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

IDP Número 32 (Marzo, 2021)

Revista de los Estudios de Derecho y Ciencia Política de la UOC

Universitat Oberta de Catalunya

https://idp.uoc.edu
ISSN 1699-8154

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

https://idp.uoc.edu

IDP Número 32 (Marzo, 2021)

ARTÍCULOS

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

https://idp.uoc.edu

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

https://idp.uoc.edu

ARTÍCULO

Presentación del monográfico sobre la COVID-19

Ivan Serrano
Profesor de Derecho y Ciencias Políticas
Universitat Oberta de Catalunya

Fecha de publicación: marzo de 2021

Este número de *IDP. Revista de Internet, Derecho y Política* recoge las contribuciones surgidas a partir de la convocatoria especial que realizó la revista con motivo de la crisis de la COVID-19. El enorme e incierto impacto que esta situación está generando en nuestras sociedades ponía de manifiesto la importancia de analizar aquellos aspectos relacionados con las tecnologías de la información y la comunicación en los ámbitos propios de la revista como son el derecho, la administración pública, la política, la resolución de conflictos, la criminología, las relaciones internacionales o la ciudad.

Los artículos que presentamos en este número especial recogen ciertamente esta diversidad de aproximaciones, señalando también las múltiples implicaciones de la actual crisis en diversos ámbitos de nuestras sociedades. Unas implicaciones que con toda seguridad serán objeto de estudio ineludible para las ciencias sociales y donde este número de la revista quiere ser una contribución tanto para el análisis actual como para la agenda futura de investigación.

El primer artículo recogido en este número expone el trabajo de Francisca Ramón Fernández, bajo el título «La desconexión digital y docencia universitaria *online* en tiempos de pandemia por la COVID-19: una ilusión más que una realidad». La autora analiza el impacto en la actividad laboral que está teniendo la pandemia en el sector de la docencia universitaria. Señala el artículo cómo la situación actual está poniendo a prueba regulaciones anteriores en el ámbito de los derechos digitales, señalando algunas de sus limitaciones, como aquellas referentes a la conciliación entre vida laboral y familiar, debido al fenómeno de la hiperconexión, y cómo regulaciones posteriores en esta materia pueden o no ofrecer un marco regulador más adecuado.

El artículo de Miguel Ángel Sevilla, «Las medidas de contención de la COVID-19 frente al derecho a la protección de datos personales sanitarios de la CDFUE», aborda la protección de datos en el ámbito de la gestión sanitaria, un aspecto relevante puesto que su buen uso es un factor importante para la elaboración de políticas públicas. Como señala el autor, algunas de estas mesuras pueden contravenir disposiciones respecto a la protección de datos personales, por lo que es necesario estudiar las implicaciones y las vías de conciliación entre la importancia de su uso –mediante por ejemplo técnicas de *Big Data*– para combatir la pandemia y la protección de derechos básicos como la privacidad.

En un ámbito diferente, el artículo «Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos», de Fernando Miró-Llinares, aborda el impacto que este nuevo contexto tiene en la cibercriminalidad. A partir de una revisión de los trabajos existentes y de la evidencia original aportada por el propio estudio, los resultados sugieren que las prácticas de cibercrimen se han adaptado ciertamente a las nuevas oportunidades surgidas del actual contexto, donde se ha incrementado sustancialmente la digitalización en la práctica cotidiana de nuestras sociedades. A pesar de ello, el artículo señala como este proceso de digitalización no es novedoso en sí, de modo que cabe concebir la crisis de la COVID-19 como un acelerador más que como un factor causal novedoso.

En el artículo de Cristina Güerri, Marta Martí y Albert Pedrosa «Abriendo ventanas virtuales en los muros de la prisión. En torno a la digitalización penitenciaria a propósito de la COVID-19», se aborda un ámbito de investigación relevante –más aún en el contexto de la COVID-19– como son sus repercusiones en el ámbito de las prisiones. Los numerosos elementos que son objeto de preocupación en el ámbito penitenciario se ven amplificados por los riesgos derivados de las peculiaridades de la reclusión. Una de las mesuras aplicadas, suspender permisos y visitas, tiene unas derivadas importantes en relación con uno de los objetivos fundamentales de la política penitenciaria como es la reinserción social de los presos. El trabajo tiene como objetivo resaltar esta importancia –mayor aún dada la situación actual– y cómo la insuficiente digitalización de las prisiones no permite aprovechar el potencial que tendría para facilitar vías de comunicación entre las personas presas y sus allegados.

Por último, en relación con otro aspecto que se viene discutiendo durante los últimos meses, el artículo «COVID-19, alquiler turístico y políticas de cancelación: ¿Emergencia en tiempos de pandemia de la oculta(da) naturaleza de las plataformas digitales?», de Apol·lònia Martínez Nadal, incide en cómo la situación actual pone de manifiesto los límites de ciertos conceptos jurídicos tradicionales de aplicación en el ámbito del comercio electrónico. El análisis del pronunciamiento por parte del Tribunal de Justicia de la Unión Europea sobre la condición de Airbnb nos indica, según la autora, la necesidad de nuevas categorías jurídicas respecto a las plataformas digitales, lo que el actual contexto ha evidenciado aún más dada la posición de fuerza que tienen dichas plataformas, que son mucho más que meras intermediarias neutrales entre terceros.

En definitiva, los artículos recogidos en el presente número muestran, como se señalaba al principio, no solo la relevancia que tiene la investigación desde los ámbitos propios de la revista en el contexto de la actual pandemia de la COVID-19, sino la importancia de señalar aspectos que, más allá del día a día de la actualidad ligados a sus efectos inmediatos, tendrán fuertes implicaciones que se consolidarán a largo plazo y que generarán una agenda de investigación necesaria en relación con los retos a los que se enfrentan nuestras sociedades.

Cita recomendada

SERRANO, Ivan (2021). «Presentación del monográfico sobre la COVID-19». *IDP. Revista de Internet, Derecho y Política*, núm. 32 (marzo). UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i32.381596

Sobre el autor

Ivan Serrano
Profesor de Derecho y Ciencias Políticas
Universitat Oberta de Catalunya

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

https://idp.uoc.edu

ARTÍCULO

Las medidas de contención de la COVID-19 frente al derecho a la protección de datos personales sanitarios de la CDFUE

Miguel Ángel Sevilla Duro
Universidad de Castilla-La Mancha

Fecha de presentación: mayo de 2020
Fecha de aceptación: agosto de 2020
Fecha de publicación: enero de 2021

Resumen

El 31 de diciembre de 2019 se comunicó por vez primera la existencia de 27 casos de una neumonía de etiología desconocida, posteriormente denominada SARS-CoV-2 (COVID-19). Durante los primeros meses de 2020 la enfermedad se extendió hasta alcanzar la práctica totalidad de los Estados del mundo.

Para hacer frente a la pandemia, las instituciones europeas y los Estados miembros han adoptado medidas de diversa índole, especialmente sanitarias y económicas, que, en algunos casos, confrontan con lo dispuesto en la Carta de Derechos Fundamentales de la Unión Europea. Considerando el régimen jurídico de la Carta, a lo largo de este artículo se analizarán las modulaciones y limitaciones al derecho fundamental a la protección de datos personales sanitarios (art. 8 CDFUE) provocadas por las medidas adoptadas ante la crisis sanitaria. El estudio, a la luz del ordenamiento y la jurisprudencia europeas, focaliza en las autoridades habilitadas, el procedimiento requerido, los requisitos de las medidas limitadoras y la problemática tanto del tratamiento individualizado de datos como del *big data*.

Palabras clave

coronavirus, protección de datos, *big data*, CDFUE, COVID-19

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

https://idp.uoc.edu

Measures to contain COVID-19 in view of the EU CFR right to the protection of personal data concerning health

Abstract

31 December 2019 saw the first communication referring to 27 existing cases of a pneumonia of unknown aetiology, later named SARS-CoV-2 (COVID-19). During the initial months of 2020, the illness spread to practically every country in the world.

To tackle the pandemic, European institutions and member states have adopted various kinds of measures, particularly concerning health and economics, which in some cases conflict with that which is set out in the Charter of Fundamental Rights of the European Union. In considering the legal framework of the Charter, throughout this article there will be an analysis of the modulations and limitations to the fundamental right to the protection of personal data concerning health (art. 8 of the CFR) brought about by the measures adopted in response to the health crisis. Examining European laws and jurisprudence, the study focuses on the relevant authorities, the necessary proceedings, the requirements of the restrictive measures and the problems of both personal data processing and Big Data.

Keywords

coronavirus, data protection, big data, EU CFR, COVID-19

Introducción: cronología de una pandemia

El 31 de diciembre de 2019 la Comisión Municipal de Salud y Saneamiento de la ciudad de Wuhan (provincia de Hubei, China) comunicó la existencia de 27 casos, siete de ellos graves, de neumonía de etiología desconocida, cuyo foco de contagio inicial se atribuye a un mercado mayorista de mariscos, pescado y animales vivos en Wuhan[1]. El 7 de enero de 2020 las autoridades chinas identificaron como agente causante del brote un nuevo tipo de virus de la familia *Coronaviridae*, posteriormente denominado como SARS-CoV-2. La enfermedad causada por este nuevo virus ha sido denominada por las autoridades internacionales «COVID-19». El 24 de enero Francia comunicó el primer caso en la UE, y el 11 de marzo de 2020 la Organización Mundial de la Salud (en adelante, OMS), única autoridad habilitada para declarar alarmas sanitarias internacionales[2], elevó la emergencia de salud pública causada por la COVID-19 a pandemia internacional. A las puertas de la publicación de este artículo hay más de 33 millones de casos de contagio confirmados y más de un millón de fallecidos en todo el mundo[3].

Para hacer frente a la pandemia, las instituciones europeas y los Estados miembros han adoptado medidas de diversa índole, especialmente sanitarias y económicas. Estas, en muchos casos, confrontan con lo dispuesto en la Carta de Derechos Fundamentales de la Unión Europea (en adelante, CDFUE).

Considerando el régimen jurídico de la Carta, a lo largo de este artículo se realizará un análisis de las limitaciones al derecho fundamental a la protección de datos personales sanitarios (art. 8 CDFUE) en el contexto de las medidas adoptadas ante la crisis sanitaria de la COVID-19.

1. La limitación de derechos a la luz de los arts. 51 y 52.1 CDFUE

Las instituciones y órganos de la UE y los Estados miembros en aplicación del Derecho de la Unión reconocen y respetan los derechos, libertades y principios de la CDFUE, que, por virtud del art. 6.1 del Tratado de la Unión Europea (en adelante, TUE), tiene el mismo valor jurídico que los Tratados. Ello se concretiza en el art. 51 CDFUE, que, sin ampliar el ámbito de aplicación del Derecho de la Unión ni crear o modificar competencia alguna, especifica que tanto los Estados como las instituciones de la integración observarán y promoverán los derechos y libertades con arreglo a sus respectivas competencias y en los límites de lo atribuido por los tratados.

El art. 51.1 CDFUE proclama la existencia de un extenso catálogo de derechos fundamentales en un limitado ámbito de aplicación: el derecho de la Unión. Su naturaleza de *question préalable* conlleva que todas las demás vicisitudes relativas a la protección de derechos fundamentales partan de la determinación del ámbito y alcance de aplicación de la Carta[4]. El Tribunal de Justicia ha apuntado en numerosas ocasiones la obligación de los Estados miembros de respetar los derechos fundamentales definidos por el ordenamiento europeo únicamente cuando actúen en el ámbito de aplicación del Derecho de la Unión[5], no respecto del Derecho interno, lo que es aplicable tanto a las autoridades centrales como a las instancias regionales y locales y cualesquiera organismos públicos[6]. Por lo tanto, el reparto de competencias entre la UE y los Estados miembros determina la aplicación o no de las disposiciones de la Carta[7].

La CDFUE no es un instrumento de protección de dere-

1. OMS (2020). *Pneumonia of unknown cause-China*.
2. VON AGUILAR, L. G. (2019). *Derecho y pandemias*. México: Tirant Lo Blanch, pág. 15.
3. Datos actualizados y desglosados por Estados en JOHNS HOPKINS UNIVERSITY (2020). *COVID-19 Dashboard*.
4. SARMIENTO, D. (2013). «Who's afraid of the Charter? The Court of Justice, national courts and the new framework of fundamental rights protection in Europe». *Common Market Law Review*, vol. 50, núm. 5, pág. 1.272.
5. Por todas, Sentencia del Tribunal de Justicia de 18 de diciembre de 1997, C-309/96, *Annibaldi*.
6. UNIÓN EUROPEA (2007). *Explicaciones sobre la Carta de los Derechos Fundamentales* (2007/C 303/02), pág. 32.
7. Sentencia del Tribunal de Justicia de 17 de febrero de 1998, 249/96, *Grant*, párr. 45. La complejidad del reparto competencial genera numerosos conflictos resueltos por el TJUE mediante meticulosos exámenes sobre el ámbito de aplicación de la Carta. Un recientísimo ejemplo en la Sentencia de 19 de septiembre de 2019, C-467/18, *EP*, párrs. 67-68.

chos fundamentales de carácter autónomo y aplicación y eficacia directa general[8], por lo que para aplicar sus preceptos debe realizarse una interpretación sistemática. Consiguientemente, la Carta solo es vinculante para los Estados miembros por medio de la legislación de la UE, esto es, resulta una consecuencia de la aplicación del ordenamiento europeo a un caso particular, pero no es su causa, pues no determina por sí misma la aplicabilidad del derecho de la Unión[9]. Así, dado que la Carta no crea derechos fundamentales autónomos que sustituyan a los de las Constituciones de los Estados miembros, el art. 51.1 CDFUE convierte la declaración de derechos en la «sombra» del derecho de la UE, y «una sombra no puede proyectar su propia sombra»[10].

Esta necesaria ligazón de la Carta al resto del ordenamiento no permite, sin embargo, que cualquier norma pueda limitar el ejercicio de lo reconocido por la CDFUE. El art. 52.1 establece cuatro condiciones para admitir una limitación de algún derecho fundamental. En primer lugar, la limitación debe venir establecida por la ley[11] (dictada, en función del reparto competencial, por la UE o los Estados miembros); en segunda instancia, debe respetarse el contenido esencial del derecho restringido[12]; en tercer lugar, ha de respetarse el principio de proporcionalidad[13] por último, debe ser una restricción necesaria o bien para responder efectivamente a objetivos de interés general reconocidos por la UE o bien para proteger los derechos y libertades del resto de ciudadanos[14].

Debe precisarse en este punto que el Tribunal de Justicia ha sido deferente con el legislador de la UE en la comprobación del principio de proporcionalidad. Es doctrina consolidada que en los ámbitos complejos en los que el legislador europeo dispone de una amplia facultad de apreciación «solo el carácter manifiestamente inadecuado de una medida adoptada en estos ámbitos, en relación con el objetivo que tiene previsto conseguir la institución competente, puede afectar a la legalidad» de las medidas que adopte, siendo irrelevante si eran las únicas posibles o si existían otras que podrían haberse adoptado[15]. Sin embargo, ello no exime al legislador «de basar su elección

8. Sentencia del Tribunal de Justicia de 26 de febrero de 2013, C-617/10, *Åklagaren c. Fransson*, párrs. 17-23.
9. PEREZ FERNANDES, S. (2018). «Fundamental rights at the crossroads of EU Constitutionalism». *Revista de Derecho Comunitario Europeo,* vol. 60, págs. 688-689. La viabilidad de relegar la CDFUE a un segundo plano en pro de los estándares nacionales fue negada en el célebre asunto *Melloni* (C-399/11) y, con matices, admitida en el asunto *Åkerberg Fransson* (C-617/10) por las particularidades del caso, recurriendo al «efecto útil» del Derecho de la UE, que no determinaba «totalmente» la acción de los Estados. En este ambiguo panorama deben precisarse con claridad las limitaciones al desplazamiento del estándar nacional en ausencia de margen de maniobra de los Estados miembros (ALONSO GARCÍA, R., [2014]. *Sistema Jurídico de la Unión Europea,* Madrid: Civitas, pág. 302.
10. 1Conclusiones del Abogado General Michael Bobek de 7 de septiembre de 2017, C-298/16, asunto *Ispas*, párr. 30. En un sentido similar, pero desde la doctrina, LENAERTS, K.; GUTIÉRREZ-FONS, J. A. (2014). The Place of the Charter in the EU Constitutional Edifice. En: PEERS, S. *et al.* (eds.). *The EU Charter of Fundamental Rights. A Commentary.* Oxford: Hart Publishing, pág. 1.592.
11. La ambigüedad del sustantivo «ley» no es casual. Se utiliza para hacer referencia tanto a los actos legislativos europeos (reglamentos, directivas y decisiones) adoptados por codecisión cuanto a las leyes nacionales (TRIANTAFYLLOU, D. [2002]. «The European Charter of fundamental rights and the "rule of law": restricting fundamental rights by reference». Common Market Law Review, vol. 39, núm. 1, págs. 60-62). La noción «establecida por ley» del art. 52 es igual que la de la CEDH (Conclusiones del Abogado General Saugmandsgaard de 19 de julio de 2016, C-203/15 y C-698/15, asuntos Tele2 y Watson, párr. 140). A este respecto, debe considerarse también la «calidad de la ley» (Conclusiones del Abogado General Cruz Villalón de 14 de abril de 2011, C-70/10, asunto Scarlet Extended, párr. 100).
12. Las limitaciones no pueden ser tan extensivas que eliminen el núcleo esencial y básico de un derecho, desnaturalizando y haciendo difícil o imposible su ejercicio. Ello se viene advirtiendo desde la Sentencia de 14 de mayo de 1974, 4/73, asunto Nold. Posteriormente es reseñable la Sentencia de 13 de abril de 2000, C-292/97, asunto Karlsson, párr. 97. En una línea similar, STJUE de 6 de octubre de 2015, C-362/14, asunto Schrems.
13. Las limitaciones deben ser lo menos restrictivas posibles y las desventajas ocasionadas no han de exceder los objetivos perseguidos, algo establecido por el Tribunal de Justicia en el referido asunto Nold. Más recientemente, STJUE de 8 de abril de 2012, C-293/12 y C-594/12, asuntos acumulados Digital Rights Ireland y Kärntner, párrs. 38 y 40.
14. La mención a los intereses generales reconocidos abarca tanto a los objetivos de los arts. 2 y 3 TUE (valores y objetivos generales de la UE) cuanto a los específicos de los arts. 5, 26 y 41 TUE y 36, 39, 42.3, 45.3 y 346 TFUE (UNIÓN EUROPEA [2007]. Explicaciones sobre la Carta..., págs. 32-33).
15. Con gran claridad, Sentencia de 10 de enero de 2006, C-344/04, *International Air Transport Association*, párr. 80 y sigs. De igual modo, Sentencia de 12 de noviembre de 1996, C-84/94, *Reino Unido c. Consejo,* párr. 58 y Sentencia de 10 de diciembre de 2002, C-491/01, *British American Tobacco*, párr. 123.

en criterios objetivos»[16]. Esta flexibilización del requisito es mayor para el legislador europeo que para los Estados miembros, que inexcusablemente «deben recurrir a medios que, al tiempo que permitan alcanzar eficazmente tal objetivo, causen el menor menoscabo a los objetivos y principios establecidos por la legislación de la Unión»[17].

No obstante, algunos de los derechos de la CDFUE, concretamente los ligados a la dignidad de los sujetos (prohibición de la tortura del art. 4 y prohibición de la esclavitud del art. 5), no pueden limitarse. Por contrapartida, la restante mayoría de derechos y libertades recogidos en el ordenamiento europeo, entre los que se incluye la protección de datos personales sanitarios, están condicionados, modulados y limitados por la legislación estatal y supraestatal.

2. La afección de la COVID-19 a la protección de datos personales sanitarios (art. 8 CDFUE)

El art. 8 CDFUE, en línea con el art. 16.1 TFUE, estipula que todos los ciudadanos de la UE tienen «derecho a la protección de los datos de carácter personal» y al tratamiento de los mismos de manera «leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley».

Las políticas adoptadas ante la pandemia de la COVID-19 requieren, en ocasiones, el procesamiento masivo de datos personales, muchos de ellos de tipo sanitario, para evaluar la situación de los territorios y aplicar medidas que permitan superar la coyuntura. A este respecto, el desarrollo del art. 8 CDFUE, concretamente el Reglamento Europeo de Protección de Datos (GDPR), en vigor desde mayo de 2018, trata de hacer compatible la plena garantía de la protección de los datos con la no obstaculización de la prevención e investigación frente al virus. De la existencia del Reglamento se desprende el cumplimiento de lo expuesto en el art. 51.1 CDFUE sobre el ámbito de aplicación de la Carta de Derechos Fundamentales. Dado que la CDFUE se dirige a los Estados miembros únicamente cuando apliquen el Derecho de la Unión, y puesto que la regulación de la protección de datos es competencia de la UE (art. 16.2 TFUE), las disposiciones de la CDFUE son aplicables a todas las medidas adoptadas frente a la COVID-19 que modulen o restrinjan el derecho a la protección de datos.

El GDPR considera que los datos sanitarios son de categoría especial (art. 9.1), por lo que prohíbe su uso en términos generales, exceptuando la posibilidad de utilizarlos si se da alguno de los supuestos expresamente tasados por el Reglamento. Entre estos supuestos se incluye el tratamiento de los datos «por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud» (art. 9.2.i). Este «interés público» engloba, de acuerdo con el considerando 46 GDPR, «el control de epidemias y su propagación», circunstancia que en la actualidad concurre tanto para el Derecho de la UE (*vid*. art. 168 TFUE) cuanto para otros organismos internacionales como la OMS, como se ha expuesto con anterioridad. A ello se suma que el art. 6.1.d GDPR considera el «interés vital» de un ciudadano como motivo suficiente para adoptar medidas limitadoras de la protección de los datos personales de otro ciudadano. Este hecho también concurre aunque el objetivo sea proteger a personas no identificables ajenas a aquel de quien se obtienen los datos[18]. De ambas cuestiones se extrae que el ordenamiento europeo permite modular y limitar el derecho a la protección de datos personales de tipo sanitario en el caso de epidemias o pandemias como la actual; algo también previsto por los ordenamientos de los Estados miembros[19].

16. Sentencia de 8 de junio de 2010, C-58/08, *Vodafone*, párr. 53. De modo similar, el Protocolo núm. 3 anexo al TJUE exige la motivación ligada al principio de proporcionalidad en la adopción de los actos legislativos (arts. 1 y 5).
17. Sentencia de 26 de abril de 2018, C-81/17, *Zabrus Siret*, párr. 50. Con profundidad, CHANO REGAÑA, L. (2015). «Igualdad y principio de proporcionalidad en el Derecho Europeo: Especial referencia a los derechos fundamentales». *Revista Universitaria Europea*, núm. 23, pág. 165.
18. Así lo han entendido numerosas autoridades de protección de datos de Estados miembros. Por todas, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2020). *Informe 17/2020 sobre la protección de datos frente al COVID-19*, pág. 2.
19. COMISIÓN EUROPEA (2020). *Comunicación. Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos* (2020/C 124 I/01), pág. 5.

Surge entonces la cuestión de qué órganos están legitimados para llevar a cabo esas restricciones. Las medidas limitadoras del art. 8 CDFUE son aquellas que determinen los responsables del tratamiento de los datos (art. 23.1 GDPR); así pues, la responsabilidad recaerá sobre la UE o los Estados en función de quién sea competente en la materia. En este caso, el motivo que justificaría la limitación de los datos es el «interés público general en el ámbito de la sanidad pública» (art. 23.1.d GDPR), cuestión que se enmarca indubitadamente en la materia de protección de la salud. De acuerdo con el reparto competencial del Tratado de Lisboa, esta materia corresponde a los Estados miembros, sin perjuicio de la armonización de estrategias y el complemento y apoyo de la UE (arts. 168 y 114 TFUE). Consecuentemente, las condiciones y el alcance de la limitación a la protección de datos se deben fijar en las normas promulgadas por cada Estado miembro, siempre en el marco del GDPR, el resto del Derecho de la Unión[20] y las directrices de las autoridades estatales de protección de datos y el Comité Europeo de Protección de Datos. A este respecto, todas las autoridades estatales de protección de datos han emitido directrices relacionadas con la recopilación y el tratamiento de datos sanitarios personales, algunas de las cuales han coincidido en la necesidad de adoptar medidas extraordinarias o actos de emergencia (como República Checa, Polonia e Italia).

En todo caso, estas medidas extraordinarias no pueden modular el art. 8 CDFUE hasta el punto de suspender los derechos de transparencia, acceso, información, rectificación, supresión, limitación u oposición de los datos de los ciudadanos de la Unión (arts. 12 a 22 del GDPR), sino que solo pueden restringir funcionalmente algunos de los mencionados en atención al art. 89 GDPR[21]. Dicha restricción debe realizarse a la luz de la jurisprudencia del TJUE, que exige que cualesquiera limitaciones a la protección de datos se apliquen únicamente en la medida en que sean estrictamente necesarias ponderando los derechos fundamentales en juego[22], puesto que el incorrecto uso de los datos sanitarios, entendidos en sentido amplio, puede tener graves y adversas repercusiones para los afectados[23]. Esta difícil ponderación se agudiza por cuanto la recopilación y el tratamiento de los datos no solo se realiza a título individual, sino también mediante el *big data*. Así pues, podemos distinguir dos escenarios de limitación del derecho fundamental a la protección de datos: por un lado, la limitación en el caso del tratamiento de los datos de modo colectivo (*big data*); por otro, la limitación en el tratamiento de los datos de modo individual.

En primer lugar, en cuanto al tratamiento colectivo, el *big data* sanitario consiste en la acumulación masiva de datos médicos, estructurados o no estructurados, a través de un sistema informático que organice lo compilado y facilite la extracción de conclusiones a partir del examen de esas grandes cantidades de información[24]. Ello facilita la adopción de decisiones en un período temporal muy reducido contrastando datos de una amplia muestra de población, lo que permite que se mejore no solo la asistencia sanitaria de los individuos cuyos datos son tratados sino también la del conjunto de la sociedad. Son muchos los sistemas de *big data* puestos en funcionamiento durante la crisis de la COVID-19; pueden destacarse el portal de datos lanzado por la Comisión para que los Estados miembros compartan secuencias de ADN, estructuras de proteínas, investigaciones preclínicas, ensayos clínicos y datos epidemiológicos[25]

20. El art. 4.2 TUE obliga a la UE a respetar las funciones esenciales de los Estados, y por ende sus medidas de contención sanitaria, destinadas a «garantizar su integridad territorial, mantener el orden público y salvaguardar la seguridad nacional», cuestiones amenazadas por la crisis sanitaria.
21. EUROPEAN DATA PROTECTION BOARD (2020). *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*, pág. 10.
22. *Vid*. Sentencia de 14 de febrero de 2019, C-345/17, asunto *Buivids*, párr. 64. Similarmente, Sentencia de 16 de diciembre de 2008, C-73/07, asunto *Satakunnan Markkinapörssi,* párr. 56.
23. STJUE de 9 de noviembre de 2010, C-92/09 y C-93/09, asuntos acumulados *Volker und Markus* y *Hartmut Eifert,* párr. 65 y sigs.
24. SERRANO PÉREZ, M. M. (2018). «La necesidad de una ley de protección de datos en salud». *Revista internacional de investigación en Bioderecho*, núm. 8, pág. 2. Junto a los datos estructurados (informes y registros informáticos, secuencias genéticas...), la recopilación masiva de datos no estructurados (recetas médicas, escaneos, archivos contables...) contribuye a realizar seguimientos individualizados a los pacientes y a la búsqueda de mecanismos colectivos contra la propagación del virus. A este respecto, y con especial énfasis en el proyecto VISC+ (*big data* del sistema sanitario de Cataluña), vid. SERRANO PÉREZ, M. M. (2015). «Big Data o la acumulación masiva de datos sanitarios. Derechos en riesgo en el marco de la sociedad digital». *Derecho y salud*, vol. 25, núm. extra 1, especialmente págs. 52-55.
25. COMISIÓN EUROPEA (2020). *Big Data. COVID-19 Data Portal.*

y la base de datos creada por el Gobierno español a partir del análisis continuo de más de trece millones de líneas móviles para adoptar restricciones a la movilidad que minimicen el contagio[26].

En segundo lugar, en cuanto al tratamiento individualizado de los datos sanitarios, la COVID-19 ha generado conflictos especialmente en el ámbito laboral y la comunicación.

Por una parte, en relación con el ámbito del trabajo, algunos ordenamientos internos (Alemania, Austria, Dinamarca, Eslovaquia, España, Finlandia, Irlanda, Lituania y Polonia) permiten que los empleadores puedan solicitar a sus trabajadores información personal sobre síntomas y/o infecciones si se demuestra que dicha recopilación es necesaria (por ejemplo, para diseñar planes de contingencia en caso de contagio). Por contrapartida, otros ordenamientos lo prohíben salvo expresa y voluntaria aceptación de los trabajadores (Bélgica, Estonia, Francia, Hungría, Italia, Luxemburgo y Países Bajos). Algo similar sucede con la recopilación de datos personales sobre viajes recientes de los empleados: mientras que unos consideran que se puede solicitar información a los trabajadores sobre sus estancias en «zonas de riesgo» (Dinamarca, España, Francia, Irlanda, Letonia, Lituania, Luxemburgo y Polonia), otros solo permiten la recopilación de datos voluntariamente cedidos (Bélgica, Finlandia, Hungría, Italia y Países Bajos)[27].

Por otra parte, en el ámbito de la comunicación se producen dos situaciones conflictivas diferenciadas. La primera consiste en la divulgación de datos agregados sobre la afección de la COVID-19 en un territorio, lo cual no parece suponer una vulneración del art. 8 CDFUE, toda vez que contribuye al ejercicio de la libertad de información del art. 11 CDFUE. La segunda se basa en la divulgación de información personal sobre la infección o estado médico de un ciudadano sin su consentimiento, lo que, con independencia de la relevancia pública de este, parece contrario a la Carta. Así lo han recordado explícitamente autoridades de protección de datos como la chipriota[28].

3. Evaluación de las limitaciones al art. 8 CDFUE y consideraciones conclusivas

Por lo expuesto a lo largo de este breve trabajo puede afirmarse que en el marco de la crisis de la COVID-19 la limitación del derecho a la protección de datos personales de tipo sanitario (art. 8 de la CDFUE), por su especial y crítica naturaleza (9.1 GDPR), está supeditada al cumplimiento de cuatro condiciones, la última de las cuales se compone de varios requisitos.

En primer lugar, el art. 51.1 CDFUE y la jurisprudencia del Tribunal de Justicia en su desarrollo sostienen que las disposiciones de la Carta de Derechos Fundamentales de la Unión Europea afectan a los Estados miembros únicamente cuando aplican el Derecho de la Unión. Como la regulación de la protección de datos personales es competencia de la UE (art. 16.2 TFUE), la CDFUE se aplica a los Estados en la adopción de medidas frente a la COVID-19.

En segundo lugar, los arts. 52.1 CDFUE y 23.1 GDPR condicionan la validez de las medidas limitadoras de derechos, y por ende del art. 8 CDFUE, a que se amparen en un motivo suficiente. El motivo por el que se limita el derecho es la protección frente a amenazas transfronterizas graves para la salud, lo que, de acuerdo con los arts. 9.2.i y 23.1.d GDPR, es razón válida para la restricción. Así pues, las medidas adoptadas por los Estados miembros de la UE modulando el art. 8 CDFUE cumplen con esta condición[29].

En tercer lugar, de la lectura conjunta de los arts. 51 y 52.1 CDFUE y 23.1 GDPR se desprende que la protección de datos solo puede limitarse o por el Derecho de la Unión o por los Estados miembros, y ello en función de la materia en que se englobe el motivo justificador de la limitación. La crisis de la COVID-19 es de tipo sanitario y, de acuerdo

26. MINISTERIO DE TRANSPORTES DE ESPAÑA (2020). *Big Data. Análisis de la movilidad en España durante el Estado de Alarma*. Google también ha creado una base de datos similar por medio de la geolocalización de un número indeterminado de dispositivos, multimillonario en todo caso, de 130 Estados.
27. Un análisis detallado de las medidas adoptadas por las autoridades de protección de datos de los Estados miembros en EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2020). *Coronavirus Pandemic in the EU. Fundamental rights implications*. Anexo, págs. 44-46.
28. *Ibid*., pág. 42.
29. Las medidas objeto de estudio son las recopiladas en *ibid*., págs. 41-42.

con el reparto competencial actual, la responsabilidad en la protección de la salud corresponde a los Estados miembros[30]. Consecuentemente, son los legisladores de los Estados miembros quienes, en el marco del GDPR y su ordenamiento, pueden realizar la limitación. En apariencia, las normas promulgadas también cumplen con esta condición.

En cuarto lugar, de los arts. 51 y 52.1 CDFUE, en correlación con el conjunto del GDPR, se extrae que las medidas limitadoras del derecho a la protección de datos personales sanitarios están condicionadas al cumplimiento de cuatro requisitos para ser válidas: primero, deben estipularse en normas de rango legal; segundo, deben respetar el contenido esencial del derecho a la protección de datos personales[31]; tercero, deben respetar el principio de proporcionalidad[32]; y cuarto, deben responder al objetivo de interés general de protección frente a la COVID-19. Son estos los elementos clave para evaluar la correcta limitación del art. 8 CDFUE. Si bien se presume el cumplimiento del cuarto requisito y la fácil detección en caso de incumplimiento del primero, el respeto al contenido esencial y al principio de proporcionalidad solo puede concluirse tras un análisis pormenorizado de cada concreta medida[33], para lo que es esencial diferenciar si la obtención y el tratamiento de los datos se prevé de modo individualizado o colectivo. Es preciso tomar en consideración la doctrina del TJUE acerca del principio de proporcionalidad, deferente con el margen de apreciación del legislador de la UE en tanto estima que, salvo manifiesta inadecuación o arbitrariedad con los objetivos perseguidos, las medidas adoptadas serán legales; doctrina que matiza en el caso del legislador de los Estados miembros[34].

A este respecto, los datos personales compilados por las autoridades sanitarias deben ser procesados para la realización de tareas específicas y determinadas, nunca de modo genérico o abstracto; y los ciudadanos han de recibir información transparente sobre el tratamiento y período de almacenamiento de sus datos. Ello, en todo caso, se debe fijar de acuerdo con estrictas medidas de seguridad y confidencialidad que garanticen el anonimato y la prohibición de consulta por personas o entidades no autorizadas[35], lo que se torna especialmente crítico en el tratamiento colectivo de datos por medio del *big data*.

Considerando lo anterior, es posible concluir resaltando tres aspectos que tal vez debieran ser considerados para una mejor protección del art. 8 CDFUE en situaciones de excepcionalidad como la actual. En primer lugar, se requiere un refuerzo de los principios de transparencia

30. Elevando a una perspectiva supraestatal las reflexiones de NOGUEIRA LÓPEZ, A. (2020). «Confinar el coronavirus. Entre el viejo Derecho sectorial y el Derecho de excepción». *El Cronista del Estado Social y Democrático de Derecho,* núm. 86-87, págs. 29-30, cabe cuestionarse la efectividad de tener 27 políticas sanitarias de excepción diferentes en la UE, una por Estado, para combatir la pandemia. Debe reflexionarse sobre si una transferencia de competencias a la Unión en esta materia contribuiría a una mejor respuesta en el conjunto de la integración.
31. Del análisis de la jurisprudencia sobre el art. 8 la doctrina ha considerado que son dos los elementos esenciales del derecho: el respeto de los derechos del interesado y la independencia en el control de los datos recopilados (HUSTINX, P. [2013]. «EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation». *Collected courses of the European University Institute's Academy of European Law).*
32. En el ámbito de la protección de datos, el test de proporcionalidad debe realizarse en cuatro pasos: considerando la dimensión fáctica de la medida limitadora, identificando los derechos afectados, definiendo los objetivos de la medida y eligiendo la opción más efectiva y menos intrusiva (EUROPEAN DATA PROTECTION BOARD [2017]. *Assessing the necessity of measures that limit the fundamental right to the protection of personal data).* Una aplicación práctica, con variaciones, en las Sentencias de 30 de octubre de 1978, 209 a 215/78, asunto *Van Landewyck c. Comisión*, 26 de junio de 1980, 136/79, asunto *National Panasonic c. Comisión*, 21 de septiembre de 1989, 46/87, *Hoechst c. Comisión* y 22 de octubre de 2002, C-94/00, asunto *Roquette et frères* (MANGAS MARTÍN, A. [2008]. «Artículo 52. Alcance e interpretación de los derechos y principios». En: MANGAS MARTÍN, A. (dir.). *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo.* Bilbao: Fundación BBVA, págs. 834-835).
33. Sobre el cumplimiento de estos requisitos por las medidas adoptadas en España, *vid*. MARTÍNEZ MARTÍNEZ, R. (2020). «Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública». *Diario La Ley,* núm. 38. Con concreción respecto de las relativas a la geolocalización, MARTÍNEZ MARTÍNEZ, R. (2020). «Protección de datos y geolocalización en la Orden SND/297/2020». Hay Derecho. Expansión, 31 de marzo.
34. *Vid. supra* notas 15, 16 y 17.
35. EUROPEAN DATA PROTECTION BOARD (2020). *Statement on the processing of personal data in the context of the COVID-19 outbreak,* pág. 2.

y proporcionalidad en el uso de datos personales en la investigación y transferencia de *big data* entre Estados de la UE y/o extracomunitarios[36]. Por otro lado, parece necesaria una más concreta delimitación del alcance de las modulaciones y restricciones al art. 8 CDFUE, con especial énfasis en lo relativo a la geolocalización y difusión de la condición de contagiados de los ciudadanos. Finalmente, resultaría positivo elaborar protocolos específicos para la compartición de datos en toda la UE, lo que promovería una comprensión más global de la crisis a abordar y facilitaría la toma conjunta de decisiones de los Estados miembros.

Si la historia demuestra que la UE ha salido reforzada tras cada crisis que ha soportado, la superación de la pandemia de la COVID-19 parece esencial para el progreso de la integración. Solo la cooperación y el estricto respeto a los derechos fundamentales lo hará posible.

36. Muestra de ello es la recientísima STJUE de 16 de julio de 2020, C-311/18, asunto *Schrems II*, que invalida el *Privacy Shield* y, consecuentemente, paraliza las transferencias de datos entre la UE y Estados Unidos basadas en la decisión de adecuación. Esta resolución se fundamenta en tanto el nivel de protección de datos estadounidense no alcanza lo exigido por el GDPR. En el futuro próximo y en ausencia de una decisión de adecuación, las transferencias de datos personales a países terceros deben adecuarse a lo exigido por el art. 49 GDPR (párrs. 198-201).

Referencias bibliográficas

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2020). *Informe 17/2020 sobre la protección de datos frente al COVID-19*. [en línea] https://www.aepd.es/es/documento/2020-0017.pdf [Fecha de consulta: 28 de septiembre de 2020].

ALONSO GARCÍA, R. (2014). *Sistema jurídico de la Unión Europea*. 4.ª ed. Madrid: Civitas.

CHANO REGAÑA, L. (2015). «Igualdad y principio de proporcionalidad en el Derecho Europeo: Especial referencia a los derechos fundamentales». *Revista Universitaria Europea,* núm. 23, págs. 151-174.

COMISIÓN EUROPEA (2020). *Comunicación. Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos*. (2020/C 124 I/01), págs. 1-9.

COMISIÓN EUROPEA (2020). *Big Data. COVID-19 Data Portal* [en línea] https://www.covid19dataportal.org/ [Fecha de consulta: 28 de septiembre de 2020].

EUROPEAN DATA PROTECTION BOARD (2017). *Assessing the necessity of measures that limit the fundamental right to the protection of personal data* [en línea] https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf [Fecha de consulta: 28 de septiembre de 2020].

EUROPEAN DATA PROTECTION BOARD (2020). *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak* [en línea] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf [Fecha de consulta: 28 de septiembre de 2020].

EUROPEAN DATA PROTECTION BOARD (2020). *Statement on the processing of personal data in the context of the COVID-19 outbreak* [en línea] https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf [Fecha de consulta: 28 de septiembre de 2020].

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2020). *Coronavirus Pandemic in the EU. Fundamental rights implications* [en línea] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin_en.pdf [Fecha de consulta: 28 de septiembre de 2020].

HUSTINX, P. (2013). «EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation». *Collected courses of the European University Institute's Academy of European Law.*

JOHNS HOPKINS UNIVERSITY (2020). *COVID-19 Dashboard* [en línea] https://coronavirus.jhu.edu/map.html [Fecha de consulta: 28 de septiembre de 2020].

LENAERTS, K.; GUTIÉRREZ-FONS, J. A. (2014). «The Place of the Charter in the EU Constitutional Edifice». En: PEERS, S. *et al.* (eds.). *The EU Charter of Fundamental Rights. A Commentary*. Oxford: Hart Publishing, págs. 1.600-1.637. https://doi.org/10.5771/9783845259055_1600 [Fecha de consulta: 28 de septiembre de 2020].

MANGAS MARTÍN, A. (2008). «Artículo 52. Alcance e interpretación de los derechos y principios». En: MANGAS MARTÍN, A. (dir.). *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo.* Bilbao: Fundación BBVA, págs. 826-851.

MARTÍNEZ MARTÍNEZ, R. (2020). «Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública». *Diario La Ley,* núm. 38.

MARTÍNEZ MARTÍNEZ, R. (2020). «Protección de datos y geolocalización en la Orden SND/297/2020». *Hay Derecho. Expansión*, 31 de marzo [en línea] https://hayderecho.expansion.com/2020/03/31/proteccion-de-datos-y-localizacion-en-la-orden-snd-297-2020/ [Fecha de consulta: 28 de septiembre de 2020].

MINISTERIO DE TRANSPORTES DE ESPAÑA (2020). *Big Data. Análisis de la movilidad en España durante el Estado de Alarma* [en línea] https://www.mitma.gob.es/ministerio/covid-19/evolucion-movilidad-big-data [Fecha de consulta: 28 de septiembre de 2020].

NOGUEIRA LÓPEZ, A. (2020). «Confinar el coronavirus. Entre el viejo Derecho sectorial y el Derecho de excepción». *El Cronista del Estado Social y Democrático de Derecho*, núm. 86-87, págs. 22-31.

OMS (2020). *Pneumonia of unknown cause-China* [en línea] https://www.who.int/csr/don/05-january-2020-pneumonia-of-unkown-cause-china/es/ [Fecha de consulta: 28 de septiembre de 2020].

PEREZ FERNANDES, S. (2018). «Fundamental rights at the crossroads of EU Constitutionalism». *Revista de Derecho Comunitario Europeo,* vol. 60, págs. 677-715 [en línea] https://doi.org/10.18042/cepc/rdce.60.06 [Fecha de consulta: 28 de septiembre de 2020].

SARMIENTO, D. (2013). «Who's afraid of the Charter? The Court of Justice, national courts and the new framework of fundamental rights protection in Europe». *Common Market Law Review*, vol. 50, núm. 5, págs. 1.267-1.304.

SERRANO PÉREZ, M. M. (2015). «Big Data o la acumulación masiva de datos sanitarios. Derechos en riesgo en el marco de la sociedad digital». *Derecho y salud,* vol. 25, núm. extra 1, págs. 51-64.

SERRANO PÉREZ, M. M. (2018). «La necesidad de una ley de protección de datos en salud». *Revista internacional de investigación en Bioderecho*, núm. 8, págs. 1-6 [en línea] https://doi.org/10.6018/bioderecho.389951 [Fecha de consulta: 28 de septiembre de 2020].

TRIANTAFYLLOU, D. (2002). «The European Charter of fundamental rights and the "rule of law": restricting fundamental rights by reference». *Common Market Law Review*, vol. 39, núm. 1, págs. 53-64. https://doi.org/10.1023/A:1014517214935 [Fecha de consulta: 28 de septiembre de 2020].

UNIÓN EUROPEA (2007). *Explicaciones sobre la Carta de los Derechos Fundamentales* (2007/C 303/02), págs. 17-35.

VON AGUILAR, L. G. (2019). *Derecho y Pandemias*. México: Tirant Lo Blanch.

Jurisprudencia del Tribunal de Justicia de la Unión Europea

Sentencia de 14 de mayo de 1974, 4/73, *Nold*.

Sentencias de 30 de octubre de 1978, 209 a 215/78 y 218/78, *Van Landewyck*.

Sentencia de 26 de junio de 1980, 136/79, *National Panasonic*.

Sentencia de 21 de septiembre de 1989, 46/87, *Hoechst*.

Sentencia de 12 de noviembre de 1996, C-84/94, *Reino Unido c. Consejo*.

Sentencia de 18 de diciembre de 1997, C-309/96, *Annibaldi*.

Sentencia de 17 de febrero de 1998, C-249/96, *Grant*.

Sentencia de 13 de abril de 2000, C-292/97, *Karlsson*.

Sentencia de 22 de octubre de 2002, C-94/00, *Roquette et frères*.

Sentencia de 10 de diciembre de 2002, C-491/01, *British American Tobacco*.

Sentencia de 10 de enero de 2006, C-344/04, *International Air Transport Association*.

