.

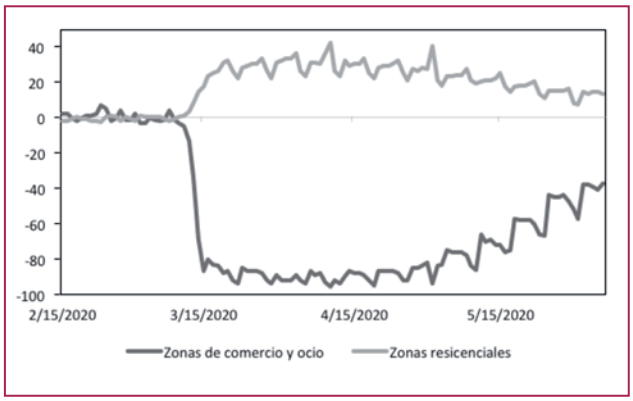

Gráfico 2. Porcentaje de cambios en la movilidad entre zonas de comercio y ocio y zonas residenciales. Elaboración propia a partir de los datos facilitados por Google.

Aunque para realizar análisis profundos habría que desagregar los datos al máximo posible dado que no en todos los lugares, ni desde el mismo momento, se produjo la misma reducción de movilidad, parece indiscutible el aumento del tiempo en casa y, según un estudio realizado

10. Europol (2020*b*).
11. Sí es posible que haya más victimización debido a que los cibercriminales adaptasen su ingeniería social, pero demostrarlo exigiría comparar la evolución antes y después del confinamiento.
12. Véase Bruinsma y Johnson (2018); Miró Llinares (2011); Holt y Bossler (2008); Miró Llinares y Moneva (2020).
13. Apple Maps (2020).
14. Google (2020*b*).

por GlobalWebIndex sobre los hábitos de la población durante el confinamiento[15], ello también derivó en un mayor tiempo en el ciberespacio mediante el uso de distintas tecnologías (gráfico 3).

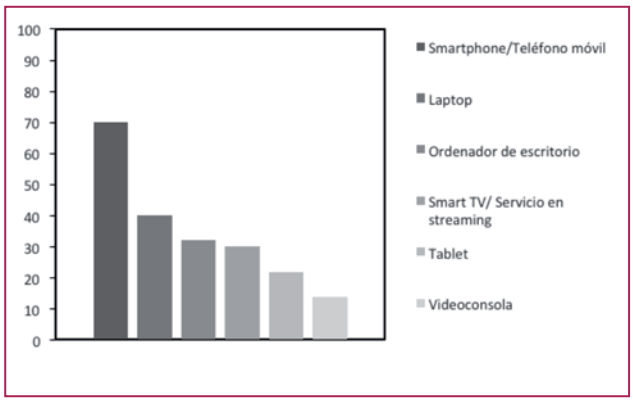

Gráfico 3. Proporción de encuestados que afirma hacer mayor uso de dispositivos conectados. Elaboración propia a partir de los datos ofrecidos por GlobalWebIndex (2020).

La conexión de los datos de movilidad con el marco teórico de la oportunidad, que convierte en plausible el pronóstico del aumento de la cibercriminalidad, debe someterse, sin embargo, al menos a dos matizaciones. La primera es que lo que determina la victimización o la perpetración de ciberdelitos no es tanto «pasar tiempo en internet» sino la generación de ámbitos particulares de interacción o convergencia que, además, serán distintos en términos de riesgo (u oportunidad) criminal según las características del lugar[16]. No se trata de que más tiempo en internet conllevará más victimización, sino que hacer más cosas en internet, y en particular hacer en internet cosas que antes no se hacían a través de internet, determinará nuevas formas de convergencia que llevará a nuevos crímenes perpetrados por los agresores sobre más víctimas. La segunda matización es que el término «cibercriminalidad» no describe una tipología delincuencial, ni un conjunto de ellas, sino una macrocategoría de formas delincuenciales exclusivamente unidas por acontecer en el ciberespacio, que es lo mismo que decir que en todas ellas internet se convierte en un elemento esencial del evento delictivo. Y precisamente por eso, el que cada cibercrimen aumente dependerá de la concreta conexión de cada ciberdelito con las oportunidades que se han visto aumentadas o reducidas a raíz de la crisis de la COVID-19.

Respecto al impacto que ha tenido la COVID-19 en la cibercriminalidad, a la espera de que el informe estadístico de la cibercriminalidad se actualice a lo largo de este año y nos ofrezca datos oficiales en España –datos que, de todos modos, deberán adoptarse con la máxima cautela– y al margen de declaraciones más llamativas que rigurosas como la del aumento de los ciberdelitos en un 600%[17], hay otro tipo de estudios y datos oficiales de informes de agencias privadas y públicas en el ámbito internacional que apuntan al citado aumento «de la cibercriminalidad», concretado en tipologías concretas pertenecientes, además, a cada uno de los tres grandes ámbitos de delincuencia en el ciberespacio: la ciberdelincuencia económica, final o instrumental, la ciberdelincuencia social o personal y la ciberdelincuencia política o ideológica[18]. Comenzando por los primeros, la alerta de Europol sobre el posible incremento de la ciberdelincuencia durante la crisis de la COVID-19 incluía su predicción de un aumento de delitos como el *ransomware*, los ataques por denegación de servicio (*DDoS*) y la creación de dominios maliciosos[19]. Algunas de estas predicciones parecen confirmarse, en concreto los ataques de denegación de servicio. El Centro de Ciberdelincuencia de Cambridge recogió, mediante sensores *honeypot* los ataques de denegación de servicio desde principios del año 2020 en todo el mundo, mostrando una clara tendencia al alza desde finales de febrero[20]. La empresa Kaspersky también muestra resultados similares; en su informe indica que los ataques *DDoS* se duplicaron en el primer trimestre de 2020 en relación con los dos trimes-

15. GLOBALWEBINDEX (2020).
16. Véase Ngo *et al.* (2020).
17. Declaración en el consejo de seguridad de NU, según Newtral, en: https://www.newtral.es/la-pandemia-traslada-mas-delitos-al-mundo-digital/20200604/ [Fecha de consulta: 10 de enero de 2021]. Sobre cifra negra y medición del cibercrimen, Fafinski, Dutton y Margetts (2010); Miró Llinares (2012); véase recientemente Kemp, Miró Llinares y Moneva (2020).
18. Miró Llinares (2020).
19. Europol (2020*a*).
20. Collier *et al.* (2020).

tres anteriores[21]. Los informes de transparencia de Google también muestran, desde el 15 de marzo, tanto un incremento acelerado del número de sitios de suplantación de identidad existentes como de los detectados por semana[22]. El informe sobre ciberseguridad durante los cien primeros días de la COVID-19 de MIMECAST[23] muestra que la detección de *spam* tuvo un incremento del 26,3%, la detección de suplantación de identidad aumentó en 30,3%, la detección de *malware* un 35,16% y el bloqueo de clics por URL peligrosas se incrementó en un 55,8% en relación con la primera semana del año.