Sentencia de 8 de junio de 2010, C-58/08, *Vodafone*.

Sentencia de 16 de diciembre de 2008, C-73/07, *Satakunnan Markkinapörssi*.

Sentencia de 9 de noviembre de 2010, C-92/09 y C-93/09, *Volker und Markus y Hartmut Eifert*.

Sentencia de 24 de noviembre de 2011, C-70/10, *Scarlet Extended*.

Sentencia de 26 de febrero de 2013, C-617/10, *Åklagaren*.

Sentencia de 26 de febrero de 2013, C-399/11, *Melloni*.

Sentencia de 7 de mayo de 2013, C-617/10, *Åkerberg Fransson*.

Sentencia de 8 de abril de 2012, C-293/12 y C-594/12, *Digital Rights Ireland y Kärntner*.

Sentencia de 6 de octubre de 2015, C-362/14, *Schrems*.

Sentencia de 21 de diciembre de 2016, C-203/15 y C-698/15, *Tele2 y Watson*.

Sentencia de 9 de noviembre de 2017, C-298/16, *Ispas*.

Sentencia de 14 de febrero de 2019, C-345/17, *Buivids*.

Sentencia de 19 de septiembre de 2019, C-467/18, *EP*.

Sentencia de 16 de julio de 2020, C-311/18, *Schrems II*.

Cita recomendada

SEVILLA DURO, Miguel Ángel (2020). «Las medidas de contención de la COVID-19 frente al derecho a la protección de datos personales sanitarios de la CDFUE», IDP. Revista de Internet, Derecho y Política, núm. 32. UOC [Fecha de consulta: dd/mm/aa] https://dx.doi.org/10.7238/idp.v0i32.373802

Sobre el autor

Miguel Ángel Sevilla Duro
MiguelAngel.Sevilla@alu.uclm.es
Universidad de Castilla-La Mancha

Miguel Ángel Sevilla Duro (Albacete, España, 1997). Graduado en Derecho por la Universidad de Castilla-La Mancha (UCLM) con Premio Extraordinario Fin de Grado al mejor expediente académico. Máster en Derecho Constitucional en el Centro de Estudios Políticos y Constitucionales (Ministerio de la Presidencia del Gobierno de España). Doctorando (FPU) del Área de Derecho Constitucional de la Facultad de Derecho de Albacete (UCLM). E-mail: MiguelAngel.Sevilla@alu.uclm.es

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

https://idp.uoc.edu

ARTÍCULO

La desconexión digital y docencia universitaria *online* en tiempos de pandemia por la COVID-19: una ilusión más que una realidad[1]

Francisca Ramón Fernández
Universitat Politècnica de València

Fecha de presentación: marzo de 2020
Fecha de aceptación: junio de 2020
Fecha de publicación: marzo de 2021

Resumen

La declaración del estado de alarma por la pandemia de la COVID-19 ha supuesto que la actividad laboral sea realizada de forma telemática en los colectivos en los que ha sido posible. Uno de ellos es el ámbito universitario, en el que el profesorado ha pasado de la presencialidad a la virtualidad. El derecho a la desconexión digital que contempló la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales deja en el aire numerosas cuestiones que dificultan la aplicación de este derecho, junto a su ausencia de desarrollo en el contexto de la universidad. Nos proponemos en este trabajo reflexionar sobre lo que ha supuesto más una ilusión que una realidad, abordando las carencias, limitaciones y falta de garantías de este derecho, ya que en esta coyuntura que nos ha tocado vivir no hemos podido desconectar en ningún momento. Al respecto, debemos tener en cuenta que el escenario que nos hemos encontrado no ha ido acompañado de unas medidas, instrucciones y protocolos en donde el derecho a la desconexión digital se contemplara, y que el número de horas empleadas en la docencia *online* ha sido muy superior al habitualmente dedicado a la docencia presencial. Cuestiones como la dificultad de conciliación de la actividad laboral con la vida familiar en un marco de actividades virtuales con una hiperconexión continuada determinan que sea preciso el establecimiento de límites legales y personales para el ejercicio de este derecho a la desconexión digital, y que recientemente se han determinado en el Real Decreto Ley 28/2020, de 22 de septiembre, de trabajo a distancia , y en el Real Decreto-ley

1. Trabajo realizado en el marco del Proyecto I+D+i «Retos investigación» del Programa estatal de I+D+i orientado a los Retos de la Sociedad del Ministerio de Ciencia, Innovación y Universidades: RTI2018-097354-B-100 (2019-2022) y del Proyecto de I+D+i Retos de Investigación, MICINN, del Programa Estatal de I+D+i orientada a los retos de la sociedad (PID2019-108710RB-I00, 2020-2022).

29/2020, de 29 de septiembre, de medidas urgentes en materia de teletrabajo en las Administraciones Públicas y de recursos humanos en el Sistema Nacional de Salud para hacer frente a la crisis sanitaria ocasionada por la COVID-19.

Palabras clave

desconexión digital, docencia universitaria, COVID-19, derechos, trabajo

Digital disconnection and university teaching online in times of pandemic for COVID-19: an illusion more than a reality

Abstract

The declaration of the state of alarm about the COVID-19 pandemic has meant that work activity is carried out in a telematic way, in the collectives in which it has been possible. One of them is the university sphere, in which the teaching staff has moved from the classroom to the virtual world. The right to digital disconnection provided for in Organic Law 3/2018, of 5 December, on Personal Data Protection and Digital Guarantee leaves many issues in the air that make it difficult to implement this right, together with its lack of development within the university. In this paper we intend to reflect on what has been more an illusion than a reality, addressing its shortcomings, limitations and lack of guarantees of this right, since in this scenario that we have lived we have not been able to disconnect at any time. We have to take into account that the scenario that we have encountered has not been accompanied by measures, instructions, or protocols in which the right to digital disconnection is contemplated, and that the increase in hours dedicated to online teaching has been much higher than if it had been face-to-face teaching. Issues such as the difficulty of reconciling work activity with family life in a framework of virtual activities with a continuous, excessive connection to the internet determines that it is necessary to establish legal and personal limits for the exercise of this right to digital disconnection and that have recently been determined in the Royal Decree-Law 28/2020, of September 22, on distance work, and the Royal Decree-Law 29/2020, of September 29, on urgent measures regarding teleworking in Public Administrations and human resources in the National Health System to face the health crisis caused by COVID-19.

Keywords

Digital disconnection, university teaching, COVID-19, rights, work

Introducción

La pandemia mundial por la COVID-19 ha supuesto un escenario muy diferente al habitual, de manera que, como consecuencia de la crisis sanitaria, se declaró el estado de alarma por Real Decreto 463/2020, de 14 de marzo[2].

Durante el estado de alarma se restringió la libre circulación[3] siguiendo lo indicado en el artículo 17 de la Constitución española, y se confinó a la población para evitar la propagación del coronavirus. Como excepción se establecieron servicios esenciales que se regularon por la Orden SND/310/2020, de 31 de marzo[4], pero la actividad docente universitaria no fue considerada como esencial.

El Real Decreto Ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social de la COVID-19[5], en su artículo 5, estableció el carácter preferente del trabajo a distancia, debiendo las empresas adoptar las medidas oportunas y entendiéndose cumplida la obligación de efectuar la evaluación de los riesgos. Asimismo, el Real Decreto Ley 15/2020, de 21 de abril, de medidas urgentes complementarias para apoyar la economía y el empleo[6], también prorrogó esa consideración preferencial del teletrabajo.

Durante dicho período, con el curso académico 2019-2020 ya comenzado, se pasó automáticamente de la docencia presencial a la modalidad *online*, dada la imposibilidad de acudir a los centros universitarios.

Ello supuso una situación sobrevenida y no previsible que ha determinado el planteamiento de diferentes cuestiones que nos interesa examinar en el presente trabajo. Al respecto, vamos a abordar, en el ámbito de la docencia *online*, el encaje del nuevo derecho que regula la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[7], denominado «derecho a la desconexión digital», determinando algunos elementos de interés, así como carencias y criterios de aplicación del precepto.

1. El derecho a la desconexión digital

Como un nuevo derecho digital –siguiendo las directrices del artículo 18.4 de la Constitución española respecto a que la «ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»–, se regula, en el artículo 88 de la Ley Orgánica 3/2018, el derecho a la desconexión digital en el ámbito laboral[8], con el siguiente tenor literal:

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

El derecho a la desconexión digital es el derecho que tiene todo trabajador a no estar conectado a dispositivos elec-

2. Boletín Oficial del Estado (14 de marzo de 2020, págs. 25.390-25.400).
3. Sobre ello puede verse, sin ánimo de exhaustividad: Cotino Hueso (2020a, págs. 88-102) y (2020b, págs. 1-20).
4. Boletín Oficial del Estado (1 de abril de 2020, págs. 27.984-27.987).
5. Boletín Oficial del Estado (18 de marzo de 2020, págs. 25.853-25.898).
6. Boletín Oficial del Estado (22 de abril de 2020, págs. 29.473-29.531).
7. Boletín Oficial del Estado (6 de diciembre de 2018, págs. 119.788-119.857).
8. Véase Gutiérrez Colominas (2020, pág. 3).

trónicos (correo, teléfono, mensajería instantánea u otras aplicaciones informáticas) durante su tiempo de descanso y vacacional[9], tal y como indica el Informe de la Organización Internacional del Trabajo-Eurofound «Working anytime, anywhere: the effects on the wordl of work»[10].

Es un derecho predicable del entorno internet que, no obstante, se regula sin definir en qué consiste[11], y que se relaciona con el derecho a la intimidad en el uso de dispositivos digitales en el trabajo regulado en el artículo 87 de la Ley Orgánica 3/2018. Representa una garantía para la separación efectiva del tiempo dedicado al trabajo y el tiempo de descanso, de tal forma que se asegure una desconexión de las herramientas digitales utilizadas en el quehacer profesional. Al respecto, en aras de su efectividad, debe especificarse e identificarse de forma muy clara cuál es el horario dedicado a la actividad a distancia, debiendo acordarse este por ambas partes (empresa y trabajador), así como la posibilidad de ser modificado y determinar los límites y condiciones en los que se realizará. La pretensión del precepto es evitar el peligro de trabajar en cualquier momento y sitio, lo que se conoce como *smart working*.

Podemos extraer las siguientes notas distintivas: es un derecho con distintas modalidades de ejercicio según la naturaleza y el objeto de la relación laboral, incidiéndose en su preservación no solo en los casos en que el trabajo se efectúe de forma parcial o total, sino también cuando se realice en el domicilio del empleado, como sucedió a lo largo de la pandemia, durante la cual la actividad laboral se desarrolló mayoritariamente desde la propia casa y con dispositivos electrónicos no empleados en el ámbito profesional presencial[12].

No se trata de un derecho de alcance constitucional, sino derivado de una limitación de nuestra Constitución[13].

Hay que tener en cuenta que este derecho no se aplica solo a aquellos casos en los que se efectúe una actividad laboral a distancia, sino a toda actividad laboral, utilice o no el trabajador instrumentos electrónicos, ya que se refiere también a la comunicación que se establece con el trabajo más allá del horario estrictamente laboral. Es decir, que fuera del horario legal o pactado, el trabajador tiene derecho a su descanso, así como a su intimidad, que podría verse afectada por el uso de las TIC, por ejemplo, en el caso de llamada con imagen en un dispositivo electrónico. En este sentido, se indica que el derecho a la desconexión digital constituye una expresión singular del derecho a la intimidad, en una dimensión específica caracterizada por las nuevas tecnologías[14].

El precepto, además, no establece la imposición del deber de negociar, ni se incluye en el contenido mínimo para el convenio colectivo[15]. Se refiere a lo que se establezca en la negociación colectiva, y a falta de ella, a lo que se haya pactado entre la empresa y los representantes laborales. En defecto de ello, habrá que establecer unas pautas para el cumplimiento de este derecho, que el precepto, sin embargo, no precisa.

También encontramos la delimitación del contenido de este derecho en distintos convenios colectivos. Así, el artículo 24 de la Resolución de 13 de febrero de 2020, de la Dirección General de Trabajo, por la que se registra y publica el convenio colectivo de Siemens Healthcare, SLU,[16]delimita el contenido del derecho de desconexión digital, indicando que «los/as empleados/as no tendrán que responder a *emails*, mensajes profesionales o llamadas telefónicas fuera de su horario de trabajo, ni durante los tiempos de descanso o vacaciones, salvo circunstancias excepcionales, guardias y/o disponibilidades de emergencia». En el mismo sentido se dispone en el artículo 78 de la Resolución de 14 de febrero de 2020, de la Dirección General de Trabajo, por la que se registra y publica el convenio colectivo de Carlson Wagonlit España, SLU[17], que

9. Véanse Torres García (2020) y Cardona Ruber (2020).
10. Eurofound y Oficina Internacional del Trabajo (2017).
11. Vallecillo Gámez (2020).
12. Véase González Tapia (2020).
13. Cfr. Gutiérrez Colominas (2020, pág. 6 y sigs).
14. Requena Montes (2020, pág. 545).
15. Domingo Monforte y Salvador Álvarez (2020, pág. 1).
16. Boletín Oficial del Estado (28 de febrero de 2020, págs. 20.934-20.981).
17. Boletín Oficial del Estado (27 de febrero de 2020, págs. 18.186-18.224).

establece este derecho en términos de no obligatoriedad: «ninguna persona trabajadora está obligada a atender llamadas y/o contestar posibles correos electrónicos que, en su caso, pudiera recibir durante el tiempo de descanso, sin perjuicio de que puedan darse situaciones excepcionales de necesidad o urgencia».

Este derecho ha sido considerado como tal para los trabajadores, pero no obligatorio para la empresa, «pudiendo escoger hacer uso o no», como se plasma en el artículo 65 de la Resolución de 1 de marzo de 2020, de la Dirección General de Trabajo, por la que se registra y publica el convenio colectivo de CTC Externalización, SLU[18], que incluso, en virtud del principio de autonomía de la voluntad, indica que «a pesar de que la empresa se esfuerza en promover una cultura que disminuya las conexiones voluntarias realizadas fuera de la jornada laboral ordinaria, estas no serán consideradas contrarias al derecho a la desconexión o imputables a la empresa».

El artículo 20 de la Resolución de 21 de enero de 2020, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Servicios Dix 2012, SL[19], menciona el supuesto de fuerza mayor, al que también alude el artículo 44 de la Resolución de 21 de enero de 2020, de la Dirección General de Trabajo, por la que se registra y publica el convenio colectivo del Grupo Selecta (AB Servicios Selecta España, SLU; Acorn Spain1, SL; y Servecave, SL)[20].

La salud laboral, no solo del trabajador, sino también del resto de los trabajadores, así como del conjunto de las personas trabajadoras, se menciona en el manifiesto tercero de la Resolución de 22 de enero de 2020, de la Dirección General de Trabajo, por la que se registra y publica el acuerdo sobre registro diario de jornada del convenio colectivo del sector de la banca[21], el cual se precisa con más detalle en el punto VII del Acuerdo sobre Registro Diario de Jornada, al señalar que se aplica a todos los dispositivos y herramientas (móviles, tabletas, aplicaciones de la empresa, correos electrónicos y sistemas de mensajería). Cabe destacar que se adoptan una serie de medidas consideradas como mínimas para garantizar el cumplimiento del derecho a la desconexión digital.

Además, a causa de la crisis sanitaria, el Real Decreto Ley 16/2020, de 28 de abril, de medidas procesales y organizativas para hacer frente a la COVID-19 en el ámbito de la Administración de Justicia[22], ha modificado la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en dicha Administración[23], en concreto su disposición adicional quinta, haciendo referencia a que se garantice el derecho a la desconexión digital que se establece en el artículo 14.j.bis[24] y en el artículo 88 del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público[25].

Este derecho a la desconexión digital ha sido reconocido por la doctrina judicial y la jurisprudencia, habiéndose pronunciado en STSJ Barcelona, Sala de lo Social, 464/2020, de 24 de enero[26]; SAN, Sala de lo Social, 126/2019, de 29 de octubre[27]; STSJ A Coruña, Sala de lo Social, 17 de octubre de 2019[28]; STSJ Granada, Sala de lo Social, 835/2019, de 28 de marzo[29]; STSJ A Coruña, Sala de lo Social, 21/218, de

18. Boletín Oficial del Estado (18 de marzo de 2020, págs. 25.982-26.018).
19. Boletín Oficial del Estado (4 de febrero de 2020, págs. 10.462-10.487).
20. Boletín Oficial del Estado (30 de enero de 2020, págs. 9.283-9.323).
21. Boletín Oficial del Estado (4 de febrero de 2020, págs. 10.488-10.495).
22. Boletín Oficial del Estado (29 de abril de 2020, págs. 30.623-30.645).
23. Boletín Oficial del Estado (6 de julio de 2011, págs. 71.320-71.348).
24. La Ley Orgánica 3/2018 añadió esta letra j bis) en el artículo 14, con la siguiente redacción: «j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales».
25. Boletín Oficial del Estado (31 de octubre de 2015, págs. 103.105-103.159).
26. ECLI: ES: TSJCAT:2 020: 1.218.
27. ECLI: ES: AN: 2019: 4.065.
28. ECLI: ES: TSJGAL: 2019: 5.679.
29. ECLI: ES: TSJAND: 2019: 2.579.

18 de diciembre, [30] y STSJ Valladolid, Sala de lo Social, de 8 de abril de 2019[31], que incidió en considerar que:

Existe una evidente tensión entre la pretensión de los poderes públicos de que las empresas, profesionales y ciudadanos estén permanentemente conectados para recibir notificaciones y comunicaciones de las autoridades y el derecho de esos sujetos a la desconexión digital. En ese sentido resulta extraordinariamente significativo que la Ley 39/2015, de procedimiento administrativo común, haya derogado y sustituido a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y con tal motivo haya desaparecido de nuestro ordenamiento jurídico positivo el principio de igualdad que reconocía la anterior Ley 11/2007.[32]

2. El escenario de la docencia *online* y el derecho a la desconexión digital en tiempo de pandemia por COVID-19: algunas cuestiones

Se podría comenzar este epígrafe indicando que no ha habido desconexión digital en la docencia *online* provocada por la pandemia de la COVID-19. Esta aseveración, sin duda, debe ser precisada y matizada. La suspensión de la actividad presencial en el ámbito docente y la necesidad de desarrollar una enseñanza *online* se centra en la forma de realización de la actividad profesional, pero, al convertirse la presencialidad en virtualidad, el derecho a la desconexión digital no se ha producido.

Consideramos que la suspensión de la presencialidad ha infringido el respeto al tiempo de descanso, a los permisos y vacaciones, al igual que a la intimidad personal y familiar del profesorado universitario que propugna el artículo 88 de la Ley Orgánica 3/2018. Y esto ha sucedido por la inexistencia de una organización y normativa que delimitara los tiempos de trabajo y descanso, pero también a causa de la falta de adaptación del entorno doméstico para poder llevar a cabo la docencia *online* (carencias de espacio y de equipo informático), ya que el confinamiento no ha significado que el docente estuviera aislado: en la mayoría de los casos convivió con otras personas durante ese período (familiares, entre otros).

El Real Decreto 463/2020 contempló las «medidas de contención en el ámbito educativo y de la formación», en su artículo 9, e indicó la suspensión de toda actividad educativa presencial. Esta disposición afectó a todos los centros, etapas y niveles de enseñanza que contempla la Ley Orgánica 2/2006, de 3 de mayo, de Educación[33], con inclusión de la docencia universitaria. Durante dicho período de estado de alarma, se mantendría la actividad educativa en la modalidad a distancia y *online*, siempre que fuera posible. Se ha producido así una «suspensión sin suspensión»[34] de la actividad docente en las universidades que impartían docencia presencial, sin que esa supresión de la presencialidad menoscabe el derecho a la educación recogido en el artículo 27 de la Constitución. Asimismo, tampoco se contempla la suspensión de este derecho en el artículo 55 del mismo texto legal, al no mencionar el anterior precepto[35].

A título de ejemplo, y en referencia a la adopción por parte de las universidades de medidas para la adaptación durante el estado de alarma, en la Universitat Politècnica de València –siguiendo lo indicado en la Resolución de 13 de marzo de 2020 de la Conselleria de Innovación, Universidades, Ciencia y Sociedad Digital, por la que se desarrolla para el ámbito universitario y de enseñanzas artísticas superiores la Resolución de 12 de marzo, de la Conselleria de Sanidad Universal y Salud Pública, de suspensión temporal de la actividad educativa y formativa presencial en todos los centros, etapas, ciclos, grados, cursos y niveles de enseñanza de la Comunidad Valencia como consecuencia de la situación y evolución del coronavirus[36]– el vice-

30. ECLI: ES: TSJGAL: 2018: 5.854.
31. ECLI: ES: TSJCL: 2019: 1.523.
32. Fundamento de Derecho Quinto STSJ Valladolid, Sala de lo Social, de 8 de abril de 2019.
33. Boletín Oficial del Estado (4 de mayo de 2006, págs. 17.158-17.207).
34. Cotino Hueso (2020c, pág. 1).
35. Cotino Hueso (2020c, pág. 6).
36. Diari Oficial de la Comunitat Valenciana (13 de marzo de 2020, págs. 10.165-10.166).

rrectorado de Estudios, Calidad y Acreditación emitió una instrucción el 13 de marzo de 2020 indicando una serie de directrices para la adaptación a la docencia a distancia, completada por otra instrucción, de 25 de marzo de 2020, para el seguimiento de las actividades y utilización de las herramientas en un entorno virtual. Junto a ello, se emitió por parte del vicerrectorado de Ordenación Académica y Profesorado las condiciones de impartición de dicha docencia durante el estado de alarma, haciendo mención a la observancia de las obligaciones docentes en cumplimiento de lo indicado en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades; en el Real Decreto 898/1985, de 30 de abril, sobre régimen del profesorado universitario, y en los estatutos de la propia universidad, pero sin hacer ningún tipo de referencia a si existía una obligación o no de conexión más allá del horario de docencia asignado, y sin referirse, en ningún momento, al derecho a la desconexión digital.

En cuanto a la organización y docencia, el 13 de marzo de 2020[37] el vicerrectorado de Estudios, Calidad y Acreditación de la Universitat Politècnica de València –en coordinación con el vicerrectorado de Alumnado, Cultura y Deporte y el vicerrectorado de Recursos Digitales y Documentación– facilitó unas pautas a seguir destinadas a organizar la enseñanza y aprendizaje a distancia frente a la suspensión de la docencia presencial por causa de la epidemia.

De igual modo, se creó una plataforma específica para la docencia y aprendizaje *online* denominada Virtual UPV, en la que se facilitaban, en abierto, todas las pautas y directrices para alumnado y profesorado relativas a la docencia virtual durante la crisis de la COVID-19[38].

Los sucesivos protocolos internos de actuación ante la activación de la alerta sanitaria por SARS-CoV-2 aprobados por el Comité de Seguridad y Salud de la Universitat Politècnica de València, siendo el último de ellos de 27 de julio de 2020[39], ya en el escenario de la «nueva normalidad», hacen referencia a distintas medidas higiénicas y de protección, pero ninguna mención a medidas relacionadas con el derecho a la desconexión digital.

A continuación, nos vamos a centrar en varios aspectos y cuestiones derivadas de tal situación: en concreto, los distintos problemas que se plantean en el ámbito del teletrabajo docente en relación con el derecho a la desconexión digital y su encaje con el derecho a la intimidad, así como la observancia del derecho a tal desconexión en el colectivo docente como medida para evitar riesgos en la salud del profesorado, formulando algunas propuestas concretas de mejora.

2.1. El paso de la presencialidad al teletrabajo sin solución de continuidad y los problemas de la desconexión en dichas circunstancias en relación con el derecho a la intimidad

Tal y como hemos indicado, la docencia presencial pasó a ser *online* de forma inmediata. Ello ha provocado que el profesorado que impartía de modo habitual su profesión presencialmente se haya visto inmerso en un escenario diferente, sin disponer de un tiempo de adaptación ni contemplarse por parte de las instituciones correspondientes cómo efectuar la desconexión digital debido a lo inesperado de la coyuntura.

Seguidamente, apuntaremos cuáles han sido las causas por las cuales la desconexión no se ha podido realizar: en el ámbito de la docencia *online*, en donde no se contempló inicialmente, las razones han sido varias, todas ellas derivadas de una situación sobrevenida que ha supuesto una alteración de la «normal». Lejos de pretender establecer una generalización de las mismas, podríamos apuntar las siguientes:

–*Falta de un plan efectivo de teletrabajo.* En la docencia habitual de carácter presencial sí que hay unas pautas para la impartición de la misma, con la finalidad de conciliar la vida familiar y laboral teniendo en cuenta lo indicado en la Ley 39/1999, de 5 de noviembre, para promover la conciliación de la vida familiar y laboral de las personas trabajadoras,[40] y la Directiva (UE) 2019/1158 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa

37. Vicerrectorado de Estudios, Calidad y Acreditación (UPV, 2020).
38. Virtual UPV (2020).
39. Servicio Integrado de Prevención y Salud Laboral (UPV, 2020).
40. Boletín Oficial del Estado (6 de noviembre de 1999, págs. 38.934-38.942).

a la conciliación de la vida familiar y la vida profesional de los progenitores y los cuidadores, y por la que se deroga la Directiva 2010/18/UE del Consejo[41].

Como hemos señalado anteriormente, y por lo que se refiere a la experiencia propia, en la Universitat Politècnica de València las instrucciones y directrices facilitadas para la adaptación a la docencia *online* no especificaban los tiempos de conexión. Informaban que la tutorización del alumnado debía indicar el medio, fecha y horario de realización; y que las clases remotas que se fueran a impartir debían especificar contenido, fecha y horario, recomendándose el acceso a la plataforma docente PoliformaT a fin de atender peticiones o consultas en el menor plazo y evitar así el abandono. Sin embargo, no se precisaba ni la frecuencia ni el horario, ya que otra de las recomendaciones se refería a establecer una comunicación «regular» con el alumnado con objeto de recordarle la planificación de las actividades, o mostrar el profesorado disponibilidad para la resolución de dudas. En tales directrices no se hacía ninguna mención a la necesidad de conciliar trabajo y vida familiar y al derecho a la desconexión digital.

–*Ausencia de un control horario*. La eliminación de la presencialidad y su sustitución por aplicaciones informáticas de conexión con el alumnado propicia que se utilicen de forma continua, ya sea para la resolución de dudas o problemas con los materiales, o la tutorización de trabajos. Y es precisamente esta proliferación de herramientas de comunicación con los alumnos y alumnas lo que dificulta el ejercicio del derecho a la desconexión digital. En la Universitat Politècnica de València, por ejemplo, en la instrucción del vicerrectorado de Estudios, Calidad y Acreditación, a efectos de llevar a cabo las tutorías se apuntaban los siguientes canales de comunicación posibles con el alumnado: correo electrónico, chat de PoliformaT, Microsoft Teams, foros de PoliformaT, así como que el profesorado podría utilizar otras herramientas, en el caso de considerarlo oportuno, como podrían ser los servicios de mensajería instantánea (WhatsApp, Skype, entre los más conocidos). Ello supone que profesoras y profesores deben atender a los múltiples instrumentos de comunicación del alumnado, no estableciéndose un solo canal, lo que dificulta la desconexión digital, ya que deben estar atentos a todas las vías a través de las cuales se puede establecer contacto, a lo que hemos de sumar la no concreción de unos parámetros temporales explícitos que eviten que la jornada laboral se extienda a lo largo de todo el día.

Con anterioridad a la situación de pandemia, el profesorado determinaba sus tutorías de forma cerrada, bien con un horario predeterminado, o a demanda, para quedar posteriormente con el alumnado. Fuera de dicho horario, la tutorización no se realizaba y tanto profesorado como alumnado prefijaban su comunicación. En la situación actual, los alumnos y alumnas están permanentemente conectados, haciendo uso de las herramientas para consultas relacionadas con las asignaturas, con lo que se dificulta aún más la desconexión digital de los docentes.

En la docencia virtual es difícil la observancia de esos horarios de tutoría prefijados, ya que no se respeta el horario y el alumnado, lejos de solicitar una tutoría por los procedimientos indicados más arriba, al disponer de herramientas informáticas «instantáneas», presupone que el profesorado está disponible las veinticuatro horas del día (de hecho, son numerosas las consultas que se llevan a cabo en horas fuera de un horario laboral habitual). Una excepción fueron las defensas de TFG y TFM que se hicieron de forma virtual, en las que sí hubo un respeto del horario fijado para las defensas, de forma similar a las realizadas de modo presencial antes de la pandemia, e incluso podríamos indicar con un cumplimiento mucho más estricto y ajustado del horario disponible.

–*Falta de capacidad de reacción y ayuda para adaptarse a la situación sobrevenida*, junto con la paradoja de que, a pesar de la hiperconectividad, se ha producido una desconectividad con el resto del profesorado. Desde luego, era inimaginable un escenario como el actual: ello ha supuesto que, de un día para otro, se haya tenido que adaptar la docencia que se efectuaba de forma presencial a la modalidad *online*, lo cual ha generado algunos problemas relacionados: entre otros, la evaluación a través de videoconferencia y diversas problemáticas derivadas de la posibilidad de violación del derecho a la intimidad.

Interesa aquí traer a colación lo establecido en el artículo 18 de la Constitución española y el artículo 8.1 del Convenio Europeo de Derechos Humanos, junto con la protección de

41. Diario Oficial de la Unión Europea (12 de julio de 2019, págs. 79-93).

datos de carácter personal, así como lo indicado en la Ley Orgánica 3/2018, que añadió un nuevo artículo 20 bis al Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores[42] a fin de regular los derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión, estableciendo que tienen esos derechos frente al «uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales».

Cabe mencionar también que la red EDRi (European Digital Rights) elaboró una Carta de Derechos Digitales que recogía diez principios fundamentales[43].

-*Omisión de información, formación y sensibilización sobre la forma de ejercitar el derecho a la desconexión digital,* generándose a raíz de ello un desconocimiento en torno al ejercicio de tal derecho.

Este derecho a la intimidad en la utilización de las aplicaciones informáticas docentes ha supuesto un hándicap difícil de resolver, ya que, al no contemplarse una norma específica referente al teletrabajo o trabajo a distancia y establecer los protocolos adecuados, se han planteado problemas tanto en las clases emitidas a través de la plataforma como en la realización de exámenes por parte del alumnado, ya que consideramos que se ha podido infringir este derecho[44].

2.2. Desconexión digital en la docencia *online* como medio para evitar riesgos en la salud

La conectividad de la docencia *online* no debe ser entendida como una permanente disposición, sino contemplar las pausas y tiempos de descanso para poder desconectar. Tal modalidad de trabajo docente no se enmarca solo en las clases *online*, sino en la atención a través de tutorización, corrección de prácticas, dirección de trabajos, etc. En una situación como la actual no se perfila el tiempo dedicado a tal conjunto de actividades, convirtiéndose en un teletrabajo continuo, sin pausa, con una disponibilidad absoluta a través de las distintas herramientas informáticas mediante las cuales se desarrolla el teletrabajo.

Ello conlleva que no existan unas buenas prácticas para disponer de una buena salud en el ámbito informatizado, y que el trabajador sufra de lo que se denomina «tecnoestrés»[45]. Esto sucede porque se trabajan muchas más horas que las contempladas en el contrato y porque el trabajo interfiere de modo continuo en la vida personal, dedicándose el tiempo que se destinaría al descanso a tareas como supervisar el correo electrónico, entre otras, con lo que no se produce ningún tipo de desconexión digital[46].

Esta conectividad sin desconexión produce una serie de efectos: desmotivación, agotamiento, falta de rendimiento. Todos sabemos que el uso de las nuevas tecnologías de la información y comunicación (TIC) tiene aspectos potencialmente positivos, pero también negativos[47].

De resultas, se han establecido unas pautas a modo de guía de buenas prácticas, como medidas preventivas, en aras de una desconexión digital[48], que abordamos en las siguientes líneas.

Respecto al tiempo de trabajo y la conciliación de la vida laboral y familiar sería deseable establecer políticas de desconexión digital que garanticen los tiempos de descanso. Ello se puede lograr implantándose sistemas restrictivos de desconexión automática, de tal forma que no se reciban ni envíen correos electrónicos fuera de la jornada laboral; evitándose el uso de dispositivos fuera del horario de trabajo; incorporando las denominadas «siestas digitales»; o limitándose el acceso remoto a la intranet. Medidas todas ellas sencillas, pero muy útiles para evitar la «jornada laboral sin fin».

42. Boletín Oficial del Estado (24 de octubre de 2015, págs. 100.224-100.308).
43. Ramón Fernández (2019, pág. 216).
44. Véase Moreno Vida (2019) y Altés y Yagüe (2020).
45. Domingo Monforte y Salvador Álvarez (2020, pág. 1).
46. Messenguer et al. (2017, pág. 9 y sigs.).
47. Manzano Santamaría (2018a, págs. 1-4).
48. Manzano Santamaría (2018b, págs. 1-8).

Las condiciones en las que se ha desarrollado la docencia *online* sobrevenida por el coronavirus no han sido precisamente las más óptimas, ya que, aunque ha sido una de las medidas para evitar la propagación del virus, no siempre se disponen de los medios adecuados para precaver problemas de salud derivados por el teletrabajo[49] (falta de una estancia idónea para trabajar, de mobiliario ergonómico, de luz natural, de aislamiento acústico para la realización de las videoconferencias, así como disponer de un equipo informático adecuado con una conexión a internet que permita el desarrollo de la actividad). Al respecto, es importante el cumplimiento de la Directiva Marco del Consejo 89/391/CEE, de 12 de junio de 1989, relativa a la aplicación de medidas para promover la mejora de la seguridad y de la salud de los trabajadores en el trabajo[50], incorporada por la Ley 31/1995, de 9 de noviembre, de prevención de riesgos laborales[51], y la Ley 54/2003, de 12 de diciembre, de reforma de marco normativo de la prevención de riesgos laborales[52], ya que durante la pandemia no se ha contemplado una evaluación de los riesgos ni una comprobación de los equipos y condiciones en los que se ha desarrollado la docencia *online* desde el domicilio particular de cada sujeto, ya que la declaración del estado de alarma impidió que la enseñanza *online*, por la imposibilidad de acceder a los campus, se pudiera impartir desde el despacho de cada profesor, debiéndose efectuar en el ámbito doméstico.

La doctrina también pone de manifiesto los problemas derivados del teletrabajo que pueden afectar a los «nuevos teletrabajadores» por desarrollar estos su actividad en el seno del hogar: por ejemplo, conflictos con otros miembros de la familia que también se encontraban confinados en el mismo lugar[53]. La solución, desde luego, pasa por el establecimiento de normas y directrices claras por parte de la empresa, en este caso la universidad, atendiendo a las normas internacionales como el Convenio de la Organización Internacional del Trabajo, núm. 177, de 1996, sobre el trabajo a domicilio[54] y la Recomendación de la Organización Internacional del Trabajo, núm. 184, de 1996, sobre el trabajo a domicilio[55].

Esta jurisprudencia también se relaciona con uno de los objetivos de desarrollo, según el Programa de las Naciones Unidas para el Desarrollo, en concreto el número 8, relativo al trabajo decente y el crecimiento económico, una de cuyas metas es la incluida en el apartado 8.8: «Proteger los derechos laborales y promover un entorno de trabajo seguro y sin riesgos para todos los trabajadores»[56].

Sin duda, el impacto del teletrabajo –en este caso la docencia– durante la pandemia se ha visto reflejado en un incremento de horas laborales, una falta de desconexión y una carencia de conciliación evidente, y ello ha sido manifestado en la literatura científica de reciente publicación[57], en donde se ha puesto de manifiesto la afectación en la salud de las personas, además de la necesidad de adoptar instrumentos válidos para evitar las consecuencias negativas que hemos indicado.

Una de las soluciones es la regulación del teletrabajo o trabajo a distancia, tanto en el caso de desarrollarse de forma habitual como sobrevenida. Así, el Real Decreto Ley

49. Lago Moreda (2020, págs. 54-55).
50. Diario Oficial de las Comunidades Europeas (29 de junio de 1989, págs. 0001-0008).
51. Boletín Oficial del Estado (10 de noviembre de 1995, págs. 32.590-32.611).
52. Boletín Oficial del Estado (13 de diciembre de 2003, págs. 44.408-44.415).
53. Marín Boscán (2020, págs. 1-2).
54. https://www.ilo.org/dyn/normlex/es/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C177 [Fecha de consulta: 29 de septiembre de 2020].
55. https://www.ilo.org/dyn/normlex/es/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:R184 [Fecha de consulta: 29 de septiembre de 2020].
56. Naciones Unidas (s/f).
57. Sin ánimo de exhaustividad, se pueden consultar García García (2020) y González Torres (2020).

28/2020, de 22 de septiembre, de trabajo a distancia[58] viene a ser la norma de desarrollo y concreción de las disposiciones legales para garantizar un régimen seguro y suficiente de esta forma de prestación laboral, ya que las normas vigentes (Estatuto de los Trabajadores y la limitada vigencia del Real Decreto Ley 8/2020) no han resultado adecuadas.

Respecto a la evaluación de riesgos, la norma contempla la distribución de la jornada, garantizando los descansos y desconexiones durante la misma (artículo 16), así como el derecho a la desconexión digital en el artículo 18, no solo reconociendo el mismo e indicando que es un deber empresarial, sino además concretando que la desconexión conlleva una limitación del uso de los medios tecnológicos de comunicación empresarial y de trabajo durante los períodos de descanso, así como el respeto a la duración máxima de la jornada. También indica que se atenderá a «cualesquiera límites y precauciones en materia de jornada que dispongan la normativa legal o convencional aplicable».

Asimismo, deja en manos de la empresa, previa audiencia de los representantes legales de los trabajadores, la elaboración de una política interna en la que se definan las modalidades de ejercicio de este derecho, las acciones de formación y una sensibilización acerca de un uso razonable de las herramientas tecnológicas a fin de evitar el riesgo de fatiga informática.

Este derecho se preservará tanto si el trabajo a distancia se realiza de forma parcial o total, así como si se efectúa en el domicilio de la persona empleada vinculado al uso con fines laborales de herramientas tecnológicas.

Serán los convenios o acuerdos colectivos los que puedan establecer los medios y medidas adecuadas para garantizar el ejercicio efectivo de este derecho y la organización de la jornada de forma apropiada con la finalidad de poderla compatibilizar con la garantía de los tiempos destinados al descanso.

En este sentido, consideramos que esta norma ha desaprovechado la oportunidad de contemplar, entre otros aspectos, los tiempos máximos de trabajo y mínimos de descanso, así como determinar los dispositivos digitales y formas de trabajo en red que no desprotejan ni mermen los derechos a la privacidad.

Por último, cabe indicar que el Real Decreto Ley 29/2020, de 29 de septiembre, de medidas urgentes en materia de teletrabajo en las Administraciones Públicas y de recursos humanos en el Sistema Nacional de Salud para hacer frente a la crisis sanitaria ocasionada por la COVID-19[59] modifica el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, al que hemos hecho referencia anteriormente. Al respecto, se introduce un nuevo artículo 47 bis, en donde que define el teletrabajo y las condiciones para ser realizado:

1. Se considera teletrabajo aquella modalidad de prestación de servicios a distancia en la que el contenido competencial del puesto de trabajo puede desarrollarse, siempre que las necesidades del servicio lo permitan, fuera de las dependencias de la Administración, mediante el uso de tecnologías de la información y comunicación.

2. La prestación del servicio mediante teletrabajo habrá de ser expresamente autorizada y será compatible con la modalidad presencial. En todo caso, tendrá carácter voluntario y reversible, salvo en supuestos excepcionales debidamente justificados. Se realizará en los términos de las normas que se dicten en desarrollo de este Estatuto, que serán objeto de negociación colectiva en el ámbito correspondiente y contemplarán criterios objetivos en el acceso a esta modalidad de prestación de servicio.
   El teletrabajo deberá contribuir a una mejor organización del trabajo a través de la identificación de objetivos y la evaluación de su cumplimiento.

58. Boletín Oficial del Estado (23 de septiembre de 2020, págs. 79.929-79.971). En la consulta pública previa a la elaboración del proyecto normativo consistente en la modificación y elaboración de las condiciones para prestar trabajo por cuenta ajena a distancia que estuvo abierta hasta el 22 de junio de 2020, se indicaban algunos de los inconvenientes que hemos referido: en concreto, el horario continuo y la conectividad digital permanente. Véase: http://www.mites.gob.es/ficheros/participacion/historico/consulta-publica/2020/Proyecto_07_20200606_consulta_publica_gabinete_empleo.pdf [Fecha de consulta: 29 de septiembre de 2020]. Como texto previo, en el Anteproyecto de Ley de trabajo a distancia se propuso el artículo 18 sobre el derecho a la desconexión digital: https://d2eb79appvasri.cloudfront.net/pdf/Proyecto_teletrabajo.pdf [Fecha de consulta: 29 de septiembre de 2020].
59. Boletín Oficial del Estado (30 de septiembre de 2020, págs. 82.159-82.168).

3. El personal que preste sus servicios mediante teletrabajo tendrá los mismos deberes y derechos, individuales y colectivos, recogidos en el presente Estatuto que el resto del personal que preste sus servicios en modalidad presencial, incluyendo la normativa de prevención de riesgos laborales que resulte aplicable, salvo aquellos que sean inherentes a la realización de la prestación del servicio de manera presencial.

4. La Administración proporcionará y mantendrá a las personas que trabajen en esta modalidad los medios tecnológicos necesarios para su actividad.

5. El personal laboral al servicio de las Administraciones Públicas se regirá, en materia de teletrabajo, por lo previsto en el presente Estatuto y por sus normas de desarrollo.

Conclusiones

La pandemia que estamos sufriendo por la COVID-19 ha supuesto en el ámbito laboral el teletrabajo, y nos estamos refiriendo al trabajo que anteriormente se desempeñaba de forma presencial. En el caso de la educación universitaria, el estado de alarma limitó el acceso a los campus universitarios y, fruto de ello, la conversión de la actividad del profesorado a una docencia *online* en su totalidad.

En este escenario, se plantea cómo ejercer el derecho a la desconexión digital que contempla el artículo 88 de la Ley Orgánica 3/2018, teniendo en cuenta la situación de hiperconectividad y la falta de desarrollo de este derecho. Son muchas las cuestiones que nos hemos planteado, ya que la teledocencia, o la virtualización del profesorado, ha supuesto un incremento de la carga laboral, al no estar convenientemente contemplado el derecho a la desconexión digital. Las múltiples herramientas que se tienen que utilizar para la docencia (videoconferencias, correo electrónico, plataformas para efectuar pruebas evaluadoras, las defensas virtuales de trabajos de final de grado, máster y tesis doctorales) han hecho inviable el ejercicio de tal derecho. Ello también guarda relación con la ausencia de buenas prácticas en el ámbito de este derecho, lo cual ha supuesto un notorio incremento de la actividad laboral en comparación con las horas habituales de trabajo presencial.

El derecho a estar desconectados –que se aplica tanto a la actividad presencial como telemática– debería ser desarrollado a través de normas complementarias. Prueba de ello son los diversos convenios colectivos que sí hacen referencia al mismo, si bien no son todos los que regulan las actividades profesionales.

Quizá el sector que más ha acusado esta conexión permanente haya sido el de la docencia, pues tanto alumnado como profesorado se han visto abocados a un permanente estar conectados que lastra la productividad y la eficacia laboral y de aprendizaje. La desconexión digital debe ser una garantía y una herramienta para determinar la finalización de la jornada laboral, teniendo una potente razón de ser en el caso de la docencia *online*. En este sentido, sería conveniente concretar una distribución de la jornada y de los tiempos de disponibilidad, así como garantizar los descansos y desconexiones durante la jornada laboral.

Se necesitan, además, instrumentos adecuados y planes de trabajo establecidos, así como una «higiene mental», para evitar una saturación y provocar el estrés informático derivado de esta situación de emergencia sanitaria.

El escenario de la realización virtual de todas las actividades, sin establecimiento de límites legales y personales, ha derivado precisamente en una infracción del mismo y en una falta de tutela para su ejercicio. Consideramos, pues, que la actual regulación de trabajo a distancia no desarrolla suficientemente el derecho a la desconexión digital. En este sentido, hubiera sido deseable una precisión mayor y una delimitación de las garantías, ya que las dificultades de conciliación de la actividad laboral con la vida familiar, imposible por la inexistencia de unos criterios claros de ejecución, siguen obstaculizando en gran medida la puesta en práctica del derecho de desconexión.

Referencias bibliográficas

ALTÉS TÁRREGA, J. A.; YAGÜE BLANCO, S. (2020). «A vueltas con la desconexión digital: eficacia y garantías de lege data». *Labos. Revista de Derecho del Trabajo y Protección Social,* vol. 1, núm. 2, págs. 61-87 [en línea] https://e-revistas.uc3m.es/index.php/LABOS/article/view/5539/3912 [Fecha de consulta: 29 de septiembre de 2020].

CARDONA RUBER, Mª. B. (2020). «Los perfiles del derecho a la desconexión digital». *Revista de Derecho Social,* núm. 90, págs. 109-126.

COTINO HUESO, L. (2020a). «Los derechos fundamentales en tiempos del coronavirus: Régimen general y garantías y especial atención a las restricciones de excepcionalidad ordinaria». *El Cronista del Estado Social y Democrático de Derecho*, núms. 86-87, págs. 88-102 [en línea] http://www.elcronista.es/El-Cronista-n%C3%BAmero-86-87-Coronavirus.pdf [Fecha de consulta: 29 de septiembre de 2020].

COTINO HUESO, L. (2020b). «Confinamientos, libertad de circulación y personal, prohibición de reuniones y actividades y otras restricciones de derechos por la pandemia del Coronavirus». *Diario La Ley*, núm. 9.608, págs. 1-20.

COTINO HUESO, L. (2020c). «La enseñanza digital en serio y el derecho a la educación en tiempos del coronavirus». *Revista de Educación y Derecho,* núm. 21, págs. 1-29 [en línea] https://revistes.ub.edu/index.php/RED/article/view/31213/31283 [Fecha de consulta: 29 de septiembre de 2020].

DOMINGO MONFORTE, J.; SALVADOR ÁLVAREZ, N. (2020). «Hiperconectividad digital y salud laboral». *Diario La Ley,* núm. 9.638, págs. 1-6.

EUROFOUND; OFICINA INTERNACIONAL DEL TRABAJO (2017). Working anytime, anywhere: the effects on the wordl of work, Oficina de Publicaciones de la Unión Europea, Luxemburgo, y la Oficina Internacional del Trabajo, Ginebra [en línea] http://eurofound.link/ef1658 [Fecha de consulta: 29 de septiembre de 2020].

GARCÍA, Mª. D. (2020). «La docencia desde el hogar. Una alternativa necesaria en tiempos del Covid 19». Polo del Conocimiento. *Revista científico-profesional,* vol. 5, núm. 4, págs. 304-324 [en línea] https://polodelconocimiento.com/ojs/index.php/es/article/view/1386/2519 [Fecha de consulta: 29 de septiembre de 2020].

GONZÁLEZ TAPIA, Mª. L. (2020). «Derecho a la desconexión digital y teletrabajo». *Diario La Ley,* núm. 9.606.

GONZÁLEZ TORRES, M. (2020). «Teletrabajo durante la pandemia del Covid 19». *Observatorio de recursos humanos y relaciones laborales*, núm. 158, pág. 67.

GUTIÉRREZ COLOMINAS, D. (2020). «La desconexión digital de los trabajadores. Reflexiones a propósito de su calificación como derecho y su instrumentación». *IDP. Revista de Internet, Derecho y Política*, núm. 31, págs. 1-13 [en línea] http://dx.doi.org/10.7238/idp.v0i31.3208 [Fecha de consulta: 29 de septiembre de 2020].

LAGO MOREDA, A. (2020). «El teletrabajo en tiempos del coronavirus». *Gestión práctica de riesgos laborales: Integración y desarrollo de la gestión de la prevención*, núm. 180, págs. 54-55.

MANZANO SANTAMARÍA, N. (2018a). «Las Tecnologías de la Información y la Comunicación (TIC) (I): nuevas formas de organización del trabajo», *Instituto Nacional de Seguridad, Salud y Bienestar en el Trabajo* (INSSBT), págs. 1-4 [en línea] https://www.insst.es/documents/94886/566858/ntp-1122w.pdf/baa93260-6840-4b9b-9abb-b6980b7f8f71 [Fecha de consulta: 29 de septiembre de 2020].

MANZANO SANTAMARÍA, N. (2018b). «Las Tecnologías de la Información y la Comunicación (TIC) (II):

factores de riesgo psicosocial asociados a las nuevas formas de organización del trabajo». *Instituto Nacional de Seguridad, Salud y Bienestar en el Trabajo* (INSSBT), págs. 1-8 [en línea] https://www.insst.es/documents/94886/566858/ntp-1123.pdf/acb83bc7-e6d5-4ffa-ab7c-f05e68079ffb [Fecha de consulta: 29 de septiembre de 2020].

MARÍN BOSCÁN, F. J. (2020). «Teletrabajo por Coronavirus: Hacia una Sociedad más Igualitaria?». *Noticias CIELO*, núm. 4, págs. 1-2 [en línea] http://www.cielolaboral.com/wp-content/uploads/2020/04/marin_noticias_cielo_n4_2020.pdf [Fecha de consulta: 29 de septiembre de 2020].

MESSENGUER, J.; VARGAS LLAVE, O.; GSHWIND, L.; BOEHMER, S.; VERMEYLEN, G.; WILKENS, M. (2017). *Working anytime, anywhere: The effects on the world of work. Eurofound and the International Labour Office,* Geneva: Publicaciones Office of the European Union, pág. 80 [en línea] https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef1658en.pdf [Fecha de consulta: 29 de septiembre de 2020].

MORENO VIDA, Mª. N. (2019). «Las facultades de control fuera de la jornada de trabajo: desconexión digital y control del trabajador». *Temas laborales. Revista andaluza de trabajo y bienestar social,* núm. 150, págs. 161-185 [en línea] https://www.juntadeandalucia.es/empleo/carl/carlportal-portlets/documentos?nombre=2b21c38c-9049-41d0-b85b-c5690438dc18.pdf [Fecha de consulta: 29 de septiembre de 2020].

NACIONES UNIDAS (s/f). *Programa de las Naciones Unidas para el Desarrollo. Objetivos de Desarrollo Sostenible* [en línea] https://www.un.org/sustainabledevelopment/es/economic-growth/ [Fecha de consulta: 29 de agosto de 2020].

RAMÓN FERNÁNDEZ, F. (2019). «La normativa de protección de datos y derechos digitales en el ámbito de los recursos humanos: un reto para la sociedad y la legislación». En: *¿Se puede crear capital social? Innovación y tecnología: retos para los recursos humanos de las organizaciones.* Valencia: Tirant lo Blanch, págs. 202-227.

REQUENA MONTES, O. (2020). «Derecho a la desconexión digital: un estudio de la negociación colectiva». *Lex social: revista de los derechos sociales*, vol. 10, núm. 2, págs. 541-560 [en línea] https://www.upo.es/revistas/index.php/lex_social/article/view/5076 [Fecha de consulta: 29 de septiembre de 2020].

SERVICIO INTEGRADO DE PREVENCIÓN Y SALUD LABORAL. UPV (2020). «Protocolo interno de actuación ante la activación de la alerta sanitaria por coronavirus SARS-COV-2. Escenario de "Nueva normalidad"» [en línea] https://www.sprl.upv.es/docs_interes/2020_05_22_PROTOCOLO%20ACTUACI%C3%93N%20UPV%20V3-2.pdf [Fecha de consulta: 29 de septiembre de 2020].

TORRES GARCÍA, B. (2020). «Sobre la regulación legal de la desconexión digital en España: valoración crítica». *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo,* vol. 8, núm. 1, págs. 239-261 [en línea] http://ejcls.adapt.it/index.php/rlde_adapt/article/view/837/1053 [Fecha de consulta: 29 de septiembre de 2020].

VALLECILLO GÁMEZ, Mª. R. (2020). «El derecho a la desconexión digital: perspectiva comparada y riesgos asociados». *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo,* vol. 8, núm. 1, págs. 210-238 [en línea] http://ejcls.adapt.it/index.php/rlde_adapt/article/view/836/1052 [Fecha de consulta: 29 de septiembre de 2020].

VICERRECTORADO DE ESTUDIOS, CALIDAD Y ACREDITACIÓN UPV (2020). «Instrucción del Vicerrectorado de Estudios, Calidad y Acreditación de la Universitat Politècnica de València, sobre medidas extraordinarias en coordinación con el vicerrectorado de alumnado, cultura y deporte y el vicerrectorado recursos digitales y documentación, para organizar la docencia y aprendizaje a distancia

frente a la suspensión de la docencia presencial por causa de la epidemia del virus COVID-19» [en línea] http://www.upv.es/noticias-upv/documentos/11933-recomendacionesdocenciaadistanciaUPV.pdf [Fecha de consulta: 29 de septiembre de 2020].

VIRTUAL UPV (2020) [en línea] https://virtual.blogs.upv.es/ [Fecha de consulta: 29 de septiembre de 2020].

Cita recomendada

RAMÓN FERNÁNDEZ, Francisca (2021). «La desconexión digital y docencia universitaria *online* en tiempos de pandemia por la COVID-19: una ilusión más que una realidad». *IDP. Revista de Derecho, Internet y Política*, núm. 32 (marzo). UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i32.373744

Sobre la autora

Francisca Ramón Fernández

frarafer@urb.upv.es

Francisca Ramón Fernández es Licenciada y Doctora en Derecho por la Universidad de Valencia, y en la actualidad profesora titular de Derecho Civil en la Universidad Politécnica de Valencia, donde desarrolla su actividad profesional. En materia de Derecho TIC ha sido investigadora principal y colaboradora de diversos proyectos competitivos nacionales, bajo la dirección del profesor Lorenzo Cotino Hueso, catedrático de Derecho Constitucional de la UV, y de los profesores Javier Plaza Penadés y Luz M. Martínez Velencoso, catedráticos de Derecho civil de la UV. La difusión de la actividad investigadora se ha realizado en distintas monografías publicadas por editoriales de reconocido prestigio, y en revistas de impacto, siendo reconocida su trayectoria con diversos premios de investigación.

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).

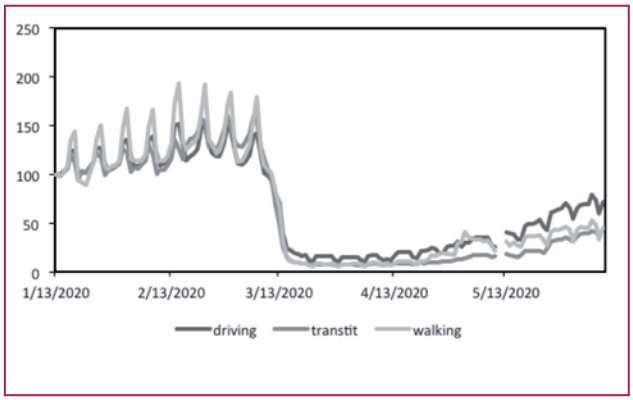

Gráfico 1. Gráfico de los porcentajes de cambios en la movilidad según el medio de transporte. Elaboración propia a partir de los datos ofrecidos por Apple.

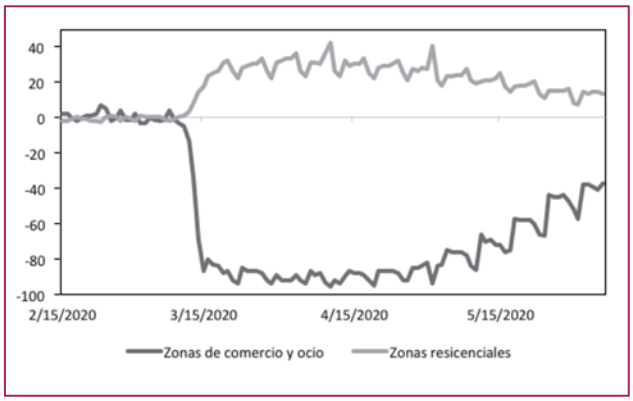

Gráfico 2. Porcentaje de cambios en la movilidad entre zonas de comercio y ocio y zonas residenciales. Elaboración propia a partir de los datos facilitados por Google.

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).

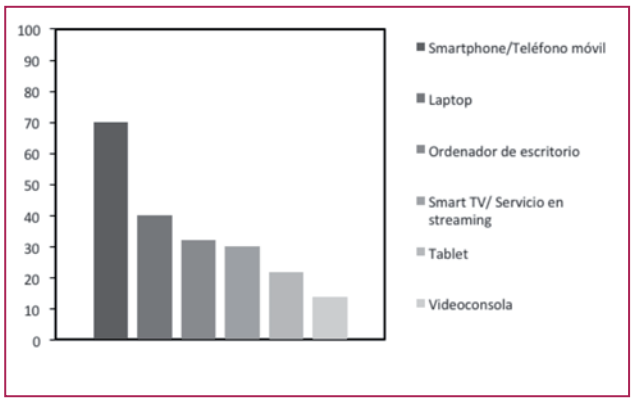

Gráfico 3. Proporción de encuestados que afirma hacer mayor uso de dispositivos conectados. Elaboración propia a partir de los datos ofrecidos por GlobalWebIndex (2020).

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).

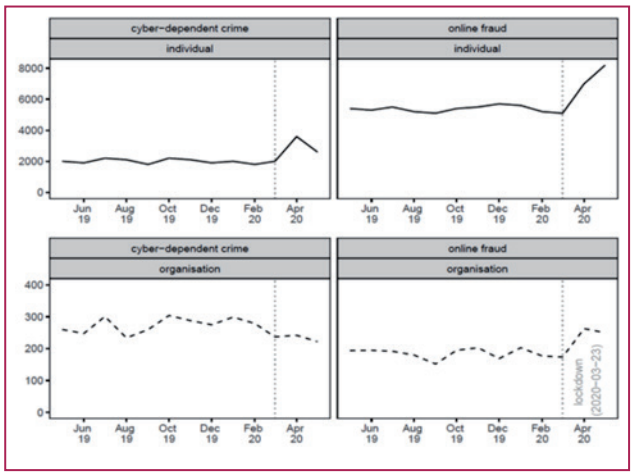

Gráfico 4. Número de delitos ciberdependientes y fraudes online conocidos por la policía de mayo de 2019 a mayo de 2020. Fuente: Buil-Gil, Miró Llinares, Moneva, Kemp y Díaz-Castaño (2020).

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).

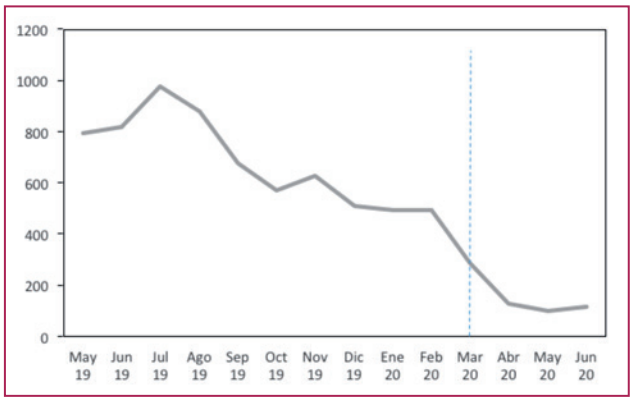

Gráfico 5. Número de delitos de fraude en entradas conocidos por la policía de mayo de 2019 a junio de 2020. Fuente: Auction Fraud. Elaboración propia.

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.

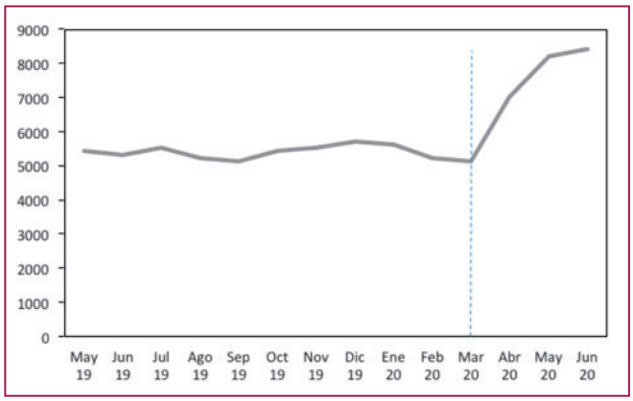

Gráfico 6. Número de delitos de fraude en compras y subastas online conocidos por la policía de mayo de 2019 a junio de 2020. Fuente: Auction Fraud. Elaboración propia.

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].

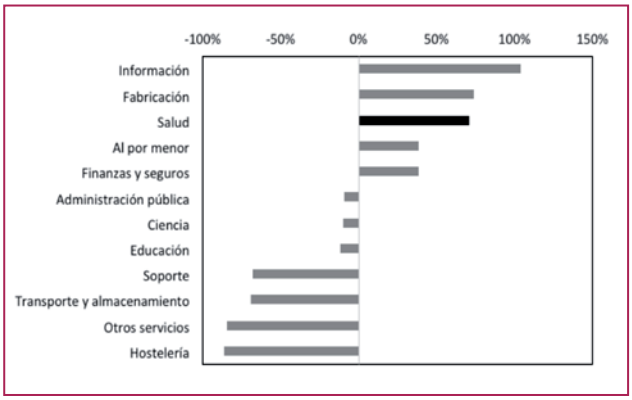

Gráfico 7. Cambios en el número de infracciones según el sector entre el primer trimestre de 2019 y el primer trimestre de 2020. Elaboración propia a partir de datos de AtlasVPN (2020).

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).

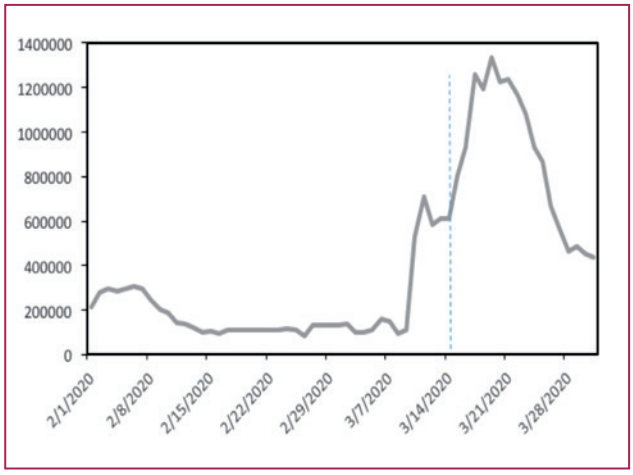

Gráfico 8. Número de ataques por fuerza bruta contra el protocolo de escritorio remoto conocidos por Kaspersky entre febrero y marzo de 2020. Elaboración propia a partir de los datos ofrecidos por Galov (2020).

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

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

https://idp.uoc.edu

ARTÍCULO

Abriendo ventanas virtuales en los muros de la prisión: reflexiones sobre la digitalización de las comunicaciones penitenciarias a propósito de la COVID-19

Cristina Güerri
Universidad de Málaga
Marta Martí
Universitat Oberta de Catalunya
Albert Pedrosa
Universitat Autònoma de Barcelona

Fecha de presentación: octubre de 2020
Fecha de aceptación: diciembre de 2020
Fecha de publicación: marzo de 2021

Resumen

La COVID-19 ha supuesto un reto para las prisiones de todo el mundo. Como en otros países, una de las medidas adoptadas en España fue suspender las visitas de familiares y otros allegados para prevenir el contagio en el interior de las prisiones. Esta medida ha evidenciado la falta de digitalización de las prisiones españolas, lo que ha sido un obstáculo a la hora de compensar la suspensión de las visitas con comunicaciones telemáticas. El objetivo de este artículo es reflexionar sobre el escaso nivel de digitalización de las prisiones españolas a propósito de la situación generada por la COVID-19. Para ello, partimos de la legislación penitenciaria en materia de comunicaciones, constatando que, actualmente, no existe una regulación adecuada que permita el uso de la tecnología para un contacto con el exterior más normalizado, siendo las visitas, las llamadas telefónicas y las cartas los únicos métodos disponibles. Posteriormente, repasamos las medidas adoptadas por la Administración penitenciaria española durante el estado de alarma causado por la pandemia, mostrando los obstáculos que han tenido las personas presas y sus familiares. A continuación, exponemos algunos de los argumentos que

explican la resistencia a la digitalización de la Administración penitenciaria, centrados principalmente en la cuestión de la seguridad. Por último, defendemos la digitalización de las prisiones, considerando que esta puede contribuir a la reinserción de las personas presas, a la humanidad de la pena y a la seguridad de los centros.

Palabras clave

prisiones, contacto con el exterior, COVID-19, digitalización, tecnología

Tema

Criminología, Derecho penitenciario

Opening virtual windows in the prison walls: Reflections on the digitalisation of prison communications in relation to COVID-19

Abstract

COVID-19's arrival has been a challenge for prisons around the world. As in other countries, one of the measures adopted in Spain was the cancellation of visits by relatives and other close friends to prevent the spread of the virus inside prisons. This measure has evidenced the lack of technology in Spanish prisons, as they have struggled to offer visits through telematic communications as compensation for the supervised visits. The main objective of this article is to reflect on the low level of technology in Spanish prisons regarding the situation generated by COVID-19. With this aim, we start by describing the prison legislation on communications, establishing that, nowadays, there is no adequate regulation that allows the use of technology for a more normalised contact with the outside, being visits, telephone calls, and letters the only methods available. Subsequently, we review the measures adopted by the Spanish prison administration during the state of alarm caused by the pandemic, showing the obstacles that prisoners and their families have faced. Next, we present some of the arguments that explain the resistance to digitisation exerted by the prison administration, mainly focused on the issue of security. Finally, we defend the adoption of new technology by prisons, considering that it can contribute to the reintegration of prisoners, increasing punishment's humanity, without becoming a risk to their safety.

Keywords

prisons, communication, COVID-19, digitalisation, technology

Topic

Criminology, Penitenciary law

Introducción

Entre febrero y marzo de 2020, la COVID-19 comenzó a percibirse como una amenaza sanitaria a nivel global y varios países implementaron medidas para prevenir la propagación del virus en los centros penitenciarios. Las enfermedades infecciosas son especialmente peligrosas en prisión porque problemáticas como la sobrepoblación, la falta de celdas individuales, los problemas de salud de muchas personas presas y la escasez de recursos médicos propician su transmisión (Penal Reform International, 2020)[1]. Por ello, una de las primeras medidas adoptadas en las prisiones de todo el mundo fue suspender las visitas de familiares y las salidas de las personas presas que disfrutaban de permisos, con el objetivo de reducir el contacto entre el exterior y el interior de las cárceles (Zevleva, 2020).

Esta limitación es particularmente sensible en el ámbito penitenciario, pues el contacto con el exterior favorece que la persona presa se sienta menos aislada e impide que sus vínculos sociales se rompan, favoreciendo su reinserción (Van Zyl y Snacken, 2013). En ocasiones esta restricción también repercute en la satisfacción de necesidades básicas como la alimentación o la higiene, ya que en algunos países los presos dependen de los bienes básicos que introducen las familias mediante las visitas (véase, por ejemplo, el caso mexicano en Pérez-Correa, 2015).

Para minimizar incidentes derivados de esta situación, y en coherencia con las recomendaciones internacionales[2], algunos países intentaron compensar la restricción de las visitas con otras medidas que incorporaran o ampliaran las comunicaciones telemáticas. Así, Bélgica, Finlandia, Lituania o el Reino Unido permitieron llamadas adicionales, mientras que otros, como Suecia, Croacia o Italia, implementaron el uso de medios telemáticos para realizar «videovisitas»[3].

La capacidad de adaptarse y responder a las necesidades de comunicación generadas por la COVID-19 ha dependido en gran parte del uso previo de los medios telemáticos en cada sistema penitenciario, pues mientras algunos países ya disponían de ellos, otros tuvieron que incorporarlos durante la contingencia sanitaria. Este último es el caso de España, donde se suspendieron las visitas y los permisos de salida, dejando las cartas y llamadas telefónicas prácticamente como las únicas vías de contacto entre los presos y sus familias. Así, la crisis generada por la COVID-19 ha evidenciado el insuficiente uso de las tecnologías de la comunicación en las prisiones españolas y obligado a la Administración a idear de forma improvisada sistemas de comunicación compensatorios como la introducción de móviles para hacer videollamadas (Rodríguez Yagüe, 2020; Solar y Lacal, 2020).

La literatura española muestra que, aunque hay margen de mejora, el uso de medios tecnológicos y digitales ha resultado útil para enriquecer la educación y potenciar las perspectivas de reinserción de las personas presas o facilitar la asistencia médica y las actuaciones judiciales en las prisiones (entre otros, Gutiérrez, Viedma y Callejo, 2010; Tocino, 2014; Contreras-Pulido, Martín-Pena, Aguedad-Gómez, 2015; Cantillo, Tena y Villegas, 2018; García-Molina, 2019). Sin embargo, los análisis relativos a la digitalización de las comunicaciones con familiares y propuestas concretas de mejora son escasos (Mapelli, 2013; Martín, 2014; Bares, 2020).

El presente artículo contribuye a este segundo grupo de trabajos y tiene el objetivo de reflexionar desde una perspectiva criminológica sobre la insuficiente digitalización de las prisiones a propósito de la situación generada por la COVID-19, poniendo especial énfasis en las vías de comunicación de las personas presas con sus allegados. Al respecto, entendemos por «digitalización» el proceso mediante el cual un sistema, en nuestro caso el penitenciario, pasa de usar instrumentos analógicos a usar la tecnología y las herramientas digitales.

Este trabajo se estructura de la siguiente manera: en primer lugar, se muestra cómo se encuentran reguladas las formas de contacto con el exterior en la Ley Orgánica General Penitenciaria (en adelante, LOGP) y el Reglamento Penitenciario (en adelante, RP), haciendo hincapié en

1. Algunas de estas condiciones también concurren en España (véase García-Guerrero y Marco, 2012).
2. Por ejemplo, OHCHR, 25/3/2020: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25745&LangID=E.
3. Véase EuroPris: COVID-19. Prevention measures in European prisons: https://www.europris.org/covid-19-prevention-measures-in-european-prisons/.

algunos de los problemas prácticos que la literatura ha destacado. En segundo lugar, se analizan las medidas tomadas en el sistema penitenciario español entre marzo y mayo de 2020 para hacer frente a la COVID-19, con base en la información oficial proporcionada por la Administración penitenciaria, la cual es complementada con fuentes periodísticas e informes de diversas entidades sociales[4]. Posteriormente, se reflexiona sobre las causas de la falta de digitalización en las prisiones españolas a partir de la revisión de los estudios que han tratado esta cuestión. En cuarto lugar, se presenta una experiencia internacional (el PrisonCloud, en Bélgica) como ejemplo de una posible forma de digitalización del sistema penitenciario. Como conclusión, se articulan varias propuestas que, a nuestro entender, podrían ayudar en el avance de la consolidación del uso de tecnologías digitales para la comunicación en las cárceles españolas.

1. El contacto con el exterior en las prisiones españolas durante la crisis de la COVID-19

1.1. Regulación legal del contacto con el exterior en el sistema penitenciario español

Las principales vías de contacto con el exterior recogidas en la LOGP son las salidas (art. 47.2), las comunicaciones orales (visitas) y escritas (art. 51.1) y las comunicaciones telefónicas (art. 51.4). El RP reconoce estas formas de relación con el exterior como un derecho de las personas presas (art. 4.2.e) y las considera, junto a los programas formativos y los programas psicosociales, uno de los tres elementos que conforman las actividades de tratamiento (art. 110.c).

Los permisos de salida y las visitas son los medios de contacto más importantes para las personas presas porque permiten la relación directa con familiares y allegados. Sin embargo, los primeros no se conceden hasta muy avanzada la condena (Rovira, Larrauri y Alarcón, 2018), por lo que en la práctica no sirven para mantener el contacto con el exterior, y los segundos presentan numerosos problemas por las condiciones del encarcelamiento en España, tales como la ubicación de los centros penitenciarios (alejados de los núcleos urbanos y mal comunicados), que convierte las visitas en algo muy costoso en términos de tiempo y dinero para las familias (OSPDH, 2006). La legislación reconoce estos inconvenientes y, por ello, aunque establece dos comunicaciones orales de veinte minutos a la semana, permite combinarlas en una única de cuarenta minutos, reduciendo la necesidad de desplazamiento (art. 42 RP). Sin embargo, esto también reduce la frecuencia del contacto, por lo que los medios de comunicación a distancia (cartas y telefonía) se vuelven especialmente importantes.

La comunicación epistolar no presenta restricciones en cuanto a su frecuencia (art. 46 RP), pero no es un medio de comunicación viable para muchas personas, puesto que alrededor del 10% de los presos son analfabetos (Gutiérrez, Viedma y Callejo, 2010). En cuanto a las llamadas telefónicas, el reglamento permite hasta cinco llamadas a la semana de cinco minutos (art. 47.5 RP), aunque en la práctica la propia Administración penitenciaria admite un número superior (SGIP, 2010). La limitación del número de llamadas y de su duración se debe a que las cabinas telefónicas disponibles son limitadas. Asimismo, el importe de la llamada debe ser satisfecho por la persona presa (art. 47.4 RP), algo que resulta problemático para las personas con escasos recursos y los extranjeros que desean llamar a su país de origen (OSPDH, 2006).

El avance de la tecnología ha dado lugar a nuevos medios de comunicación digitales, como la telefonía móvil e internet, que tendrían la capacidad de solventar, o como mínimo paliar, algunos de los problemas referidos. Por ejemplo, los móviles atenuarían la problemática del número de cabinas y dejarían de ser tan necesarias las restricciones en las llamadas; las videollamadas vía internet podrían ser más económicas y posibilitar un contacto más cercano al poder ver a la persona con quien se comunica; y el acceso a internet permitiría una correspondencia más rápida y directa, facilitando el flujo de información entre presos y allegados. No obstante, estos medios digitales apenas han

4. El artículo analizará las medidas adoptadas en el conjunto del Estado, haciendo alusión expresa cuando sea necesario a las adoptadas por la Administración catalana, que tiene competencias en materia penitenciaria.

sido incorporados al sistema de comunicaciones penitenciarias (Mapelli, 2013).

En cuanto a los teléfonos móviles, están totalmente prohibidos por razones de seguridad (Instrucciones 3/2010 SGIP y 3/2010 SMPRAV), excepto en los Centros Abiertos catalanes, donde se permiten móviles, aunque sin cámara ni internet (Instrucción 7/2006 SMPRAV).

Respecto a las comunicaciones por videoconferencia, estas sí han sido reguladas por la Administración penitenciaria central. La Instrucción 2/2007 contempla la posibilidad de emplear esta tecnología para la celebración de actuaciones judiciales, consultas médicas y comunicaciones con familiares, aunque su uso es habitual únicamente en los dos primeros supuestos (Martín, 2014; García-Molina, 2019; Montero y Nistal, 2020) y las videollamadas con familiares solo se contemplan en aquellos casos en los que exista «constancia fehaciente (...) de la imposibilidad de celebrar comunicaciones ordinarias por no residir la familia del interno en la misma localidad de ubicación del centro»[5]. Adicionalmente, la Instrucción 3/2019 autoriza las videoconferencias a los internos extranjeros cuyos familiares residen fuera de España, aunque lo considera una medida extraordinaria que debe ser autorizada por el Centro Directivo. Es decir, las videoconferencias con familiares se prevén para casos excepcionales y no son parte de la realidad penitenciaria de todos los presos[6].

1.2. La gestión del contacto con el exterior durante la crisis de la COVID-19

Las primeras medidas para hacer frente a la COVID-19 en las prisiones españolas se aplicaron el 14 de marzo de 2020, coincidiendo con la declaración del estado de alarma[7]. Estas consistieron en «la suspensión de todas las comunicaciones ordinarias de los internos en los centros penitenciarios»[8] y la cancelación de permisos y salidas programadas, dejando las llamadas telefónicas y las cartas como únicas vías de contacto con el exterior. Paralelamente, con el objetivo de paliar los efectos negativos de estas medidas, se dobló el número de llamadas que los presos podían realizar, las cuales además serían gratuitas para las personas sin recursos.

Adicionalmente, se adoptaron otras dos medidas compensatorias. En primer lugar, la SGIP suministró 205 móviles para que las personas presas pudieran realizar videollamadas de hasta diez minutos (controladas por funcionarios), y se promovió el acceso al Servicio de Orientación Jurídica por videoconferencia con representantes legales. No obstante, considerando que en España hay cerca de 50.000 personas presas, valoramos insuficiente el alcance de esta medida[9]. En segundo lugar, en Cataluña se aprobó un plan piloto en el CP Quatre Camins que, además de proporcionar televisores y llamadas gratuitas para personas sin recursos, creó una línea telefónica específica para atender y dar información a familiares de personas presas. Ambas medidas estuvieron activas hasta el inicio del desconfinamiento el 11 de mayo, cuando las comunicaciones se fueron restableciendo progresivamente[10].

En cuanto al impacto de la limitación de las comunicaciones, la Administración penitenciaria argumenta que no hubo ningún incidente de gravedad[11] y que las medidas adoptadas resultaron eficaces porque las tasas de contagios y mortalidad fueron menores que las de la población general[12].

5. Además, no se evita que los familiares deban desplazarse, pues esta instrucción establece que la videoconferencia debe realizarse desde otro centro penitenciario.
6. Adicionalmente debe mencionarse la existencia de un proyecto piloto que introduce la posibilidad de emplear las videoconferencias para poner en contacto a los abogados con los presos (Montero y Nistal, 2020), algo que había sido reclamado por autores como García-Molina (2019).
7. Esta sección se centra en describir las medidas adoptadas relacionadas con la comunicación con el exterior. Para una explicación detallada de todas las medidas, véanse Rodriguez Yagüe (2020) y Montero (2020).
8. SGIP, Orden INT/227/2020, 15/3/2020.
9. Según la SGIP, con estos móviles se realizaron 54.000 videollamadas como complemento a las que podían realizar los presos de forma regular, es decir, poco más de una llamada adicional por persona. Esto fue motivo de queja de los presos, tal y como recoge el Defensor del Pueblo (2020).
10. SGIP, Orden INT/407/2020, 12/5/2020.
11. SGIP, nota de prensa, 20/3/2020.
12. SGIP, nota de prensa, 13/5/2020. También Defensor del Pueblo (2020:180).

No obstante, varias entidades y colectivos discrepan de la versión oficial. En primer lugar, el anuncio repentino del cese de todas las comunicaciones cogió por sorpresa a presos y familiares. Esta medida se adoptó un viernes y, dado que los vis a vis y las visitas de ese fin de semana ya estaban autorizadas, muchos familiares conocieron la prohibición al llegar a los centros penitenciarios, ocasionando malestar y confusión. En segundo lugar, hubo numerosas quejas sobre la falta de medios para acceder a estas medidas compensatorias que dificultaron el acceso a las videollamadas, como la falta de infraestructura o los problemas con el audio y el vídeo, entre otros[13]. En tercer lugar, según varios reportes de prensa, en distintas prisiones se produjeron incidentes violentos como consecuencia de la tensión y el aislamiento derivados de estas restricciones, y los presos desarrollaron actos reivindicativos, como huelgas de hambre, para pedir mayor acceso a información y mecanismos de comunicación con el exterior[14].

Todo ello llevó a la emisión de un comunicado firmado por dieciséis entidades sociales y académicas reivindicando el respeto de los derechos de los presos y sus familias, la garantía de su seguridad y la de los profesionales, la provisión de más medios, y la aplicación efectiva de las recomendaciones internacionales para afrontar la pandemia en las prisiones[15].

Así, la Administración se ha centrado en la tasa de contagios como indicador para defender la efectividad (y necesidad) de las medidas adoptadas, lo que explica que su conclusión sea que, atendiendo a los datos oficiales, las medidas lograron cumplir sus objetivos. Sin embargo, este enfoque excluye otro tipo de afectaciones relacionadas con los derechos y el bienestar emocional de las personas presas y sus familias.

2. La digitalización de las prisiones y el contacto con el exterior

Las tecnologías de la información y la comunicación han avanzado notablemente en las dos últimas décadas y se han introducido mejoras en algunas prisiones, como experiencias con medios de comunicación y programas de alfabetización digital (Tocino, 2014; Contreras-Pulido, Martín-Pena y Aguedad-Gómez, 2015; Cantillo, Tena y Villegas, 2018); el acceso –aunque con limitaciones– a ordenadores e internet para quienes cursan educación universitaria a distancia (Gutiérrez, Viedma y Callejo, 2010; Fernández-Gómez, 2020), o la implementación de las videollamadas (Martín, 2014; Montero y Nistal, 2020). Sin embargo, como indicamos anteriormente, la implementación de estas últimas para el contacto con los familiares solo se admite para ciertos presos o en circunstancias muy concretas. Ello constata una evidente resistencia a la digitalización que se justifica, como es habitual en prisión, por razones de seguridad.

2.1. La actual resistencia a la digitalización de las comunicaciones

En prisión, la seguridad se invoca de manera excesivamente habitual para justificar la restricción del ejercicio de los derechos individuales. El «fantasma de la seguridad» (Goffman, 1961 [2012, pág. 94]), esto es, el temor a que las medidas de seguridad fallen y se produzcan motines o fugas, persigue constantemente al personal penitenciario. Por ello, no resulta sorprendente que un cambio tan grande como la digitalización de las prisiones genere resistencias.

Existen al menos tres argumentos relacionados con la seguridad por los cuales las Administraciones penitenciarias rechazan que los presos usen las tecnologías que permiten el contacto con el exterior. El primero es que posibilita que se dirijan actividades delictivas desde dentro de prisión, como aquellas relacionadas con la delincuencia organizada (por ejemplo, el narcotráfico) o de cuello blanco (Ma-

13. Por ejemplo, 20 Minutos, 17/4/2020: https://www.20minutos.es/noticia/4228339/0/familias-presos-carceles-catalanas-coronavirus-proteccion-comunicacion/
14. Por ejemplo, *Público*, 31/3/2020: https://www.publico.es/public/l-epidemia-les-presons-protestes-dels-interns-perque-falten-mesures-seguretat-i-dels-funcionaris-per-l-escas-material.html.
15. IRIDIA, 12/5/2020: https://iridia.cat/organitzacions-socials-sollicitem-a-la-secretaria-de-mesures-penals-rehabilitacio-i-atencio-a-la-victima-un-pla-de-desescalada-a-la-preso-que-garanteixi-el-compliment-dels-drets-humans/

pelli, 2013), o que se cometan ciberdelitos como el acoso o la distribución de pornografía infantil (Smith, 2012). Así, la prohibición de los medios digitales se justifica como una manera de prevenir delitos. Un ejemplo de cómo opera este argumento en España lo encontramos en la Instrucción 3/2010 de la SGIP, que prohíbe los móviles señalando que los internos podrían «eludir tanto el preceptivo control y registro de sus comunicaciones, como la intervención de las mismas», y que con ello podrían «mantener el contacto incontrolado con su entorno delincuencial, continuar con su actividad delictiva e incluso organizar desde el interior del Establecimiento la comisión de nuevos delitos».

En segundo lugar, la Administración considera que un «mal uso» de la libertad de expresión puede afectar tanto a la seguridad del centro penitenciario como al derecho a la intimidad de las personas presas, lo cual puede constituir un argumento que contribuye a la reticencia para introducir tecnologías. Sirva de ejemplo el caso de un preso a quien se denegó el derecho a comunicarse con un periodista por considerar la Administración penitenciaria que en su anterior comunicación con la prensa había vertido «manifestaciones falsas» sobre los profesionales de tratamiento con las que «desacreditó la actividad laboral de los mismos generando una actitud hostil y de confrontación hacia ellos tanto de internos como de sus familiares» y que tales declaraciones «podrían dar lugar a protestas que inciden negativamente en el buen orden interior y en la seguridad de los funcionarios, pudiendo alterarse la pacífica convivencia y rehabilitadora del conjunto de internos de este centro»[16]. Asimismo, la seguridad no es la única razón invocada para justificar el control de la información que sale del centro penitenciario, pues la dirección del centro señalaba en este caso que «el informado reveló datos procesales, penales y penitenciarios tanto personales como de otros internos, sin que conste autorización de los mismos, por lo que se vio afectado el derecho fundamental a la intimidad de estos internos». Bajo esta lógica, es comprensible que el libre uso de medios tecnológicos como el correo electrónico o las videollamadas puedan ser considerados por la Administración penitenciaria una amenaza a la seguridad del centro.

En esta línea, el tercer y último argumento consiste en que ciertas características de las tecnologías actuales, como la grabación de imagen y sonido de los teléfonos móviles, también pueden vulnerar, como en el caso de la información, la seguridad del centro penitenciario y de su personal y el derecho a la intimidad de las personas presas. De hecho, la Administración penitenciaria catalana justifica la limitación del uso de móviles con cámara en los centros abiertos con base en que «la disposición libre de los móviles actuales puede menoscabar la seguridad de un centro penitenciario por el hecho de que se pueden hacer fotografías y grabaciones del recinto, las dependencias y el personal» (Instrucción 7/2006, SMPRAV) y ello representa un riesgo para los espacios de seguridad del establecimiento (Mapelli, 2013). Por otra parte, la filtración de fotografías y un vídeo de algunos «presos del *procés*» dentro de prisión muestra cómo este tipo de tecnologías pueden facilitar la vulneración del derecho a la intimidad y la imagen de las personas presas.[17]

Si bien esta resistencia a la digitalización es, hasta cierto punto, comprensible, algunos de los argumentos de seguridad empleados para justificarla resultan cuestionables. Por ejemplo, como apunta Mapelli (2013), la prohibición total de los móviles para prevenir la comisión de delitos pierde fuerza si consideramos que actualmente, como la propia Instrucción 3/2010 reconoce, «ya hay móviles», introducidos de forma clandestina, en los centros penitenciarios. Esto significa que se están restringiendo los derechos de todos los presos sin alcanzar el objetivo de impedir conversaciones no controladas. Asimismo, el propio Tribunal Constitucional (STC 6/2020, de 27 de enero) señala en relación con el derecho a comunicar libremente información desde prisión que «la apelación a un interés general como es el buen orden y la seguridad del establecimiento penitenciario no puede, por sí sola, legitimar una medida limitativa de derechos» y que «para que la limitación de derechos sea constitucionalmente admisible es precisa la existencia de motivos específicos que justifiquen, en el caso concreto, que el interés general se hallaba en peligro».

En este sentido, creemos que existen razones que justifican la conveniencia de avanzar hacia la digitalización bajo

16. Informe remitido por el CP Córdoba al Juzgado de Vigilancia Penitenciaria núm. 8 de Andalucía en relación con el Acuerdo de Dirección de 25/1/2017.
17. *20 Minutos*, 7/6/2018: https://www.20minutos.es/noticia/3361521/0/primeras-imagenes-junqueras-romeva-forn-carcel/.

la supervisión y control de la Administración penitenciaria, sin perjuicio de que los medios digitales puedan restringirse en casos concretos donde tal acceso posibilitaría continuar con la actividad delictiva (por ejemplo, en delitos de crimen organizado o acoso) o atentar contra la seguridad del establecimiento, algo que ya prevé la legislación actual para las comunicaciones orales y escritas (art. 51 LOGP).

2.2. Argumentos para avanzar hacia la digitalización

A pesar de la resistencia actual, existen numerosos argumentos para avanzar hacia la digitalización de las prisiones, los cuales exponemos a continuación:

- Reinserción

El primer argumento en favor de la digitalización es que esta favorece la reinserción social, fin primordial del sistema penitenciario español. El propio Tribunal Constitucional señala que el derecho a las comunicaciones «tiene una incidencia sustancial en el desarrollo de la personalidad de los internos y adquiere por ello suma relevancia en orden al cumplimiento de la finalidad, no exclusiva, de reinserción social (...). Mediante la comunicación oral y escrita con otros sujetos, el preso no queda reducido exclusivamente al mundo carcelario y ello le permite relacionarse con el exterior y, en definitiva, mantenerse preparado para su futura vida en el seno de la sociedad» (STC 175/1997, de 27 de octubre, FJ2). En efecto, la literatura criminológica en nuestro contexto muestra que las relaciones familiares son un elemento fundamental para la reinserción de las personas presas (Ibàñez y Pedrosa, 2018), por lo que las comunicaciones resultan esenciales en la medida que pueden evitar que estas se debiliten o se rompan.

Por otro lado, la digitalización aumenta las oportunidades laborales, tanto dentro de prisión, permitiendo que se puedan realizar trabajos a distancia (Robberechts y Beyens, 2020), como fuera de la misma, al ampliar las posibilidades de formación mientras se cumple la condena, evitando que la persona «pierda» la conexión con el mundo de las comunicaciones tecnológicas (Contreras-Pulido, Martín-Pena y Aguedad-Gómez, 2015; Hopkins y Farley, 2015). Así, diversas investigaciones prueban que las personas con una larga trayectoria penitenciaria tienen mayores dificultades para adaptarse a las nuevas tecnologías (Lynch y Sabol, 2001). Por ejemplo, cuando los presos de larga duración progresan a régimen abierto, su falta de contacto con medios tecnológicos deviene un problema para realizar algunas tareas cotidianas, y los equipos técnicos deben trabajar competencias, como la utilización de un móvil con internet, para que la persona pueda «ponerse al día» (Martí, 2019). Es decir, el uso de la tecnología en prisión refuerza la autonomía de las personas presas y su autoestima (Contreras-Pulido, Martín-Pena y Aguedad-Gómez, 2015; McDougall, Pearson, Torgerson y García-Reyes, 2017; Robberechts y Beyens, 2020), reduciendo la «prisionización» y facilitando su retorno a la sociedad.

- Humanidad

En segundo lugar, la digitalización contribuye a la humanización de la vida en prisión al potenciar y normalizar el contacto de los presos con el exterior (Smith, 2012; Engbo, 2017; Robberechts y Beyens, 2020). Las videollamadas, por ejemplo, proporcionan mayor cercanía que una llamada telefónica y pueden ser más económicas. Esta opción resulta especialmente necesaria en las prisiones españolas, con un 28,1% de presos extranjeros[18], quienes suelen recibir menos visitas, bien por la lejanía de sus familias, bien porque sus allegados no pueden acreditar su vinculación con ellos si se encuentran en situación de irregularidad administrativa (Rodríguez Yagüe, 2012; Bares, 2020).