En cuanto a la cibercriminalidad «social»[24], Europol también alertó de la posibilidad de un incremento de los delitos relacionados con la explotación sexual infantil por el mayor tiempo en casa de la población[25], y aunque no hay datos concluyentes comparables con tendencias anteriores, desde España se avisó sobre un incremento del 25% de IP detectadas que habían descargado contenidos de pornografía infantil entre la segunda y la tercera semana de marzo. También se produjo un incremento del 25% de los casos reportados por ciudadanos a las autoridades en marzo en relación con febrero, relativos a contenido de pornografía infantil en internet. El número de denuncias (cerca de quinientas) es el tercero más alto en un mes desde 2017. En Italia los datos ofrecidos parecen ser similares, con 181 denuncias relativas a pornografía infantil en la primera quincena de marzo, frente a 83 denuncias en el mismo período de tiempo en 2019[26].

Finalmente, en relación con los ciberdelitos políticos, si hay un fenómeno que podría haber experimentado un significativo crecimiento por el mayor consumo ciudadano de información en la situación de pandemia es el de las *fake news* o desinformación. En un estudio publicado por el Instituto de Reuters[27] se puede observar cómo desde el mes de enero al mes de marzo el número de verificaciones de hechos aumentó más del 900%; y ya que los verificadores de hechos no disponen de capacidad para comprobar todo el contenido problemático, es muy probable que el volumen total de desinformación sobre el coronavirus haya crecido aún más. De manera similar se ha evidenciado el incremento del uso de *bots* en campañas de odio[28].

Dejando de lado este tipo de indicios referidos a formas concretas de ciberdelincuencia, el primer estudio que ha tratado de analizar de forma general el impacto de la pandemia en el cibercrimen es el de Hawdon, Parti y Dearden[29], quienes realizaron encuestas de cibervictimización para siete ciberdelitos en dos momentos diferentes, uno entre el 24 y el 30 de noviembre de 2019, y otro entre el 14 y el 17 de abril de 2020. Los autores no encontraron diferencias estadísticamente significativas para los siete delitos en conjunto y tan solo el delito de robo de datos mostró diferencias significativas, siendo el resultado el contrario al esperado, con una mayor tasa en el grupo «pre-COVID». El hecho, sin embargo, de que ambos grupos fueran preguntados sobre victimización sufrida «en el último año», y no en el período pre-COVID y pos-COVID, solapándose incluso los tiempos, resta a mi parecer significación a los resultados del estudio.

De hecho, las investigaciones que, a mi entender, mejor reflejan lo que ha pasado sí muestran un incremento de la cibercriminalidad económica y lo ligan con el cambio de actividades cotidianas y el desplazamiento de oportunidades. La primera de ellas es un estudio sobre los datos de Action Fraud[30] en el Reino Unido[31]. Partiendo del cambio de oportunidades que suponen los cambios en las actividades cotidianas como consecuencia de las medidas de confinamiento, que afectaron con mayor intensidad en los meses de abril y mayo de 2020, comparamos el número de cibercrímenes puros y ciberfraudes registrados por la policía entre mayo de 2019 y mayo de 2020 y

21. Kupreev, Badovskaya y Gutnikov (2020).
22. Google (2020*a*).
23. Mimecast (2020).
24. Miró Llinares (2012).
25. Europol (2020*a*).
26. Attanasio (2020).
27. Brennen *et al.* (2020).
28. Uyheng y Carley (2020).
29. Hawdon, Parti y Dearden (2020).
30. El Centro Nacional de Denuncias de Fraude y Delitos Cibernéticos del Reino Unido.
31. Buil-Gil, Miró Llinares, Moneva, Kemp y Díaz-Castaño (2020).

analizamos la evolución en los doce últimos meses. Los análisis mostraron que la mayoría de los ciberfraudes aumentaron en el Reino Unido durante el brote de la COVID-19, y que las tasas de cibercrímenes fueron particularmente altas durante los dos meses con las políticas y medidas de bloqueo más estrictas, lo que sugiere que los cambios en las actividades cotidianas de millones de personas, trasladándose de entornos físicos a entornos *online*, desplazó las oportunidades para cometer delitos de forma *online*. El estudio también evidenció un aumento de los fraudes en las compras *online*, que afectó tanto a personas como a empresas, mientras que el incremento de los cibercrímenes afectó principalmente a las víctimas individuales, y la mayoría de los ciberdelitos a los que se enfrentan las empresas disminuyeron; seguramente como consecuencia de que las oportunidades de dirigirse a las empresas disminuyeron dada la gran cantidad de negocios que cesaron su actividad durante el brote (véase gráfico 4).

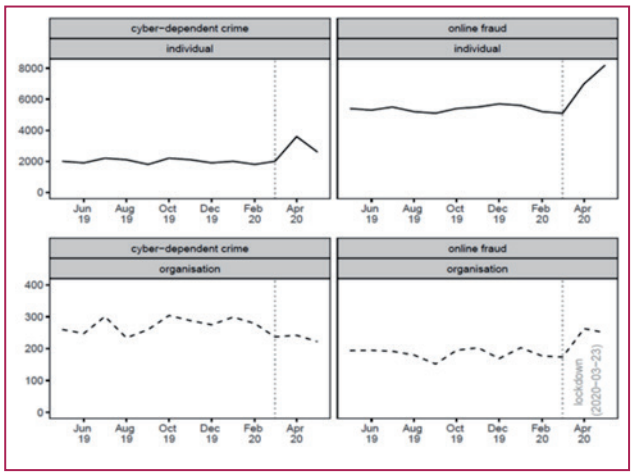

Gráfico 4. Número de delitos ciberdependientes y fraudes online conocidos por la policía de mayo de 2019 a mayo de 2020. Fuente: Buil-Gil, Miró Llinares, Moneva, Kemp y Díaz-Castaño (2020).