Adicionalmente, consideramos que las videollamadas son particularmente recomendables desde una perspectiva de género (en el mismo sentido, Bares, 2020), ya que las mujeres presas reciben menos visitas que los hombres por la mayor dispersión territorial que sufren y experimentan más dependencia afectiva y sentimientos de soledad porque suelen desarrollar vínculos más fuertes con sus familias, especialmente con los hijos (Almeda, 2005).

Por otra parte, la digitalización favorece la humanización de las prisiones al permitir un mayor acceso a la información, lo cual conlleva un menor sufrimiento para los presos y sus familias (Ibàñez y Pedrosa, 2018). De hecho, una de

18. Portal Estadístico SGIP (enero de 2020).

las recomendaciones internacionales en el pico de la pandemia de COVID-19 fue dar información suficiente y comprensible para evitar rumores y la expansión del temor en las prisiones (Coyle, 2020).

Por ello, defendemos que las videollamadas hubieran ayudado especialmente durante el confinamiento. Por ejemplo, una de las cuestiones que generó mayor ansiedad en las personas presas fue la preocupación sobre cómo el virus estaba afectando a sus familiares; y a la inversa, las familias experimentaron estrés por la dificultad de saber cómo estaban sus familiares presos (Prison Reform Trust, 2020). En este sentido, mientras en la población general las videollamadas fueron una de las vías de escape más importantes durante el confinamiento, muchos presos no pudieron reemplazar las visitas familiares con otro tipo de contacto que les permitiera ver a sus allegados de forma virtual, algo que afecta en especial a quienes tienen hijos pequeños.

Finalmente, destacamos que la libertad de comunicación de los presos con el exterior favorece la transparencia de las prisiones, lo cual, a su vez, favorece el respeto de los derechos humanos. A estos efectos, Van Zyl y Snacken (2013, págs. 328-330) señalan que el contacto con el exterior es una condición necesaria para prevenir la tortura y los tratos inhumanos o degradantes. Así, la digitalización sería una herramienta que nos permitiría avanzar en esta dirección.

- Seguridad

El tercer argumento en favor de la digitalización tiene que ver con la seguridad. Ya hemos señalado que la prohibición de móviles y otros medios tecnológicos se basa en razones de seguridad: sirve para prevenir delitos, evitar riesgos para la seguridad del centro y el personal, y proteger el derecho a la intimidad de los presos. Sin embargo, consideramos que ninguno de ellos justifica la negativa generalizada a la digitalización (posición también sostenida por Bares, 2020). Por ejemplo, es comprensible que a una persona condenada por pornografía infantil se le restrinja el acceso a internet por cuestiones de prevención, pero ello no justifica que no pueda realizar videollamadas con sus familiares. Asimismo, cuesta comprender que todos los establecimientos y tipos de módulo, independientemente de su régimen de vida, tengan las mismas normas sobre el acceso a las tecnologías[19].

En este sentido, argumentamos que la digitalización es posible en términos de seguridad porque, en primer lugar, hay distintos tipos de comunicaciones digitales, y estas pueden incorporarse y adaptarse según las características y necesidades de las prisiones, por ejemplo, permitiendo los móviles sin cámara. En segundo lugar, si es necesario, puede limitarse quién tiene acceso a determinados medios, por ejemplo, limitando ciertas herramientas en módulos conflictivos o a aquellas personas que tienen las comunicaciones restringidas.

Adicionalmente, consideramos dos motivos por los que una digitalización promovida por la Administración penitenciaria favorecería el orden en las prisiones:

Primero, resulta evidente que la actual prohibición no es efectiva, pues ya hay móviles clandestinos en prisión, y ello ocasiona problemas que podrían evitarse con una buena regulación de la tenencia de estos dispositivos. La clandestinidad de los móviles permite una economía informal entre presos que origina conflictos por deudas, y la detección y retirada de los móviles conlleva sanciones que dificultan la progresión de los presos y empeoran su relación con el personal penitenciario. Asimismo, quienes ya poseen móviles son probablemente quienes hacen un uso delictivo de los mismos, por lo que el riesgo añadido si se permite su uso puede suponerse no muy elevado (Mapelli, 2013).

Así, la introducción de los móviles por parte de la Administración reduciría la conflictividad y las sanciones, mejorando la convivencia y el buen orden sin comprometer la seguridad[20]. Por otra parte, también existen iniciativas seguras más allá de los móviles, como habilitar espacios para videollamadas (algo que comienza a verse en las prisiones españolas a raíz de la COVID-19), permitir el uso de ordenadores para enviar correos electrónicos (como en Finlandia, según indican Lindström y Puolakka, 2020) o acondicionar zonas de la prisión que funcionan a través de una red de comunicación interna (como en Bélgica, véase apartado 3).

19. La única excepción son los centros abiertos catalanes.
20. Véase McDougall, Pearson, Torgerson y García-Reyes (2017) sobre el caso británico.

El segundo motivo por el que consideramos que la digitalización sería positiva para el buen orden en prisión procede de la experiencia vivida con la COVID-19. Anteriormente, hemos mostrado que durante el confinamiento la falta de contacto entre presos y familiares generó tensión e incidentes en las prisiones. La necesaria restricción de movimientos para evitar la propagación del virus y las limitadas infraestructuras obligaron a las Administraciones a actuar precipitadamente reduciendo a mínimos la comunicación con el exterior.

En efecto, es ilustrativo que cuando la crisis sanitaria estalló en Italia, la prohibición de las visitas familiares originó una veintena de motines que se saldaron con once muertes[21] y en diversos países de Latinoamérica hubo motines, fugas masivas y huelgas de hambre causadas por la deficiente gestión de las Administraciones penitenciarias[22] y la falta de «información veraz y oportuna».[23] Es decir, permitir el contacto con el exterior no solo constituye una cuestión de humanidad sino que también contribuye a la prevención de incidentes.

En definitiva, consideramos que existen buenos argumentos de resocialización, humanidad y seguridad para digitalizar las prisiones y, como veremos, la experiencia de otros países demuestra que una digitalización penitenciaria segura es posible.

3. Más allá de la alfabetización digital y las videollamadas: Smart Prisons en el contexto internacional

En el contexto comparado, la mayoría de prisiones limitan el uso de las tecnologías de la comunicación a los presos que realizan determinados estudios (Smith, 2012). No obstante, podemos encontrar iniciativas que incorporan estas tecnologías en los centros penitenciarios de forma más amplia, como la plataforma PrisonCloud, introducida en algunas prisiones belgas en 2014 (Robberechts y Beyens, 2020). PrisonCloud es una plataforma digital que ofrece una red de comunicación en varios espacios de la prisión, como las celdas y la biblioteca, y proporciona numerosas posibilidades[24].

En primer lugar, favorece el buen funcionamiento de la prisión, pues sirve como canal de información a través del cual los presos pueden encontrar legislación relevante, consultar las normas internas del centro penitenciario, el catálogo de la biblioteca o el menú diario. Así, el personal puede enviar mensajes a través de esta aplicación anunciando cambios en las normas o nuevas actividades, mejorando la comunicación interior. Además, los presos pueden hacer llamadas y enviar mensajes directos desde sus celdas a los servicios internos de la cárcel (por ejemplo, para concretar una cita con el servicio médico) sin el control de intermediarios.

En segundo lugar, PrisonCloud contribuye a la normalización ofreciendo posibilidades de ocio (por ejemplo, películas y juegos) y de autoorganización (despertador, calendario o conexión con servicios de la cárcel como la cantina) con el objetivo de incentivar la responsabilidad de los presos en sus rutinas diarias. Asimismo, PrisonCloud facilita la comunicación con el exterior, permitiendo que las personas presas llamen desde sus celdas sin necesidad de utilizar los teléfonos ubicados en las zonas comunes, lo que les ofrece mayor privacidad.

En tercer lugar, esta plataforma proporciona acceso a cursos de formación y a trabajos remunerados. Así, desde 2017, algunos presos trabajan como operadores de atención al cliente desde sus celdas. Este ejemplo evidencia que, efectivamente, la digitalización de las prisiones puede favorecer la reinserción y mejorar la situación económica de las personas presas al ampliar sus posibilidades de trabajo.

En términos globales, la incorporación de PrisonCloud es valorada positivamente porque empodera a los presos,

21. EFE, 10/3/2020: https://www.efe.com/efe/espana/portada/once-presos-muertos-en-italia-por-los-motines-a-causa-del-coronavirus/10010-4192577. Posteriormente, Italia ha sido uno de los países europeos que mayores esfuerzos ha realizado en introducir medidas compensatorias a la restricción de las visitas (véase Ciavarella, 2020),
22. *Dalby*, 24/3/2020: https://es.insightcrime.org/noticias/analisis/coronavirus-desnuda-crisis-carcelaria-en-latinoamerica/.
23. *Forbes*, 24/5/2020: https://www.forbes.com.mx/actualidad-el-covid-19-un-peligro-mas-para-la-salud-de-los-presos-mexicanos/.
24. La explicación sobre PrisonCloud se basa en el trabajo de Robberechts y Beyens (2020).

los hace más independientes y reduce la distancia con el exterior sin comprometer el buen funcionamiento de los establecimientos penitenciarios, motivo por el cual otros países lo han usado como ejemplo (véase el proyecto finlandés Smart Prison, analizado por Lindström y Puolakka [2020]).

Conclusiones e implicaciones

En el momento de escribir estas líneas, la crisis generada por la COVID-19 aún sigue lejos de desaparecer. Con nuevos rebrotes y el aumento de casos, se han vuelto a restringir las visitas en la mayoría de prisiones españolas[25]. Ante esta situación, el uso de móviles se ha mantenido en las prisiones catalanas y la SGIP ha anunciado la instalación de cabinas para la realización de videollamadas en todas las prisiones del Estado a lo largo de 2021 con el fin de «regular su uso para que permanezcan como fórmula para las comunicaciones de las personas privadas de libertad»[26]. No obstante, hasta el momento, estas solo se han instalado en cuatro centros y el servicio será de pago, si bien se introduce la posibilidad de cobro revertido[27]. Por lo tanto, podemos afirmar que poco ha cambiado en estos meses para minimizar el impacto de una nueva restricción de las comunicaciones.

En este artículo hemos expuesto que la limitación de las comunicaciones durante el estado de alarma comportó problemas en el ámbito de la seguridad y el bienestar de las personas presas y sus familias al afectar el derecho al contacto con el exterior. Sin embargo, dicha problemática no es atribuible únicamente a las circunstancias derivadas de la pandemia, pues estas solo han acentuado un problema estructural preexistente del sistema penitenciario: la falta de digitalización e infraestructuras de comunicación telemática.

A pesar de los avances tecnológicos, las prisiones españolas siguen ancladas en la era analógica, y los medios de comunicación digitales son escasos. La resistencia de la Administración penitenciaria a la digitalización se basa en razones de seguridad, pues considera que esta limitación previene delitos, mantiene la seguridad del centro y el personal penitenciario y protege el derecho a la intimidad de los presos. Sin embargo, argumentamos que ninguna de ellas justifica la negativa generalizada a la digitalización, pues existen distintos tipos de comunicaciones digitales, y estas pueden incorporarse y adaptarse según las necesidades de cada prisión. Adicionalmente, sostenemos que existen buenas razones, de reinserción y de humanidad, pero también de seguridad, para digitalizar las prisiones españolas.

El contexto internacional ofrece ejemplos exitosos de digitalización penitenciaria (entre otros, el programa PrisonCloud implementado en Bélgica) y la situación derivada de la COVID-19 ha demostrado que en las prisiones españolas también se puede hacer un mayor uso de estas tecnologías sin que ello amenace la seguridad (Rodríguez Yagüe, 2020; Solar y Lacal, 2020). Por ello, proponemos:

- A corto plazo, dotar de más recursos tecnológicos para afrontar las posibles nuevas limitaciones provocadas por la COVID-19 proveyendo de más móviles y fomentando las videollamadas.
- Actualizar la regulación de las videollamadas para que dejen de ser una medida excepcional.
- Regular el uso de móviles e internet en prisión, adaptándose a la tecnología actual y permitiendo un contacto normalizado con el exterior. Por la importancia de los derechos afectados, esta regulación debería incorporarse en la LOGP y desarrollarse en el RP, y no mediante instrucciones como hasta ahora.
- La nueva regulación debe contemplar las necesidades específicas de los colectivos vulnerables, como las personas sin recursos, las personas extranjeras o las mujeres (también Bares, 2020).

25. Departament de Justícia, nota de prensa, 21/7/2020. SGIP, nota de prensa, 14/9/2020.
26. SGIP, nota de prensa, 21/5/2020.
27. SGIP, nota de prensa, 14/12/2020

- Proveer a todas las prisiones de los recursos e infraestructuras necesarios para la implementación efectiva de esta nueva regulación.

- Garantizar un uso seguro de los dispositivos tecnológicos mediante sistemas e infraestructuras como, por ejemplo, la creación de listas de contactos autorizados para las videollamadas o listas seguras de navegación por internet mediante un *firewall* (véase Lindström y Puolakka, 2020).

- La experiencia belga recomienda que la digitalización comience por pequeños proyectos basados en un análisis de necesidades y riesgos (Knight y Van de Steene, 2017). En este sentido, proponemos empezar por las prisiones abiertas y áreas de menor riesgo como los módulos de respeto (también Mapelli, 2013).

En definitiva, en nuestra sociedad los avances tecnológicos deben estar al servicio de las personas, mejorando su calidad de vida, y las personas presas no pueden ser una excepción. Esperamos que la introducción de tecnologías digitales durante la crisis provocada por la COVID-19 no se quede en una anécdota de pandemia y sea el punto de inflexión que permita abrir ventanas virtuales en los muros de las prisiones.

Referencias bibliográficas

ALMEDA, E. (2005). «Women's imprisonment in Spain». *Punishment & Society*, vol. 7, núm. 2, págs.183-199 [en línea] DOI: https://doi.org/10.1177/1462474505050442 [Fecha de consulta: 8 de enero de 2021].

BARES, M. (2020). «Internet en prisión. Los derechos digitales de las personas privadas de libertad». *Revista Digital Nuevas Tecnologías,* núm. 24. SP/DOCT/104223.

CANTILLO, P.; TENA, R.; VILLEGAS, G. (2018). «La alfabetización digital como instrumento de inclusión social en prisión». En: CARRERA FARRAN, F. X. *et al.* (eds.). *EDUcación con TECnología: un compromiso social*. Lleida: Universitat de Lleida, pp. 1.517-1.523 [en línea] https://repositori.udl.cat/handle/10459.1/64975 [Fecha de consulta: 8 de enero de 2021].

CIAVARELLA, C. (2020). «Impact of Covid-19 on the use of technology during and after the crisis. An Italian experience». EuroPris «ICT in prisons», 29-30 de septiembre.

CONTRERAS-PULIDO, P.; MARTÍN-PENA, D.; AGUEDAD-GÓMEZ, J. I. (2015). «Derribando el autoestigma: medios de comunicación en prisiones como aliados de la inclusión social». *Cuadernos.Info*, núm. 36, págs. 15-26 [en línea] DOI: https://doi.org/10.7764/cdi.36.708 [Fecha de consulta: 8 de enero de 2021].

COYLE, A. (2020). «Introducción y valoración general del tema». Mesa Internacional de Seguimiento al Coronavirus en las Prisiones (23 de marzo). Aula Penitenciaria Latinoamericana [en línea] https://www.prisonstudies.org [Fecha de consulta: 8 de enero de 2021].

DEFENSOR DEL PUEBLO (2020). *Actuaciones ante la pandemia de COVID-19*. [en línea] https://www.defensordelpueblo.es/wp-content/uploads/2020/12/Documento_COVID-19.pdf [Fecha de consulta: 15 de diciembre de 2020].

ENGBO, H. (2017). «Normalisation in nordic prisons from a prison governor's perspective». En: SMITH, P.; UGELVIK, T. (eds.). *Scandinavian penal history, culture and prison practice*. Palgrave Macmillan, págs. 327-352.

FERNÁNDEZ-GÓMEZ, C. (2020). «Technological developments on education of inmates in Spanish prisons». EuroPris «ICT in prisons», 29-30 de septiembre.

GARCÍA-GUERRERO, J.; MARCO, A. (2012). «Sobreocupación en los Centros Penitenciarios y su impacto en la salud». *Revista Española de Sanidad Penitenciaria*, vol. 14, núm. 3, págs. 106-113 [en línea] DOI: https://doi.org/10.4321/S1575-06202012000300006 [Fecha de consulta: 8 de enero de 2021].

GARCÍA-MOLINA, P. (2019). «Las comunicaciones por videoconferencia de los internos con el abogado defensor». *Revista Brasileira Direito Processual Penal*, vol. 5, núm. 3, págs. 1.219-1.254 [en línea] DOI: https://doi.org/10.22197/rbdpp.v5i3.255 [Fecha de consulta: 8 de enero de 2021].

GOFFMAN, E. (1961[2012]). *Internados: Ensayos sobre la situación social de los enfermos mentales*. Buenos Aires: Amorrutu.

GUTIÉRREZ, J.; VIEDMA, A.; CALLEJO, J. (2010). «Estudios superiores en la educación penitenciaria española: un análisis empírico a partir de los actores». *Revista de Educación*, núm. 353, págs. 443-468.

HOPKINS, S.; FARLEY, H. (2015). «E-learning incarcerated: prison education and digital inclusion». *International Journal of Humanities Education*, vol. 13, núm. 2, págs. 37-45.

IBÀÑEZ, A.; PEDROSA, A. (2018). *El papel de las familias en la reinserción de las personas que salen de prisión*. Barcelona: Centre d'Estudis Jurídics i Formació Especialitzada [en línea] https://ddd.uab.cat/pub/worpap/2018/191957/paperFamiliesReinsercio_SPA.pdf [Fecha de consulta: 8 de enero de 2021].

KNIGHT, V.; VAN DE STEENE, S. (2017). «Digitizing the prison». *Prison Service Journal*, núm. 231, págs. 22-30.

LINDSTRÖM, B.; PUOLAKKA, P. (2020). *Smart Prison: the preliminary development process of digital self-services in Finnish prisons*. ICPA [en línea] https://icpa.org/ [Fecha de consulta: 8 de enero de 2021].

LYNCH, J.; SABOL, W. (2001). «Prisoner reentry in perspective». *Crimen Policy Report*, vol. 3. Urban Institute [en línea] http://webarchive.urban.org/UploadedPDF/410213_reentry.PDF [Fecha de consulta: 8 de enero de 2021].

MAPELLI, B. (2013). «¿Pueden los privados de libertad usar móviles para comunicarse?». *Anales de Derecho*, vol. 31, págs. 1-18.

MARTÍ, M. (2019). «Prisiones abiertas: la supervisión de la pena en semilibertad». *RECPC*, vol. 21, núm. 7, págs. 1-26.

MARTÍN, F. (2014). «La utilización del sistema de videoconferencia en el marco de instituciones penitenciarias». En: MATA Y MARTÍN, R. (dir.); JAVATO MARTÍN, A. M. (coord.). *Sistema penitenciario y nuevas tecnologías*. Valladolid: Lex Artis, págs. 45-62.

McDOUGALL, C.; PEARSON, D.; TORGERSON, D.; GARCÍA-REYES, M. (2017). «The effect of digital technology on prisoner behaviour and reoffending». *J.Exp.Criminol.,* vol. 13, núm. 4, págs. 455-482 [en línea] DOI: https://doi.org/10.1007/s11292-017-9303-5 [Fecha de consulta: 8 de enero de 2021].

MONTERO PÉREZ, E. (2020). «Telematic control and semi-freedom as a response to the pandemic: the Spanish penitentiary system experience. *Victims & Offenders*, págs. 1-17 [en línea] DOI: https://doi.org/10.1080/15564886.2020.1819496 [Fecha de consulta: 8 de enero de 2021].

MONTERO PÉREZ, E.; NISTAL BURÓN, J. (2020). «The use of new technologies in the execution of prison sentences in Spain: latest developments». EuroPris «ICT in prisons», 29-30 de septiembre.

OSPDH (2006). *La cárcel en el entorno familiar. Estudio de las repercusiones del encarcelamiento sobre las familias*. Barcelona: Universitat de Barcelona [en línea] https://www.academia.edu/1085273/La_c%C3%A1rcel_en_el_entorno_familiar_Estudio_de_las_repercusiones_del_encarcelamiento_sobre_las_familias_problem%C3%A1ticas_y_necesidades [Fecha de consulta: 8 de enero de 2021].

PENAL REFORM INTERNATIONAL (2020). *Coronavirus: Healthcare and human rights of people in prison* [en línea] https://cdn.penalreform.org/ [Fecha de consulta: 8 de enero de 2021].

PÉREZ-CORREA, C. (2015). *Las mujeres invisibles. Los costos de la prisión y los efectos indirectos en las mujeres*. BID [en línea] https://publications.iadb.org/es/publicacion/15473/las-mujeres-invisibles-los-costos-de-la-prision-y-los-efectos-indirectos-en-las [Fecha de consulta: 8 de enero de 2021].

PRISON REFORM TRUST (2020). Covid-19 Action Prisons Project: tracking innovation valuing experience. *Prison Reform Trust* [en línea] http://www.prisonreformtrust.org.uk/ [Fecha de consulta: 8 de enero de 2021].

ROBBERECHTS, J.; BEYENS, K. (2020). «PrisonCloud: The beating heart of the digital prison cell». En: TURNER, J.; KNIGHT, V. (eds.). *The Prison Cell*. Palgrave Macmillan, págs. 283-303 [en línea] DOI: https://doi.org/10.1007/978-3-030-39911-5_13 [Fecha de consulta: 8 de enero de 2021].

RODRÍGUEZ YAGÜE, C. (2012). «El modelo político-criminal español frente a la delincuencia de inmigrantes». *RECPC,* vol. 1, núm. 7, págs. 1-42.

RODRÍGUEZ YAGÜE, C. (2020). «COVID-19 y prisiones: un desafío no sólo sanitario y de seguridad, también humanitario». *Revista General de Derecho Penal*, núm. 33.

ROVIRA, M.; LARRAURI, E.; ALARCÓN, P. (2018). «La concesión de permisos penitenciarios». *RECPC*, núm. 20, vol. 2, págs. 1-26.

SGIP (2010). *La prisión paso a paso*. Madrid: Secretaría General de Instituciones Penitenciarias [en línea] https://www.iipp.es/documents/20126/0/Paso_a_Paso_en_castellano.pdf/183c67dd-8dea-c060-b23a-39b07d320dba [Fecha de consulta: 8 de enero de 2021].

SMITH, P. (2012). «Imprisonment and Internet-Access». *Nordic Journal of Human Rights*, vol. 30, núm. 4, págs. 454-482.

SOLAR, P.; LACAL, P. (2020). «Lo que el COVID 19 ha venido a enseñarnos. Propuestas penitenciarias para un futuro inmediato». *Revista General de Derecho Penal*, vol. 33, núm. 1.

TOCINO, C. (2014). «Internet en la cárcel». En: MATA Y MARTÍN, R. (dir.); JAVATO MARTÍN, A. M. (coord.). *Sistema penitenciario y nuevas tecnologías*. Valladolid: Lex Artis, págs. 29-44.

VAN ZYL, D.; SNACKEN, S. (2013). *Principios de derecho y política penitenciaria europea: penología y derechos humanos*. Valencia: Tirant lo Blanch.

ZEVLEVA, O. (2020). «Coronavirus in prisons, a global perspective: tracking policy responses, releases, and riots». *Gulag Echoes* [en línea] https://blogs.helsinki.fi/gulagechoes/2020/04/01/coronavirus-in-prisons-a-global-perspective-tracking-policy-responses-releases-and-riots/ [Fecha de consulta: 8 de enero de 2021].

Cita recomendada

GÜERRI, Cristina; MARTÍ, Marta; PEDROSA, Albert (2021). «Abriendo ventanas virtuales en los muros de la prisión: reflexiones sobre la digitalización de las comunicaciones penitenciarias a propósito de la COVID-19». *IDP. Revista de Internet, Derecho y Política*, núm. 32 (marzo). UOC [Fecha de consulta: dd/mm/aa]. http://dx.doi.org/10.7238/idp.v0i32.375209

Sobre los autores

Cristina Güerri
cristina.guerri@uma.es
Universidad de Málaga

Doctora en Derecho (Criminología) por la Universitat Pompeu Fabra (Barcelona). Es investigadora posdoctoral Juan de la Cierva-Formación en el Instituto Andaluz Interuniversitario de Criminología de la Universidad de Málaga (2020-2022) y colaboradora del Grupo de Investigación UPF en Criminología y Sistema Penal. Su actividad investigadora, se ha centrado en el sistema penitenciario y explora cuestiones diversas como la percepción de las personas presas de su calidad de vida en prisión, la visión de los funcionarios de interior de su trabajo y su rol en la institución penitenciaria o la situación de las personas extranjeras presas. Entre sus méritos destacan haber sido Europaeum Scholar (2018-2019), la obtención de una Ayuda de Formación del Profesorado Universitario 2014 (FPU, Ministerio de Educación) y el Premio Nacional Fin de Carrera de Educación Universitaria 2013-2014 (Ministerio de Educación).

Marta Martí
mmartibarr@uoc.edu
Universitat Oberta de Catalunya

Doctora en Derecho (Criminología) por la Universitat Pompeu Fabra. Ha sido beneficiaria de la Ayuda de Formación de Personal Universitario (FPU, Ministerio de Educación) para la realización de su tesis doctoral, y de la Ayuda para Estancias Breves (Ministerio de Educación) para realizar una estancia de investigación en la Aarhus University (Dinamarca). Actualmente es profesora colaboradora de la Universitat Oberta de Catalunya y consultora de investigación en criminología. Ha trabajado en proyectos de investigación para organismos internacionales como el Comité Internacional de la Cruz Roja (El Salvador) y Amnistía Internacional (México). Sus temas de interés son el sistema de penas, las prisiones y el análisis del sistema penal y la delincuencia desde una perspectiva de género.

Albert Pedrosa
albert.pedrosa@uab.cat
Universitat Autònoma de Barcelona

Estudiante de doctorado en Derecho (Criminología) por la Universitat Autònoma de Barcelona. En el año 2015 fue beneficiario de una Ayuda para la Formación de Personal Investigador (FPI, Ministerio de Educación). Actualmente forma parte del grupo de investigación «Desistimiento del delito y políticas de reinserción» de la UAB. En 2018 recibió el Premio para la Promoción de Jóvenes Investigadores otorgado por la Sociedad Española de Investigación Criminológica (SEIC) por su investigación sobre la progresión penitenciaria. Sus áreas de interés son el estudio del uso de la prisión, la situación de las familias de personas encarceladas y el control penal sobre colectivos en riesgo de exclusión.

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

https://idp.uoc.edu

ARTÍCULO

COVID-19, alquiler turístico y políticas de cancelación ¿emergencia en tiempos de pandemia de la oculta(da) naturaleza de las plataformas digitales?*

Apol·lònia Martínez Nadal
Universidad de las Islas Baleares

Fecha de presentación: octubre de 2020
Fecha de aceptación: febrero de 2021
Fecha de publicación: marzo de 2021

Resumen

La naturaleza jurídica de las plataformas digitales es una cuestión polémica y debatida. En el caso de las plataformas de comercialización de estancias turísticas breves, el Tribunal de Justicia de la Unión Europea se ha pronunciado sobre la condición de Airbnb declarando que tiene la sola condición de prestador de servicios de la sociedad de la información a los efectos de la Directiva de comercio electrónico, con las consecuencias que de ello se derivan. Consideramos que este pronunciamiento es cuestionable y revisable pues existen elementos que permiten considerar que esta plataforma tiene un control o influencia decisivos que la alejan de tal neutralidad de mero intermediario tecnológico. En concreto, consideramos que la política de cancelación aplicada por Airbnb en estos tiempos de pandemia, de forma unilateral, es, junto con otros elementos de su modelo negocial, una manifestación de tal posición de control o influencia decisivos, en la medida que decide sobre la existencia y continuidad de una relación de la que pretende ser ajena. En el fondo, se plantea la insuficiencia de los conceptos jurídicos tradicionales y la necesidad de nuevas categorías jurídicas para abordar el tratamiento jurídico de las plataformas digitales.

* Trabajo realizado en el marco del Proyecto RTI2018-097225-B-I00 «Plataformas de intercambio electrónico y nuevos modelos económicos disruptivos; problemática jurídica. En particular, el denominado alquiler turístico vacacional» financiado por el Ministerio de Ciencia e Innovación, la Agencia Española de Investigación y Fondos FEDER de la UE.

Palabras clave

Airbnb, naturaleza jurídica, prestador de servicios de la sociedad de la información, políticas de cancelación por COVID-19

COVID-19, vacation rentals and cancellation policies: is there an emergency, in these times of pandemic, regarding the hidden nature of digital platforms?

Abstract

The legal nature of the digital platforms is a controversial and debated issue. In the case of the platforms for the commercialisation of short-term tourist stays, the European Court of Justice has made a pronouncement on the status of Airbnb, declaring that it is only to be classified as an information society service as defined in the e-Commerce Directive, along with the consequences that arise from this. We consider that this declaration is questionable and revisable as factors exist which allow us to consider that this platform has a decisive control or influence, meaning that this view of its neutrality as a mere technological intermediary is way off the mark. Specifically, we believe that the cancellation policy applied by Airbnb in these times of pandemic, in its one-sided nature, together with other elements of its business model, is evidence of said position of decisive control or influence, as it decides on the existence and continuation of a relationship to which it claims to be unconnected. Ultimately, we outline the insufficiency of the traditional legal concepts and the need for new categories in order to address the legal approach to digital platforms.

Keywords

Airbnb, legal nature, information society service, cancellation policies due to COVID-19

* This work was carried out as part of Project RTI2018-097225-B-I00, "Electronic exchange platforms and new disruptive economic models; legal problems. In particular, the short-term vacation rentals", financed by the Ministry of Science and Innovation, the State Research Agency and the EU European Regional Development Fund.

1. La pandemia por la COVID-19 y su impacto en el alquiler vacacional

Como es sabido, la distópica situación de pandemia provocada por la COVID-19 que nos ha tocado vivir, iniciada formalmente con la declaración por parte de la Organización Mundial de la Salud (OMS) el pasado 11 de marzo de 2020 y con final todavía incierto, ha tenido repercusiones no solo sanitarias y de salud pública sino también, entre otras, económicas y sociales, por todos conocidas, debido a las distintas medidas adoptadas para hacer frente a la misma: confinamientos, cierre de fronteras, clausura de establecimientos...

Estas medidas restrictivas han afectado de forma muy especial al sector del turismo, dadas las limitaciones a la circulación de personas que, consiguientemente, afectan a los viajes, junto con medidas como el cierre obligatorio de establecimientos de alojamiento en los momentos iniciales, las restricciones de aforo, o la exigencia de cuarentena o pruebas de diagnóstico a los viajeros procedentes de territorios de riesgo (entre ellos, desafortunadamente, España), en momentos posteriores.

Esta incidencia sobre el turismo ha afectado, como no podía ser de otra forma, al alquiler turístico provocando una debacle a nivel mundial frente a la que han reaccionado las plataformas más paradigmáticas, como Airbnb, que, desde el inicio de la pandemia ha adoptado medidas diversas: publicación de protocolos sanitarios de desinfección de alojamientos o medidas tendentes al cumplimiento de las medidas legales de contención de la COVID-19 (estableciendo máximos de ocupación, suprimiendo los filtros para búsqueda de alojamientos que permitan fiestas), entre otras.

De entre estas actuaciones, nos centrarnos en la relativa a la aplicación por parte de la plataforma Airbnb de una «Política de Causas de Fuerza Mayor relativa al coronavirus (COVID-19)». Consideramos que esta actuación debe ser analizada, como hacemos en el apartado siguiente, y tenida muy en cuenta a fin de determinar el verdadero papel y naturaleza de esta plataforma, cuestión, como veremos en el último apartado, controvertida, incluso pese a la existencia de recientes pronunciamientos judiciales en la materia en el ámbito comunitario.

2. Políticas de cancelación de Airbnb con ocasión de la pandemia por la COVID-19

Como hemos señalado, tras el inicio de la pandemia, Airbnb (cuyo ejemplo inicial fue seguido por otras plataformas) adoptó una medida que consideramos muy relevante desde el punto de vista jurídico, a fin de poner de manifiesto la verdadera naturaleza de esta plataforma: la publicación y aplicación de una «Política de Causas de Fuerza Mayor relativa al coronavirus (COVID-19)» que permite la cancelación de reservas de alojamiento por causas relacionadas con la nueva situación de emergencia sanitaria mundial.

De entrada, llama la atención su carácter unilateral, pues es creada, publicada, aplicada e impuesta por Airbnb, sin previa consulta ni comunicación a los propietarios afectados, siendo, como es, una decisión que tiene una innegable y relevante repercusión (si no se trata directamente de una injerencia) en la relación contractual bilateral entre propietarios arrendadores y clientes arrendatarios («anfitriones» y «usuarios» en la terminología de Airbnb); relación respecto de la que, paradójicamente, la plataforma pretende ser totalmente ajena (como establece en sus Términos de uso)[1].

Así, de forma general, y antes del inicio de la excepcional situación de crisis sanitaria, según consta en la web de la plataforma: «En Airbnb, los anfitriones pueden elegir qué políticas de cancelación ofrecen a los huéspedes y estos pueden consultarlas antes de efectuar una reserva»[2]. Y se ofrecen de forma predeterminada distintos tipos de cancelación, siendo las ordinarias la flexible, la moderada y la estricta.

1. En efecto, conforme al término 1.2 Airbnb se presenta como mero proveedor tecnológico de la plataforma ajeno a la relación contractual de prestación del servicio de hospedaje entre anfitrión y huésped. En el mismo sentido, el término 7.1.7, relativo al anfitrión.
2. Apartado «Cómo funcionan las cancelaciones de estancias»: https://www.airbnb.es/home/cancellation_policies.

Pues bien, junto a la política de cancelación ordinaria respecto de la que Airbnb realiza distintas propuestas pero cuya decisión final depende del gestor del alojamiento (que elige dentro de las políticas propuestas por la plataforma), en esta atípica situación de emergencia mundial Airbnb publicó, de forma también atípica y además unilateral, sin siquiera consulta previa a sus «anfitriones» una nueva «Política de Causas de Fuerza Mayor relativa al coronavirus (COVID-19)» que ha pasado a ser de aplicación de forma obligatoria y que rige las relaciones entre arrendador y arrendatario (anfitrión y huésped) respecto de las que, como es sabido, Airbnb se declara completamente ajena en sus «Términos de uso».

Como se explica en la propia web de la plataforma (en la versión actualizada con fecha de 15 de septiembre de 2020), tras la declaración el pasado 11 de marzo de 2020 por la OMS de pandemia mundial por el brote de coronavirus, Airbnb, para hacer frente a la situación, presentó una «Política de Causas de Fuerza Mayor» con cobertura específica para la pandemia con el objetivo de proteger a los miembros de la comunidad. De forma resumida, este es su contenido:

a) Reservas realizadas hasta el 14 de marzo de 2020: están cubiertas las reservas de alojamientos realizadas hasta el 14 de marzo de 2020 y programadas entre el 14 de marzo de 2020 y el 31 de octubre de 2020 y se podrán cancelar antes del comienzo. En consecuencia, los viajeros que cancelen acogiéndose a la política recibirán un reembolso completo. Por su parte, los anfitriones que cancelen en virtud de la política no tendrán que pagar ninguna penalización. Además, los reembolsos y el crédito de viaje que emita Airbnb incluirán todas las comisiones de servicio.

b) Reservas realizadas después del 14 de marzo: en cambio, como señala Airbnb: «Nuestra Política de Causas de Fuerza Mayor no cubrirá las reservas de alojamientos y experiencias en Airbnb realizadas después del 14 de marzo de 2020, excepto en caso de que el viajero o el anfitrión contraigan la COVID-19». La razón alegada es la desaparición de la imprevisibilidad: «Desde que la Organización Mundial de la Salud declaró la COVID-19 como pandemia mundial, no podemos aplicar la Política de Causas de Fuerza Mayor a las cancelaciones relacionadas con el coronavirus y sus consecuencias, puesto que han dejado de considerarse una circunstancia imprevista o inesperada». En esos casos, «aplicaremos la política de cancelación del anfitrión como de costumbre».

c) Reservas de alojamientos realizadas hasta el 14 de marzo de 2020 que tengan una fecha de inicio posterior al 31 de octubre de 2020: no pueden acogerse a la Política de Causas de Fuerza Mayor relativa al coronavirus. En esos casos, «aplicaremos la política de cancelación del anfitrión como de costumbre». No obstante, Airbnb recuerda que está actualizando continuamente la cobertura de esta política por lo que recomienda una consulta periódica de la misma[3].

Como ya hemos apuntado, esta política de cancelación de reservas (en su versión inicial y sus posteriores actualizaciones) se creó, publicó y aplicó por Airbnb de forma total y absolutamente unilateral, sin acuerdo previo y ni siquiera consulta o comunicación anterior a las principales partes afectadas desde el punto de vista jurídico, anfitrión y huésped (arrendador y arrendatario), y ni siquiera información previa al operador más afectado desde el punto de vista económico (el propietario o gestor de la vivienda), al que ni siquiera se ha exigido aceptación expresa o siquiera tácita de la nueva política de cancelación.

Esta actuación unilateral es reconocida por la propia plataforma: tras publicar la primera versión de la política de cancelación por COVID-19 en marzo de 2020, publicó el día 1 de abril una «Carta a los anfitriones» firmada por Brian Chesky, director ejecutivo de Airbnb, en la que se disculpa formalmente por ello: «Sin embargo, aunque creo que hicimos lo correcto priorizando la salud y la seguridad, quiero disculparme por cómo os comunicamos esta información y por no haber pedido vuestra

3. Esta política se actualiza de forma periódica desde la declaración de pandemia; la última actualización en el momento de redactar este trabajo era la de 15 de septiembre de 2020. Justo al cierre del trabajo se ha publicado una versión con fecha 1 de octubre que amplía la cobertura a las reservas realizadas hasta el 14 de marzo y con fecha de inicio en los próximos cuarenta y cinco días: https://www.airbnb.es/help/article/2701/pol%C3%ADtica-de-causas-de-fuerza-mayor-relativa-al-coronavirus%C2%A0covid19.

opinión»[4]. En cualquier caso, esta nueva política ha pasado a ser de aplicación de forma obligatoria y rige las relaciones entre arrendador y arrendatario (anfitrión y huésped), habiendo surgido al margen de los mismos.

Llama la atención que una decisión sobre tal cuestión de tanta trascendencia contractual, que afecta a la existencia y continuidad del contrato bilateral entre anfitrión y usuario (del que, no se olvide, Airbnb no forma parte de acuerdo con su modelo económico y jurídico oficial) sea tomada, decidida e impuesta por una persona ajena a dicha relación. A no ser que realmente no sea tan ajena; en suma, que tal elemento de ajenidad no esté presente o al menos no con tanta pureza e intensidad como se pretende, por ostentar la plataforma una posición de control de tal relación en aspectos tan esenciales como el de su cancelación, posición de control o influencia decisiva, como veremos, especialmente relevante para la determinación de la naturaleza de la plataforma conforme a los postulados de la Unión Europea. En el fondo, sería una muestra de la insuficiencia de esta construcción contractual bilateral para hacer frente a una relación materialmente triangular en la que la plataforma tiene un papel especialmente relevante, tan relevante que se convierte en «regulador» de la misma.

Podría argumentarse que tal actuación la ha realizado la plataforma para hacer frente, de forma ágil y aplicando soluciones uniformes a todos sus «anfitriones» y «huéspedes», a la problemática derivada de la crisis sanitaria. Lo cierto es que, pese a que este objetivo pudiera ser loable desde el punto de vista material, a efectos de agilización de la resolución de estas incidencias en ese atípico momento, se hubiera debido realizar respetando la formal autonomía de la voluntad de las partes contractuales, muy especialmente del anfitrión, que puede ser el más perjudicado económicamente por dicha política de cancelaciones. A no ser, nuevamente, que nos hallemos realmente ante una relación triangular sin el adecuado tratamiento jurídico hoy día.

Como planteamos a continuación, esta decisión de Airbnb sobre políticas de cancelación en tiempos de pandemia debe ser tenida muy en cuenta en el esclarecimiento de la naturaleza de esta plataforma, cuestión, como veremos seguidamente, controvertida, incluso pese a la existencia de recientes pronunciamientos judiciales, como la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 19 de diciembre de 2019 (caso Airbnb Ireland), cuyo planteamiento consideramos revisable.

3. Naturaleza jurídica de las plataformas digitales: estado de la cuestión. En especial el caso de Airbnb

Como es sabido, y antes de la crisis generalizada causada por la COVID-19, en los últimos años el alquiler turístico de viviendas había experimentado un gran desarrollo no solo en España y sus comunidades y ciudades más turísticas sino también en otros muchos países y ciudades emblemáticas.

No es un fenómeno nuevo: desde hace años existe este tipo de actividad, tradicionalmente gestionada de forma directa entre particulares o, a lo sumo, a través de agencias tradicionales. El elemento novedoso, y en buena medida causante del mencionado auge, es la aparición de plataformas digitales especializadas que, de forma simple, permiten no solo a profesionales sino también a particulares ofertar una vivienda para su utilización temporal con fines normalmente turísticos en multitud de países y a una gran variedad de potenciales usuarios a los que de otra forma probablemente no podrían llegar. Consideramos importante remarcar este papel de las plataformas como factor clave y esencial de esta eclosión del alquiler turístico a nivel mundial y probablemente instrumento imprescindible para determinados arrendadores.

La plataforma paradigmática es, sin duda, Airbnb, surgida en 2008 en San Francisco como iniciativa de unos, por entonces, estudiantes (Brian Chesky, Joe Gebbia y Nathan Blecharczyk) y que se ha convertido hoy en un gigante económico con una amplia oferta de inmuebles en casi doscientos países. Aunque Airbnb sea probablemente la más conocida, existen otras y numerosas plataformas para la comercialización de estancias breves: entre ellas,

4. Véase en este sentido la «Carta a los anfitriones»: https://news.airbnb.com/es/carta-a-los-anfitriones/.

Booking.com, HomeAway o TripAdvisor. No obstante, el modelo económico no es siempre totalmente coincidente; así, por ejemplo, mientras Airbnb cobra una comisión («tarifa de servicio») sobre el precio del alojamiento reservado, HomeAway aplica un modelo de suscripción del propietario arrendador de tal forma que este debe pagar una tasa anual por la inclusión de su propiedad en la plataforma.

Algunas de estas plataformas digitales pretenden incardinar su modelo de negocio en el ámbito de la denominada «economía colaborativa» o «economía compartida», concepto actualmente amplio, difuso, ambiguo y objeto de tales usos y abusos que ha sido calificado más bien como un «anticoncepto», pues, en efecto, y, paradójicamente, no se ha conseguido todavía una noción compartida de lo que sea dicha «economía compartida»[5].

En este sentido, consideramos significativo que Airbnb se presente actualmente como simple proveedor de una plataforma tecnológica que actúa como simple mercado en línea, punto de encuentro que posibilita que los «anfitriones» (propietarios, arrendadores) puedan ofrecer sus viviendas a los «huéspedes» (futuros usuarios)[6]. Llama la atención, de entrada, la terminología utilizada (anfitriones, huéspedes), que huye de las categorías jurídicas establecidas (propietario arrendador, cedente; cliente arrendatario, cesionario, usuario) y, sobre todo, de las consecuencias jurídicas que se derivan de las mismas para entrar en ese «limbo jurídico» que se pretende por algunos operadores económicos que sea la economía colaborativa. Y más llama la atención todavía que esta terminología sea el resultado de un cambio en los términos de uso de la plataforma producido en el año 2016, en que publica una nueva versión en la que se elimina toda referencia a términos (y conceptos) como alquiler, subarriendo o inmobiliarios, u otras palabras derivadas. Lo cual afecta a la propia definición de la plataforma y la descripción de su actividad, que deja de ser «alquilar» para pasar a ser «anunciar y reservar»[7].

Y es que, si las palabras en general no son inocuas, en este caso, visto el trasfondo, lo son menos que nunca. Esta pretensión de huir de las categorías jurídicas tradicionales y de ubicarse confortablemente en el ámbito de la economía colaborativa y de la simple intermediación tecnológica neutral es seguramente interesada y del todo cuestionable por los intereses espurios que se hallan tras la misma y que nos llevan a cuestionar el propio concepto actual de economía colaborativa y la utilización que del mismo se realiza; y ello nos conduce a la búsqueda de términos y categorías más conformes a la realidad económica de estos nuevos modelos negociales disruptivos como, por ejemplo, economía de plataformas o economía digital, entre otros. Todo lo cual obliga a replantear la verdadera naturaleza jurídica de estas grandes plataformas digitales como grandes intermediarias que abren nuevos e inmensos mercados a los propietarios de viviendas a la vez que plantean nuevas cuestiones e incógnitas desde el punto de vista jurídico.