Continuando con este enfoque, y con los mismos datos, he llevado a cabo para este trabajo un análisis específico buscando comprender mejor el significado del «desplazamiento de oportunidades al ciberespacio». Las restricciones impuestas durante la cuarentena obligaron a algunas personas a hacer en internet actividades que antes no hacían allí (especialmente compras), y es eso lo que aumentó el ciberfraude. No obstante, hay ciberfraudes íntimamente relacionados con actividades del espacio físico y era de imaginar que si, como consecuencia del confinamiento, aquellas actividades se veían afectadas, ello repercutiera en una reducción de los mismos. Para comprobarlo, comparo el delito de fraude *online* por venta de entradas (generalmente espectáculos en el espacio físico) con los fraudes en compras y subastas *online*. En ambos casos el agresor y la víctima están en el ciberespacio, pero la actividad se da en el espacio físico. Como era de esperar, el fraude por venta de entradas muestra una tendencia decreciente cuyo descenso se intensifica en marzo de 2020, coincidiendo con la anulación de importantes eventos[32]. Cuando comparamos los meses de mayo de 2019 y mayo de 2020 observamos una reducción del 88%. En contraposición, la tendencia de los fraudes en compras y subastas *online* perdió la estabilidad que la caracterizaba en el período anterior al brote de la COVID-19, experimentando un fuerte crecimiento a partir del inicio del confinamiento. Al comparar los meses de mayo de 2019 y 2020 observamos un incremento del 52% (véanse gráficos 5 y 6).

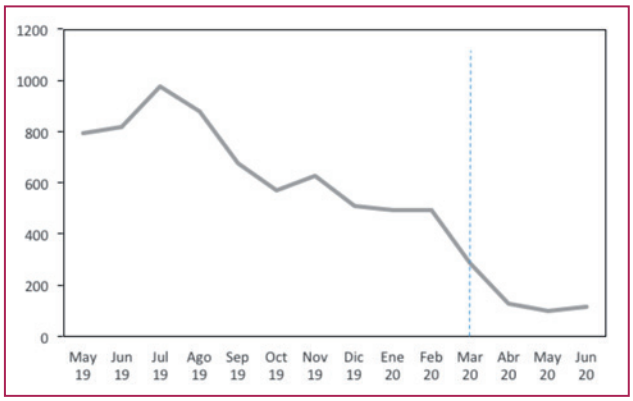

Gráfico 5. Número de delitos de fraude en entradas conocidos por la policía de mayo de 2019 a junio de 2020. Fuente: Auction Fraud. Elaboración propia.

32. Por ejemplo, la cancelación de distintos eventos deportivos como la Premier League (BBC SPORT): https://www.bbc.com/sport/football/51760339; o de los eventos de boxeo (SKYSPORTS): https://www.skysports.com/boxing/news/12183/11958895/coronavirus-british-boxing-board-of-control-cancels-all-events-due-to-pandemic.

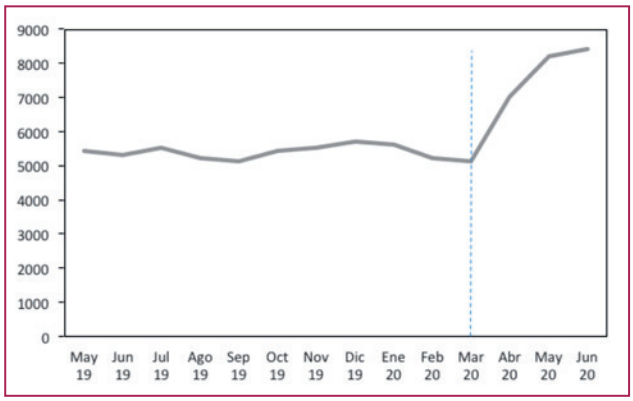

Gráfico 6. Número de delitos de fraude en compras y subastas online conocidos por la policía de mayo de 2019 a junio de 2020. Fuente: Auction Fraud. Elaboración propia.

Estos resultados se ven, de algún modo, consolidados al observar los de una investigación más reciente realizada por los mismos investigadores con datos de Action Fraud desde 2017. Usando modelos ARIMA se ve que tanto la ciberdelincuencia propiamente dicha como el fraude *online* (especialmente el fraude en compra y subasta) subieron durante el confinamiento más allá de lo que la tendencia pronosticaba. Lo interesante es que al terminar el confinamiento el cibercrimen puro ha vuelto a los niveles pronosticados, pero el ciberfraude no. La razón, de nuevo, es que, si bien un mayor tiempo en internet no tiene por qué crear más oportunidades para el cibercrimen puro, algunas oportunidades cuyo traslado se había acelerado con el confinamiento (mayor uso del ciberespacio para compras) podrían haberse quedado y, con ello, el aumento de los cibercrímenes réplica[33].

3. La adaptación de los cibercriminales al contexto COVID-19

3.1. Algunas bases teóricas: adaptación mejor que desplazamiento del cibercrimen

Que sea erróneo hablar del desplazamiento de los cibercriminales para referirse a la relación entre la tendencia de descenso de la delincuencia en las calles y el aumento en el ciberespacio, no significa que algunos criminales no estén desplazando sus actividades al ciberespacio (organizaciones delictivas) ni que no haya existido desplazamiento de la cibercriminalidad o, algo similar a eso, adaptación[34]. Ante la constatación de que el crimen no tiene éxito, de que las medidas de prevención funcionan, o de que hay nuevas o mejores oportunidades, los delincuentes, también los cibercriminales, cambian los objetivos, los medios o tácticas para su ejecución, los tipos de infracción o, incluso, la identidad virtual o «ciberlugar» desde donde se realiza el ataque[35].

Adaptación tipológica	Los delincuentes responden al bloqueo de un determinado tipo de acto delictivo, cometiendo delitos totalmente diferentes.
Adaptación de objetivo	Los cibercriminales desechan el ataque a objetivos bien protegidos y centran sus esfuerzos en otros más vulnerables.
Adaptación técnica	El cibercriminal mejora su ataque y utiliza nuevos instrumentos para superar las nuevas barreras.
Adaptación de ciberlugar	Los cibercriminales cambian el lugar en el ciberespacio desde el que realizan el ataque o el nombre de la web desde el que actúan criminalmente.

Tabla 1. Adaptación del crimen al ciberespacio. Fuente: Miró Llinares (2012).

La crisis de la COVID-19 ha derivado en cambios en los intereses, necesidades y actividades cotidianas de la población y esto en nuevas oportunidades para los ciberdelincuentes, que han tratado de adaptarse y sacar provecho de la situación, principalmente mediante adaptaciones relacionadas con el cambio de objetivo y de ciberlugar. En relación con la adaptación al objetivo, el sistema sanitario se ha convertido en un objetivo de mayor interés. Así lo muestran los resultados relativos a los ataques sufridos por sector que proporciona Atlas, en los que se observa que en el primer cuatrimestre de 2020 el sector sanitario sufrió un 70% más de ataques que en el mismo período del año anterior, mientras que otros sectores, como el sector

33. John (2020).
34. Mattei (2017).
35. Interpol (2020).

hotelero, mostraron una clara disminución de ataques[36] (véase gráfico 7). Si bien el sector sanitario ya era una infraestructura crítica de interés antes de la pandemia[37], la crisis de la COVID-19 lo situó en una posición más vulnerable y, seguramente por ello, aumentaron los ataques tipo *ransomware* contra hospitales y otras instituciones sanitarias dedicadas a la lucha contra el virus[38], viendo la oportunidad de que la crisis ofreciese mayores garantías de pago por la mayor urgencia de evitar el colapso. Pero la pandemia también ha convertido en un objetivo estratégico a los centros de investigación, debido al valor económico e industrial que suponen las investigaciones relacionadas con el desarrollo de tratamientos y vacunas: así, el FBI ha detectado un incremento en los accesos ilícitos a información e investigaciones relacionadas con el tratamiento y la vacuna[39].

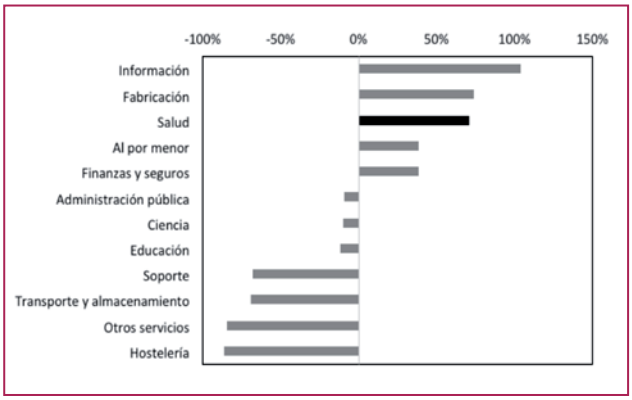

Gráfico 7. Cambios en el número de infracciones según el sector entre el primer trimestre de 2019 y el primer trimestre de 2020. Elaboración propia a partir de datos de AtlasVPN (2020).

También hay adaptación de objetivo en el desplazamiento de algunos ciberataques hacia los trabajadores individuales debido al teletrabajo. El aumento del uso de herramientas de acceso remoto ha coincidido, según los datos ofrecidos por Kaspersky, con un aumento en el número de ataques «al protocolo de escritorio remoto», una de las herramientas de acceso remoto más habituales que busca identificar nombre de usuario y contraseña para poder acceder a la red de la organización. El objetivo sigue siendo la organización, pero el vector de ataque es ahora el teletrabajador, más vulnerable ahora al no acceder a la red desde la oficina, una infraestructura normalmente configurada, monitoreada y controlada por un departamento tecnológico, sino desde su ordenador personal y red doméstica, normalmente menos segura. Según los datos ofrecidos por Kaspersky, el número de este tipo de ataques ascendió desde los 28,8 millones en febrero hasta los 96,7 millones en marzo, lo que supone un incremento del 236%[40]. Los datos ofrecidos por la compañía ESET también muestran un incremento significativo de este tipo de ataques[41]. Por otro lado, la situación de teletrabajo y teleformación ha popularizado el uso de herramientas de videoconferencia. El FBI ha advertido sobre el secuestro y toma de control de este tipo de sesiones, con el objetivo de entorpecerlas, actuando de forma vandálica, convirtiendo por lo tanto a los teletrabajadores en objetivo del ciber-vandalismo[42]. Además del vandalismo asociado con las videoconferencias, también han aparecido aplicaciones y webs falsas, suplantando a las aplicaciones legítimas de videoconferencia, con el fin de instalar *software* malicioso[43], aunque en este caso estaríamos hablando de una adaptación de ciberlugar.

36. John (2020).
37. Mattei (2017).
38. Interpol (2020).
39. Federal Bureau Of Investigation (2020).
40. Galov (2020).
41. ESET (2020).
42. FBI (2020).
43. Es el caso de ZOOM, Cyvare Social (2020). Véase también Naidoo (2020).

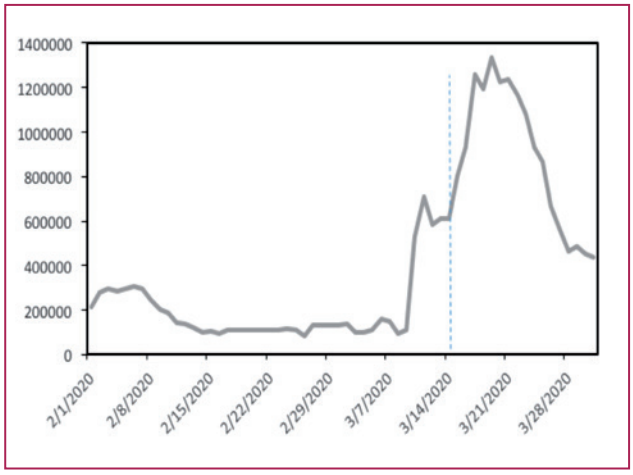

Gráfico 8. Número de ataques por fuerza bruta contra el protocolo de escritorio remoto conocidos por Kaspersky entre febrero y marzo de 2020. Elaboración propia a partir de los datos ofrecidos por Galov (2020).