3.1 Modelo económico y clasificación dual

Para ello, y para conocer el estado de la cuestión sobre la naturaleza jurídica de las plataformas digitales, podemos tomar como punto de partida que, tradicionalmente, se han distinguido dos modelos económicos con distintas consecuencias jurídicas en materia de obligaciones y responsabilidad, especialmente por la ejecución de la

5. A los efectos de la Comunicación titulada «Una Agenda Europea para la economía colaborativa», presentada por la Comisión Europea en junio de 2016, el término «economía colaborativa» se refiere a modelos de negocio en los que se facilitan actividades mediante plataformas colaborativas que crean un mercado abierto para el uso temporal de mercancías o servicios ofrecidos a menudo por particulares. Por lo general, las transacciones de la economía colaborativa no implican un cambio de propiedad y pueden realizarse con o sin ánimo de lucro.
6. En efecto, conforme al término 1.1 la plataforma es un mercado electrónico, un punto de encuentro virtual entre anfitriones y huéspedes: «La Plataforma de Airbnb es un mercado en línea que permite que los usuarios registrados ["miembros"] y ciertos terceros que ofrecen servicios [los miembros y terceros que ofrecen servicios son "anfitriones" y los servicios que ofrecen son "Servicios de Anfitrión"] publiquen dichos Servicios de Anfitrión en la Plataforma de Airbnb ["Anuncios"] y comuniquen y gestionen directamente con los miembros que desean reservar dichos Servicios de Anfitrión [los miembros que utilizan los Servicios de Anfitrión son "huéspedes"]. Y conforme al término 1.2 es un mero proveedor tecnológico de la plataforma: "En calidad de proveedor de la Plataforma de Airbnb, Airbnb no posee, crea, vende, revende, suministra, controla, gestiona, ofrece, entrega ni presta ningún Anuncio ni Servicio de Anfitrión ni constituye un organizador o minorista de viajes combinados, de conformidad con la Directiva (UE) 2015/2302».
7. Cfr. respecto de este cambio, MORELL RAMOS, J. (2016). «Así se "reinventa" Airbnb en sus nuevos términos y condiciones: https://terminosycondiciones.es/2016/11/14/asi-airbnb-reinventa-nuevos-terminos-y-condiciones/.

relación subyacente: las plataformas puras, meramente intermediadoras, o las plataformas que, yendo más allá, tienen el papel de prestador de la obligación derivada de la relación subyacente (o, como mínimo, responsable de la misma). Jurisprudencialmente se ha entendido que BlaBlaCar sería un mero intermediario (un prestador de servicios en línea que se dedica a explotar su plataforma y que no tiene la condición de transportista)[8], mientras que Uber, en cambio, sí tendría la condición de empresario del sector del transporte (es considerado un servicio de intermediación indisociablemente vinculado a un servicio de transporte y, por lo tanto, ha de calificarse de «servicio en el ámbito de los transportes»)[9].

Para el caso que nos ocupa, en fecha de 19 de diciembre de 2019 se ha pronunciado el Tribunal de Justicia de la Unión Europea (C-390/18) en el sentido de que procede calificar de «servicio de la sociedad de la información» comprendido en el ámbito de aplicación de la Directiva 2000/31 un servicio de intermediación como el de Airbnb, prestado a cambio de una remuneración, que tiene por objeto poner en contacto mediante una plataforma electrónica a potenciales arrendatarios con arrendadores, profesionales o no profesionales, que proponen servicios de alojamiento de corta duración y que, además, ofrece otras prestaciones accesorias de ese servicio de intermediación. Por tanto, entiende el Tribunal que Airbnb es un simple intermediario que no interviene en la prestación del servicio de alojamiento, siendo por ello un mero «prestador de servicios de la sociedad de la información».

En el fondo, la pretensión de acogerse y beneficiarse de la condición de simple intermediario digital, esto es, en términos jurídicos, de «prestador de servicios de la sociedad de la información», es una cuestión estratégica para estas plataformas porque de ella se deriva la aplicación de un marco jurídico y legal que les resulta sumamente favorable.

Así, a modo de ejemplo, la Directiva 2000/31 de comercio electrónico, y los relevantes principios establecidos en la misma tales como la denominada «cláusula del mercado interior» (el prestador está sujeto a la ley del país en el que está establecido, cláusula aplicada a Airbnb Ireland en la mencionada Sentencia del TJUE de 19 de diciembre de 2019); el principio de no autorización previa (no exigencia de autorización específica para los prestadores de servicios de la sociedad de la información, principio objeto de análisis también en esta última sentencia); o la eventual inexistencia de responsabilidad de los intermediarios por los contenidos de la plataforma (cuestión sumamente polémica en los últimos tiempos en derecho español a raíz de la exigencia de responsabilidad a las plataformas de alquiler turístico por la inclusión de viviendas sin el correspondiente número de registro y resuelta de forma divergente por nuestra jurisprudencia).

Pues bien, pese al pronunciamiento del Tribunal de Justicia de la Unión Europea de 19 de diciembre de 2019 en el sentido de que Airbnb es un mero «prestador de servicios de la sociedad de la información», entendemos que, a la vista del funcionamiento y actuaciones de Airbnb, existen argumentos para sostener y considerar que no es realmente tal simple prestador y que, por ello, no podría beneficiarse del régimen jurídico favorable derivado de tal condición.

Veamos a estos efectos con mayor detalle la posición comunitaria en la materia y cómo de la misma pueden extraerse tales argumentos para negar, o como mínimo cuestionar, dicha condición de simple prestador a Airbnb, pese a que el Tribunal europeo haya llegado a la conclusión contraria.

8. En este sentido, existen en España distintos pronunciamientos judiciales: así, por ejemplo, la Sentencia de la Audiencia Provincial de Madrid de 2 de febrero de 2017, que proclama la condición de la plataforma de prestador de servicios de la sociedad de la información a los efectos de la Ley 34/2001; y también la Sentencia de la Audiencia Provincial de Madrid, de 18 de febrero de 2019, en la que se concluye que la actividad de BlaBlaCar no es la de un servicio de transporte, sino la de prestación de servicios en línea, la explotación de una plataforma web.
9. La sentencia del TJUE de 20 de diciembre de 2017 (asunto C-434/15) declaró que «un servicio de intermediación (...) que tiene por objeto conectar mediante una aplicación para teléfonos inteligentes, a cambio de una remuneración, a conductores no profesionales que utilizan su propio vehículo con personas que desean efectuar un desplazamiento urbano, está indisociablemente vinculado a un servicio de transporte, y por lo tanto ha de calificarse de servicio en el ámbito de los transportes (...). En consecuencia, un servicio de esta índole está excluido del ámbito de aplicación del artículo 56 TFUE, de la Directiva 2006/123 y de la Directiva 2000/31». Este mismo criterio resolutivo ha sido aplicado en España por el Tribunal Supremo, en Sentencias de 24 y 25 de enero de 2018, señalando que Uber: «No es un mero servicio de intermediación, sino que constituye una parte sustancial de la prestación de servicio de transporte de viajeros, estando por ello sujeta a la autorización exigida en el artículo 42.1 de la Ley 16/1987, de 30 de julio, de Ordenación de los Transportes Terrestres».

3.2. La posición comunitaria. El criterio del control o influencia decisiva y su aplicación a la «Política de Causas de Fuerza Mayor relativa al coronavirus (COVID-19)» de Airbnb, entre otros elementos

La Comisión Europea presentó en junio de 2016 una Comunicación titulada «Una Agenda Europea para la economía colaborativa» en la que se establecen una serie de pautas que han sido seguidas después, en buena medida, por el Tribunal de Justicia de la Unión Europea:

1. En la Comunicación se establece que en la medida en que las plataformas colaborativas proporcionan un «servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un prestatario de servicios»[10], ofrecen un servicio de la sociedad de la información, por lo que no pueden estar sujetas a autorizaciones previas o cualquier requisito equivalente dirigidos específica y exclusivamente a dichos servicios[11].

2. Sin embargo, la misma Comisión admite que puede haber casos en los que plataformas colaborativas ofrecen otros servicios además de los servicios de la sociedad de la información. En particular, en determinadas circunstancias, una plataforma puede ser también un proveedor del servicio subyacente (por ejemplo, servicio de transporte o de alquiler a corto plazo). En tal caso, las plataformas colaborativas podrían estar sujetas a la normativa sectorial específica, incluidos los requisitos de autorización y concesión de licencias empresariales aplicados por lo general a los prestadores de servicios.
   Obsérvese que la Comisión se mantiene en la tradicional clasificación dual de la naturaleza de las plataformas: o son intermediarias puras o son prestadoras del servicio subyacente, clasificación que actualmente consideramos insuficiente y superada por la realidad económica actual y los nuevos modelos económicos disruptivos. Propugnamos, por ello, la superación de la misma y la aparición de una nueva categoría jurídica que resulte aplicable a las plataformas digitales.

3. En estas coordenadas de la tradicional clasificación dual, la Comisión señala que, normalmente, deberá establecerse caso por caso si una plataforma colaborativa ofrece también el servicio subyacente. Y apunta a que varios elementos desempeñan un papel a este respecto. Así, el nivel de control o influencia que la plataforma colaborativa ejerce sobre el prestador de dichos servicios tendrá por lo general una importancia significativa. Y, en particular, este nivel de control o influencia, según la Comisión, puede establecerse a la luz de los siguientes criterios clave:

   a) Precio: ¿fija la plataforma colaborativa el precio final que debe pagar el usuario como beneficiario del servicio subyacente?

   b) Otras condiciones contractuales clave: ¿establece la plataforma colaborativa términos y condiciones distintos del precio que determinan la relación contractual entre el prestador de los servicios subyacentes y el usuario?
   En este apartado, incluye la Comisión, a título de ejemplo, la existencia de instrucciones obligatorias sobre la prestación del servicio subyacente, incluida cualquier obligación de prestar el servicio. Por nuestra parte, apuntamos esta cuestión para el caso que nos ocupa: ¿acaso el establecimiento unilateral de la política de cancelación del contrato de alojamiento entre huésped y anfitrión por parte de Airbnb no es la fijación de una cuestión contractual clave, un término o condición distintos del precio «que determinan la relación entre el prestador de los servicios subyacentes y el usuario», tanto que de ella depende la existencia y continuidad misma del contrato bilateral, del que ni siquiera es parte la plataforma, conforme a sus «Términos de uso»?

   c) Propiedad de activos clave: ¿posee la plataforma activos clave para prestar el servicio subyacente? Como sabemos, Airbnb no es titular de los activos (viviendas) que permiten prestar el servicio de alojamiento; lo que caracteriza a su modelo económico

10. Véase el art. 2, letra a) de la Directiva sobre el comercio electrónico; y el art. 1, apdo. 1, letra b), de la Directiva 2015/1535. También el anexo I de esta última Directiva para una lista indicativa de los servicios no cubiertos por esa definición.
11. Véase el art. 4 de la Directiva sobre el comercio electrónico.

es, precisamente, la inexistencia de ese tipo de activos empresariales; sin embargo, la plataforma en sí es un activo que resulta, para muchos usuarios, imprescindible para la oferta y contratación del servicio de alojamiento vacacional, pues, de otra forma no podría llegar su oferta a tantos potenciales clientes.

Pues bien, cuando se cumplen estos criterios, según la posición de la Comisión, hay indicios claros de que la plataforma ejerce una influencia o control significativos sobre el prestador del servicio subyacente, lo que puede indicar a su vez que debe considerarse que presta también el servicio subyacente (además de un servicio de la sociedad de la información). Como ya hemos señalado, la Comisión se mueve en los parámetros de la clasificación dual tradicional (prestadores meramente intermediarios y prestadores del servicio subyacente) pero la realidad y los modelos económicos son tan complejos y variados que, como venimos señalando, posiblemente sea conveniente la existencia de una tercera (o simplemente una nueva) categoría con un régimen jurídico propio y diferenciado, en materia de acceso, responsabilidad por la prestación subyacente, responsabilidad por contenidos, implicaciones fiscales, laborales... De tal forma que, en el ámbito de esta tercera o nueva categoría, un prestador puede no ser necesariamente un prestador del servicio subyacente, pero tampoco un simple intermediario, formando parte de una categoría intermedia con un régimen jurídico diferenciado en un mayor o menor número de aspectos y más ajustado y conforme al modelo económico real, en función de la mayor o menor influencia de la plataforma.

En cualquier caso, obsérvese que el criterio de la fijación de una condición contractual esencial como la política de cancelación analizada es muestra de posición de control de la plataforma, como lo son también, entendemos, otros elementos derivados del modelo económico de la misma y que se derivan de los términos de uso que rigen su relación con «anfitriones» y «huéspedes», elementos que ponen de manifiesto que Airbnb no es un simple intermediario tecnológico neutral ajeno a la relación contractual bilateral de arrendadores y arrendatarios.

En efecto, más allá de la alegada condición de mero proveedor tecnológico de una plataforma que es punto de encuentro entre propietarios y usuarios resulta que 1) Airbnb impone la forma y condiciones de pago del precio del hospedaje e incluso retiene la cantidad pagada en su poder hasta el inicio del servicio de alojamiento; 2) influye en la forma y la presentación de los anuncios; 3) puede cancelar reservas; 4) e incluso la configuración de su modelo de «tasas de servicio» se asemeja más al modelo de comisionista (comisionista impuro, por su posición dominante) que recibe en pago una comisión por reserva realizada que al modelo de simple alojador de datos («tablón de anuncios») que cobra por el simple anuncio, con independencia de las reservas posteriores; 5) por ello, más allá de un simple alojador de contenidos, la propia plataforma está interesada en promocionar las reservas, ya que su remuneración depende de la efectiva reserva, no de la simple inclusión del anuncio.

En suma, tras este análisis del trasfondo económico de la relación materialmente triangular entre Airbnb y sus usuarios (anfitrión y huésped), y conforme a los criterios de la propia Comisión, consideramos que existen elementos acreditativos suficientes de la posición de control o influencia de la plataforma que permiten cuanto menos cuestionar su condición de mero prestador de servicios de la sociedad de la información con funciones de intermediación neutral.

Estos criterios derivados de la Comunicación de la Comisión Europea «Una Agenda Europea para la economía colaborativa» establecidos en 2016 que acabamos de exponer de forma resumida han sido seguidos después, en buena medida, por el Tribunal de Justicia de la Unión Europea. En concreto, y por lo que nos interesa a efectos de este trabajo, hemos de volver a la ya conocida Sentencia del TJUE de 19 de diciembre de 2019 (Asunto C-390/118) que, como es sabido, se pronuncia por primera vez sobre la naturaleza jurídica de la plataforma Airbnb.

Recordemos que la sentencia declara que el servicio prestado por Airbnb Ireland debe entenderse como un «servicio de la sociedad de la información» en el sentido de la Directiva 2000/31 de Comercio Electrónico. A continuación, el Tribunal declara que por ello no es conforme a la Directiva que Francia exija a Airbnb Ireland contar con una autorización para realizar su actividad, ya que esta prohíbe que los Estados impongan restricciones a los operadores establecidos en otros Estados miembros (Airbnb Ireland está establecido en Irlanda), a menos que hayan

tramitado previamente un procedimiento previsto en el artículo 3.4 de la propia Directiva, el cual requiere que se haya notificado al Estado de establecimiento del operador y a la Comisión.

La sentencia dedica apenas el apartado 68 al examen de la existencia de una posición de control y de influencia decisiva, un examen breve y sobre una base fáctica incompleta que no refleja el verdadero modelo negocial de Airbnb y que le lleva a descartar tal posición. Mayor extensión hallamos en la Posición del Abogado General, con los apartados 69 a 79 dedicados al análisis del control o influencia decisiva ejercidos sobre las condiciones de la prestación de servicios; especialmente interesante a nuestros efectos es el párrafo 74 en el que se señala: «es preciso observar que son los arrendadores quienes fijan las condiciones del alquiler. Es cierto que AIRBNB Ireland establece determinadas opciones predefinidas en cuanto a las condiciones de cancelación. Sin embargo, es, en todo caso, el arrendador quien elige, de manera deliberada, una de las opciones propuestas y, por tanto, en quien recae la decisión final sobre las condiciones de cancelación». Como hemos visto, la política de cancelación por causas de fuerza mayor que aplica Airbnb a causa de la COVID-19 impide afirmar que «en todo caso» es del arrendador la decisión final sobre las cancelaciones y muestra la influencia decisiva de la plataforma (incluso antes de la pandemia Airbnb tenía una política de cancelación por fuerza mayor con efectos similares).

Esta sentencia, obviamente, ha sido acogida muy favorablemente por el sector de las plataformas de alojamiento, no solo por el pronunciamiento en sí sino también por las consecuencias jurídicas y prácticas, que pretenden derivarse del mismo, no siempre de forma fundamentada (caso de la exención de responsabilidad por publicación de contenidos).

Pues bien, aunque es cierto que este único pronunciamiento judicial proclama que Airbnb tiene tal condición, consideramos que, a la vista de lo expuesto en este trabajo sobre el modelo económico y la posición de control y de influencia decisiva de esta plataforma sobre el prestador del servicio de hospedaje y su relación contractual con el usuario, no se ha realizado un adecuado análisis de la verdadera naturaleza de la actuación de esta plataforma, de la que las políticas de cancelación por la COVID-19 no son más que «una punta del iceberg» que muestra, siquiera parcialmente, una parte oculta(da) de esta plataforma, más allá de la de un simple intermediario neutral.

Conclusiones

Resoluciones como la Sentencia del Tribunal de Justicia de la Unión Europea de 19 de diciembre de 2019 calificando a la plataforma Airbnb como mero prestador de servicios de la sociedad de la información conforme a la Directiva de comercio electrónico ponen de manifiesto la dificultad de establecer la naturaleza jurídica de las plataformas digitales.

Beneficiarse de esta calificación es un tema estratégico crucial para las plataformas digitales, pero entendemos que, en la actualidad, esta categoría jurídica no resuelve satisfactoriamente la problemática subyacente a estos nuevos modelos económicos disruptivos.

De lege data, consideramos que es cuanto menos cuestionable, en el supuesto de Airbnb, su calificación como mero prestador de servicios de la sociedad de la información. Actuaciones como la publicación durante la pandemia de la política de cancelación por COVID-19, junto con otros elementos característicos de su actuación, permiten sostener que esta plataforma tiene un control o influencia decisiva sobre las partes de la relación de hospedaje que impiden calificarla como un simple intermediario neutral, mero prestador de servicios de la sociedad de la información, con las consecuencias que de esa condición se derivan.

De lege ferenda, y para abordar de forma adecuada el tratamiento jurídico de las plataformas digitales, consideramos recomendable superar la tradicional clasificación dual de las plataformas (intermediarias vs. ejecutoras) y las actuales categorías establecidas (prestador de servicios de la sociedad de la información) que tuvieron su razón de ser en los momentos iniciales de surgimiento del comercio electrónico pero que resultan inadecuadas para la economía de plataformas. Hay que avanzar hacia nuevas categorías que den una mejor cobertura a estos nuevos modelos económicos disruptivos, como se ha planteado doctrinalmente. Es necesario, pues, establecer nuevos regímenes jurídicos adaptados y adecuados al verdadero papel y funciones de las plataformas digitales.

En este sentido, puede tomarse como referencia el documento «Model rules on online platforms» presentado por el European Law Institute, en cuyo artículo 18 se regula precisamente la «Responsabilidad del operador de la plataforma con influencia predominante» y se establece como principio general que si el cliente puede confiar razonablemente en que el operador de la plataforma tendrá una influencia predominante sobre el proveedor, «el cliente puede ejercer los derechos y recursos disponibles por el incumplimiento contra el proveedor en virtud del contrato proveedor-cliente también contra el operador de la plataforma». Aparece, pues, también la idea de «influencia predominante», para cuya evaluación se propone considerar distintos criterios, buena parte de los cuales son cumplidos por Airbnb: por ejemplo, conclusión del contrato proveedor-cliente exclusivamente a través de la plataforma; ocultación de la identidad del proveedor o los datos de contacto hasta después de la conclusión del contrato proveedor-cliente; retención por la plataforma de los pagos realizados por el cliente al proveedor; determinación de términos esenciales del contrato por la plataforma; marketing centrado en la plataforma y no en los proveedores. A mayor cumplimiento de estos criterios, existirá mayor influencia decisiva y mayor probabilidad de ejercicio de una acción de responsabilidad contra el intermediario, pese a no ser parte de la relación bilateral cliente-proveedor, bilateralidad que debería ser también superada con el reconocimiento jurídico de la estructura triangular derivada de la economía de plataformas y la posición de predominio de estas.

En suma, estamos en un momento clave en el que se pone de manifiesto la necesidad de superar, replantear y definir nuevas categorías jurídicas para estos nuevos modelos económicos disruptivos.

Adenda

Una vez finalizada en el mes de octubre de 2020 la redacción de este trabajo, la Comisión Europea presentó el pasado mes de diciembre de 2020 dos propuestas para regular los servicios digitales a través de dos instrumentos: la Propuesta de Reglamento de Mercados Digitales (conocida abreviadamente como DMA por sus siglas en inglés, «Digital Markets Act») y la Propuesta de Reglamento de Servicios Digitales (conocida como DSA, por «Digital Services Act»); ambas forman parte del denominado «Digital Services Act Package» y proponen una nueva regulación aplicable a las plataformas digitales, especialmente las grandes plataformas tecnológicas.

Por ello, en la posterior fase de revisión final del trabajo previa a su publicación, consideramos necesaria como mínimo una breve referencia a estas iniciativas y al tema planteado de la naturaleza jurídica y responsabilidad de las grandes plataformas. Del análisis de estas propuestas, en su estado actual, no se deduce una solución clara para el problema planteado en nuestro trabajo, aun cuando aparecen algunas ideas interesantes; por ejemplo, la posible responsabilidad ex artículo 5, párrafo 3 de la propuesta de Reglamento de Servicios Digitales de las plataformas ante consumidores en el supuesto de que la plataforma permita que la transacción se desarrolle de tal forma que lleve a un consumidor medio y razonablemente bien informado a creer que la información, o el producto o servicio objeto de la transacción, son proporcionados por la propia plataforma en línea o por un destinatario del servicio que actúa bajo su autoridad o control. Es solo un primer paso, en la línea de nuestras propuestas, que consideramos necesitaría una mayor concreción, la cual esperamos se consiga en el largo recorrido que les espera todavía a estas dos relevantes propuestas de Reglamento.

Referencias bibliográficas

BUSCH, C.; SCHULTE-NÖLKE, H; WIEWIOROWSKADOMAGALSKA A.; ZOLL, F. (2016). «The rise of the platform economy: A new challenge for EU Consumer Law? *EuCML. Journal of European and Consumer Law*, pág. 3 y sigs.

CUENA CASAS, M. (2020). «La contratación a través de plataformas intermediarias en línea». *Cuadernos de Derecho Transnacional*, vol. 12, núm. 2, págs. 283-348 [en línea] DOI: https://doi.org/10.20318/cdt.2020.5612 [Fecha de consulta: 8 de febrero de 2021].

DE MIGUEL ASENSIO, P. (2019). «La ordenación de las plataformas de intermediación tras la(s) sentencia(s) Airbnb» [en línea] https://pedrodemiguelasensio.blogspot.com [Fecha de consulta: 8 de febrero de 2021].

EUROPEAN COMMISSION (2016). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, SWD (2016) 172 final, COM (2016) 288 final Brussels, 25 May 2016.

EUROPEAN COMMISSION (2016). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Agenda for the collaborative economy, SWD (2016) 184 final, COM (2016) 356 final Brussels, 2 June 2016.

EUROPEAN LAW INSTITUT (2019). *Model rules on online platforms* [en línea] https://www.europeanlawinstitute.eu [Fecha de consulta: 8 de febrero de 2021].

FERNÁNDEZ GARCÍA DE LA YEDRA, A. (2020). «Calificación jurídica de las plataformas de alojamiento colaborativo». En: MUNAR, P. (dir.). *Turismo, vivienda y economía colaborativa*. Pamplona: Aranzadi, págs. 421-446.

JIMÉNEZ HORWITZ, M. (2019). «La situación jurídica de la plataforma Airbnb en el marco de la economía colaborativa». *Revista Aranzadi Doctrinal,* núm. 3.

MARTÍNEZ NADAL, A. (2020). *Alquiler turístico de viviendas de uso residencial y Derecho de la Competencia.* Pamplona: Aranzadi.

PAZOS CASTRO, Ricardo (2020). «Uber, Airbnb y la llamada "influencia decisiva" de las plataformas digitales». *IDP. Revista de Internet, Derecho y Política*, núm. 31, págs. 1-14. UOC [en línea] DOI: https://doi.org/10.7238/idp.v0i31.3224 [Fecha de consulta: 8 de febrero de 2021].

RODRÍGUEZ DE LAS HERAS BALLELL, T. (2017). «The legal anatomy of electronic platforms: A prior study to assess the need of a Law of Platforms in the EU». *The Italian Law Journal,* vol. 3, núm. 1, pág. 149 y sigs [en línea] https://www.academia.edu/34575454/T_Rodriguez_de_las_Heras_Ballell_The_Legal_Anatomy_of_Electronic_Platforms_A_Prior_Study_to_Assess_the_Need_of_a_Law_of_Platforms_in_the_EU [Fecha de consulta: 8 de febrero de 2021].

RODRÍGUEZ RUIZ DE VILLA, D. (2020). «Enseñanzas de la Sentencia Airbnb del TJUE para el corretaje inmobiliario en España» [en línea] https://almacendederecho.org [Fecha de consulta: 8 de febrero de 2021].

Cita recomendada

MARTÍNEZ NADAL, Apol·lònia (2021). «COVID-19, alquiler turístico y políticas de cancelación ¿emergencia en tiempos de pandemia de la oculta(da) naturaleza de las plataformas digitales?». *IDP. Revista de Internet, Derecho y Política*, núm. 32 (marzo). UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i32.374912

Sobre la autora

Apol·lònia Martínez Nadal
Catedrática de Derecho Mercantil
Universidad de las Islas Baleares
apollonia.martinez@uib.es

Apol·lònia Martínez Nadal, catedrática de Derecho Mercantil de la Universidad de las Islas Baleares. Investigadora responsable del CEDIB (Centro de Estudios del Derecho de la Informática de Baleares). Ha sido vocal adscrita de la Comisión General de Codificación para la elaboración de la Propuesta de Código Mercantil de 2013. Entre sus líneas de investigación destacan las relativas al derecho de las nuevas tecnologías y al derecho del turismo. En estos ámbitos es autora de distintas monografías sobre firma electrónica, comercio electrónico, pagos electrónicos o contratos turísticos, entre otras. Ha dirigido y participado en numerosos proyectos de investigación competitivos. Actualmente es investigadora principal del Proyecto de Investigación RTI2018-097225-B-I00 «Plataformas de intercambio electrónico y nuevos modelos económicos disruptivos; problemática jurídica. En particular, el denominado alquiler turístico vacacional».

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

www.uoc.edu/idp

ARTICLE

Els conceptes tributaris de l'establiment permanent i els punts de connexió en relació amb l'adveniment d'*Internet of Things*

Ignasi Belda
Universitat Oberta de Catalunya

Data de presentació: juliol de 2019
Data d'acceptació: juliol de 2020
Data de publicació: març 2021

Resum

La internet de les coses, o *Internet of Things* (IoT), obre un nou paradigma tecnològic en què no solament molts dels objectes quotidians estan connectats a internet, sinó que, a més, aquests tenen delegades facultats per prendre decisions de compra. Tanmateix, els algorismes d'intel·ligència artificial que prenen aquestes decisions normalment no estan ubicats dins de l'electrònica dels objectes connectats a internet, sinó que estan deslocalitzats al *núvol*. Aquest paradigma, doncs, obre nous interrogants en l'àmbit tributari que aquest article analitza. En particular, estudia la definició actual i les evolucions dels conceptes jurídics d'establiment permanent i punts de connexió –o nexe– en relació amb el paradigma tecnològic de l'IoT.

Paraules clau

fiscalitat, noves tecnologies, *Internet of Things*, establiment permanent, punts de connexió, nexe

Tòpic

dret tributari, dret econòmic, tecnologies de la informació, *Internet of Things*

The tax concepts of permanent establishment and connection points in relation to the advent of the Internet of Things

Abstract

The Internet of Things (IoT) opens up a new technological paradigm where not only many everyday objects are connected to the Internet, but also have delegated powers to make purchase decisions. However, artificial intelligence algorithms that take these decisions are not usually located within the electronics of objects connected to the internet, but are in the cloud*. This paradigm, then, brings up new questions in the tax area that this article analyses. In particular, we analyse the current definition and evolution of the legal concepts of Permanent Establishment and Connection Points –or nexus– in relation to the technological paradigm of the IoT.*

Keywords

taxation, new technologies, Internet of Things*, permanent establishment, connection points, nexus*

Topic

tax law, economic law, information technologies, Internet of Things

1. Introducció

L'actual paradigma tecnicoeconòmic, el de l'economia del coneixement, està caracteritzat per un desenvolupament tecnològic exponencial (Castells, 2000; Romera, 2017). Aquesta gran velocitat en el desenvolupament tecnològic provoca que, sovint, el debat jurídic vaja molt endarrerit respecte al progrés inexorable de la tecnologia. N'abunden els exemples en pràcticament totes les àrees del dret: civil, laboral, mercantil i, per descomptat, en l'àmbit tributari.

En el cas concret del dret tributari succeeix, a més, que els paradigmes tributaris fa dècades que han quedat obsolets. Això explica perquè les noves empreses tecnològiques aconsegueixen pagar tipus impositius efectius tan reduïts sense violar les normes tributàries locals ni internacionals. Davant d'aquesta evidència són múltiples les veus doctrinals, nacionals i internacionals, acadèmiques i institucionals, que reivindiquen una actualització substancial dels paradigmes tributaris (Rosembuj, 2015; OECD, 2018; Álamo Cerrillo i Lagos Rodríguez, 2015; Borrego Zabala, 2014; Colin, 2013).

Aquest article, doncs, se centra en dos aspectes molt concrets del dret tributari com són l'establiment permanent (EP) i els punts de connexió o nexe. De fet, diverses veus doctrinals també reivindiquen l'actualització d'aquests dos conceptes jurídics en relació amb el comerç electrònic i l'economia digital, en general (Álamo Cerrillo, 2015). Per ser més concrets, aquest article posa el focus en la relació dels conceptes d'EP i els punts de connexió amb un nou paradigma tecnològic com és el d'*Internet of Things* (IoT) o la internet de les coses i analitza si cal actualitzar aquestes definicions jurídiques, tal com apunten diversos autors acadèmics, o no.

El paradigma tecnològic de l'IoT és el context tecnològic caracteritzat per la connexió massiva d'objectes quotidians a internet. Per si sola aquesta definició tindria poques implicacions tributàries, però la combinació del concepte amb la intel·ligència artificial provoca que els objectes intel·ligents[1] interconnectats a internet ara tinguen l'autonomia suficient per poder realitzar compres de béns i serveis digitals o físics. Aquest fet deixa ja, fins i tot, obsolets els conceptes tributaris més innovadors com el de la presència digital significativa proposat recentment per l'OCDE (OECD, 2015).

1. Vehicles, televisors, neveres, rentadores i qualsevol altra mena d'electrodomèstic.

2. *Internet of Things*

La història d'internet està marcada per la progressiva connexió dels centres productors de dades a la xarxa, en funció de llur velocitat en la generació de dades. Als inicis d'internet solament els centres militars tenien accés a la xarxa, atès que internet és una d'entre moltes innovacions militars que han acabat beneficiant la població civil a més dels fins bèl·lics.[2] Poc més tard, els centres acadèmics van connectar els seus establiments a la xarxa, ja que aquests eren grans centres de producció de dades. A continuació, s'hi van connectar grans empreses basades en la gestió de dades de forma massiva, com els bancs, quedant les empreses industrials relegades d'aquest progrés. El següent pas va ser la democratització de les connexions a internet entre la població general per mitjà dels ordinadors personals. En la segona dècada del segle XXI, les connexions a internet van continuar creixent exponencialment gràcies a la popularització de la telefonia mòbil. De fet, segons dades de l'estudi «Digital 2019: Global Digital Yearbook» (Hootsuite, 2019), a Espanya el 93 % de la població té accés a internet i, de mitjana, cada ciutadà gasta 5 h i 18 m connectat a internet al dia.

Finalment, una volta superada l'onada d'hiperconnexió personal en què cada individu està permanentment connectat a internet per mitjà de múltiples canals –mòbil, ordinador, rellotge, tauleta, televisor, etc.– arriba el moment de connectar els objectes, des de tasses per beure cafè fins a elements del mobiliari urbà –i açò connecta amb el concepte d'*smart city*–. Aquests objectes que ara s'estan començant a connectar a internet són l'última baula de la cadena en la generació d'informació, és a dir, els que generen dades d'interès a menor velocitat i, per tant, seguint la lògica exposada, els últims a ser connectats massivament a internet. I açò és el que es coneix com a IoT.

Ara bé, els avenços que en paral·lel a les telecomunicacions ha experimentat la intel·ligència artificial fa que haguem de fer front a un nou paradigma en què els elements quotidians més insignificants poden prendre decisions per nosaltres, algunes, fins i tot, amb implicacions de despesa. N'abunden els exemples, però solament per il·lustrar el concepte parlarem d'alguns, presents i potencials. El primer exemple més evident i present és el d'algunes neveres intel·ligents –o *smart refrigerator*– que poden detectar quan un producte –llet, ous, etc.– està a punt d'exhaurir-se i poden llançar una comanda de manera completament automatitzada i autònoma. Un altre exemple, en l'àmbit de l'automoció, és quan un cotxe autònom detecta que està baix de bateries i, de forma automàtica, es dirigeix a una «electrolinera» per recarregar les bateries. Finalment, per parlar d'un exemple més utòpic però amb el qual algunes empreses ja estan experimentant, en el futur proper hi haurà assistents personals –tipus l'Alexa d'Amazon– que podran decidir per nosaltres mateixos si ha arribat el moment de comprar roba nova o contractar un o altre servei digital que ens pot interessar.

Per tant, és imprescindible que el debat doctrinal vaja preparant el terreny al legislador amb vista al fet que quan tot això siga una realitat popularitzada, no es produïsquen les contradiccions fiscals a les que malauradament cada volta estem més acostumats (Menéndez Moreno, 2019).

3. L'establiment permanent

Com es comenta a la introducció, l'objecte d'estudi d'aquest article és la relació entre el concepte tributari de l'EP i els punts de connexió amb l'IoT governat per sistemes autònoms amb intel·ligència artificial. Per tant, en aquest punt fixarem l'atenció al concepte d'EP i la seua relació amb el món digital. De fet, els comentaris de l'OCDE al seu model de conveni per evitar la doble imposició (OCDE, 2017) han d'establir les bases doctrinals d'aquest tema. Tanmateix, en els comentaris al 5è. article del model –l'article que defineix el marc regulador dels EP–, en la secció sobre comerç electrònic (paràgrafs del 122 al 131), no s'estableixen amb la precisió necessària la definició de l'EP en relació amb el comerç electrònic internacional, i encara menys en relació amb la prestació de serveis digitals.[3] De fet, el que estableixen els citats comentaris és que solament en determinades circumstàncies es podria determinar que hi ha un «lloc de negocis» i, per tant, un EP, si hi ha un servidor

2. Altres exemples són el radar, els satèl·lits artificials, el GPS o el forn microones.
3. En la secció posterior, sobre l'EP en relació amb la prestació de serveis (paràgrafs del 132 al 169) tampoc se cita, en cap moment, els serveis de caràcter digital.

físic instal·lat al país on es vol fer la imposició i aquest està plenament controlat i operat pel subjecte passiu. La mera existència, per tant, d'una pàgina web, sense un servidor físic ubicat en aquell país, no és un element suficientment constitutiu per establir l'existència d'un EP. És més, si és el cas que hi ha un servidor físic instal·lat al territori, però aquest servidor pertany i és operat per un tercer no vinculat al subjecte passiu, per exemple, un *Internet Service Provider*, tampoc això pot ser considerat un EP. Davant d'aquesta indefinició, per tant, no sorprèn que diversos països importadors de serveis tecnològics[4] no subscriguen aquest criteri, segons informa la mateixa OCDE. Ja que, amb aquest criteri, les compres per internet, és a dir, el comerç electrònic, realitzat a webs que no estan allotjades a servidors locals, no poden ser taxades apropiadament.

Segons les conclusions del Grup d'Experts de la Comissió Europea en Fiscalitat de l'Economia Digital (Comissió Europea, 2014), aquest punt es podria solucionar mitjançant la revisió del paper dels comissionistes en el negoci del comerç electrònic i, sobretot, amb la redefinició de les activitats auxiliars o preparatòries. Ja que, segons les definicions actuals de l'OCDE, perquè un magatzem local puga servir comandes de comerç electrònic d'origen internacional ha de ser considerat com una activitat auxiliar o preparatòria, però el grup d'experts de la CE considera que ara, en l'economia digital, un magatzem d'aquestes característiques no hauria de ser considerat com una activitat auxiliar, sinó central. Certament, que una empresa de comerç electrònic, tipus Amazon, tinga magatzems logístics locals, li dona determinats avantatges competitius respecte d'altres empreses de comerç electrònic que no els tenen. Aquests centres logístics permeten a les empreses servir comandes a les principals capitals en menys de dues hores.

En relació amb tot l'esmentat, en una recent comunicació de la Comissió Europea al Parlament i al Consell Europeu (Comisión Europea, 2018), se subratlla que: «... gràcies a les tecnologies digitals, ara les empreses poden tenir una presència econòmica significativa en la jurisdicció d'un mercat sense que hagen de tenir necessàriament una presència física important. Així doncs, cal comptar amb indicadors alternatius de presència econòmica important a fi de determinar i protegir els drets impositius en relació amb els nous models empresarials digitals».

Els problemes en aquest sentit no solament són endèmics d'Europa. Recentment, el Tribunal Suprem dels EUA ha fet canviar la doctrina a causa del cas Dakota del Sud v. Waifair, et al., núm. 17494, de 21 de juny de 2018 (Falcón i Tella, 2018). En aquest cas, el Tribunal Suprem dona un gir radical a la doctrina tradicional, establerta l'any 1992 amb el cas Quill v. North Dakota, mitjançant la qual els comerciants minoristes no podien quedar gravats als estats on no tenien una presència física, com ara una tenda, una oficina o un magatzem. Ara, però, s'estableix que el requisit de presència física no és correcte i que no constitueix una exigència de la clàusula de comerç. Tanmateix, l'alt tribunal no acaba de precisar quan es dona aquesta presència virtual i econòmica que sí que donaria lloc a una tributació. Tot i que dona per vàlida la norma de Dakota del Sud que exigeix unes vendes mínimes de $100.000 anuals o un mínim de 200 transaccions en el mateix període.

Davant d'aquesta evidència d'una necessitat jurídica no coberta, són múltiples les veus acadèmiques que demanen redefinir el concepte de PE (Álamo Cerrillo, 2015; Álamo Cerrillo i Lagos Rodríguez, 2015; Cruz Padial i Sánchez-Archidona Hidalgo, 2017). Per exemple, Sánchez-Archidona (Sánchez-Archidona Hidalgo, 2016) es pregunta, amb molt de criteri, si «les pàgines web mereixen ser considerades partícips de la vida econòmica d'un país quan el volum de negocis que genera superen en l'actualitat el de les seus físiques radicades en llocs fixes de negocis». Evidentment, l'autor respon afirmativament la qüestió, ja que una pàgina web, encara que estiga situada en un lloc indefinit de l'espai geogràfic, implica una presència permanent en la vida econòmica d'un país tal que pot, en ocasions, arribar a ser una important presència econòmica. Tot i això, l'OCDE ha renunciat al concepte de presència digital significativa basant-se en les expectatives que el projecte BEPS tinguera un impacte major en l'economia del coneixement, determinades mesures antielusió atenuaren certs aspectes dels desafiaments fiscals generalitzats que sorgeixen en l'àmbit digital i que s'implanten nous impostos indirectes al comerç electrònic en destinació.

L'alternativa a la situació actual és el que alguns autors han batejat com a presència digital –o econòmica– significativa (Cruz Padial i Sánchez-Archidona Hidalgo, 2017). La presència digital solament es pot donar per part

4. Xile, Grècia, Mèxic, Portugal i Turquia; i el Regne Unit amb matisos.

d'empreses amb activitats totalment desmaterialitzades, les quals són definides per: *i*) que l'activitat principal de l'empresa siga el comerç de serveis digitals, i que no entre en joc cap activitat o element físic –a part dels servidors–, *ii*) els contractes es generen a distància, *iii*) els pagaments s'efectuen per mitjà de targetes de crèdit o altra forma de pagament electrònica, *iv*) les pàgines web són l'única manera de relacionar-se amb l'empresa, *v*) tots o la major part dels beneficis són imputables a la prestació de serveis digitals, *vi*) el client no té en compte la ubicació ni el domicili del venedor per efectuar les seues compres, i *vii*) el bé o servei digital no requereix la presència física o l'ús d'un producte material diferent d'un ordinador o altres dispositius assimilables. Per tant, atesa una activitat totalment desmaterialitzada, una presència digital significativa ve donada per: *i*) que se signe un nombre significatiu de contractes de subministrament de béns o serveis digitals entre l'empresa i els clients residents en un determinat país, *ii*) que els béns o serveis digitals s'utilitzen o consumisquen, en gran mesura, en el citat país, *iii*) que els clients situats en aquell país efectuen pagaments substancials a favor de l'empresa com a contraprestació d'allò contractat, i *iv*) que una sucursal de l'empresa ubicada en aquell país desenvolupe activitats secundaries, com és el cas de l'assessorament i comercialització dirigits a clients residents en aqueix país.

Cal fer notar, però, que davant d'aquestes definicions, una plataforma «clàssica» de comerç electrònic de béns tangibles i mercaderies, quedaria exclosa de la definició de presència digital significativa, ja que el mer fet de comerciar amb béns tangibles, ja exclou les activitats de la categoria de desmaterialitzades.

4. Els punts de connexió o nexe

El debat sobre els punts de connexió i el nexe és molt similar al de l'EP. Se'ns dubte, aquest és un concepte jurídic que també necessita una profunda revisió amb vista als nous models de negoci de l'economia del coneixement i les veus acadèmiques així ho han fet notar (Cruz Padial i Sánchez-Archidona Hidalgo, 2017).

Deixant de banda les consideracions ja fetes sobre l'EP i el comerç electrònic, el nexe és important per determinar la subjecció fiscal de determinades rendes econòmiques no relacionades amb el comerç de béns i serveis digitals entre empreses i particulars. Ens referim, per exemple, als negocis de la publicitat en línia, la compravenda de dades d'usuaris entre corporacions, o les comissions generades per determinats comissionistes[5] en els negocis d'intermediació de comerç electrònic. Per exemple, la Directiva 2018/0073 del Consell Europeu relativa al sistema comú de l'impost sobre els serveis digitals que grava els ingressos procedents de la prestació de determinats serveis digitals estipula que els drets d'imposició respecte a les rendes obtingudes en les compravendes de dades d'usuaris recauen sobre els estats on estan situats els citats usuaris. Per tant, en aquest cas el nexe és l'estat on estan situats els usuaris sobre els quals s'han recollit les dades i no pas en les jurisdiccions on es materialitzen les compravendes ni als domicilis de les corporacions implicades.

L'*Action* 1 dels BEPS (OECD, 2015) també senyala aquest últim punt quan parla del nexe en els negocis digitals. De fet, en la citada acció es dibuixa un nou tipus de nexe basat en la presència econòmica significativa, definit per mitjà de la combinació de tres tipus d'elements que a continuació es detallen. L'esperit, per tant, és tractar d'identificar les situacions en què les corporacions digitals participen en la vida econòmica d'un determinat país d'una forma regular i sostinguda, sense la necessitat de tenir presència física de cap tipus en aquell país. D'aquesta manera, les rendes, per si soles, no serien suficients per establir un nexe, però en combinació amb aquests altres tipus d'elements, sí que es pot determinar una presència econòmica significativa al país en qüestió.

Els tres tipus d'elements que definirien aquest nou concepte de nexe són: *i*) els factors relacionats amb el nivell de les rendes, *ii*) factors digitals, i *iii*) factors relacionats amb l'usuari.

Pel que fa al primer tipus de factors, els relacionats amb el nivell de les rendes, l'OCDE especifica que cal tenir en compte tres elements. En primer lloc, el tipus de transaccions cobertes. És a dir, cal tenir en compte específicament les transaccions digitals, però també altres tipus

5. Com és el cas d'Amazon o eBay.

de transaccions remotes que no són precisament digitals, com ara les vendes telefòniques o les vendes per correu. Això, suggereix l'OCDE, s'ha de fer així per desincentivar dinàmiques de compravenda en línia en què l'últim pas de la compra es realitza per via telefònica mitjançant un *call center*. El segon element a tenir en compte és el nivell del llindar. És a dir, cal especificar un llindar per sobre del qual es considera que hi ha presència econòmica significativa i aquest ha de ser suficientment elevat per minimitzar la burocràcia improductiva, però suficientment baix per no deixar passar situacions evidents en funció de la mida del mercat en qüestió. També l'OCDE recomana que aquest llindar siga fixat en la moneda local per evitar manipulacions i, alhora, que es prevegin elements tècnics per evitar el frau de llei mitjançant la fragmentació de la compra de forma artificial per mitjà de diverses jurisdiccions. Finalment, cal establir mecanismes de control –similars, potser, als establerts amb l'IVA, diu l'OCDE– perquè les agències tributàries puguen tenir un seguiment i control precís del nivell de vendes d'una determinada empresa internacional en aquella jurisdicció.