Esta es, en efecto, la segunda modalidad más clara de adaptación propiciada por la pandemia, aquella en la que el sujeto «desplaza» el ciberlugar, o la apariencia del mismo, desde el que ataca. El cambio en las necesidades de los ciudadanos derivadas de la crisis también ha modificado sus actividades *online*. Un claro ejemplo es el incremento del interés por mantenerse informado en relación con el virus. Si atendemos a los datos relativos a las tendencias de consultas realizadas en Google podemos observar un fuerte crecimiento en las búsquedas relacionadas con la COVID-19 y el coronavirus a partir del mes de marzo[44]. Este interés de la población ha supuesto una oportunidad para los cibercriminales, que han creado multitud de dominios en los que se emplea el término coronavirus, COVID-19 u otras palabras relacionadas con la enfermedad. Así lo evidencian los informes ofrecidos por diferentes empresas tecnológicas como Check Point[45], Forcepoint[46], DomainTools, vía Cyber Threat Coalition[47] o la Unidad 42 de Paloalto Networks[48]. Check Point indica que, de los más de 30.000 dominios relacionados con el coronavirus que analizaron, el 0,4% eran maliciosos y un 9% eran sospechosos, lo que según esta empresa supone que los dominios relacionados con el coronavirus tienen un 50% más de probabilidades de ser maliciosos que otros dominios.

El interés respecto al coronavirus también ha supuesto una oportunidad para la propagación de *spam*. A finales de abril, Trend Micro había detectado más de novecientos mil mensajes de *spam* relacionados con el virus[49]. Forcepoint también muestra cómo los correos de *spam* relacionados con el coronavirus crecieron fuertemente durante los meses de marzo y abril. Los delitos de *phishing* también han visto la oportunidad de aprovechar la pandemia mediante la simulación de agencias relacionadas con la lucha contra el virus, situación de la que han alertado la propia Organización Mundial de la Salud[50] o el Centro de Control de Enfermedades de Estados Unidos[51] al advertir la presencia de sitios web que trataban de suplantarlos con la finalidad de obtener datos personales de las víctimas o instalar *software* malicioso.

Por último, una mezcla de adaptación tipológica y de lugar es la que ha existido en relación con la falsa venta de mascarillas y otros productos sanitarios. Ante el fuerte interés social por adquirir estos productos, algunos delincuentes, de los cuales es posible que operaran como organizaciones criminales principalmente en el espacio físico, han aprovechado el tiempo para crear supuestas tiendas *online*, vendiendo productos sanitarios como mascarillas o desinfectantes que finalmente nunca llegaban, ya que se trataba de una estafa o que, simplemente, no ofrecían las especificaciones ofertadas[52]. Por su parte, Amazon también tuvo que suspender miles de cuentas por crear anuncios falsos, o con precios abusivos relacionados con productos sanitarios[53].

44. En: https://trends.google.es/trends/
45. Según Checkpoint (2020), se registraron 15.000 dominios diarios durante las primeras semanas de marzo.
46. Forcepoint (2020).
47. Cyberdata Coalition (2020).
48. Szurdi, Chen, Starov, McCabe y Duan (2020).
49. Trendmicro (2020).
50. Mackey, Li, Purushothaman, Nali, Shah, Bardier y Liang (2020). Véase también: World Health Organization (2020).
51. Center for Disease Control and Prevention (2020).
52. Szurdi, Chen, Starov, McCabe y Duan (2020).
53. Hilder (2020).

4. Conclusiones

La crisis de la COVID-19 ha sido de tal impacto que, por un lado, resulta difícil calibrar ahora todos los cambios que causará, pero, por otro, resulta imposible no anticipar ejemplos evidentes e inmediatos del mismo. En relación con el cibercrimen hemos visto cómo ha habido un aumento de algunos ciberdelitos debido al incremento (y al desplazamiento) de oportunidades en el ciberespacio, así como una adaptación de los cibercriminales al contexto COVID-19 tanto en objetivos y métodos como, sobre todo, en ciberlugares de ataque. Que ello haya coincidido con un descenso de la delincuencia en el espacio físico, especialmente en las calles, no es casualidad, pero tampoco es causalidad: no se trata de que se hayan desplazado los delincuentes de un lugar a otro (aunque en algún caso podrían haberlo hecho, como hemos señalado), sino de que las actividades cotidianas que dibujan las oportunidades delictivas sí han cambiado de lugar y con ello se han desvanecido algunas oportunidades por un lado y han aparecido otras por otro. En realidad, no es que el confinamiento haya desplazado a los delincuentes de las calles a las casas, sino que ha desplazado muchas actividades de las calles al ciberespacio y, con ello, ha configurado nuevas oportunidades fruto de la convergencia entre agresores y víctimas en ausencia de guardianes. Por otro lado, los delincuentes sí se han desplazado, pero sobre todo lo han hecho dentro del ciberespacio, adaptándose, aprovechando nuevas circunstancias, nuevos intereses sociales, nuevas preocupaciones, para incrementar el éxito en los fraudes de siempre.

Sería un error, sin embargo, pensar que el desplazamiento de oportunidades es fruto de la crisis de la COVID-19. En realidad, la pandemia lo que ha hecho es acelerar significativamente, durante un tiempo primero, pero con potenciales efectos duraderos después, una tendencia que venía de lejos. El traslado de las oportunidades delictivas del espacio físico al ciberespacio viene de antes, aunque ahora se haya hecho más evidente, y está íntimamente relacionado con el cambio de muchas actividades cotidianas que antes se desarrollaban en el *meatspace* exclusivamente y que ahora también ocupan el *cyberspace*. El ocio, las compras, las relaciones sociales, incluso las sexuales, cada vez más se llevan a cabo en el ciberespacio dando lugar a nuevas oportunidades delictivas, y por el contrario cada vez hay más actividades que se llevaban a cabo en el espacio físico para las que hay menos tiempo, como el deambular de los jóvenes en las calles que, junto a otros factores, podría estar relacionado con el descenso de algunas formas de delincuencia en las últimas décadas. Obviamente, la COVID-19 ha exagerado y profundizado esta tendencia: el teletrabajo, las videoconferencias, las compras *online*, han recibido un impulso espectacular durante la pandemia y, aunque tras el confinamiento pueden haber descendido, desde luego es difícil imaginar que lo haga a niveles anteriores. El confinamiento ha acelerado y acelerará la digitalización, que, a su vez, ya estaba desplazando al ciberespacio actividades cotidianas y con ello oportunidades que hacen que aumenten los ciberdelitos.

Referencias bibliográficas

ABRAMS, D. (2020). «COVID and crime: an early empirical look». U of Penn. ILERP, núm. 20-49 [en línea] DOI: https://doi.org/10.2139/ssrn.3674032 [Fecha de consulta: 10 de enero de 2021].

ACTION FRAUD. Centro Nacional de Denuncias de Fraude y Delitos Cibernéticos del Reino Unido [en línea] https://www.actionfraud.police.uk/data [Fecha de consulta: 10 de enero de 2021].

APPLE MAPS (2020). Informes de tendencias de movilidad [en línea] https://www.apple.com/covid19/mobility [Fecha de consulta: 10 de enero de 2021].

ASHBY, M. P. J. (2020). «Initial evidence on the relationship between the coronavirus pandemic and crime in the United States». Crime Science, vol. 9, págs. 1-16 [en línea] DOI: https://doi.org/10.31235/osf.io/ep87s [Fecha de consulta: 10 de enero de 2021].

ATTANASIO, A. (2020). «Coronavirus: el dramático incremento del consumo de pornografía infantil en el confinamiento por el covid-19». BBCNews [en línea] https://www.bbc.com/mundo/noticias-internacional-52385436 [Fecha de consulta: 10 de enero de 2021].

BAUMER, E. P.; VELEZ, M. B.; ROSENFELD, R. (2018). «Bringing crime trends back into criminology: a critical assessment of the literature and a blueprint for future inquiry». Annual Review of Criminology, vol. 1, págs. 39-61 [en línea] DOI: https://doi.org/10.1146/annurev-criminol-032317-092339 [Fecha de consulta: 10 de enero de 2021].

BRADBURY JONES, C.; ISHAM, L. (2020). «The pandemic paradox: the consequences of COVID 19 on domestic violence». Journal of Clinical Nursing, vol. 29, núm. 13-14 [en línea] DOI: https://doi.org/10.1111/jocn.15296 [Fecha de consulta: 10 de enero de 2021].

BRENNEN, J. S. et al. (2020). «Types, sources, and claims of Covid-19 misinformation». Reuters Institute [en línea] http://www.primaonline.it/wp-content/uploads/2020/04/COVID-19_reuters.pdf [Fecha de consulta: 10 de enero de 2021].

BRUINSMA, G. J. N.; JOHNSON, S. D. (2018). «Environmental criminology: scope, history, and state of the art». The Oxford Handbook of Environmental Criminology. Oxford University Press [en línea] DOI: https://doi.org/10.1093/oxfordhb/9780190279707.013.38 [Fecha de consulta: 10 de enero de 2021].

BUIL-GIL, D.; MIRÓ LLINARES, F.; MONEVA, A., KEMP, S.; DÍAZ-CASTAÑO, N. (2020). «Cybercrime and shifts in opportunities during COVID-19 a preliminary analysis in the UK». European Societies in the Time of the Coronavirus Crisis, págs. 1-13 [en línea] DOI: https://doi.org/10.1080/14616696.2020.1804973 [Fecha de consulta: 10 de enero de 2021].

BULLINGER, L. R.; CARR, J. B.; PACKHAM, A. (2020). «COVID-19 and crime: effects of stay-at-home orders on domestic violence», núm. 27667. National Bureau of Economic Research [en línea] DOI: https://doi.org/10.3386/w27667 [Fecha de consulta: 10 de enero de 2021].

CAMPEDELLI, G. M.; FAVARIN, S.; AZIANI, A.; PIQUERO, A. R. (2020). «Disentangling community-level changes in crime trends during the COVID-19 pandemic in Chicago». Crime Science, vol. 9, núm. 1, págs. 1-18 [en línea] DOI: https://doi.org/10.1186/s40163-020-00131-8 [Fecha de consulta: 10 de enero de 2021].

CENTER FOR DISEASE CONTROL AND PREVENTION (2020). «COVID-19-Related phone scams and phishing attacks [en línea] https://www.cdc.gov/media/phishing.html [Fecha de consulta: 10 de enero de 2021].

CHECKPOINT (2020). «Coronavirus update: in the cyber world, the graph has yet to flatten» [en línea]

https://blog.checkpoint.com/2020/04/02/coronavirus-update-in-the-cyber-world-the-graph-has-yet-to-flatten/ [Fecha de consulta: 10 de enero de 2021].

COLLIER, B. et al. (2020). «The implications of the COVID-19 pandemic for cybercrime policing in Scotland: a rapid review of the evidence and future considerations» [en línea] https://www.researchgate.net/profile/Ben_Collier/publication/341742472_Issue_No_1_The_implications_of_the_COVID-19_pandemic_for_cybercrime_policing_in_Scotland_A_rapid_review_of_the_evidence_and_future_considerations/links/5ed4f73a458515294527b273/Issue-No-1-The-implications-of-the-COVID-19-pandemic-for-cybercrime-policing-in-Scotland-A-rapid-review-of-the-evidence-and-future-considerations.pdf [Fecha de consulta: 10 de enero de 2021].

CYBERDATA COALITION (2020). «Weekly Threat Advisory: Domain trends» [en línea] https://www.cyberthreatcoalition.org/advisories/2020-05-20-weekly-threat-advisory-domain-trends [Fecha de consulta: 10 de enero de 2021].

CYVARE SOCIAL (2020). «How are cybercriminals capitalizing on Zoom's popularity?» [en línea] https://cyware.com/news/how-are-cybercriminals-capitalizing-on-zooms-popularity-6db91920 [Fecha de consulta: 10 de enero de 2021].

ESET (2020). «Brute-force attacks targeting remote access increased during the COVID-19 pandemic» [en línea] https://www.eset.com/int/about/newsroom/press-releases/products/brute-force-attacks-targeting-remote-access-increased-during-the-covid-19-pandemic-eset-confirms/ [Fecha de consulta: 10 de enero de 2021].