Pel que fa al segon tipus de factors, els digitals, l'OCDE suggereix que es tinguen en compte factors com la possessió d'un domini local; la implementació d'una plataforma digital local que, per exemple, estiga en l'idioma local, oferisca descomptes seguint criteris locals o cumplisca amb la normativa de consum local, etc.; o que l'empresa oferisca mètodes de pagament locals amb, per exemple, preus calculats amb la moneda local.

Finalment, pel que fa al tercer tipus de factors, els relacionats amb l'usuari, l'OCDE suggereix tenir en compte elements com el nombre mensual d'usuaris actius, el nombre de compravendes realitzades –o contractes conclosos– o l'origen de les dades d'usuaris recollides.

La combinació de tots aquests factors, segons l'OCDE, és el que conduirà a la definició de noves definicions de nexes i punts de connexió. En aquesta línia, països com Israel ja han redefinit el concepte de nexe[6] amb la presència digital significativa basada en: a) nombre de contractes en línia tancats, b) nombre d'usuaris israelians que fan ús dels serveis, c) opcions locals com ara l'ús de la llengua hebrea, preus calculats amb ILS –la moneda d'Israel–, o descomptes basats en ofertes locals, i d) volum de negoci generat a Israel. Això sí, aquesta redefinició no aplica en aquells llocs on hi ha un conveni signat de no doble imposició. També en el cas d'Hongria es fa ús de les recomanacions de l'OCDE per establir la definició de presència digital significativa en la seua taxa sobre la publicitat, fixant llindars en moneda local, el fòrint, o l'ús de l'hongarès a la publicitat en línia.

En canvi, en altres jurisdiccions d'àmbit nord-americà, on la llengua local és l'anglès i la moneda el dòlar, probablement els criteris de l'OCDE no són suficients. És segurament per això que diversos estats nordamericans, com Colorado o Nova York, han desenvolupat un nou concepte de nexe conegut com a *click-through*[7] (Lunder i Pettit, 2015). En els negocis d'intermediació, com és el cas d'Amazon.com, Alibaba.com o Ebay.com, el paradigma del nexe *click-through* estipula que la generació de valor succeeix quan l'intermediari –és a dir, la plataforma d'intermediació– ofereix productes d'un tercer que finalment són comprats. A més, aquesta operació té lloc a l'espai virtual creat en destinació, és a dir, a l'ordinador del comprador. Per tant, la generació de valor no es produeix en un servidor remot que pot estar ubicat en alguna part concreta del planeta o un núvol deslocalitzat que empreses com Amazon, Google o Microsoft han popularitzat.

En el cas de Colorado, la normativa exigeix tres obligacions informatives a les plataformes d'intermediació. La primera és informar els seus clients residents a Colorado que qualsevol compra mitjançada digitalment realitzada per ells està subjecta a aquesta nova taxa. La segona obligació és informar anualment a cadascun dels seus clients residents a Colorado sobre les seves compres intermediades digitalment, ja que, formalment, el contribuent no és la plataforma d'intermediació, sinó la persona –física o jurídica– que realitza la compra. I, finalment, les plataformes d'intermediació han d'informar l'agència tributària de Colorado sobre el detall de les vendes realitzades en aquest estat. Les multes per incomplir aquestes obligacions d'informació són de $5 per cada dada incomplerta en el context de la primera obligació i $10 per la segona i tercera obligació.

6. Circular Administrativa N. 04/2016, d'11 d'abril de 2016, desenvolupada per clarificar les circumstàncies amb les quals una empresa estrangera que desenvolupa activitats en línia («activitats via internet») pot quedar subjecta a l'impost de societats a Israel.
7. Col·loquialment conegut com a «Lleis Amazon».

D'aquesta manera, la normativa aconsegueix que, en haver dos implicats en el procés impositiu: la plataforma i el comprador, les autoritats puguen creuar dades d'uns i d'altres per fer aflorar, així, el frau amb millors garanties que si el contribuent efectiu fora únicament la plataforma d'intermediació. Amb aquest esquema tributari, la plataforma d'intermediació té menys incentius per al frau, sent els compradors finals sobre els quals recau l'obligació tributària final.

Tot i l'aparent idoneïtat d'aquest innovador concepte de nexe, sobretot a Colorado, la iniciativa està vivent un fort debat doctrinal en relació amb la seua constitucionalitat. El motiu és que les lleis americanes prohibeixen expressament taxar empreses que no estan domiciliades en un determinat estat, a no ser que es puga demostrar una forta connexió o nexe entre les operacions de l'empresa i l'estat en qüestió i, segons alguns acadèmics, el *click-through* no siga un punt de connexió prou fort.

5. IoT, la intel·ligència artificial i la fiscalitat

Analitzats els conceptes jurídics d'EP i el dels punts de connexió i descrit el concepte de l'IoT en relació amb la intel·ligència artificial, vegem la interrelació d'aquests conceptes a efectes tributaris.

Ja hem analitzat com l'OCDE –i conseqüentment així ho preveuen la gran majoria de jurisdiccions– recomana limitar el concepte d'EP a l'estricta presència física. Tanmateix, alguns països, seguint les recomanacions de les veus doctrinals, estan començant a experimentar amb redefinicions que passen per l'establiment d'una presència digital significativa. Tanmateix, quan analitzem el detall del que es defineix com a presència digital significativa, veiem que gran part dels elements que defineixen el concepte, en particular els digitals i els relacionats amb l'usuari, estan pensats per interaccions home-màquina.

En la disciplina de les tecnologies de la informació, les interaccions home-màquina, en contraposició de les interaccions home-home o màquina-màquina, són aquelles interaccions entre els individus –persones naturals– i els dispositius. Les interaccions home-màquina sempre es realitzen per mitjà d'interfícies que tracten de ser el més amigables possibles per a la ment humana. Per exemple, tracten d'exposar la informació en llenguatge natural –i no pas en codi binari–, de mica en mica tracten també de recollir la informació en llenguatge natural[8], ens mostren la informació mitjançant imatges en lloc d'especificacions tècniques, o tracten d'ordenar la informació de tal manera que siga fàcilment digerible per la ment humana. No en va hi ha una puixant professió derivada de la psicologia que es consagra en el disseny d'interfícies home-màquina amigables.[9] Amb tots aquests elements, la definició de la presència digital significativa i els seus factors digitals, com ara l'ús d'una llengua local, una moneda local o promocions que culturalment encaixen en un determinat context social,[10] tenen sentit, ja que estan pensats expressament per preveure les interaccions home-màquina.

Tanmateix, si ara ens traslladem al món de l'IoT, la interacció entre els dispositius són interaccions màquina-màquina. Per tant, els elements que recullen els factors digitals que defineixen el concepte de la presència digital significativa, com ara l'ús de llengües locals o, fins i tot, l'ús de moneda local per materialitzar les transaccions econòmiques, deixen de tenir sentit. En el cas de les llengües locals, les màquines no es comuniquen entre elles per mitjà d'interfícies amigables per a la ment humana, sinó per mitjà del que es coneix com a API –de les sigles en anglès d'*Application Programming Interface*–, que en cap cas podem dir que s'assimilen a un llenguatge natural. Una cosa semblant passa amb els mitjans de pagament, en què els dispositius poden fer servir criptoactius (Belda, 2019) per materialitzar les transaccions econòmiques, atès que l'ús de criptomonedes per part dels dispositius quasi-impossibilita el control econòmic per part de les autoritats tributaries, monetàries o duaneres.

Si ara posem el focus en els factors relacionats amb el nivell de vendes i els factors relacionats amb l'usuari que defineixen la presència digital significativa apareix una

8. N'abunden els exemples, però Siri d'Apple o Alexa d'Amazon en són dos de representatius.
9. Més coneguda pel seu nom en anglès UX & UI Designer.
10. Per exemple, promocions de Nadal, promocions per a sant Valentí o promocions de llibres per al dia de sant Jordi.

nova dimensió i és qui (què?) pren la decisió de compra i on està ubicat aquest ens. En les interaccions home-màquina, qui pren les decisions és un individu localitzat en una jurisdicció concreta –és a dir, per definició no es pot deslocalitzar– i, sobretot, amb personalitat jurídica pròpia, la qual cosa facilita la identificació per la meritació d'imposts com l'IVA, etc. Tanmateix, en el món de l'IoT la «intel·ligència» de l'objecte tant pot estar ubicat dins de l'electrònica del propi objecte com, el més usual, al núvol.[11] Per tant, si la «intel·ligència» que té el poder de compra no està ubicada en la jurisdicció, veiem que la presa de decisions es desacobla de l'ens que acaba gaudint del bé o servei digital o físic.

Aquest concepte ens condueix a l'última reflexió rellevant del tema que ens ocupa i és on s'ha d'ubicar l'obligació de tributació. De fet, la reflexió és vàlida tant per a serveis com béns digitals o serveis,[12] i també per a la contractació de béns o serveis físics. Per simplificar, però, d'ara endavant solament parlarem de serveis digitals.

Vist el paradigma que ens obre l'IoT, hi hauria tres opcions. La primera és «en origen» és a dir, el lloc des d'on es presta el servei digital. La segona és des d'on s'ha pres la decisió de compra, per tant, parlarem del «núvol», per ser la ubicació més comuna on s'ubica la «intel·ligència» de l'IoT. I, finalment, la tercera, «en destí», és a dir, el lloc des d'on un individu gaudeix del servei digital.

La resposta a la pregunta formulada, és a dir, on radica l'obligació tributària, ha d'estar necessàriament vinculada a la generació del valor afegit. Per tant, tot i estar l'opinió pública en contra, tal com es dedueix de les dotzenes d'articles periodístics que cada setmana apareixen en la premsa generalista i els discursos dels nostres dirigents polítics, seguint les recomanacions de l'OCDE, es pot constatar a la normativa vigent[13] que l'obligació tributària se situa en aquells llocs on estan domiciliades les empreses tecnològiques i, per tant, presumiblement, de forma directa o indirecta, allà on s'han desenvolupat els algorismes que implementen els sistemes d'intel·ligència artificial autònoms. Tot i l'anterior, com ja s'ha insistit, cal tenir en compte que la normativa vigent no ha estat dissenyada pensant amb un paradigma tecnicoeconòmic de l'economia del coneixement.

La imposició fiscal en l'economia del coneixement és una temàtica relativament nova però que, a causa del gran interès que ha despertat en la societat en general i, en particular, en el legislador, comença a haver un gran volum de literatura al respecte. Tot i la novetat de la temàtica, i en previsió d'un món abastament globalitzat, la Lliga de les Nacions ja va encarregar al principi de la dècada de 1920 un estudi a quatre economistes sobre els impactes de la doble imposició internacional, des d'un punt de vista acadèmic i científic (Bruins, Einaudi, Seligman i Stamp, 1923). La principal conclusió d'aquest estudi és que hi ha punts de connexió que poden guiar la imposició: *i*) l'origen de la riquesa o les rendes; *ii*) el lloc on s'ubica la riquesa o les rendes; *iii*) el lloc des d'on es controla la riquesa o les rendes; i *iv*) el lloc de residència o domicili de la persona que té el dret a disposar de la riquesa o les rendes. Dels quatre factors, l'estudi determina que el primer i l'últim són els que haurien de tenir més prioritat a l'hora de dissenyar nous sistemes impositius.

Per tant, traslladant aquesta conclusió als temps moderns –100 anys després de la conclusió del citat estudi–, hem de dir que la conclusió d'aquest estudi històric reafirma l'*status quo* actual, ubicant les obligacions tributaries «en origen», és a dir, allà on estan domiciliades les empreses tecnològiques que proveeixen els serveis digitals a clients de tot el món. Tot i això, i tenint en compte que la ubicació de les empreses tecnològiques està molt concentrat en una regió mundial, concretament al nord de l'estat nord-americà de Califòrnia, el conegut com a *Silicon Valley*, aquesta política crea situacions econòmiques molt desequilibrades, les quals condueixen a discursos proteccionistes i aquests, alhora, cap a polítiques fiscals unilateralistes (Sánchez-Archidona Hidalgo, 2019) que tracten de promoure una imposició «en destí». Així ho estem veient aquests darrers mesos amb la legislació de l'impost

11. La computació al núvol, concepte tecnològic més conegut amb el seu nom anglès, *cloud computing*, és el paradigma tecnològic mitjançant el qual la capacitat de càlcul es deslocalitza en un entorn difús i remot que metafòricament es representa com un núvol. El maquinari concret que realitza la computació és canviant i remot, per tant, gairebé impossible de localitzar a efectes tributaris.
12. No és objecte d'anàlisi la reflexió entre serveis i béns digitals, però se'ns dubte, aquest és un altre tema que també presenta grans dificultats i dilemes jurídics.
13. Convenis de no doble imposició, text refós de la Llei de l'impost sobre la renda de no residents, etc.

sobre determinats serveis digitals (Belda, 2019) i que ja està causant greus conflictes diplomàtics a Espanya[14] i a altres països.[15]

En definitiva, tot i que sembla que la voluntat popular i política és la contrària, tant els organismes internacionals, com l'OCDE, i els estudis històrics citats recomanen ubicar les obligacions tributàries «en origen».

Discussió

Amb l'anàlisi de la situació tributària que es crea amb l'IoT hem vist que la tònica general és molt similar a la que es dona en la imposició de la resta de l'economia digital, és a dir, que de forma general, tal com actualment estan definits els conceptes com l'EP o els punts de connexió, l'obligació tributària s'ubica «en origen», és a dir, al lloc on estan domiciliades les empreses tecnològiques.

Tanmateix, en el cas particular de l'IoT s'obre una nova derivada. Aquesta nova derivada és que qui pren la decisió de compra està deslocalitzat, atès que són sistemes d'intel·ligència artificial residents al núvol. Per tant, les evolucions internacionals –Israel, Hongria, Colorado o Nova York, entre d'altres– que s'estan desenvolupant per redefinir els conceptes d'EP o de nexe per tal de reubicar l'obligació tributària «en destí», poden quedar ràpidament obsoletes, ja que els elements culturals i locals que exigeixen aquestes legislacions es poden veure circumdats per ens electrònics que treballen de manera deslocalitzada, usant criptomonedes com a mitjà de pagament i sense fer ús de cap llenguatge natural sinó llenguatges artificials preprogramats. Per tant, en aquests supòsits difícilment el legislador podrà defensar que la generació de valor s'ha situat «en destí», perquè ni el venedor –o prestador del servei–, ni tampoc la decisió de compra es produeix «en destí». L'única cosa que se situa «en destí» és el beneficiari últim. En definitiva, caldrà retorçar molt l'argumentació juridicopolítica per defensar que allà on el bé o servei és consumit –i per tant on el valor de la cosa és «destruït»– és allà on s'ha generat el valor de la transacció econòmica i, com a conseqüència, on merita la imposició. Sí que és més fàcil de justificar, però, que una part de la generació de valor de la transacció econòmica es genera allà on es pren la decisió de compra.

En opinió d'aquest autor, caldria buscar una fórmula justa i equilibrada per taxar aquest tipus de consum, immaterial, entre allà on es genera, «en origen», tal com recomanen les institucions internacionals; i allà on es pren la decisió de compra. Quan el comprador és un ser humà, i per tant, és aquest qui pren la decisió, és senzill ubicar-lo geogràficament i fer-lo taxar, per exemple, amb el paradigma del nexe *click-through*. Tanmateix, per ubicar geogràficament un ens autònom i automàtic caldrà desenvolupar conceptes com la personalitat jurídica dels robots per determinar la *residència fiscal* dels ens digitals. En matèria de personalitat jurídica de les entitats digitals ja s'ha endegat el debat doctrinal, però sempre en el terreny del dret penal (Quintero Olivares, 2017; Vallejo de Hoyos, 2017). Tenint perfectament identificades les entitats digitals, es podrien fins i tot elaborar protocols de transparència digital que permitisquen inspeccions digitals realitzades per ens igualment autònoms i automàtics. En aquest sentit, les ciències de la informació han avançat de manera substancial en l'elaboració de protocols informàtics per al compliment de la normativa legal i la reputació dels agents intel·ligents (Perreau de Pinninck Bas, Sierra i Schorlemmer, 2010).

Tot i l'anterior, ja hem vist que l'opinió popular més estesa és la de transportar les obligacions tributàries «d'origen» a «destí» i, de fet, algunes jurisdiccions així ho estan treballant. Aquest tipus de polítiques pot obrir, però, una via molt perillosa i és la d'anular els incentius per implantar incentius fiscals a l'R+D+i. Molts països desenvolupats, com és el cas d'Espanya, França o Canadà, estan fent importants esforços pressupostaris per al foment de l'R+D+i per mitjà d'incentius fiscals (Belda, 2016). L'aposta política que hi ha al darrere d'aquest esforç és que, aquests països, mentre que ara són importadors tecnològics nets, en el mitjà o llarg termini puguen equilibrar aquesta balança de pagaments. D'altra banda, altres països com Alemanya, han apostat per no fer cap esforç pressupostari en aquest sentit i, és més, intenten per via diplomàtica que els països del seu entorn limiten les actuacions en aquest sentit (HM Treasury, HM Revenue i Customs, David Gauke, 2014). Per tant, eliminant les

14. Montero considera «inadmisible» l'amenaça d'EUA i confirma la taxa Google: «Nuestra condición es firme». *El Mundo*. (17/07/2019).
15. «EE UU investiga la 'tasa Google' que ha aprobado Francia este jueves». *El País*. (11/07/2019).

obligacions tributaries «en origen» pot fer que a nivell pressupostari els estats tinguen pocs incentius per fomentar l'R+D+i, almenys, en el curt termini[16].

Conclusió

En el cas particular de l'economia del coneixement, hi ha una gran pressió popular per traslladar la pressió fiscal «d'origen» a «destí», és a dir, de fer pagar les empreses tecnològiques allà on els seus béns i serveis són consumits i no pas on són produïts.

Per contra, institucions internacionals com l'OCDE, dicten directives per mantenir la tributació en origen i així es fa en la majoria de països, tot i alguns moviments tímids de països desenvolupats per canviar-ho. Tímids en el sentit que tindran poc impacte. Per exemple, en el cas d'Israel, la prevalença és la dels tractats internacionals, que, per norma general, mantenen la tributació «en origen». Per tant, la tributació «en destí» solament aplicarà als negocis creuats entre Israel i països sense conveni de no doble tributació, és a dir, aquells on la relació econòmica amb Israel és tan minsa que no ha pagat la pena desenvolupar un conveni específic de no doble tributació.

Aquest article ha analitzat el cas concret de l'IoT i com hauria de ser el paradigma tributari per taxar de forma justa la generació de valor. La conclusió principal és que en el cas de l'IoT no convé modificar els esquemes tributaris, ja que en desplaçar la tributació «a destí» es desincentiva els estats a invertir en el desenvolupament tecnològic del país. Una tributació «en destí» dona nous recursos econòmics a aquells països que no han fet un correcte foment del desenvolupament tecnològic del sector empresarial i, per contra, treu recursos econòmics a aquells territoris que sí que han fet l'esforç d'adaptar el teixit econòmic a la nova economia.

En conseqüència, per taxar correctament l'economia del coneixement, d'una forma justa i equitativa segons els nostres valors constitucionals,[17] cal buscar altres focus de tributació, com poden ser els serveis digitals, la publicitat en línia o els negocis derivats de les anàlisis de dades. De fet, justament aquests tres elements de tribut són en els que es focalitza la Directiva 2018/0073 del Consell Europeu relativa al sistema comú de l'impost sobre els serveis digitals que grava els ingressos procedents de la prestació de determinats serveis digitals. Tot i això, com que aquesta directiva presenta importants mancances conceptuals i tècniques a les quals ja han apuntat múltiples autors (Menéndez Moreno, 2019; Belda, 2019), aquest autor ha proposat un nou paradigma de tributació sobre els serveis digitals basat en la meritació de l'IVA dels serveis digitals prestats a títol gratuït tenint com a única contraprestació les dades de navegació dels propis usuaris (Belda, 2020).

Al marge dels elements de tribut sobre els quals descansa la proposta del Consell Europeu, també s'han identificat a la literatura altres fonts de tributació relacionades amb l'economia del coneixement, com ara la criptoeconomia o la robòtica. Pel que fa al primer àmbit, la criptoeconomia, Bal (Bal, 2014) ha desenvolupat una profunda revisió internacional de les diferents modalitats de tributació que es poden donar en aquest context. En el cas particular del *blockchain* i els *smart-contracts*, aquest autor ha desenvolupat un estudi sobre l'impacte que pot tenir la popularització d'ambdues tecnologies sobre l'impost espanyol sobre els actes jurídics documentats.

Finalment, la imposició a la robòtica és un tema controvertit. Mentre que determinats autors acadèmics defensen la seua imposició (Sánchez-Archidona Hidalgo, 2019), altres com aquest (Belda, en premsa) defensen treure el focus de la tributació d'aquestes tecnologies.

16. No cal oblidar que una de les tres funcions dels impostos és la de servir com a instrument de política econòmica; a més del sosteniment de la despesa pública i la redistribució justa i equitativa de la riquesa (Belda, 2019). L'ús d'incentius fiscals per al foment de l'R+D+i encaixa dins d'aquesta primera finalitat en la mesura que s'utilitzen per ordenar –o, almenys, per ajudar a dirigir– el funcionament econòmic i empresarial del país en una determinada direcció.
17. 17 D'acord amb el que estableix l'article 31.1 de la Constitució espanyola.

Bibliografia

ÁLAMO CERRILLO, R. (2015). La inadecuación del concepto de establecimiento permanente y las propuestas de cambio de la OCDE. *Quincena Fiscal*(5), 1-8.

ÁLAMO CERRILLO, R. i LAGOS RODRÍGUEZ, G. (2015). Necesidad de adaptación de los conceptos tributarios a la realidad económica digital. *Quincena Fiscal*(3), 19-30.

BAL, A. M. (2014). *Taxation of virtual currency.* Leiden University.

BELDA, I. (en prensa). ¿Por qué no debemos tasar la robótica? Argumentaciones en contra de tasar la robótica. *Nueva Fiscalidad.*

BELDA, I. (2016). *Fiscalitat internacional del coneixement*. Universitat Oberta de Catalunya.

BELDA, I. (2019). La constitucionalidad de los gravámenes sobre las rentas virtuales o potenciales en contraposición a la de los gravámenes sobre las rentas ficticias o inexistentes. *Revista Aranzadi Doctrinal,* 9, 1-6.

BELDA, I. (2019). La cripto-economia, una aproximació des de la fiscalitat. *Revista d'Internet, Dret i Política,* 30, 1-12.

BELDA, I. (2019). La difícil comprobación del Impuesto sobre Determinados Servicios Digitales proyectado en contraposición a otras soluciones adoptadas en el de-recho internacional. *Quincena Fiscal,* 17, 1-7.

BELDA, I. (2020). Una nueva propuesta tributaria para la justa tributación de la eco-nomía digital en base a una reinterpretación de la ley del Impuesto Sobre el Valor Añadido. *Nueva Fiscalidad*, 1, 177-206.

BORREGO ZABALA, B. (2014). La necesaria adaptación de los tributos a las nuevas tendencias de los negocios electrónicos. *Revista de Internet, Derecho y Política*(18), 51-59.

BRUINS, EINAUDI, SELIGMAN i STAMP, J. (1923). *Report on Double Taxation submitted to the Financial Committee.* Ginebra: League of Nations.

CASTELLS, M. (2000). *La era de la información* (Vol. 1: La sociedad red). Madrid: Alianza Editorial.

COLIN, N. (2013). Corporate Tax 2.0: Why France and the world need a new tax system for the digital age. *Forbes*.

COMISIÓN EUROPEA (2018). Un sistema impositivo justo y eficaz en la Unión Europea para el Mercado Único Digital. *Comunicación de la Comisión al Parlamento Europeo y al Consejo.*

COMISSIÓ EUROPEA (2014). *Report: Commission Expert Group on Taxation of the Digital Economy.*

CRUZ PADIAL, I. i SÁNCHEZ-ARCHIDONA HIDALGO, G. (2017). Economía digital, establecimiento permanente y presencia digital significativa tras las conclusiones del informe GEFED. *Quincena Fiscal* (18), 1-22.

FALCÓN i TELLA, R. (2018). El "nexus" en la doctrina del Tribunal Supremo de Estados Unidos: el asunto Dakota del Sur v. Wayfair. *Quincena Fiscal*(18), 1-3.

HOOTSUITE (2019). Digital 2019: Global Digital Yearbook (España).

LUNDER, E. K. i PETTIT, C. A. (2015). *"Amazon Laws" and Taxation of Internet Sales: Constitutional Analysis.* Congressional Research Service.

MENÉNDEZ MORENO, A. (2019). El nuevo Impuesto sobre determinados servicios digitales. *Quincena Fiscal*(6), 7-16.

OCDE (2017). *Model Tax Convention on Income and on Capital: Condensed Version.* Paris: OCDE.

OECD (2015). *Addressing the Tax Challenges of the Digital Economy, Action 1 - 2015 Final Report.* Paris: OECD Publishing.

OECD (2018). T*ax Challenges Arising from Digitalisation - Interim Report.* Paris: OECD Publishing.

PERREAU DE PINNINCK BAS, A., SIERRA, C. i SCHORLEMMER, M. (2010). A multiagent network for peer norm enforcement. *Autonomous Agents and Multi Agent Systems,* 21, 397-424.

QUINTERO OLIVARES, G. (2017). La robótica ante el Derecho Penal: el vacío de respuesta jurídica a las desviaciones incontroladas. *Revista Electrónica de Estudios Penales y de la Seguridad*, 1, 1-23.

ROMERA, F. (2017). *Una aproximación histórica y apasionada al sistema de in-novación andaluz desde el Parque Tecnológico de Andalucía.* Academia Andaluza de Ciencia Regional, Sevilla.

ROSEMBUJ, T. (2015). *Taxing Digital.* El Fisco - Gabinete Jurídico Estudios Legales Tributarios.

SÁNCHEZ-ARCHIDONA, Hidalgo G. (2016). La influencia de la economía digital en el concepto de establecimiento permanente en un entorno post-beps. *Quincena Fiscal*(13), 1-17.

SÁNCHEZ-ARCHIDONA, Hidalgo G. (2019). La tributación de la robótica y la inteligencia artificial como límites del Derecho financiero y tributario. *Quincena Fiscal*, 12.

SÁNCHEZ-ARCHIDONA, Hidalgo G. (2019). Unilateralismo fiscal en el siglo XXI. *Quincena Fiscal*(1), 1-17.

TREASURY, H.M.,REVENUE i CUSTOMS, H. M. i GAUKE, D. (2014). Germany – UK Joint Statement. Proposals for New Rules for Preferential IP Regimes.

VALLEJO DE HOYOS, C. (2017). *Inteligencia Artificial* (Trabajo de Fin de Grado ed.). Almería: Universidad de Almería.

Citació recomanada

BELDA, Ignasi (2021). «Els conceptes tributaris de l'establiment permanent i els punts de connexió en relació amb l'adveniment d'*Internet of Things*». *IDP. Revista d'Internet, Dret i Política*, núm. 32, pàgs. 1-13. UOC [Data de consulta: dd/mm/aa]
http://dx.doi.org/10.7238/idp.v0i32.3209

Sobre l'autor
Ignasi Belda
ibeldareig@gmail.com

Doctor en intel·ligència artificial. Ha destacat en la seua trajectòria emprenedora en l'àmbit de la biotecnologia, en què ha fundat diverses empreses biotecnològiques, com Intelligent Pharma, i ha rebut 15 premis per aquesta trajectòria, entre els quals cal destacar el Premi Princesa de Girona 2014. També ha ostentat diversos càrrecs públics de responsabilitat com, per exemple, director general del Parc Científic de Barcelona o vicepresident d'APTE, la xarxa de parcs científics i tecnològics d'Espanya. En l'actualitat, està reali-tzant una segona tesi doctoral en dret fiscal i tributari, després d'haver cursat un màster en Fiscalitat.

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

www.uoc.edu/idp

ARTÍCULO

Estudio del tratamiento y transferencia de datos de mensajería financiera entre la Unión Europea y Estados Unidos a los efectos de la lucha contra la financiación del terrorismo

Covadonga Mallada Fernández
Universidad de Valladolid

Fecha de presentación: marzo de 2020
Fecha de aceptación: junio de 2020
Fecha de publicación: marzo de 2021

Resumen

En este artículo analizaremos el intercambio de información entre la Unión Europea y Estados Unidos para luchar contra la financiación del terrorismo dentro del acuerdo TFTP: «Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la UE a los Estados Unidos a efectos del Programa de seguimiento de la financiación del terrorismo». Así pues, en primer lugar, haremos una pequeña introducción de la situación actual de la lucha contra la financiación del terrorismo en Europa. En segundo lugar, analizaremos los acuerdos de intercambio de información entre Europa y Estados Unidos. En tercer lugar, nos detendremos en el proyecto en ciernes del sistema europeo de seguimiento de la financiación del terrorismo (TFTS), y, ya, por último, en las conclusiones, intentaremos efectuar un análisis crítico de la situación actual y cómo creemos que se desarrollará este intercambio de información dentro del marco del TFTP y del TFTS en un futuro próximo.

Palabras clave

financiación del terrorismo, intercambio de información, sistema europeo de seguimiento de la financiación del terrorismo, SWIFT

Study on the processing and transfer of financial messaging data between the European Union and the United States for the purposes of the fight against the financing of terrorism

Abstract

In this article there will be an analysis of the exchange of information between the European Union and the United States in order to fight against the financing of terrorism within the TFTP agreement: "Agreement between the European Union and the United States of America relating to the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Financing Tracking Programme." As such, firstly, there will be a short introduction on the current situation in the fight against the funding of terrorism in Europe. Secondly, we will analyse the agreements on the exchange of information between Europe and the United States. Thirdly, we will study the incipient project that is the European Terrorist Finance Tracking System (TFTS), and lastly, in the conclusion we will attempt to carry out a critical analysis of the current situation and how we believe this exchange of information will be developed within the framework of the TFTP and the TFTS in the near future.

Keywords

financing of terrorism, exchange of information, European Terrorist Financing Tracking System, SWIFT

1. Introducción

Antes de comenzar con el estudio del tratamiento y transferencia de datos de mensajería entre la Unión Europea y Estados Unidos a los efectos de la lucha contra la financiación del terrorismo (TFTP), vamos a analizar la situación actual de la lucha contra el terrorismo y su financiación en Europa. Así pues, la vigente Estrategia de la Unión Europea de lucha contra el terrorismo se centra en cuatro pilares: «prevenir, proteger, perseguir y responder». Además, estos cuatro pilares siempre se apoyan en el intercambio de información con terceros países y organismos internacionales.

a) Primer pilar: prevenir

En este primer pilar, la UE se ha centrado en la legislación preventiva para evitar la radicalización. Desde este pilar, se ha elaborado la Estrategia de la Unión Europea para luchar contra la radicalización y la captación de terroristas en 2008, que fue revisada en junio de 2014 con objeto de incluir medidas de lucha contra los lobos solitarios, los combatientes extranjeros terroristas y el uso de redes sociales por parte de los terroristas.

b) Segundo pilar: proteger

Dentro de este bloque se refuerza la seguridad en las fronteras exteriores, se mejora la seguridad de los transportes, se protegen los objetivos estratégicos y, por último, se reduce la vulnerabilidad de las infraestructuras críticas. Todo ello en aras de proteger a la ciudadanía y las infraestructuras y reducir la vulnerabilidad ante los atentados. Así pues, para dar respuesta a este segundo bloque, se dictó en abril de 2016 la Directiva (UE) 2016/681, que reglamenta la utilización de los datos del registro de nombres de los pasajeros (PNR).

c) Tercer pilar: perseguir

Este pilar se centra en la persecución de las organizaciones terroristas a fin de desmantelarlas y enjuiciarlas. Al respecto, la UE ha centrado sus esfuerzos en las siguientes líneas de actuación:

- reforzar las capacidades nacionales;
- mejorar la cooperación y el intercambio de información entre las autoridades policiales y judiciales;
- combatir la financiación del terrorismo; y
- privar a los terroristas de sus medios de apoyo y comunicación.

En este marco se ha desarrollado, por un lado, la normativa preventiva de lucha contra la financiación del terrorismo, es decir, la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018 por la que se modifica la Directiva (UE) 2015/849, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y las Directivas 2009/138/CE y 2013/36/UE, y, por otro, la normativa punitiva con la tipificación penal de los delitos de terrorismo a través de la Directiva relativa a la lucha contra el terrorismo. Esta directiva introduce la tipificación penal del adiestramiento o el viaje con fines terroristas; la organización o facilitación de este tipo de movimientos; la aportación o recaudación de fondos en relación con grupos o actividades terroristas; y, por último, la financiación del terrorismo.

d) Cuarto pilar: responder

En este pilar, la estrategia se centra en desarrollar y gestionar planes para poder reducir las posibles consecuencias de un ataque terrorista. Estos planes incluirían los siguientes puntos[1]:

- la elaboración de dispositivos de coordinación de la UE en caso de crisis;
- la revisión del mecanismo de protección civil;
- la elaboración de instrumentos de evaluación de riesgos; y
- la puesta en común de buenas prácticas en la asistencia a las víctimas del terrorismo.

1. Así pues, podemos destacar entre las prioridades de los últimos años de la Estrategia de lucha contra el terrorismo las siguientes: «definir los mecanismos de aplicación de la cláusula de solidaridad por la UE, mediante una Decisión del Consejo adoptada en junio de 2014; revisar los dispositivos de coordinación de la UE en caso de emergencias y crisis, sustituidos en junio de 2013 por el Dispositivo Integrado de Respuesta Política de la UE a las Crisis (DIRPC); y revisar la legislación de la UE en materia de protección civil a finales de 2013».

Por otro lado, dentro de esta estrategia se encuentra el Reglamento para reforzar los controles en las fronteras exteriores, adoptado por el Consejo el 7 de marzo de 2017, mediante el cual se modifica el Código de fronteras Schengen. Con este reglamento se obliga a los Estados miembros a llevar a cabo comprobaciones sistemáticas de todas las personas que crucen las fronteras exteriores mediante la consulta de las correspondientes bases de datos[2].

Por último, también en relación con esta estrategia se ha creado en enero de 2016 el Centro Europeo de Lucha contra el Terrorismo (ECTC/CELT). Enmarcado dentro de la Europol, en dicho organismo se desarrollan varios proyectos, entre ellos el que nos ocupa en este trabajo: el proyecto TFTP. Además, el ECTC trabaja en estrecha colaboración con otros centros operativos de Europol, como el Centro Europeo de Delitos Cibernéticos (EC3) o el Centro Europeo de Tráfico Ilícito de Migrantes (EMSC).

A través del CELT, los Estados miembros pueden intercambiar información y cooperar en asuntos relacionados con los combatientes terroristas extranjeros, el tráfico de armas de fuego ilegales y la financiación del terrorismo.

2. El intercambio de información entre los Estados para luchar contra la financiación del terrorismo

La lucha preventiva contra la financiación del terrorismo se lleva a cabo en la mayor parte de los Estados en legislaciones compartidas con la lucha contra el blanqueo de capitales[3].

Algunos autores[4] críticos con las normativas de lucha contra la financiación del terrorismo consideran que un terrorista –con un presupuesto limitado y una mochila llena de explosivos– puede cometer un ataque terrorista y el rastreo de la fuente de financiación para cometerlo es casi imposible. No obstante, a pesar de que la mayoría de los últimos ataques terroristas han sido cometidos por lobos solitarios[5], todavía nos encontramos con grupos terroristas organizados cuyas redes, aunque tengan células independientes entre sí, van más allá del país de origen del terrorista y tienen una gran fuente de financiación[6]. Por ende, aquí es donde cobra lógica la lucha conjunta contra la financiación del terrorismo y la cooperación de los Gobiernos para erradicar este tipo de delincuencia. A través de la cooperación internacional, los países pueden poner en práctica una de las herramientas más eficaces para luchar contra el terrorismo: eliminar y confiscar los fondos de los que disponen estos grupos criminales, ya que las organizaciones terroristas necesitan financiación para poder seguir reclutando y formando en su escuela del terror a nuevos miembros. Tal y como expone Richard[7], dado que el terrorismo es una amenaza actual global, la respuesta al mismo debe ser también global; no cabe una respuesta individual de Europa, de Estados Unidos, o de los países afectados por el azote del terrorismo en particular: a este peligro que a todos nos concierne debe responderse mediante una lucha en *networking* de los países implicados y las organizaciones internacionales tales como GAFI, IMF u OSCE, entre otras.

Por ello, creemos que uno de los instrumentos más efectivos a la hora de luchar contra la financiación del terrorismo es la firma de acuerdos de intercambio de información entre países y actores internacionales[8]. Pero no solo es necesario que se firmen estos acuerdos; también lo es que el intercambio de información sea efectivo y eficaz, ya que mediante este intercambio se podrá rastrear los movimientos del dinero del

2. Véase también la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza.
3. Para profundizar en la relación entre blanqueo de capitales y financiación del terrorismo véase Mallada Fernández (2015).
4. Véase Buesa Blanco (2016) y Mallada Fernández (2018, págs. 239-263).
5. Recordemos los ataques en Barcelona o en Londres en 2017, por ejemplo.
6. Si echamos la vista atrás, podemos observar que algunos ataques terroristas apenas necesitaron presupuesto para perpetrarse (París 1995: 680 francos; Bali 2002: 20.000 dólares), si bien hubo otros –como el 11S– que costaron entre 400.000 y 500.000 dólares llevarse a cabo. Véase: http://www.9-11commi-ssion.gov/staff_statements/911_Terrfin_Monograph.pdf [Fecha de consulta: 2 de septiembre de 2020].
7. Richard (2006, págs. 9-10).
8. Palicio (2010, págs. 5 y sigs.).

grupo terrorista, y, una vez cortada su fuente de financiación, debilitar a la organización terrorista, ya que sin presupuesto económico no pueden llevar a cabo los ataques.

Es cierto que, al no existir un concepto universal de terrorismo y financiación del terrorismo, es necesario intentar crear unos mínimos estándares internacionales de obligado cumplimiento para los Estados con objeto de homogeneizar la lucha contra el terrorismo y su financiación y que, de este modo, el intercambio de información entre los Estados y los organismos internacionales sea eficaz. De este modo, tanto la UE como Naciones Unidas han trabajado en las últimas décadas sin descanso para crear unos estándares internacionales mínimos que sean de obligado cumplimiento para los Estados. Entre estos estándares, destacaremos los siguientes[9]:

- Convenio Internacional para la Represión de la Financiación del Terrorismo (1999).
- Resolución 1373 (2001) del Consejo de Seguridad. De acuerdo con esta resolución se crea el Comité contra el Terrorismo de las Naciones Unidades, y, además, los Estados deben sancionar la financiación del terrorismo y la ayuda en actividades terroristas en unos listados.
- Convenio Europeo para la Represión del Terrorismo de 1977 (modificado en 2003).
- Convenio del Consejo de Europa sobre la Prevención del Terrorismo (2005).
- Convenio relativo al blanqueo, seguimiento, embargo y comiso de los productos del delito y a la financiación del terrorismo, firmado en Varsovia el 16 de mayo de 2005.
- Decisión marco del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo.
- Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo.
- Las nueve recomendaciones especiales del GAFI (Grupo de Acción Financiera Internacional) sobre la financiación del terrorismo.

En general, podemos destacar que, para homogeneizar la lucha contra el terrorismo internacional y su financiación, casi todos los instrumentos internacionales actuales establecen la necesidad de una regulación autónoma del delito de financiación del terrorismo del delito de terrorismo[10]. Además, las medidas preventivas para luchar contra la financiación del terrorismo son prácticamente las mismas que las medidas establecidas para luchar contra el blanqueo de capitales: conozca a su cliente, conservación de los documentos de cinco a diez años (dependiendo de la legislación del país), etc.[11], ya que los cauces de movimiento del dinero son prácticamente los mismos[12].

3. La lucha transnacional contra la financiación del terrorismo: relación entre Estados Unidos y Europa

Hacer frente a las organizaciones terroristas globales necesita estrategias y respuestas globales que van más allá de un Estado. Por ello, las redes transnacionales de lucha contra el terrorismo y su financiación no deben estar formadas solo por los países; también la sociedad civil y las instituciones financieras y el sector privado deben estar comprometidos en esta lucha, involucrarse y colaborar ac-

9. Ertl, B. (2004). «Der Kampf gegen Geldwäscherei und Terrorismusfinanzierung». *Working Paper 4/2004.* Viena: Bundesministerium für Finanzen [en línea] https://www.yumpu.com/de/document/view/5535509/der-kampf-gegen-geldwascherei-und-terrorismusfinanzierung [Fecha de consulta: 3 de septiembre de 2020].
10. Cuestión que se ha trasladado a los ordenamientos jurídicos nacionales: como el español, donde se ha tipificado el delito de financiación del terrorismo como delito autónomo del delito de terrorismo.
11. Para profundizar sobre este tema véase Mallada Fernández (2015).
12. De todos modos, los mecanismos de investigación para la lucha contra la financiación del terrorismo son muy diferentes de los mecanismos de lucha contra la prevención del blanqueo de capitales. Al respecto, véase Mallada Fernández (2018).

tivamente proporcionando información a las autoridades y facilitando la posible congelación de los activos.

La solución a la lucha contra la financiación del terrorismo no está en una organización, legislación o Estado sino en la cooperación de todos ellos, es decir, en una lucha conjunta de Estados, organizaciones internacionales como GAFI, Naciones Unidas, Europol o Interpol y organizaciones no gubernamentales como el Comité de Supervisión Bancaria de Basilea[13].

No obstante, esta lucha conjunta se puede tornar complicada por las distintas políticas de lucha contra la financiación del terrorismo de los distintos países. Así, por ejemplo, Estados Unidos trata siempre de luchar contra el terrorismo de manera *bilateral*, es decir, aunque participe en organizaciones como la OTAN, sus esfuerzos de cooperación transatlántica siempre se centran en establecer convenios bilaterales con otros países. En cambio, Europa intenta luchar contra el terrorismo y su financiación con mecanismos multilaterales, a través de las directivas que se transponen en los distintos ordenamientos jurídicos de los Estados miembros. Así pues, para superar este escollo de las distintas maneras de enfrentarse al terrorismo por parte de Estados Unidos y de Europa, debemos llamar la atención acerca de que Estados Unidos intenta aumentar su cooperación con Europa a través del cumplimiento de la Recomendación 3 de GAFI de financiación del terrorismo sobre congelación de activos o la Resolución 1373 de Naciones Unidas[14]. Sin embargo, hay problemas en esta cooperación entre Europa y Estados Unidos que aún están pendientes de resolver: entre otros, la congelación de activos y los fondos económicos de las organizaciones benéficas. Así pues, por ejemplo, en cuanto a la congelación de activos, esta cooperación se torna complicada, ya que las listas de terroristas que manejan Estados Unidos y Europa no coinciden, lo cual dificulta el intercambio de información y la congelación de activos de esos terroristas.

3.1. El caso de Estados Unidos: Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos, a efectos del Programa de Seguimiento de la Financiación del Terrorismo

Dentro de los acuerdos de intercambio de información para luchar contra el terrorismo y su financiación podemos destacar el Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y transferencia de datos de mensajería financiera de la UE a los Estados Unidos, a efectos del Programa de Seguimiento de la Financiación del Terrorismo[15]. Este programa es conocido como el Acuerdo SWIFT, PSFT o, por sus siglas en inglés, TFTP, gracias al cual Estados Unidos y la UE pueden intercambiar los datos obtenidos en la plataforma SWIFT a efectos de la lucha contra la financiación del terrorismo. Esto permite a las autoridades acceder a información sobre envío de datos de mensajería financiera entre instituciones bancarias a través de la red SWIFT.

SWIFT es una plataforma de intercambio de información privada y segura entre entidades financieras para efectuar intercambios de información financiera entre ellas. La Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT, Society for Worldwide Interbank Financial Telecommunication) es una cooperativa propiedad de sus miembros a través de la cual el sector financiero lleva a cabo buena parte de sus operaciones comerciales. SWIFT nació en Bélgica en 1973 y tiene oficinas en los principales centros financieros del mundo.