EUROPOL (2020a). «Catching the virus cybercrime, disinformation and the COVID-19 pandemic» [en línea] https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic [Fecha de consulta: 10 de enero de 2021].

EUROPOL (2020b). «Pandemic profiteering how criminals exploit the COVID-19 crisis» [en línea] https://www.europol.europa.eu/sites/default/files/documents/pandemic_profiteering-how_criminals_exploit_the_covid-19_crisis.pdf [Fecha de consulta: 10 de enero de 2021].

FAFINSKI, S.; DUTTON, W. H.; MARGETTS, H. (2010). «Mapping and measuring cybercrime». OII Working Paper, núm. 18 [en línea] DOI: https://doi.org/10.2139/ssrn.1694107 [Fecha de consulta: 10 de enero de 2021].

FBI (2020). «FBI warns of teleconferencing and online classroom Hijacking during COVID-19 pandemic» [en línea] https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic [Fecha de consulta: 10 de enero de 2021.]

FEDERAL BUREAU OF INVESTIGATION (2020). «People's Republic of China (PRC) targeting of COVID-19 research organizations» [en línea] https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations [Fecha de consulta: 10 de enero de 2021].

FORCEPOINT (2020). «Three-Month Trend Analysis: COVID and Coronavirus-Themed Web and Email Traffic» [en línea] https://www.forcepoint.com/blog/x-labs/covid-coronavirus-web-email-traffic-analysis [Fecha de consulta: 10 de enero de 2021].

GALOV, D. (2020). «Remote spring: the rise of RDP bruteforce attacks». Kaspersky [en línea] https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/ [Fecha de consulta: 10 de enero de 2021].

GLOBALWEBINDEX (2020). Coronavirus Research. March 2020. Release 3: Multi-market research [en

línea] https://www.globalwebindex.com/hubfs/1.%20Coronavirus%20Research%20PDFs/GWI%20coronavirus%20findings%20March%202020%20-%20Multi-Market%20data%20(Release%203).pdf [Fecha de consulta: 10 de enero de 2021].

GOOGLE (2020a). Informe de transparencia [en línea] https://transparencyreport.google.com/safe-browsing/overview [Fecha de consulta: 10 de enero de 2021].

GOOGLE (2020b). Informes de movilidad local sobre el COVID-19 [en línea] https://www.google.com/covid19/mobility/ [Fecha de consulta: 10 de enero de 2021].

HALFORD, E. et al. (2020). «Coronavirus and crime: social distancing, lockdown, and the mobility elasticity of crime». Crime Science, vol. 9, núm. 1, págs. 1-12 [en línea] DOI: https://doi.org/10.31235/osf.io/4qzca [Fecha de consulta: 10 de enero de 2021].

HAWDON, J.; PARTI, K.; DEARDEN, T. E. (2020). «Cybercrime in America amid COVID-19: the initial results from a natural experiment». American Journal of Criminal Justice, núm. 45, págs. 1-17 [en línea] DOI: https://doi.org/10.1007/s12103-020-09534-4 [Fecha de consulta: 10 de enero de 2021].

HIDER, A. (2020). «Amazon says it's removed 200k items, suspended 4k accounts due to price» [en línea] https://www.thedenverchannel.com/news/national/coronavirus/amazon-says-its-removed-500k-items-suspended-4k-accounts-due-to-price-gouging [Fecha de consulta: 10 de enero de 2021].

HODGKINSON, T.; ANDRESEN, M. A. (2020). «Show me a man or a woman alone and I'll show you a saint». Journal of Criminal Justice, vol. 69 [en línea] DOI: http://dx.doi.org/10.1016/j.jcrimjus.2020.101706 [Fecha de consulta: 10 de enero de 2021].

HOLT, T. J.; BOSSLER, A. M. (2008). «Examining the applicability of lifestyle-routine activities theory for cybercrime victimization». Deviant Behavior, vol. 30, núm. 1, págs. 1-25 [en línea] DOI: https://doi.org/10.1080/01639620701876577 [Fecha de consulta: 10 de enero de 2021].

INTERPOL (2020). «Cybercriminals targeting critical healthcare institutions with ransomware» [en línea] https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware [Fecha de consulta: 10 de enero de 2021].

JOHN C. (2020). «Number of breached records surged by 273% in 2020 Q1». Atlasvpn [en línea] https://atlasvpn.com/blog/number-of-breached-records-surged-by-273-in-2020-q1 [Fecha de consulta: 10 de enero de 2021].

KEMP, S.; BUIL-GIL, D.; MONEVA, A.; MIRÓ LLINARES, F.; DÍAZ-CASTAÑO, N. (en prensa). [Special issue] «Empty streets, busy Internet. A time series analysis of cybercrime and fraud trends during COVID-19». Journal of Contemporary Criminal Justice.

KEMP, S.; MIRÓ LLINARES, F.; MONEVA, A. (2020). «The dark figure and the cyber fraud rise in Europe: evidence from Spain». European Journal on Criminal Policy and Research, vol. 26, núm. 4 [en línea] DOI: https://doi.org/10.1007/s10610-020-09439-2 [Fecha de consulta: 10 de enero de 2021].

KUPREEV, O.; BADOVSKAYA, E.; GUTNIKOV, A. (2020). «DDoS attacks in Q1 2020». Kapersky [en línea] https://securelist.com/ddos-attacks-in-q1-2020/96837/ [Fecha de consulta: 10 de enero de 2021].

LARRAZ, I. (2020). «La pandemia traslada los delitos al mundo digital». Newtral [en línea] https://www.newtral.es/la-pandemia-traslada-mas-delitos-al-mundo-digital/20200604/ [Fecha de consulta: 10 de enero de 2021].

LESLIE, E.; WILSON, R. (2020). «Sheltering in place and domestic violence: evidence from calls for service during COVID-19». Journal of Public Economics [en línea] DOI: https://doi.org/10.2139/ssrn.3600646 [Fecha de consulta: 10 de enero de 2021].

MACKEY, T. K.; LI, J.; PURUSHOTHAMAN, V.; NALI, M.; SHAH, N.; BARDIER, C.; LIANG, B. (2020). «Big Data, natural language processing, and deep learning to detect and characterize illicit COVID-19 product sales: infoveillance study on Twitter and Instagram». JMIR public health and surveillance, vol. 6, núm. 3 [en línea] DOI: https://doi.org/10.2196/preprints.20794 [Fecha de consulta: 10 de enero de 2021].

MATTEI, T. A. (2017). «Privacy, confidentiality, and security of health care information: lessons from the recent Wannacry cyberattack». World neurosurgery, vol. 104, págs. 972-974 [en línea] DOI: https://doi.org/10.1016/j.wneu.2017.06.104 [Fecha de consulta: 10 de enero de 2021].

MIMECAST (2020). «100 days of Coronavirus» [en línea] https://www.mimecast.com/globalassets/cyber-resilience-content/100-days-of-coronavirus-threat-intelligence.pdf [Fecha de consulta: 10 de enero de 2021].

MIRÓ LLINARES, F. (2011). «La oportunidad criminal en el ciberespacio». RECPC. Revista Electrónica de Ciencia Penal y Criminología, núm. 7, págs. 1-7.

MIRÓ LLINARES, F. (2012). El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.

MIRÓ LLINARES, F.; MONEVA, A. (2019). «What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks "Did cybercrime cause the crime drop?"». Crime Science, vol. 8, núm. 1, pág. 12 [en línea] DOI: https://doi.org/10.1186/s40163-019-0107-y [Fecha de consulta: 10 de enero de 2021].

MIRÓ LLINARES, F.; MONEVA, A. (2020). «Environmental criminology and cybercrime: shifting focus from the wine to the bottles». The Palgrave Handbook of International Cybercrime and Cyberdeviance, págs. 491-511 [en línea] DOI: https://doi.org/10.1007/978-3-319-78440-3_30 [Fecha de consulta: 10 de enero de 2021].

MOHLER, G. et al. (2020). «Impact of social distancing during COVID-19 pandemic on crime in Los Angeles and Indianapolis». Journal of Criminal Justice, vol. 68 [en línea] DOI: https://doi.org/10.1016/j.jcrimjus.2020.101692 [Fecha de consulta: 10 de enero de 2021].

NAIDOO, R. (2020). «A multi-level influence model of COVID-19 themed cybercrime». European Journal of Information Systems, págs. 1-16 [en línea] DOI: https://doi.org/10.1080/0960085X.2020.1771222 [Fecha de consulta: 10 de enero de 2021].

NGO, F. T. et al. (2020). «Victimization cyberspace: Is it how long we spend online, what we do online, or what we post online?». Criminal Justice Review, vol. 45, núm. 4, págs. 430-451 [en línea] DOI: https://doi.org/10.1177/0734016820934175 [Fecha de consulta: 10 de enero de 2021].

NIKOLOVSKA, M.; JOHNSON, S. D.; EKBLOM, P. (2020). «"Show this thread": policing, disruption and mobilisation through Twitter. An analysis of UK law enforcement tweeting practices during the Covid-19 pandemic». Crime Science, vol. 9, núm. 1, págs. 1-16 [en línea] DOI: https://doi.org/10.1186/s40163-020-00129-2 [Fecha de consulta: 10 de enero de 2021].

PAYNE, J.; MORGAN, A. (2020). «COVID-19 and violent crime [PAYNE, J.; MORGAN, A.; PIQUERO, A. R. (2020). «Covid-19 and social distancing measures in Queensland, Australia are associated with short-term decreases in recorded violent crime». Journal of Experimental Criminology. DOI: https://doi.org/10.1007/s11292-020-09441-y.

PEREDA, N.; DÍAZ-FAES, D. A. (2020). «Family violence against children in the wake of COVID-19 pandemic: a review of current perspectives and risk factors». Child Adolesc Psychiatry Ment Health, vol. 14, núm. 40 [en línea] DOI: https://doi.org/10.1186/s13034-020-00347-1 [Fecha de consulta: 10 de enero de 2021].

PIQUERO, A. R. et al. (2020). «Staying home, staying safe? A short-term analysis of COVID-19 on Dallas domestic violence». American Journal of Criminal Justice, vol. 45, págs. 1-35 [en línea] DOI: https://doi.org/10.1007/s12103-020-09531-7 [Fecha de consulta: 10 de enero de 2021].

ROSENFELD, R. (2018). «Studying crime trends: normal science and exogenous shocks». Criminology, vol. 56, núm. 1, págs. 5-26 [en línea] DOI: https://doi.org/10.1111/1745-9125.12170 [Fecha de consulta: 10 de enero de 2021].

STICKLE, B.; FELSON, M. (2020). «Crime rates in a pandemic: the largest criminological experiment in History». American Journal of Criminal Justice, vol. 45, núm. 4, págs. 525-536 [en línea] DOI: https://doi.org/10.1007/s12103-020-09546-0 [Fecha de consulta: 10 de enero de 2021].

SZURDI, J.; CHEN, Z.; STAROV, O.; MCCABE, A.; DUAN, R. (2020). «Studying how cybercriminals prey on the COVID-19 pandemic». UNIT42 [en línea] https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/ [Fecha de consulta: 10 de enero de 2021].

TRENDMICRO (2020). «Developing story: COVID-19 used in malicious campaigns» [en línea] https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains [Fecha de consulta: 10 de enero de 2021].

UYHENG, J.; CARLEY, K. M. (2020). «Bots and online hate during the COVID-19 pandemic: case studies in the United States and the Philippines». Journal of Computational Social Science, núm. 3, págs. 1-24 [en línea] DOI: https://doi.org/10.1007/s42001-020-00087-4 [Fecha de consulta: 10 de enero de 2021].

WORLD HEALTH ORGANIZATION (2020). «Beware of criminals pretending to be WHO» [en línea] https://www.who.int/about/communications/cyber-security [Fecha de consulta: 10 de enero de 2021].

Cita recomendada

MIRÓ LLINARES, Fernando (2021). «Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos». *IDP. Revista de Internet, Derecho y Política*, núm. 32 (marzo). UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i32.373815

Sobre el autor

Fernando Miró-Llinares
f.miro@crimina.es
Catedrático de Derecho Penal y Criminología de la Universidad Miguel Hernández de Elche