Cada banco que forma parte de esta plataforma tiene un código internacional ISO 9632 que le identifica en el sistema. El código SWIFT de un banco está formado por el código del país, el código del banco y una serie de datos adicionales, como la localización o el tipo

13. Morris (2002).
14. Resolución 1373 de Naciones Unidas: «Internationally, we are focusing our efforts on achieving greater European cooperation and support for our terrorist financing designations. We are capitalizing on our progress in improving and clarifying international standards for freezing terrorist-related assets under FATF Special Recommendation III by: (i) pursuing bilateral and multilateral efforts to reform the EU Clearinghouse process, and (ii) encouraging national implementation of UN member state obligations under United Nations' Security Council Resolution 1373».
15. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:22010A0113(01)&from=EN. [Fecha de consulta: 2 de septiembre de 2020].

de sucursal[16]. El sistema SWIFT solo transmite información, que incluye datos personales del remitente y del destinatario de la transferencia, pero nunca se mueve dinero ni se almacena la información de manera permanente ya que los mensajes permanecen en los centros operativos durante 124 días[17]. Durante este período, los mensajes son guardados en los dos centros de computación de SWIFT y después son borrados de todas sus bases de datos. La plataforma es usada por más de once mil organizaciones bancarias y de valores y está presente en más de doscientos países.

Hasta finales de 2009, SWIFT disponía de dos plataformas: una en Europa (Bélgica) y otra en Estados Unidos. Por motivos de seguridad, todos los mensajes procesados por SWIFT se almacenaban en ambos centros mediante un sistema de almacenaje «en espejo»[18]: Estados Unidos podía acceder a la información de operaciones realizadas en Europa y viceversa. Pero, después de toda la controversia internacional que causó el hecho de que Estados Unidos tuviera acceso a esa información sin implementar ningún requerimiento a la UE[19], para evitar dicha polémica, a partir del 1 de enero de 2010 SWIFT cambió todo su sistema de procedimiento y creó una nueva plataforma en Estados Unidos para que los datos de las transacciones realizadas en Europa y en Estados Unidos estuvieran separadas[20]. De este modo, por un lado, se encuentra una plataforma situada en Estados Unidos para las operaciones efectuadas en Estados Unidos y, por otro lado, otra plataforma situada en Europa para las operaciones llevadas a cabo en Europa. Además, se sigue conservando la plataforma original situada en Bélgica, donde se guardan las operaciones realizadas en ambos continentes como respaldo o *back-up* para posibles fallos de los sistemas de las otras dos plataformas. Así pues, a partir del 1 de enero de 2010 Estados Unidos dejó de tener acceso a toda la información almacenada en las plataformas SWIFT y planteó la posibilidad de firmar un acuerdo con la UE para garantizar el intercambio de información de todas las plataformas SWIFT siempre y cuando esa información solo se usara para la lucha contra la financiación del terrorismo.

Como se puede observar, todos los movimientos financieros quedan grabados en estas plataformas; por ello, tener acceso a las mismas, es un gran avance para la lucha contra la financiación del terrorismo ya que, de este modo, los Gobiernos pueden seguir, detectar y, en su caso, congelar los movimientos relacionados con la financiación de los grupos terroristas, siempre que la congelación de esos activos no ponga en alerta a los terroristas. Debemos recalcar en este punto que si bien la congelación de activos se puede realizar preventivamente en el caso de que las autoridades tengan pruebas fehacientes de que se va a cometer de manera inminente un ataque terrorista, lo más normal es que la congelación se efectúe a *posteriori,* con una orden judicial, ya que cualquier movimiento extraño por parte de la entidad financiera podría levantar sospechas por parte de los terroristas.

Pero ¿cómo es posible que Estados Unidos tuviera acceso a información sensible sobre operaciones realizadas en Europa? Pues bien, como ya hemos mencionado varias veces en este trabajo, los ataques del 11S supusieron un antes y un después en el desarrollo de la legislación para luchar contra la financiación del terrorismo. Así pues, luego de estos ataques, Estados Unidos aprobó el Programa de Seguimiento de la Financiación del Terrorismo (Terrorism Finance Tracking Program, TFTP). Dentro de este programa, el Departamento del Tesoro de Estados Unidos (US Treasury, UST) cursó requerimiento administrativo al centro operativo de SWIFT en Estados Unidos solicitando datos de transferencias bancarias dentro y fuera de Estados Unidos que pudieran estar relacionados con el terrorismo. Como SWIFT tenía información sobre operaciones efectuadas en Estados Unidos y en la UE, el Departamento del Tesoro de Estados Unidos tuvo acceso también a información de operaciones financieras llevadas

16. Palicio (2010); Cremona (2011); De Goede (2012); Santos Vara (2012, págs. 355-380).
17. Véase: https://www.swift.com [Fecha de consulta: 2 de septiembre de 2020].
18. Bosch Moliné (2014, pág. 160 y sigs).
19. Sobre la controversia suscitada por el acceso de Estados Unidos a los datos de transacciones realizadas dentro de Europa del sistema SWIFT, véase Monar (2010, págs. 143-151) y Pfisterer (2009, págs. 1.173-1.189).
20. Véase: «SWIFT: el Parlamento Europeo rechaza el acuerdo con Estados Unidos» [en línea] http://www.europarl.europa.eu/sides/getDoc.do?language=es&type=IM-PRESS&reference=20100209IPR68674 [Fecha de consulta: 2 de septiembre de 2020].

a cabo dentro de Europa sin la autorización de las agencias nacionales de protección de datos europeas[21]. Esto derivó en varias investigaciones por parte de la agencia belga de protección de datos concluyendo en septiembre de 2006 que se había «sometido a vigilancia durante años a una cantidad masiva de datos personales de forma secreta y sistemática, sin justificación suficiente y clara y sin control independiente conforme al derecho belga y europeo»[22]. Como consecuencia de todo ello, y para evitar posteriores problemas con las autoridades europeas, SWIFT cambió su estructura, como ya hemos mencionado, a partir del 1 de enero de 2010, con lo cual Estados Unidos ya no tendría acceso a las operaciones realizadas en Europa. Por ello, el Gobierno estadounidense decidió intentar alcanzar un acuerdo con las autoridades europeas para poder hacer requerimientos sobre estos datos[23], firmando así el Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la UE a los Estados Unidos a efectos del Programa de seguimiento de la financiación del terrorismo[24]. El acuerdo entró en vigor el 1 de agosto de 2010 (publicado en el DOUE L 195, de 27 de julio de 2010, pág. 1)[25]. En este nuevo acuerdo se respetaban las exigencias del Parlamento Europeo, en concreto «la limitación estricta del objetivo de las transferencias a la lucha contra el terrorismo, la exclusión de los datos del sistema europeo de pagos (SEPA), la prohibición de las transferencias en bloque, la limitación a cinco años del período de conservación de los datos, la posibilidad de denunciar el acuerdo en caso de incumplimiento de las normas de protección de datos y el derecho a la reparación administrativa y judicial»[26].

Sin embargo, tras sendas comunicaciones en 2011 y 2013, la Comisión concluyó que la necesidad de establecer este sistema no está claramente demostrada y suspendió cautelarmente dicho acuerdo[27] debido al escándalo Snowden[28]. El Parlamento consideraba que debía hacerse una suspensión cautelar del acuerdo para investigar si la Agencia Nacional de Seguridad de Estados Unidos (NSA, National Securiry Agency) había tenido acceso directo a los datos proporcionados por SWIFT para usarlos en casos no relacionados directamente con la financiación del terrorismo, lo que supondría una violación de los términos del Programa de seguimiento de financiación del terrorismo.

A principios de 2014, el Informe Moraes sobre los diversos programas de vigilancia de la NSA, realizado por el euro-

21. Es decir, sin la autorización de los Estados miembros.
22. Dictamen 37/2006 del 27 de septiembre de 2006 de la Comisión Belga para la Protección de la Intimidad relativa a la transferencia de datos personales por parte de SWIFT por los requerimientos del UST (OFAC), pág. 27 [en línea] (en francés y en holandés).El nuevo acuerdo se firmó el 28 de junio de 2010 para un período de cinco años renovable.
23. No debemos olvidar que el Tratado de Lisboa entró en vigor el 1 de diciembre de 2009, y que una de las novedades que incluía era el requisito del consentimiento del Parlamento Europeo para la conclusión de acuerdos internacionales, por lo que el acceso del Departamento del Tesoro a los datos del SWIFT europeo debía pasar por la aprobación del Parlamento Europeo.
24. También conocido como Acuerdo SWIFT.
25. La premura en alcanzar un acuerdo fue debido a que, como ya hemos señalado, SWIFT almacena los datos durante 124 días, con lo cual, si Estados Unidos dejaba de tener acceso al sistema durante un período más largo, hubiera perdido la posibilidad de analizar los datos de ese período.
26. Este intercambio de información funciona en ambas direcciones, por lo que, del mismo modo, tanto Europa podrá proporcionar información a Estados Unidos como al contrario (artículo 1.1 del acuerdo). El procedimiento de dicho acuerdo funciona del siguiente modo. En primer lugar, el Departamento del Tesoro de Estados Unidos solicitará al proveedor designado que se encuentre en el territorio de Estados Unidos la puesta a disposición de los datos necesarios para «la prevención, investigación, detección o persecución del terrorismo o de la financiación del terrorismo que estén almacenados en el territorio de la Unión Europea» (artículo 4 del acuerdo). En la solicitud se ha de detallar claramente los motivos y los datos que se requieren quedando siempre al margen del acuerdo los datos sobre el espacio único de pagos en euros. De todos modos, aunque el acuerdo establezca limitaciones, no se van a evitar la transferencia masiva de datos personales a las autoridades estadounidenses ya que las transferencias no son individualizadas sino por categorías. En segundo lugar, el Departamento del Tesoro debe enviar a Europol una copia de la solicitud. Europol comprueba que la solicitud cumple los requisitos del acuerdo y acto seguido «el proveedor designado queda autorizado para facilitar y debe facilitar los datos al Departamento del Tesoro de Estados Unidos».
27. Communication from the Commission to the European Parliament and the Council on a European Terrorist Finance Tracking System (TFTP) (COM (2013) 842 final).
28. Véase: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0449+0+DOC+XML+V0//ES [Fecha de consulta: 2 de agosto de 2020].

diputado Claude Moraes, reiteró la recomendación de la suspensión del acuerdo con Estados Unidos[29]. Sin embargo, una investigación efectuada por las autoridades belgas y holandesas de protección de datos no encontró ninguna prueba que apoyara las afirmaciones de que un tercero había adquirido ilegalmente el acceso a la base de datos de SWIFT[30].

En 2015, Estados Unidos se negó a permitir el acceso del Parlamento Europeo a un documento sobre la implementación del programa SWIFT (TFTP) escrito por el propio comité interno de protección de datos de Europol, la Autoridad Común de Control. Las modalidades técnicas del acuerdo entre Estados Unidos y Europa requieren que Europol obtenga un permiso de las autoridades de Estados Unidos antes de divulgar cualquier registro relacionado con el programa. Las autoridades estadounidenses han rechazado el acceso público, argumentando que el documento contiene información clasificada de Estados Unidos y que el requisito de «need to know» (necesidad de saber) no se había cumplido. La Defensora del Pueblo de la UE, Emily O'Reilly, se opuso a esta decisión arguyendo que esta negativa le impedía realizar una supervisión democrática sólida del TFTP[31].

El último informe de la Comisión, publicado el 19 de enero de 2017[32], demuestra los beneficios importantes del TFTP para los esfuerzos internacionales de lucha contra el terrorismo.

De todos modos, a pesar de las críticas, el programa ha seguido en vigor hasta la actualidad, ya que, como es sabido, el Parlamento Europeo no tiene poder para suspender la aplicación de ningún acuerdo, lo cual compete al Consejo de la UE[33].

El acuerdo salvaguarda los derechos de protección de datos relacionados con la transparencia, los derechos de acceso, la rectificación y el borrado de datos inexactos. Además, garantiza que cualquier persona cuyos datos se procesen en virtud del acuerdo tendrá derecho a solicitar una reparación judicial en Estados Unidos por cualquier acción administrativa adversa.

Una parte importante del acuerdo se encuentra en que los datos del programa puedan ser transferidos a terceros. Sin embargo, esta transferencia queda supeditada a la autorización por parte de ambos Estados salvo causa de fuerza mayor relacionada con la financiación del terrorismo.

Europol evalúa si los datos solicitados en un caso determinado son necesarios para la lucha contra el terrorismo y su financiación verificando que cada solicitud use la menor cantidad de datos posibles solicitados. Además, todas las búsquedas realizadas dentro del marco del programa son supervisadas por supervisores independientes y en el caso de que haya dudas sobre el nexo terrorista pueden bloquear todas las búsquedas relacionadas con ese nexo en virtud del artículo 5 del acuerdo.

En resumen, creemos que este programa de seguimiento de la financiación del terrorismo entre Estados Unidos y Europa es uno de los instrumentos más importantes para luchar contra la financiación del terrorismo no solo porque propone una cooperación recíproca entre Estados Unidos y Europa para intercambiar información en ambos sentidos, sino también por permitir observar los movimientos del dinero de los grupos terroristas para que los cuerpos y fuerzas de seguridad puedan adelantarse a sus movimientos, cortando sus fuentes de financiación.

29. European Parliament (2014).
30. Belgian Privacy Commission (2014).
31. 31 European Ombudsman (2015): https://www.ombudsman.europa.eu/en/speech/en/58851 [Fecha de consulta: 2 de septiembre de 2020]; y NIELSEN, N. (2015): https://euobserver.com/justice/127142 [Fecha de consulta: 2 de septiembre de 2020].
32. Informe de la Comisión al Parlamento Europeo y al Consejo (2017): https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0031&from=EN [Fecha de consulta: 2 de septiembre de 2020].
33. El acuerdo debía estar en vigor durante cinco años, pero, aunque ya se ha pasado ese plazo, sigue vigente a la espera de la aprobación del nuevo pilar de protección de datos de la UE.

4. Sistema europeo de seguimiento de la financiación del terrorismo (TFTS)

En el ámbito europeo se está pergeñando desde hace algunos años la posible creación de un sistema europeo de seguimiento de la financiación del terrorismo (TFTS) capaz de seguir las transacciones de los presuntos terroristas en la zona del euro paralelo al programa que actualmente existe con Estados Unidos según el cual se intentarían detectar las redes terroristas a través del rastreo de la cadena de financiación en Europa. Este programa aún no ha visto la luz, pero en este apartado haremos un pequeño resumen de cómo están actualmente las negociaciones al respecto.

En una comunicación del 27 de noviembre de 2013, la Comisión Europea concluyó que una propuesta para un TFTS propio de la UE no está claramente demostrada. Así pues, sorprendentemente, el resultado de esta evaluación de impacto fue el abandono de un TFTS de la UE. En su informe, la Comisión presentaba dudas sobre los impactos potenciales en términos de derechos fundamentales y sobre el coste del nuevo y más amplio[34] sistema propuesto[35].

Sin embargo, este programa sería beneficioso para cubrir todas las transacciones que se realicen dentro de la zona SEPA pero que estén excluidas del acuerdo con Estados Unidos, por ejemplo los pagos dentro de la UE en euros. Además, el acuerdo con Estados Unidos no proporciona una herramienta para rastrear actividades de financiación del terrorismo dentro de los países SEPA[36], ni entre ellos, en el caso de transacciones SEPA. Como consecuencia, resulta imposible detectar y obtener información relativa a los combatientes terroristas extranjeros y a sus socios dentro de los países SEPA; y, a pesar de la integración de la Red de Unidades de Inteligencia Financiera (UIF) en Europol, esta laguna no se subsana, ya que el TFTP no forma parte de los métodos de trabajo de las UIF[37].

Después de los recientes ataques acaecidos en Europa (París, Niza, Barcelona) la idea del TFTS europeo volvió a ponerse sobre la mesa[38] en aras de mejorar la lucha contra la financiación del terrorismo en territorio europeo. Así pues, la eurodiputada conservadora francesa Rachida Dati, durante una sesión de preguntas parlamentarias con la Comisión Europea el 28 de enero 2015[39], expuso que había que retomar el programa de seguimiento de financiación de terrorismo europeo dado que las amenazas terroristas en Europa y en Estados Unidos a día de hoy son complemente opuestas. La mayor preocupación actual europea es la amenaza de los ciudadanos europeos retornados de Siria o Irak o de aquellos lobos solitarios inspirados por la ideología del Dáesh y dispuestos a perpetrar un ataque terrorista en territorio europeo. Así pues, el Plan de Acción de la UE establece que la Comisión Europea acuerda que se retomará la iniciativa para complementar el actual programa firmado con Estados Unidos adicionando las transacciones excluidas en dicho acuerdo[40].

Por tanto, abogamos por la creación de un sistema europeo de seguimiento de la financiación del terrorismo (TFTS) capaz de seguir las transacciones de los presuntos terroristas en la zona del euro, además del Programa de Seguimiento de la Financiación del Terrorismo (TFTP) existente entre Estados Unidos y la UE.

Por último, dentro de Europol se encuentra el Centro Europeo de Lucha contra el Terrorismo (ECTC)[41]. Entre sus objetivos principales se encuentran, por un lado, aumentar el intercambio de información entre los Estados

34. European Commission (2013, pág. 37).
35. Así pues, la Comisaria de Asuntos de Interior, Cecilia Malmström, confirmó que la Comisión no tenía la intención de presentar una propuesta específica para un TFTS de la UE, ya que «no aportaría ninguna inteligencia adicional».
36. Aquellos que excluyen los datos de transacciones financieras relativos a la zona única de pagos en euros.
37. Maricaa (2017). La UIF española es el Servicio ejecutivo de prevención de blanqueo de capitales (SEPBLAC). Todas las UIF europeas comparten información a través de FIU.net.
38. De Goede y Wesseling (2017).
39. Dati (2015): https://www.europarl.europa.eu/doceo/document/P-8-2015-001000_EN.pdf [Fecha de consulta: 2 de septiembre de 2020].
40. European Commission (2016, pág. 12).
41. Los proyectos que se llevan a cabo son AP Hydra, Travellers, Dolphin, TFTP y Check the Web.

miembros y Europol, y, por otro intensificar los rastreos de las actividades de financiación del terrorismo[42].

5. Conclusiones

En primer lugar, podemos afirmar que los instrumentos para luchar contra la financiación del terrorismo más eficaces son aquellos que, en primer lugar, son preventivos, y que, en segundo lugar, abogan por el intercambio efectivo de información entre los Estados y las organizaciones internacionales, ya que el *modus operandi* del terrorismo ha cambiado en las últimas décadas para pasar a ser un terrorismo internacional. Por ello, la herramienta por excelencia para la prevención de la financiación del terrorismo es facilitar el intercambio de información entre Estados y organizaciones internacionales.

El terrorismo actual no es un problema nacional, sino internacional, que cruza las fronteras nacionales del país en cuestión. De ahí la necesidad de compartir información con otros países para una lucha exitosa en contra de la financiación del terrorismo.

Aunque en la actualidad ya existan bases de datos de terrorismo[43], algunos autores apuntan la posibilidad de desarrollar bases de datos más específicas que puedan compartir Estados Unidos y Europa a fin de poder llevar a cabo esta medida preventiva[44], lo cual creemos que es harto complicado ya que el principal problema que existe con el intercambio de información entre países es el relativo a aquella información que está considerada como inteligencia clasificada (*classified intelligence*)[45]. Así, por ejemplo, si Estados Unidos tiene evidencias de actividades terroristas será más fácil lograr la cooperación con países europeos; el problema es cuando no pueden compartir la información de origen de esas pruebas de terrorismo porque está considerada como clasificada. Sin esa información de origen, los países europeos serán más reacios a colaborar con Estados Unidos. De todos modos, la línea actual que se está llevando a cabo en Europa y en Naciones Unidas prevé una homogeneización cada vez más mayor de la normativa de lucha contra el terrorismo y su financiación con un concepto universal de terrorismo y de su financiación, lo cual ayudará a disminuir estas barreras entre países a fin de lograr un intercambio de información más rápido y eficaz.

42. Además de efectuar investigaciones más específicas contra el tráfico ilícito de armas de fuego con fines de actividades terroristas, así como investigaciones con objeto de detectar el material de propaganda extremista violenta en internet, funciones ideadas para tener un mayor impacto operativo contra las redes terroristas y los llamados combatientes extranjeros.
43. En cambio, Europol sí que tiene una amplia base de datos de terroristas. Así pues, los distintos Estados miembros de la UE pueden proporcionar información a la Europol según los distintos códigos de manejo. El primer código es el «H0» o «no-código», ya que si se selecciona significa que la información puede distribuirse a todos los Estados miembros sin ningún tipo de restricción. En segundo lugar, el código «H1» prohíbe compartir la información antes de que se termine el procedimiento judicial a no ser que exista una autorización previa por el Estado miembro que incorporó los datos. En tercer lugar, el código «H3» permite incorporar las restricciones que el Estado miembro crea convenientes, y por ello se puede añadir texto en una casilla en blanco (por ejemplo, que solo se pueda compartir la información con un determinado centro focal). Véase Blasi Casagran (2016, pág. 20).
44. Richard (2006, pág. 25 y ss.).
45. Los países pueden contribuir a proporcionar información a Europol, siendo los propios dueños de la misma a través de los códigos de manejo. Estos códigos de tratamiento constituyen un medio para proteger una fuente de información. Garantizan su seguridad, así como su tratamiento protegido y adecuado, de conformidad con los deseos del propietario de la información y con plena observancia de las normas jurídicas nacionales de los Estados miembros. Los códigos de tratamiento indican qué puede hacerse con una información determinada y quién dispone de acceso a ella en el futuro.

Referencias bibliográficas

BELGIAN PRIVACY COMMISSION (2014). Only available in Dutch or French at https://www.privacycommission.be/fr/news/les-instances-chargees-de-controler-le-respect-de-la-vie-privee-ne-constatent-aucune-infraction (en línea). [Fecha de consulta: 18 de marzo de 2020].

BLASI CASAGRAN, C. (2016). «El Reglamento europeo de Europol: un nuevo marco jurídico para el intercambio de datos policiales en la UE». *Revista General de Derecho Europeo*, núm. 40.

BOSCH MOLINÉ A. (2014). La dimensión exterior de EUROPOL desde el punto de vista de la protección de datos. En: PI LLORENS. M., ZAPATER DUQUE, E. (coord.). *El caso del acuerdo TFTP en La dimensión exterior de las agencias del espacio de libertad, seguridad y justicia* Barcelona: Marcial Pons.

BUESA BLANCO, M. (2016). «Financiación del terrorismo». *Economía*, núm. 893.

CREMONA, M. (2011). «Justice and home affairs in a globalised world: ambitions and reality in the tale of the EU-US SWIFT Agreement». *Institute for European integration Research* (Working Paper No. 4/2011).

DATI, R. (2015). «Parliamentary Questions» [en línea] https://www.europarl.europa.eu/doceo/document/P-8-2015-001000_EN.pdf [Fecha de consulta: 2 de septiembre de 2020].

DE GOEDE, M. (2012). «The SWIFT affair and the Global Politics of European Security». *Journal of Common Market Studies*, vol. 50, pág. 214.

DE GOEDE, M.; WESSELING, M. (2017). «Secrecy and security intransatlantic terrorism finance tracking». *Journal of European Integration,* núm. 39, vol. 3, págs. 253-269.

ERTL, B. (2004). «Der Kampf gegen Geldwäscherei und Terrorismusfinanzierung». W*orking Paper 4/2004*. Viena: Bundesministerium für Finanzen [en línea] https://www.yumpu.com/de/document/view/5535509/der-kampf-gegen-geldwascherei-und-terrorismusfinanzierung [Fecha de consulta: 2 de septiembre de 2020].

EUROPEAN COMMISSION (2013). *Commission Staff Working Document.*

EUROPEAN COMMISSION (2016). «Communication from the Commission to the European Parliament and the Council on an Action Plan for Strengthening the Fight against Terrorist Financing», COM/2016/050 final.

EUROPEAN PARLIAMENT (2014). «Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens, Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs» en *Committee on Civil Liberties, Justice and Home Affairs,* 2013/2188(INI).

EUROPEAN OMBUDSMAN (2015). «Presentation by the European Ombudsman, Emily O'Reilly– Decision of the European Ombudsman Closing the Inquiry into Complaint 1148/2013/TN as Regards Europol», 8 de enero de 2015 [en línea] https://www.ombudsman.europa.eu/en/speech/en/58851 [Fecha de consulta: 2 de septiembre de 2020].

INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO (2017). Sobre la revisión conjunta de la aplicación del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo [en línea] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0031&from=EN [Fecha de consulta: 2 de septiembre de 2020].

MALLADA FERNÁNDEZ, C. (coord.) (2015). *Guía práctica de prevención del blanqueo de capitales.* Madrid: Lex Nova.

MALLADA FERNÁNDEZ, C. (2018). «La financiación del terrorismo desde la perspectiva de las nuevas tecnologías: a propósito de la quinta Directiva de la UE de prevención del blanqueo de capitales y la financiación del terrorismo». *Anuario de derecho penal y ciencias penales*, tomo 71, fasc. 1, págs. 239-263.

MARICAA, A. (2017). «Medidas y cambios normativos en la UE para intensificar la lucha contra el terrorismo global». *Revista del IEEE*, núm. 10 [en línea] http://revista.ieee.es/article/view/190/310 [Fecha de consulta: 2 de septiembre de 2020].

MONAR, J. (2010). «The rejection of the EU-US SWIFT interim agreement by the European parliament: a historic vote and its implications». *European foreign affairs review*, vol. 15, núm. 2, págs. 143-151.

MORRIS, S. (2002). «Following the money trail: where corruption meets terrorism». *TIQ: Transparency International's Quartely Newsletter.*

NIELSEN, N. «US Gag Order on EU Police Agency Stirs Controversy», *EU Observer* [en línea] https://euobserver.com/justice/127142 [Fecha de consulta: 2 de septiembre de 2020].

PALICIO, I. (2010). «El intercambio internacional de información financiera y la lucha contra la financiación del terrorismo: el acuerdo UE-EEUU sobre SWIFT». *ARI 49/2010.*

PFISTERER, V. (2009). «The second SWIFT Agreement between the European Union and the United States of America: an overview». *German Law Journal,* vol. 11, núm. 10, págs. 1.173-1.189 [en línea] https://doi.org/10.1017/S2071832200020174 [Fecha de consulta: 2 de septiembre de 2020].

RICHARD, A. (2006). *Fighting terrorism financing: transatlantic cooperation and international institutions.* Center for Transatlantic Relations.

SANTOS VARA, J. (2012). «El Acuerdo SWIFT con Estados Unidos: génesis, alcance y consecuencias». En: MARTÍN Y PÉREZ DE NANCLARES, J. (coord.). *La dimensión exterior del espacio de libertad, seguridad y justicia de la Unión Europea.* Madrid: IUSTEL, págs. 355-380.

Cita recomendada

MALLADA FERNÁNDEZ, Covadonga (2021). «Estudio del tratamiento y transferencia de datos de mensajería financiera entre la Unión Europea y Estados Unidos a los efectos de la lucha contra la financiación del terrorismo». *IDP. Revista de Derecho, Internet y Política,* núm. 32, págs. xx-xx. UOC [Fecha de consulta: dd/mm/aa] https://dx.doi.org/10.7238/idp.v0i32.373741

Sobre la autora

Covadonga Mallada Fernández
covadonga.mallada@gmail.com
Universidad de Valladolid

Licenciada en Derecho (2006). Máster en Asesoría Fiscal por la Universidad Pontificia de Salamanca (premio al mejor expediente de la promoción 2008). Doctora por la Universidad de Oviedo (2012) y premio extraordinario de doctorado (2013). Premio jóvenes investigadores menores de treinta y cinco años del Max Planck Institute (2015) e investigadora en varios proyectos nacionales, entre ellos investigadora principal del proyecto DER2014-58257-R Ciberlaundry (2014-2017). Asimismo, fue investigadora posdoctoral en la Universidad Humboldt de Berlín bajo la dirección del profesor Heinrich durante el curso 2012-2013, profesora adjunta de la UDIMA entre 2013 y 2017 y profesora de tributación del CEF entre 2013 y 2017. Actualmente es profesora ayudante doctor de la Universidad de Valladolid.

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

https://idp.uoc.edu

ARTICLE

An Exploratory Investigation of Traditional Stalking and Cyberstalking Victimization among University Students in Spain and the United States: A Comparative Analysis

Victoria Fernández-Cruz
Universitat Internacional de Catalunya
José R. Agustina
Universitat Abat Oliba CEU
Fawn T. Ngo
University of South Florida

Date of submission: July 2020
Accepted in: September 2020
Published in: March 2021

Abstract

Traditional stalking and cyberstalking have become a significant legal and social issue in today's society. Although a sizeable body of research on stalking victimization and perpetration currently exists, very little is known about cyberstalking victimization. Relatedly, there is a dearth of comparative research on the topics of traditional stalking and cyberstalking. Examining the prevalence and nature of stalking victimization across national settings will allow for an exploration of the significance of social context in affecting victims' experiences as well as help highlight the competing influences operating in different contexts. Cross-national research on stalking will also provide an opportunity to consider a wide range of alternative options and solutions to the problem. The aim of this study is to compare and contrast the prevalence and nature of traditional stalking and cyberstalking victimization between American and Spanish university students. This study focuses

on university students because there is evidence that they have a higher risk of becoming victims of stalking relative to the general population. Moreover, the comparative analysis undertaking in this study involves a country that has criminalized stalking for almost three decades (the United States) and a country that has just recently enacted an anti-stalking statute (Spain). Such analysis is warranted as it will allow the researchers to engage in critical analyses of current anti-stalking statutes and advocate for innovative, sensible, and effective solutions in addressing the crime of stalking. In addition to presenting the results, the policy implications derived from the study will also be discussed..

Keywords
stalking, cyberstalking, cross-national research, university students

Investigación exploratoria y análisis comparativo del acoso convencional y el ciberacoso de estudiantes universitarios en España y Estados Unidos

Resumen

El acoso convencional y el ciberacoso constituyen un problema social y jurídico en la sociedad actual. Si bien se cuenta con un considerable corpus de investigaciones sobre el acoso, sus víctimas y los perpetradores, no ocurre lo mismo en el caso de la victimización por ciberacoso, sobre el que se sabe muy poco. Existe supuestamente un cúmulo de investigaciones comparativas en torno al acoso convencional y el acoso on-line*. El estudio de la prevalencia y la naturaleza del acoso del que son objeto las víctimas en sus contextos nacionales permite explorar la importancia del contexto social y la manera en que éste afecta la experiencia de la víctima, así como resaltar las influencias concurrentes que operan en diferentes contextos. Asimismo, la investigación comparativa del acoso en países diferentes permitirá considerar una amplia variedad de opciones alternativas y soluciones al problema. El presente estudio se centra en comparar y contrastar la prevalencia y las características del acoso tradicional y el ciberacoso en los estudiantes universitarios de España y de EE.UU., pues existen evidencias de que estos están en mayor riesgo de ser víctimas en comparación con su población en general. Asimismo, el análisis comparativo se centra en los Estados Unidos, donde el acoso es tipificado como delito desde hace casi tres décadas, y en España, un país cuya legislación contra el acoso ha sido promulgada recientemente. Este enfoque se justifica por cuanto posibilita un análisis crítico de las leyes anti-acoso por parte de los investigadores y la promoción de soluciones innovadoras, razonables y eficaces para hacer frente a los delitos de acoso. Además de presentar sus resultados, el estudio se complementa con una discusión acerca de las implicaciones para las políticas derivadas de éste.*

Palabras clave

acoso, ciberacoso, investigación transnacional, estudiantes universitarios

1. Introduction

Stalking is a relatively new crime in Spain. In 2001, at the Council of Europe's Convention on Preventing and Combating Violence against Women and Domestic Violence in Istanbul, the subject of combatting violence against women emerged as a top priority on the European Union political agenda. In particular, a series of behaviors were identified as criminal at the meeting and the signatory countries subsequently introduced a series of unwanted and harassing behaviors in their penal codes. Among these behaviors was stalking. In March 2015, *stalking* was outlawed and included in the Spanish Criminal Code through the organic law 1/2015 (article 172b).

Several studies in the stalking field have highlighted certain limitations on the methodology since there is –as of now– no consensus on how stalking should be defined (Nobles et al., 2012). On one hand, American studies often define stalking as repeated and unwanted –usually non-physical– contact imposed on another in a manner which could be expected to cause distress and or fear for their safety (Basile, Swahn, Chen & Saltzman, 2006; Baum, Catalano & Rand, 2009). In Spain, on the other hand, stalking is defined as persistent or repetitive behavior or activities imposed on another person in a manner that results in a disruption of the individual's daily life (Villacampa & Pujols, 2017). Article 172 ter of the Spanish Criminal Code also includes a list of conducts and activities that the Spanish criminal system considers *stalking*. Although the American and Spanish definitions of *stalking* both highlight persistence, repetition and intrusiveness when defining this crime, the American definition requires the victim to feel distressed and/or fear, while the Spanish definition emphasizes how the events negatively affect or alter the victim's life.

In prior studies on stalking there was no explicit mentioning of the different characteristics that would indicate cyberstalking is different from offline stalking. Further, these studies did not cast doubt upon whether cyberstalking and traditional stalking could be separate phenomena. However, there is currently a persisting debate on whether cyberstalking should be considered an individual phenomenon –it can happen without there being any signs of offline stalking– (Bocij & McFarlane, 2003), or acknowledging there is a conceptual overlap between online and offline stalking and that the only difference between those two is the space where they take place. (Nobles et al., 2012; Sheridan & Grant, 2007). The debate shines a light on the necessity for more research on this topic.

The definition of cyberstalking varies in the literature and there is terminological confusion. However, cyberstalking is generally defined as a pattern of reiterated and insistent behaviour associated with the use of Information and Communications Technology (ICT) –such as laptops, mobile phones, or tablets– which induces in the victim fear or distress (Maple, Short, & Brown, 2011; Nobles et al., 2012; Short, Linford, Wheatcroft, & Maple, 2014).

1.1. Stalking and cyberstalking prevalence

The prevalence rate of stalking victimisation in the U.S. for the general population is estimated to be between 5% and 28%, increasing to between 7% and 56% among college students (Spitzberg & Cupach, 2014). A similar pattern has been documented in Spain where the prevalence rate for the general population is estimated at 11% (FRA, 2014) and the prevalence rate for the university population is estimated to be between 30% and 70% (Villacampa & Pujols, 2017; León & Aizpurúa, 2019). As evident from the research conducted in the United States and Europe, the age group with a heightened risk for stalking victimization are women and men between the ages of 18 and 20. Hence, it is not surprising that a large proportion of prior research has focused on university students. In the United States, the prevalence rate for female university students is estimated to be between 13% to 30% and for male university students, it is between 11% to 19% (eg, Fisher, Cullen & Turner, 2002; Fremouw, Westrup & Pennypacker, 1997; Nobles, Fox, Piquiero & Piquiero, 2009; Reynes & Scherer, 2018; Shorey, Cornelius, & Strauss, 2015).

Studies about cyberstalking in the U.S. indicate that the prevalence rate of cyberstalking victimisation is around 3-18% to 40% (Alexy, Burgess, Baker & Smoyak, 2005; Bocij & McFarlane, 2003; Finn, 2004; Nobles et al., 2014). It is noteworthy that the disparity found in the prevalence of cyberstalking and traditional stalking is due to differences in the methodology and the operationalization of the variables and the sample used. (Cavezza & McEwan, 2014; Nobles et al., 2014).

Although studies examining offline stalking or online stalking abound, only a handful of studies have focused on the

relationship between these two types of stalking. One such study is the one conducted by Alexy et al. (2005) which is considered to be one of the most important studies on the topic to date. The sample in Alexy et al.'s study consists of 765 university students. The researchers found that although females were more likely to be stalked offline, males were more likely to be cyberstalked than females and were likely to have also been victimized offline. Some researchers point out that it is common, for stalkers, to start showing stalking behaviours in cyberspace and later threaten the victim to continue them in the physical world (Bocij, Griffiths, & McFarlane, 2002; Lee, 1998), coming to be considered a predictor of offline harassment behaviour (Reynes, Henson & Fisher, 2011).

In a more recent study conducted by Reyns & Fisher (2018) a sample of 3,488 university students was used to investigate the relation between online and offline stalking victimization. Reyns & Fisher (2018) concluded that there is, in fact, a relation between the two. They found online stalking to be an added strategy for the stalker to commit such acts. Their study also concludes that gender plays a big part in the type of received stalking and the relation between online and offline stalking. The chances for men to become victims of offline stalking increased when they had been stalked online beforehand. Women were more likely to be stalked online when they had previously experienced offline stalking. And women who were stalked online in the first place had a lower risk to become victims of offline stalking.

Other studies have examined the differences between online and offline stalking through the stalker's point of view. One example of such is the study conducted by Cavezza & McEwan (2014). They were the first to examine and compare a forensic sample of perpetrators who had stalked their victims online and offline. The authors concluded that most cyberstalkers had also acted similarly in the offline world and that they were more likely to use a larger variety of methods to come into contact with the victims than offline stalkers. This study also pointed out that perpetrators stalked mostly women and that there was usually a previous relationship between victim and perpetrator.

As we have seen, the data gathered by the literature around the topic remains scarce and, in some cases, inconsistent. Therefore, more research is needed.

2. Present Study

There is a growing interest among Spanish academics in examining the crime of stalking as evidenced by a series of recent publications. In this exploratory investigation we seek to contribute to the existing body of scholarship on this topic by exploring the prevalence of stalking and cyberstalking victimization among Spanish and American university students and describing the differences between the two. Besides, the characteristics of the victims will be analyzed in greater detail for a better understanding of the phenomenon. We hypothesize, after studying the previous body of research, that: (1) the victimization rate for stalking behavior will stand higher for women than men in both countries (Basile, 2006; Villacampa & Pujols, 2017), (2) the victimization rate for cyberstalking behavior will be higher for men than for women in both countries (Alexy *et al*., 2005; Reyns & Fisher, 2018).

3. Method

3.1. Procedure

Data from the present study came from an online self-report survey of victimization and perpetration of stalking behavior. The instrument used is a version of the Supplemental Victimization Survey (SVS) of the National Crime Victimization Survey (NCVS) (Baum et al., 2009) translated into Spanish. On February 6, 2018, the survey was approved by the Committee of Research Ethics (CER) of the International University of Catalonia (UIC Barcelona). During the last week of February 2018 an email was sent by the coordinators of different undergraduate and graduate programs from different universities of Spain and the U.S. The participation was voluntary and anonymous. The students were informed that the average time to answer the questions was 20 to 25 minutes (including the average time response). The researcher's contact also appeared in the survey instructions in case the participants needed help or additional information. The survey included questions related to sociodemographic information of the respondents and divided the succeeding questions into two large blocks: the first part consisted of 35 questions about stalking victimization and the second block centered around stalking perpetration (10 questions). The survey avoids using the word harassment or stalking, although

reference is made to the term "unwanted behavior". All data have been analyzed using the statistical package SPSS version 26.

3.2. Sample

A total of 2,610 students participated in the study, 1,796 from Spain (68.8%) and 814 from the U.S. (31.2%). A total of 1,879 of the sample is female (72%) and 718 (27.5%) is male. Participants ranged in age from 18 to 64 (*M* = 21.2 years, *SD* = 4.31). Regarding the procedure of sample collection, a mixed methodology was chosen: a total of 717 (27.5%) of the Spanish surveys were administered in person, and the rest (72.5%) using the Qualtrics online platform. This fact will be taken into account in the analysis of the data and interpretation of the results. Approximately half of the sample is single (55.5%), while 41.3% declare that they have a partner; 1.4% are married and 0.9% indicate they have a common-law partner; 0.6% are divorced. None of those surveyed indicate that they are a widow. Regarding the living situation, 45.7% of the sample (1,185) live with their parents, 27% (704) recognize living in a students' apartment, 3.7% live in an off-campus dorm (97) and 11.2% (293) live in an on-campus dorm, 6.6% (171) live with a significant other and 5.5% (143) live by themselves.

In this regard, it is important to point out the differences between Spanish and American students regarding their living situation. More than half of the Spanish students admitted to living with their parents, while a greater part of the American students were independent and lived either in a student apartment or on a dormitory campus. This fact is interesting to analyze because it could be a cultural difference to take into account. Regarding their employment status, more than half of the sample was unemployed and the other approximate half had a part-time job. Exactly 5.5% of the sample had a full-time job and studied at the same time.

	Full sample		Spain		USA	
Variables	N	%	n	%	n	%
Gender						
Male	718	27.5	494	27.5	224	27.5
Female	1,879	72	1,289	71.8	590	72.5
Total	2610	100	1,783	68.8	814	31.2
Marital Status						
Single	1,444	55.3	995	55.4	449	55.2
Boyfriend/Girlfriend	1,078	41.3	741	41.3	37	41.4
Married	44	1.7	25	1.4	19	2.3
Common-Law Partner	24	0.9	19	1.1	5	0.6
Divorced	16	0.6	12	0.7	4	0.5
Living Situation						
With their parents	1,185	45.4	1,096	61	89	10.9
Student apartment	704	27	413	23	291	35.7
Off campus dorm	97	3.7	75	4.2	22	2.7
On campus dorm	293	11.2	16	0.9	277	34
With sgnificant other	143	5.5	72	4	71	8.7
By themselves	171	6.6	107	6	64	7.9

Work Situation						
Not employed	1,608	61.6	1,228	68.6	380	46.7
Full-time employed	143	5.5	87	4.8	56	6.9
Part-time employed	851	32.6	473	26.3	378	46.4

Table 1. Sample characteristics (N= 2,610)

Regarding their employment status, more than half of the sample was unemployed and the other approximate half had a part-time job. Exactly 5.5% of the sample had a full-time job and studied at the same time.

3.3. Measures

In order to know the characteristics of the victims a questionnaire was designed to measure the following constructs:

- *Age*. The variable age will be measured in years. The participants in this study had to be 18 years old or more.
- *Sex*. The variable sex will be coded as 1 = female, 0 = male;
- *Country*. The variable country will be coded as 1 = Spain, 2 = The U.S.
- *Marital Status*. This variable was coded as follows: (1) Single, (2) Boyfriend/Girlfriend, (3) Married, (4) Common-Law Partner and (5) Divorced.
- *Living Situation*. This variable was coded as follows: (1) living with their parents, (2) student apartment, (3) off-campus dorm, (4) on-campus dorm, (5) with significant other and (6) by themselves.
- *Stalking victimization*. For the present investigation, we have considered victims of stalking those who have indicated that they have experienced at some point in their life and on more than one occasion any of the following unwanted contacts that could have been committed by a stranger, acquaintance, friend, relative or partner: a) received unwanted calls or unwanted messages on the answering machine; b) having been followed or spied on; c) someone had waited for them outside or inside a room; d) someone had appeared in unsuspected places; e) someone had given unwanted things, gifts or flowers. The answers, of a dichotomous nature, will be coded as 1 = the person has experienced an intrusive behavior at some time and 0 = the person has not experienced any intrusive behavior. If the person indicates that they have only suffered one of the exposed behaviors, they will be differentiated from those who have indicated that they have suffered more than one of the behaviors, coded as multiple forms of victimization by stalking.
- *Cyberstalking victimization*. We have considered victims of cyberstalking those who have indicated that they have experienced at some point in their life and on more than one occasion any of the following unwanted contact that could have been committed by a stranger, acquaintance, friend, relative or partner: a) receiving unsolicited or unwanted e-mails and b) having information about them posted on the Internet. The answers, of a dichotomous nature, will be coded as 1 = the person has experienced an intrusive behavior at some time and 0 = the person has not experienced any intrusive behavior. If the person indicates that they have only suffered one of the exposed behaviors, they will be differentiated from those who have indicated that they have suffered more than one of the behaviors, coded as multiple forms of victimization by cyberstalking.
- *Duration of stalking and cyberstalking behavior*: students were asked for how long had they experienced those unwanted behaviors: (1) between 1 and 6 days, (2) between 1 and 3 weeks, (3) between 1 and 11 months, (4) years or (5) I do not know.
- *Relationship with the author:* the variable relationship with the author of the unwanted behaviors will be coded as (1) husband or wife, (2) ex-husband or ex-wife, (3) parents or step-parents, (4) son, daughter or step-

child, (5) sibling or step-sibling, (6) other relative, (7) boyfriend or girlfriend, (8) ex-boyfriend or ex-girlfriend, (9) friend or ex-friend, (10) roommate, (11) classmate, (12) neighbour, (13) client, (14) student, (15) patient, (16) supervisor, (17) work partner, (18) known, (19) unknown, (20) other, (21) impossible to identify the person.

4. Results

The study found that 7.5% (197) of the sample had been stalked offline on more than one occasion during their lifetime and 12.1% (316) reported to be cyberstalked. The frequencies with which respondents reported being victimized online or offline are presented in Table 2. When we analyze all the victims, we see that 18.1 % (197) were stalked offline and 29.1% (316) were cyberstalked. As we can see, cyberstalking is more prevalent than offline stalking. In relation to the victims' gender, females have a higher victimization rate online and offline than males. This fact is not surprising, since there are many investigations that have obtained the same results (eg, Tjaden & Thoennes, 1998; Miller, 2012, Mullen, MacKenzie, Ogloff, Pathé, McEwan & Purcell, 2006). These results could also be explained by the fact that in the sample there are more females represented than males. As for the age of the victims the mean age is 21.5 (*SD* = 4.9) for offline stalking victims and 21.9 (*SD* = 5.6) for cyberstalking victims.

When we analyze the results in closer detail we can see that men report more offline victimization (32%) than online (16.8%), both in Spain (30.8% offline and 15.8% online) and in the United States (34.4% offline and 18.8% online), although it is true that the difference between percentages is not very high. As for women, the results go in the opposite direction. Women report becoming more often victims of stalking in the online environment (82.3%) than offline (68%). These results are surprising, because they contradict some above-mentioned investigations (Alexy et al., 2005; Reyns & Fisher, 2018). This issue should be further analyzed in future research.

The students who indicated that they were single were the ones who reported the greatest number of stalking victimization, both online and offline. Regarding their living situation, in the case of Spain, most victims lived with their parents. However, it is interesting to see how in the United States most offline stalking victims lived on a campus dorm (43.8%) and most cyberstalking victims (40%) lived in a student apartment.

As for the gender of the stalker, regardless of the country, we can see how the majority of the victims indicate having been stalked by a male perpetrator. However, it can be seen that females who stalk tend to perform stalking in the offline world in contrast to doing it online. With respect to the relationship between the stalker and the victim, in Spain 17.3% (23) of the victims indicated that they had been stalked by an ex-boyfriend/ex-girlfriend. While regarding the victims who had been stalked online, in 25.8% (57) of cases they knew their stalker but did not have any kind of intimate relationship with them. In contrast, in the U.S. 20.3% (13) of offline victims recognised having been stalked by a friend and in the 28.4% (27) of cyberstalking cases the actions were executed by someone who the victim had met before. Being stalked by a stranger was more common in cyberstalking cases rather than offline stalking. Finally, it is interesting to see how most victims do not remember how long the stalking lasted, and those who did remember indicated that it had lasted for years.

In summary, these results show that females are at a higher risk of becoming victims of offline and online stalking regardless of the country they live in, and males tend to stalk more than their counterparts. Most of the victims are single. In Spain more than 50% of victims live with their parents. However, in the U.S. there is an existent difference between offline and online stalking victimisation in terms of their living situation, where 43.8% (28) of the offline stalking victims live on campus dorms but 40% (38) of online stalking victims live in student apartments.

	All sample (N = 513)		Spain (n = 354)		USA (n =159)	
	Offline stalking 197 (18.1)	Cyberstalking 316 (29.1)	Offline stalking 133 (37.6)	Cyberstalking 221 (62.4)	Offline stalking 64 (40.2)	Cyberstalking 95 (59.7)
Victims' Sex						
Male	63 (32)	53 (16.8)	41 (30.8)	35 (15.8)	22 (34.4)	18 (18.9)
Female	134 (68)	260 (82.3)	92 (69.2)	183 (82.8)	42 (65.6)	77 (81.1)
Marital situation						
Single	98 (49.7)	171 (54.1)	72 (54.1)	112 (50.7)	26 (40.6)	59 (62.1)
Boyfriend/Girlfriend	93 (47.2)	129 (40.8)	56 (42.1)	97 (43.9)	37 (57.8)	32 (33.7)
Married	4 (2)	6 (1.9)	3 (2.3)	4 (1.8)	1 (1.6)	2 (2.1)
Common-Law Parnter	1 (.5)	4 (1.3)	1 (.8)	4 (1.8)	-	-
Divorced	1 (.5)	5 (1.6)	1 (.8)	3 (1.4)	-	2 (2.1)
Living Situation						
With their parents	88 (44.7)	140 (44.3)	79 (59.4)	132 (59.7)	9 (14.1)	8 (8.4)
Student apartment	51 (25.9)	74 (24.7)	33 (24.8)	40 (18.1)	18 (28.1)	38 (40)
Off campus dorm	7 (3.6)	8 (2.5)	5 (3.8)	6 (2.7)	2 (3.1)	2 (2.1)
On campus drom	28 (14.2)	34 (10.8)	-	3 (1.4)	28 (43.8)	31 (32.6)
MWith signficant other	9 (4.6)	24 (7.6)	6 (4.5)	12 (5.4)	3 (4.7)	12 (12.6)
Themselves	12 (6.1)	28 (8.9)	8 (6)	24 (10.9)	4 (6.3)	4 (4.2)
Sex Stalker						
Male	131 (66.5)	258 (82.9)	91 (68.4)	184 (83.7)	40 (62.5)	74 (77.9)
Female	49 (24.9)	26 (8.2)	30 (22.6)	17 (7.7)	19 (62.5)	9 (9.5)
Don't know	6 (3)	18 (5.7)	4 (3)	12 (5.4)	2 (3.1)	6 (6.3)
Relationship with the stalker						
Relative	1 (.5)	3 (.9)	1 (.8)	2 (.9)	-	1 (1.1)
Boyfriend/Grilfriend	11 (5.6)	21 (6.6)	6 (4.5)	14 (6.3)	5 (7.8)	7 (7.4)
ExBoyfriend/ ExGirldfriend	32 (16.2)	41 (13)	23 (17.3)	28 (12.7)	9 (14.1)	13 (13.7)
Friend	35 (17.8)	22 (7)	22 (16.5)	13 (5.9)	13 (20.3)	9 (9.5)
Known	28 (14.2)	84 (26.6)	19 (14.3)	57 (25.8)	9 (14.1)	27 (28.4)
Stranger	9 (4.6)	35 (11.1)	6 (4.5)	32 (14.5)	3 (4.7)	3 (3.2)
Friends on social media	17 (8.6)	18 (5.7)	15 (11.3)	16 (7.2)	2 (3.1)	2 (2.1)
Other	17 (8.6)	29 (9.2)	12 (9)	15 (6.8)	5 (7.8)	14 (14.7)

Time of the Stalking						
Days	22 (11.2)	46 (14.6)	17 (12.8)	39 (17.6)	5 (7.8)	7 (7.4)
Weeks	11 (5.6)	21 (6.6)	9 (6.8)	16 (7.2)	2 (3.1)	5 (5.3)
Months	36 (18.3)	50 (15.8)	23 (17.3)	30 (13.6)	13 (20.3)	20 (21.1)
Years	37 (18.8)	68 (21.5)	23 (17.3)	43 (19.5)	14 (21.9)	25 (26.3)
Dont' know	52 (26.4)	80 (25.3)	40 (30.1)	60 (27.1)	12 (18.8)	20 (21.1)

Table 2. Victims' characteristics (%)

Generally, the victim and the stalker know each other; however, in the offline stalking cases the relationship between the two is closer than cyberstalking where the emotional bond is not so close.

To see if there was a relation between stalking victimization and cyberstalking victimization, a chi-square test was conducted. There was a significant relation between these two forms of victimization, χ^2 (1, n=1078) = 65.508, p<.000, although it is true that the strength of the association is weak (Cramer's V = .247) (See Table 3). The same test was carried out to analyze the same relationship between forms of victimization, but differentiating the country of origin. In the case of Spain, the relationship between the variables was significant (χ^2 (1, n = 643) = 73.123, p <.000; Cramer's V =.337), as in the United States (χ^2 (1, n = 435) = 5.225, p <.022; Cramer's V = .110). If we compare the results of both countries, we can say that Spanish students claim to have been victims of stalking both online and offline more often than U.S. students, although it is true that the difference is not very pronounced. A limitation that we must take into account is that there were more Spanish students than American students participating in the sample, which could explain the above results.

		Offline Stalking Victimization		χ^2	Cramer's V
		No	Yes		
Cyberstalking Victimization	No	53.4	17.3	65.508*	.247
	Yes	28.3	1		
p<.000					

Table 3. Relationship between stalking victimization and cyberstalking (%)

The next step was to analyze the differences based on the gender, and the country of residence of the victim, and separating them according to the type of stalking reported. In this sense, a chi-square test was conducted to investigate if there was a systematic relation between country and cyberstalking victimization on females and males. There was a significant relation in the group of females between their country and becoming a victim of cyberstalking (χ^2 (1, n =861) = 18.800, p <.000), which was absent in the case of males (χ^2 (1, n=212) = 1.278, p <.258). The same procedure was used to analyze the relation between country and offline stalking victimization in men and women. Again, there was a significant relation in the women's group (χ^2 (1, n = 860) = 5.618, p <.018) but not in men's (χ^2 (1, n = 212) = 1.185, p <.276).

Overall, these results indicate that there is a significant relation between the country where the victim lives and the type of victimization females suffer.

5. Discussion and Conclusions

The fact that there's scarce literature in Spain about the phenomenon of stalking and cyberbullying is not surprising, as it is a relatively new crime in our context. However, in Anglo-Saxon countries, and especially in the United States, there is more experience in this regard. One of the main problems when we do research on stalking is the lack of agreement to define what is stalking and what is cyberstalking (Owns, 2016). Currently, there is no universally accepted definition of stalking either in the legal sphere or in the academic arena. Nevertheless, we have identified three common and overlapping elements: the repetition, the victim or the fact that the victim does not wish to receive these behaviours and the negative consequence derived from the conduct of stalking.

As mentioned in the literature review, stalking is a phenomenon present in society that affects about 11 to 20% of the population; generally, those who are at greater risk of being victimised are young women, especially those that are in a university/college context (Basile et al., 2006; Baum et al., 2009; FRA, 2014; Tjaden & Thoennes, 1998). That explains why stalking research has focused mainly on the university context. This also accords with our earlier observations, which showed that females reported, to a greater extent, becoming victims of stalking in both Spain and the United States.

One of the objectives of the project was to identify the differences in the prevalence of stalking and cyberstalking victimization in Spain and in the U.S. The results are consistent with previous studies (Cavezza & McEwan, 2014): single females are at a higher risk of being stalked and cyberstalked by males in both countries and there is usually some kind of previous relationship between them. It has also been observed that the bond between the two parts in offline stalking cases is narrower than in cyberstalking cases. This result may be explained by the fact that stalking someone in the physical world implies a more direct contact with the victim than in an online world. Having a previous relationship between the two makes it easier to find that physical contact. In this regard, it's interesting to note that cyberstalking victims in the U.S. usually live in student apartments and offline victims tend to live in campus dorms. Thus, the closeness and proximity between victims and perpetrators could explain offline stalking.

Another important finding was that the number of victims of stalking and cyberstalking that reported that the victimization occurred during a period of years was higher than those who reported that the victimization occurred for months or weeks or days. A possible explanation for this fact is that the victims who are stalked, either offline or online, for a longer time are more aware and can better identify the stalking victimization process to which they are being subjected. The victims who have been stalked for days or weeks will not recognise the process as easily and could have a harder time identifying themselves as victims. However, caution must be applied as the findings might not be representative.

It has been suggested that men are more exposed to being victims of cyberstalking than women and that women are at a higher risk of becoming victims of offline stalking (Alexy et al., 2005; Reyns & Fisher, 2018). This does not appear to be the case. Contrary to expectations, this study found that men claim to be victims of offline stalking more often than cyberstalking, while females claim to be victims of cyberstalking more often than offline stalking in both countries. A possible explanation for this might be that both men and women are more sensitized to this type of behavior and therefore, they can identify it. Further research should be undertaken to investigate in this regard.

Finally, this is an exploratory study, therefore it is necessary to continue investigating. Future investigations will be aimed at learning about the relation between stalking and cyberstalking denounced by the victims, as well as seeing what strategies they use to face the situation of stalking. In this way, legislative and social proposals can be carried out taking into account all these issues. In addition, since it is a comparative study, it will be possible to analyze the differences between coping strategies and overcoming in each country, and to see, therefore, what works and what does not work so that what we find that does work can be implemented everywhere.

References

ALEXY, Eileen M., BURGESS, Anne W., BAKER, Timothy and SMOYAK, Shirley A. Perceptions of cyberstalking among college students. In: *Brief Treatment and Crisis Intervention*. 2005. Vol. 5, No. 3, pages 279-289. ISSN 1474-3310. DOI: http://dx.doi.org/10.1093/brief-treatment/mhi020

BASILE, Kathleen C., SWAHN, Monica H., CHEN, Jieru and SALTZMAN, Linda E. Stalking in the United States. Recent National Prevalence Estimates. In: *American Journal of Preventive Medicine*. 2006. Vol. 31, No. 2, pages 172-175. ISSN 0749-3797. DOI: https://doi.org/10.1016/j.amepre.2006.03.028

BAUM, Katrina, CATALANO, Shannan, RAND Michael and ROSE, Kristina. Stalking victimization in the United States (NCJ 224527). *Washington, DC: Bureau of Justice Programs, US Department of Justice*. 2009.

BLACK, Michele C., BASILE, Kathleen C., BREIDING, Matthew J., SMITH, Sharon G., WALTERS, Mikel L., MERRICK, Melissa T., et al. *The national intimate partner and sexual violence survey (NISVS): 2010 summary report*. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention. 2011.

BOCIJ, Paul, GRIFFITHS, Mark and MCFARLANE, Leroy. Cyberstalking: A new challenge for criminal law. In: *The Criminal Lawyer*. 2002. Vol. 122, pages 3-5. ISSN 2049-8047.

BOCIJ, Paul and MCFARLANE, Leroy. Seven fallacies about cyberstalking. In: *Prison Service Journal*. 2003. Vol. 149, pages 37-42. ISSN 2046-4215.

CAVEZZA, Cristina and MCEWAN, Troy E. Cyberstalking versus off-line stalking in a forensic sample. In: *Psychology, Crime & Law*. 2014. Vol. 20, No. 10, pages 955-970. ISSN 1068-316X. DOI: https://doi.org/10.1080/1068316X.2014.893334

FINN, Jerry. *A survey of online harassment at a university campus. In: Journal of Interpersonal Violence*. 2014. Vol. 19, No. 4, pages 468-483. ISSN 0886-2605. DOI: https://doi.org/10.1177/0886260503262083

FISHER, Bonnie S., CULLEN, Francis T. and TURNER, Michael G. Being Pursued: Stalking Victimization in a National Study of College Women. In: *Criminology & Public Policy*. 2006. Vol. 1, No. 2, pages 257-308. ISSN 1538-6437. DOI: https://doi.org/10.1111/j.1745-9133.2002.tb00091.x

FRA. *Violence against women: an EU-wide survey. Main Results*. Luxembourg: Publications Office of the European Union. 2014.

LEE, Rebecca. Romantic and Electronic Stalking in a College Context. In: *William and Mary Journal of Women and the Law*. 1998. Vol. 4, No. 2, 373-466. ISSN 1081-549X.

LEÓN, Carmen M. and AIZPURÚA, Eva. Prevalencia y denuncia de conductas de acoso en estudiantes universitarios. In: *Indret: Revista para el análisis del Derecho*. 2019. No. 1, pages 1-19. ISSN 1698-739X.

MAPLE, Carsten, SHORT, Emma and BROWN, Antony. *Cyberstalking in the United Kingdom: An analysis of the ECHO pilot survey*. University of Bedfordshire. 2011.

MILLER, Laurence. Stalking: Patterns, motives, and intervention strategies. In: *Aggression and Violent Behavior*. 2012. Vol. 17, No. 6, pages 495-506. ISSN 1359-1789. DOI: https://doi.org/10.1016/j.avb.2012.07.001

MULLEN, Paul E., MACKENZIE, Rachel, OGLOFF, James R. P., PATHÉ, Michele, MCEWAN, Troy and PURCELL, Rosemary. Assessing and Managing the Risks in the Stalking Situation. In: *Journal of the American Academy of Psychiatry and the Law Online*. 2006. Vol. 34, No. 4, pages 439-450. ISSN 1093-6793.

NOBLES, Matt R., FOX, Kathleen A., PIQUERO, Nicole and PIQUERO, Alex R. Career Dimensions of Stalking Victimization and Perpetration. In: *Justice Quarterly*. 2009. Vol. 26, No. 3, pages 476–503. ISSN 0741-8825. DOI: https://doi.org/10.1080/07418820802427833

NOBLES, Matt R., REYNS, Bradford W., FOX, Kate A. and FISHER, Bonnie S. Protection Against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization Among a National Sample. In: *Justice Quarterly*. 2014. Vol. 31, No. 6, pages 986-1014. ISSN 0741-8825. DOI: https://doi.org/10.1080/07418825.2012.723030

OWENS, Jennifer Gatewood. Why Definitions Matter: Stalking Victimization in the United States. In: *Journal of Interpersonal Violence*. 2016. Vol. 31, No. 12, pages 2196-2226. ISSN 0886-2605. DOI: https://doi.org/10.1177/0886260515573577

REYNS, Bradford W., HENSON, Billy and FISHER, Bonnie S. Being Pursued Online: Applying Cyberlifestyle–Routine Activities' Theory to Cyberstalking Victimization. In: *Criminal Justice and Behavior*. Vol. 38, No. 11, pages 1149-1169. ISSN 0093-8548. DOI: https://doi.org/10.1177/0093854811421448

REYNS, Bradford W. and FISHER, Bonnie S. The Relationship Between Offline and Online Stalking Victimization: A Gender-Specific Analysis. In: *Violence and Victims*. 2018. Vol. 33, No. 4, pages 769-786. ISSN 0886-6708. DOI: https://doi.org/10.1891/0886-6708.VV-D-17-00121

REYNS, Bradford W. and SCHERER, Heidi. *Stalking Victimization Among College Students: The Role of Disability Within a Lifestyle-Routine Activity Framework. Crime & Delinquency.* 2018. Vol. 64, No. 5, pages 650–673. ISSN 0011-1287. DOI: https://doi.org/10.1177/0011128717714794

SHERIDAN, Lorraine P. and GRANT, Tim. Is cyberstalking different? In: *Psychology, Crime & Law*. 2007. Vol. 13, No. 6, pages 627-640. ISSN 1068-316X. DOI: https://doi.org/10.1080/10683160701340528

SHOREY, Ryan C., CORNELIUS, Tara L. and STRAUSS, Catherine. Stalking in College Student Dating Relationships: A Descriptive Investigation. In: *Journal of Family Violence*. 2015. Vol. 30, No. 7, pages 935-942. ISSN 0885-7482. https://psycnet.apa.org/doi/10.1007/s10896-015-9717-7

SHORT, Emma, LINFORD, Sarah, WHEATCROFT, Jacqueline M. and MAPLE, Carsten. The impact of cyberstalking: The lived experience - A thematic analysis. In: *Stud Health Technol Inform*. 2014. Vol. 199, pages 133-137. ISSN 0926-9630. DOI: https://doi.org/10.3233/978-1-61499-401-5-133

SPITZBERG, Brian H. and CUPACH, William R. The state of the art of stalking: Taking stock of the emerging literature. In: *Aggression and Violent Behavior*. 2007. Vol. 12, No. 1, pages 64-86. ISSN 1359-1789. https://doi.org/10.1016/j.avb.2006.05.001

TJADEN, Patricia G. and THOENNES, Nancy. *Stalking in America: findings from the National Violence Against Women Survey.*

VILLACAMPA, Carolina and PUJOLS, Alejandra. Prevalencia y dinámica de la victimización por stalking en población universitaria. In: *Revista Española De Investigación Criminológica*. 2017a. Vol. 15, pages 1-27. ISSN 1696-9219.

Recommended citation

FERNÁNDEZ-CRUZ, Victoria; AGUSTINA, José R.; NGO, Fawn T. (2021). «An Exploratory Investigation of Traditional Stalking and Cyberstalking Victimization among University Students in Spain and the United States: A Comparative Analysis». *IDP. Revista de Derecho, Internet y Política*, No. 32, pp. 1-14. UOC [Accessed: dd/mm/yy] http://dx.doi.org/10.7238/idp.v0i32.373814

About the authors

Victoria Fernández-Cruz
vfcruz@uic.cat

Victoria Fernández-Cruz is a predoctoral scholar at UIC Barcelona and a counsellor at the Open University of Catalonia (UOC). Her research interests focus on criminological theories, forensic psychopathology and victimization. She is currently developing a doctoral thesis on the phenomenon of stalking and cyberstalking, analyzing the prevalence, attitudes and processes of perpetration and victimization in these types of behaviors.

José R. Agustina
jragustina@uic.es

José R. Agustina is an Associate Professor of Criminal Law at Universitat Abat Oliba CEU. Author of more than 50 articles in indexed journals and four monographs. He currently directs the Actualidad Criminológica y Penal Collection at BdeF-Edisofer. His research interest focuses on cybercrime against people (sexting, stalking and grooming) and cybervictimization in minors; crimes in the workplace, crime prevention strategies and compliance; sexual and privacy crimes; theory of crime and criminological theories.

Fawn T. Ngo
fawnngo@sar.usf.edu

Fawn T. is an Associate Professor of Criminology at the University of South Florida. Her research interests include criminological theory, interpersonal violence, cybercrime, and predictive analytic applications in criminology and criminal justice. Her work has appeared in Justice Quarterly, Crime and Delinquency, Journal of Criminal Justice, International Journal of Cyber Criminology, and Policing: An International Journal of Police Strategies and Management.

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

www.uoc.edu/idp

ARTÍCULO

Las intimaciones judiciales en la Ley de secretos empresariales

Consuelo Ruiz de la Fuente
Universidad Autónoma de Barcelona

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

Resumen

Con la Ley 1/2019 el legislador español transpone la Directiva Europea 2016/943 y da la necesaria protección a los secretos empresariales. Se trata de aportar seguridad jurídica en un ámbito delicado donde la clave está en ser eficaces. Poco se logra si se prevé la protección del secreto empresarial pero no se establecen medidas eficaces para que este secreto siga siéndolo, y en caso de vulneración, garantizar la adopción de todas las medidas necesarias para recomponer la situación hasta antes de aquella vulneración, minimizando las consecuencias negativas ocasionadas al titular del secreto que haya sido perjudicado, e incluso indemnizarlo debidamente por los daños sufridos. Por último, también se deben adoptar las medidas necesarias para evitar que dicha vulneración se repita en el futuro. Precisamente para maximizar la eficacia de la protección, surge la intimación judicial como una herramienta legal ágil, económica y disponible para los tribunales, que garantiza las acciones civiles previstas en la Ley 1/2019 y el cumplimiento de las resoluciones judiciales adoptadas en este ámbito, cuyo fin último es mejorar las condiciones, el marco para el desarrollo y la explotación de la innovación y la transferencia de conocimientos.

Palabras clave

secreto empresarial, indemnización coercitiva, intimación judicial, ejecución civil

Judicial orders in the trade secrets law

Abstract

With Law 1/2019, the Spanish legislator transposes EU Directive 2016/943, and gives the necessary protection to trade secrets, in order to contribute to legal certainty in a delicate field, where the key is effectiveness. The legal protection of the trade secret is of little use if it is not accompanied by effective measures so that this secret is kept, and in case of violation, ensuring the adoption of all the necessary measures in order to re-establish the situation to that which existed before the violation, minimising the negative consequences that the said violation has occasioned to the prejudiced owner of the secret, and also compensating him/her properly for the damages already occasioned. Finally, the necessary measures must also be adopted to prevent the said violation from happening again in the future. In order to maximise the efficacy of the protection, judicial orders arise as an agile and inexpensive legal tool, available to the Courts, that allows them to guarantee the civil actions provided in Law 1/2019 and secures compliance with the judicial decisions adopted in this field, the ultimate goal being to improve conditions, the framework for the development and use of innovation, and the transfer of knowledge.

Keywords

trade secrets, coercive compensation, judicial orders, civil enforcement

1. La nueva regulación de la intimación judicial en materia de secretos empresariales

En materia de protección de secretos empresariales, la Unión Europea aprobó la Directiva (UE) 2016/943 del Parlamento Europeo y Consejo de 8 de junio de 2016, con el objeto de proteger los secretos empresariales contra su obtención, utilización o revelación ilícitas por terceros. La directiva pretende armonizar la legislación de los Estados miembros con el fin de establecer un nivel suficiente y comparable de reparación en todo el mercado interior en caso de apropiación indebida de secretos empresariales.

Es una legislación que nace con una clara vocación de eficacia. La propia exposición de motivos de la directiva establece que «La eficacia de las medidas, procedimientos y recursos a disposición de los poseedores de secretos comerciales podría verse mermada en caso de incumplimiento de las correspondientes resoluciones adoptadas por las autoridades judiciales competentes. Por este motivo, es necesario garantizar que dichas autoridades dispongan de poderes sancionadores adecuados». Tratándose de derechos inmateriales, es lógico que tengan preponderancia las instituciones procesales que deben garantizarlos.

Siguiendo esta senda, en España se dicta la Ley 1/2019 de 20 de febrero, que regula el secreto empresarial. En la exposición de motivos, el legislador nacional reconoce que la falta de instrumentos jurídicos eficaces y comparables para la protección de los secretos empresariales menoscaba los incentivos para emprender actividades asociadas a la innovación e impiden que los secretos empresariales puedan liberar su potencial como estímulos de crecimiento económico y del empleo. Por lo tanto, se trata de garantizar que los secretos empresariales se encuentren protegidos de manera adecuada y que se mejoren las condiciones y el marco para el desarrollo y la explotación de la innovación y la transferencia de conocimientos. Prácticamente la mitad de la nueva regulación está conformada por normas procesales.

El secreto empresarial[1] es cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero que reúna las siguientes condiciones (art. 1 Ley 1/2019):

a) Ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas;

b) tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto; y

c) haber sido objeto de medidas razonables, por parte de su titular, para mantenerlo en secreto.

Algunos ejemplos de informaciones que puedan estar protegidas por secretos empresariales son: fórmulas químicas o matemáticas; procesos de fabricación; información sobre organización o mantenimiento de un producto o una planta industrial; un producto y sus especificaciones técnicas; información comercial, financiera y organizativa; estrategias, planes de negocio y *marketing*; información sobre clientes y proveedores; fuentes de financiación, contratos y costes de producción[2].

A la hora de proteger la defensa de los secretos empresariales, el legislador ha optado por convertir en acciones lo que en la Directiva 2016/943 eran los distintos tipos de requerimientos y medidas correctivas por la infrac-

1. La doctrina considera un acierto que la ley se refiera a «secretos empresariales» y no a «secretos comerciales» como lo hace la directiva, ya que el calificativo *comercial* deja fuera el secreto industrial. Por eso es más adecuado referirse al «secreto empresarial», que comprende tanto el secreto comercial como el secreto industrial, y que es equiparable al término anglosajón de *know-how*. Ver García Vidal (2019, pág. 2).

2. Protocolo de Protección del Secreto Empresarial en los Juzgados Mercantiles. Sección de Derecho de la Competencia, Tribunal Mercantil de Barcelona de 2019: https://www.oepm.es/export/sites/oepm/comun/documentos_relacionados/Noticias/2019/2019_11_22_Protocolo_Proteccion_Secreto_Empresarial_en_los_JM.pdf

la infracción de un secreto empresarial[3], y siguiendo al modelo anglosajón en esta materia, se configura en gran medida la posición jurídica del «poseedor» del secreto a través de las acciones ejercitables[4]. Se contemplan una serie de acciones civiles dirigidas a aquellas personas físicas o jurídicas que vulneren dichos secretos, o incluso a terceros que, de buena fe, hubieran obtenido acceso al secreto empresarial directa o indirectamente de un infractor. Dichas acciones civiles, previstas por el art. 9 de la Ley 1/2019, son:

a) La declaración de la violación del secreto empresarial.

b) La cesación o, en su caso, la prohibición de los actos de violación del secreto empresarial.

c) La prohibición de fabricar, ofrecer, comercializar o utilizar mercancías infractoras o de su importación, exportación o almacenamiento con dichos fines.

d) La aprehensión de las mercancías infractoras, incluida la recuperación de las que se encuentren en el mercado, y de los medios destinados únicamente a su producción, siempre que tal recuperación no menoscabe la protección del secreto comercial en cuestión, con una de las siguientes finalidades: su modificación para eliminar las características que determinen que las mercancías sean infractoras, o que los medios estén destinados únicamente a su producción, su destrucción o su entrega a entidades benéficas.

e) La remoción, que comprende la entrega al demandante de la totalidad o parte de los documentos, objetos, materiales, sustancias, ficheros electrónicos y cualesquiera otros soportes que contengan el secreto empresarial, y en su caso su destrucción total o parcial.

f) La atribución en propiedad de las mercancías infractoras al demandante, en cuyo caso el valor de las mercancías entregadas podrá imputarse al importe de la indemnización de daños y perjuicios debida, sin perjuicio de la subsistencia de la responsabilidad del infractor en lo que se refiere a la cuantía indemnizatoria que exceda del referido valor. Si el valor de las mercancías excede del importe de la indemnización, el demandante deberá compensarlo a la otra parte.

g) La indemnización de los daños y perjuicios, si ha intervenido dolo o culpa del infractor, que será adecuada respecto de la lesión realmente sufrida como consecuencia de la violación del secreto empresarial.

h) La publicación o difusión completa o parcial de la sentencia, que deberá preservar en todo caso la confidencialidad del secreto empresarial en los términos del art. 15 de esta ley.

Como se puede observar, varias de dichas acciones consisten esencialmente en obligaciones de dar, hacer o no hacer a cargo del demandado. Lo que realmente busca el legislador con esta norma es precisamente que el infractor cese en la vulneración de los derechos protegidos por el secreto empresarial; por tanto, la sentencia va a contener una orden judicial en este sentido, y para que esta sea realmente efectiva, deberá adoptar la forma de una intimación judicial.

Como parte de sus poderes de dirección del proceso, el órgano judicial está facultado para emitir intimaciones judiciales con el fin de compeler a partes o terceros a cumplir con sus obligaciones procesales y colaborar así con la buena marcha del proceso. En anteriores trabajos, hemos definido la intimación judicial como aquel acto de comunicación del órgano jurisdiccional, dirigida a cualquier persona, con el objeto de compelerla a la realización o abstención de determinada conducta, informándole también de las consecuencias jurídicas de su inobservancia, cuando sea necesaria su colaboración en un proceso determinado[5]. Así, estas resultan ser una herramienta disponible para los órganos jurisdiccionales, e idónea para hacer cumplir las obligaciones a cargo del

3. El antecedente directo lo encontramos en el art. 12 de la Directiva Europea 2016/943 UE, que establece los requerimientos y medidas coercitivas que los Estados miembros garantizarán que puedan adoptarse cuando se haya dictado una resolución judicial por la que se declare vulnerado un secreto empresarial.

4. En este sentido, Arroyo Aparicio (2019, pág. 5) considera que la parte más relevante del texto europeo viene integrada por el requerimiento dirigido a los Estados miembros a fin de garantizar el ejercicio de las acciones civiles pertinentes.

5. Ver Ruiz de la Fuente (2011, pág. 64 y sigs).

condenado. Son herramientas contenidas en la ley, y en el ámbito de los secretos empresariales, presentan caracteres específicos por las medidas concretas que pueden acompañarla.

En efecto, para reforzar el cumplimiento de estas pretensiones, el legislador establece que en los supuestos que van desde las letras a) a la f) citadas anteriormente, el juez establecerá en la sentencia una *indemnización coercitiva* por día transcurrido, hasta que se produzca el cumplimiento de la propia sentencia.

La normativa comunitaria que se está transponiendo no tiene una institución equivalente, sino que únicamente exige, para el caso de incumplimiento de las medidas impuestas en sentencia, multas coercitivas periódicas que sean «efectivas, proporcionadas y disuasorias» (art. 16 Directiva 2016/943). Esta previsión presenta algunos aspectos novedosos que se deducen de su propio nombre, al constituir un híbrido entre 1) la multa coercitiva que puede acompañar a una intimación judicial y 2) la indemnización de los perjuicios que el favorecido por la intimación sufre por su incumplimiento. Al ser la directiva solo de mínimos, nada impide que el legislador español prevea una indemnización coercitiva que en sí puede reforzar su efectividad.

La aplicación de la indemnización coercitiva consiste en una medida de especial importancia para doblegar voluntades renuentes al cumplimiento de una condena de cese en las acciones por vulneración de secreto empresarial. La imposición de una indemnización por cada día que pase sin que se dé cumplimiento a la condena refuerza la eficacia de la sentencia y garantiza el principio de seguridad jurídica. Aún habrá que esperar para saber cómo aplicarán los tribunales dicha norma. La doctrina, por su parte, en la voz de Gascón Inchausti, considera que la adecuada aplicación de la norma va a requerir que los jueces y abogados no tengan reparos en desenvolverse con aplomo en entornos caracterizados por la presencia de conceptos jurídicos indeterminados, como la razonabilidad, proporcionalidad y adecuación, lo que resulta necesario para abordar de forma eficaz una realidad compleja y a veces poco nítida[6].

2. Particularidades de las intimaciones judiciales en materia de secretos empresariales

La intimación judicial para la protección de secretos empresariales tiene la particularidad de que por regla general estará contenida, por mandato legal expreso, en la propia sentencia. Por lo que debemos partir del supuesto de que solo tendrá lugar si hay sentencia que condene al demandado por vulneración del secreto empresarial. No obstante, en atención a que la intimación formará parte del contenido de la sentencia, también se podría pedir como medida cautelar, precisamente para asegurar la eficacia de la propia sentencia, siempre que concurran los requisitos propios de estas medidas. En definitiva, si la parte lo pide, ya que es necesaria instancia de parte (art. 721 LEC), y el tribunal lo considera apropiado, antes de conocer el fondo del asunto podrá dictar como medida cautelar que el presunto infractor se abstenga de seguir realizando determinada actividad o de difundir determinada información, entre otras disposiciones.

Por otra parte, esta intimación no puede ser incorporada de oficio a la sentencia, sino que debe haber sido pedida por la actora en su demanda. Es consecuencia lógica de la aplicación del principio dispositivo que rige en este ámbito. Entendemos que no podría ser solicitada en un momento posterior, por el límite establecido en el art. 412.1 LEC. Solo podría dejarse para un momento posterior alguna petición complementaria, como la alegación de algún detalle referente al importe de la indemnización coercitiva o a la duración o extensión de la intimación judicial, pero en ningún caso se podrá alterar sustancialmente las pretensiones de la demanda.

Por lo tanto, para que exista intimación, deben concurrir los siguientes presupuestos:

1) Que se hubieren interpuesto alguna de las acciones civiles en defensa de los secretos empresariales enumerados en las letras a) a la f) del art. 9.1 de la Ley 1/2019.

2) Que el actor pida expresamente al tribunal la intimación al demandado y la imposición de una indemnización coercitiva por incumplimiento.

6. Gascón (2018, pág. 2).

3) Que exista sentencia de condena en el proceso en cuestión, sin perjuicio de que pueda ser adoptada también mediante auto de medidas cautelares.

Si concurren estos presupuestos, entendemos que el tribunal deberá incluir, en todo caso, la correspondiente intimación judicial en su sentencia, ya que el legislador no parece preverlo como una facultad del tribunal, atendida la literalidad del precepto que señala que, si se dan los supuestos, «la sentencia fijará...» (art. 9.6 Ley 1/2019).

Las intimaciones judiciales estarán vigentes desde que las dicte el órgano judicial, y serán exigibles para el demandado desde que le sea notificada la sentencia o auto de medidas cautelares en la que está contenida aquella intimación. Si la intimación contiene un plazo para el cumplimiento, serán exigibles desde que se cumpla dicho plazo.

Hay que tener en cuenta que no hace falta esperar a la ejecución para que el contenido de la orden judicial sea exigible, ni tampoco esperar que exista un incumplimiento posterior a la sentencia para reiterar el requerimiento. Esto también es predicable de las sentencias no firmes que estimen las acciones indicadas en la medida en que los pronunciamientos, por su naturaleza de condena, podrán por lo general ser objeto de ejecución provisional (art. 456.3 y 524 LEC). Precisamente, la intención del legislador es proteger el secreto empresarial desde que es declarada su existencia y vulneración en la sentencia, por lo que la propia sentencia judicial ha de contener una intimación judicial completa que ordene en forma precisa las acciones o prohibiciones que debe cumplir el requerido condenado, y también los apercibimientos o consecuencias que puede conllevar el incumplimiento de esta.

Lo que se busca con la intimación judicial es disuadir al infractor para que se abstenga de seguir vulnerando el secreto empresarial o, en su caso, reponer las actuaciones fraudulentas. Por ejemplo, si se impone la aprehensión de las mercancías fraudulentas o la entrega al actor de documentos o soportes que contengan el secreto empresarial. Excepcionalmente, si se adopta como medida cautelar, hay que recordar que su entrada en vigor quedará supeditada a la previa prestación de la caución que pueda haber fijado el juez (art. 737 LEC).

Por otra parte, las medidas de cesación y prohibición, y la consiguiente indemnización coercitiva, dejarán de tener efecto si la información en cuestión deja de tener el carácter de secreto empresarial por causas no atribuibles directa o indirectamente al infractor condenado. No obstante, en este supuesto, es el infractor quien deberá solicitar que las medidas adoptadas se extingan o queden sin efecto. Esta medida venía impuesta por la Directiva comunitaria en su art. 13.2. Esta pretensión deberá instarse por los cauces de un nuevo procedimiento declarativo, porque la ley española no establece ninguna solución procesal específica para dejarla sin efecto, aunque hubiese sido deseable que lo hiciera. Solo para el caso de que se hubieran adoptado con carácter cautelar, la ley española expresamente prevé el posible alzamiento inmediato de las medidas cautelares por este motivo (art. 24 Ley 1/2019).

3. Estructura de la intimación judicial en materia de secretos empresariales

Las intimaciones judiciales deberán tener una estructura con un contenido mínimo del cual no se podrá prescindir. En efecto, la intimación judicial es una institución procesal compleja, compuesta por una serie de elementos definitorios objetivos y subjetivos, así como de efectos procesales y extraprocesales. El legislador no siempre es lo suficientemente explícito ni regula la institución de forma sistemática, por lo que se hace necesario su sistematización y explicitación. La estructura que proponemos se fundamenta en nuestras investigaciones previas sobre la institución[7]. A continuación, analizamos pues la estructura de las intimaciones judiciales en materia de secretos empresariales y su contenido mínimo.

3.1. Requerimiento y destinatario

El destinatario de la intimación será el autor de la infracción de la Ley de secretos empresariales, ya sea una persona física o jurídica. Mediante la intimación judicial se requerirá al demandado para que cumpla con la orden judicial correspondiente.

7. Ruiz de la Fuente (2011).

Ahora bien, también puede darse que sea un tercero de buena fe quien haya adquirido las mercancías objeto de la infracción o documentos u otros soportes que infrinjan los secretos empresariales protegidos por la ley. En este supuesto, si queremos que se vea afectado por la intimación judicial, es necesario que el tercero de buena fe sea también demandado en el proceso declarativo correspondiente. Entendemos que no sería suficiente una simple notificación vía art. 150.3 LEC. La intimación judicial estará dirigida al propio tercero de buena fe como demandado, según se desprende del propio art. 9.7 de la Ley 1/2019.

Pero, en este caso del tercero de buena fe, las medidas objeto de las acciones dispuestas en el apartado 1 del art. 9 podrán sustituirse por el pago de una indemnización pecuniaria a favor de la actora, siempre que dicho pago sea suficientemente satisfactorio y la ejecución de las medidas supongan un perjuicio desproporcionado para el tercero de buena fe demandado. En todo caso, el legislador dispone que la indemnización pecuniaria que sustituya la cesación o prohibición no exceda al importe que habría tenido que pagar al titular del secreto empresarial por la concesión de una licencia que habría permitido utilizarlo durante el período en el que su utilización hubiera podido prohibirse (art. 9.7 Ley 1/2019).

La petición de sustitución deberá ser efectuada por el tercero de buena fe en su contestación a la demanda. Esta parece ser la voluntad del legislador ya que el propio art. 9.7 de la Ley 1/2019 refiere que quien tiene esta capacidad de sustitución es el «demandado». La economía procesal también aboga por esta opción. Esto implica que no cabe dejar esta petición de sustitución para un juicio posterior, una vez exista la sentencia que establezca la intimación. Y también excluye que sea solicitada en ejecución de sentencia por el tercero de buena fe demandado. Recordemos que será necesario discutir que se dan los presupuestos para la sustitución y la cuantía de la indemnización, lo que es propio de un declarativo.

Si no se sustituye en la sentencia, en caso de incumplimiento, en ejecución de sentencia, lo que deberá hacer el demandado tercero de buena fe es cumplir con la intimación judicial o abonar la indemnización coercitiva si no cumple en el marco de una ejecución no dineraria. Si en sentencia se sustituye la intimación por la indemnización, en cambio, y el tercero de buena fe no cumple voluntariamente con el contenido de la intimación judicial, deberá instarse una ejecución dineraria ya que aquí se tratará de una condena al pago de una cantidad de dinero exclusivamente.

3.2. Notificación

La notificación de la intimación judicial por vulneración de secretos empresariales no tendrá mayores complejidades, pues al estar contenida en la propia sentencia será notificada junto con ella en la forma prevista en la ley.

No obstante, hay que precisar que eventualmente, además de los apremios económicos dispuestos en la ley y que se pueden imponer en caso de incumplimiento de la intimación judicial, el requerido también podría incurrir en responsabilidad penal por un delito de desobediencia a la autoridad (art. 556 CP). Este tema lo abarcaremos más adelante; no obstante, cabe mencionar ahora que, para que exista responsabilidad penal, es necesario que la intimación judicial sea notificada de forma personal al requerido mediante la entrega de una copia literal de la resolución, o bien mediante la entrega de esta a través de correo, que deberá ser certificado y con acuse de recibo. De lo contrario, el requerimiento tendrá que ser reiterado en sede penal[8].

3.3. Plazo

La existencia de plazo para cumplir dependerá del contenido concreto de la intimación de que se trate. Generalmente, si la intimación impone una prohibición de determinados actos o conductas, o la cesación de determinada actividad, el cumplimiento será exigible en forma automática desde la notificación, por lo que no existirá plazo para cumplir.

No obstante, el tribunal podrá imponer al infractor aquella obligación de cesación o prohibición, pero limitada a cierto período de tiempo. Dicha duración, que será precisada en la intimación, deberá ser, en todo caso, suficiente para eliminar cualquier ventaja competitiva o económica que el infractor hubiera podido extraer de la violación del secreto (art. 9.4 Ley 12/2019).

8. Ver apartado 3.7.

Si la intimación obliga a la realización de conductas positivas como la aprehensión o entrega de mercancías infractoras, documentos y medios destinados a la producción de aquellas, la intimación deberá contener un plazo concreto para que se produzca el cumplimiento voluntario. El plazo será fijado por el tribunal y dependerá de las particularidades del caso concreto, pero siempre deberá ser un plazo breve, en vistas a la celeridad del proceso y de la eficacia de la propia intimación.

En principio, el plazo establecido será improrrogable, salvo que el demandado destinatario de la intimación justifique, debida y oportunamente, que necesita una prórroga del plazo para dar el cumplimiento debido a la orden judicial. Es decir, antes de que el plazo establecido en la sentencia concluya. En cualquier caso, entendemos que esta prórroga solo debiera proceder en casos muy excepcionales, con una justificación contundente y acreditada, y por causas no imputables al demandado condenado.

3.4. Contenido

En las intimaciones judiciales el órgano judicial debe precisar en forma directa y concreta en qué consiste la obligación que ha de cumplir el demandado. En su resolución el tribunal habrá concretado cuál es la información que se considera secreto empresarial, así como dónde se encuentra contenida dicha información.

Para determinar qué medidas se van a adoptar para protección de los secretos empresariales, el tribunal deberá tener en consideración la proporcionalidad y las circunstancias del caso concreto, y entre ellas el valor y características del secreto empresarial en cuestión, las medidas que ya se hubieren adoptado para su protección, el comportamiento del infractor, las consecuencias de la violación del secreto empresarial, la probabilidad de que el infractor persista en la violación, los intereses legítimos de las partes, las consecuencias que podrían tener para las partes que se estimen o no las acciones ejercitadas, los intereses legítimos de terceros, el interés público y la salvaguarda de los derechos fundamentales (art. 9.3 Ley 1/2019).

La obligación podrá consistir en cesar determinada conducta o actividad, o en la prohibición de realizar ciertas conductas o actividades que según la sentencia constituyan una violación del secreto empresarial (art. 9.1.b) Ley 1/2019).

Además, la intimación puede contener una prohibición expresa de fabricar, ofrecer, comercializar o utilizar mercancías infractoras; o bien una prohibición de importación, exportación o almacenamiento de estas (art. 9.1.c) Ley 1/2019).

Asimismo, puede disponerse una orden de aprehensión de las mercancías infractoras, incluida la recuperación de las que se encuentren en el mercado, y de los medios destinados únicamente a su producción, siempre que tal recuperación no menoscabe la protección del secreto comercial en cuestión, con una de las siguientes finalidades: su modificación para eliminar las características que determinen que las mercancías sean infractoras, o que los medios estén destinados únicamente a su producción, su destrucción o su entrega a entidades benéficas (art. 9.1.d) Ley 1/2019).

También puede contener una orden de remoción que comprenda la entrega al demandante de todo o parte de los documentos, objetos, materiales, sustancias, ficheros electrónicos o cualesquiera otros soportes que contengan secreto empresarial; y en su caso la destrucción total o parcial de ellos (art. 9.1.e) Ley 1/2019).

Por último, la intimación puede contener la obligación de atribuir en propiedad las mercancías infractoras al demandante. En este caso, la ley dispone que el valor de las mercancías entregadas podrá imputarse al valor de la indemnización de daños y perjuicios debida, sin perjuicio de la subsistencia de la responsabilidad del infractor en lo que dice relación con la cuantía indemnizatoria que exceda del referido valor. Si finalmente el valor de las mercancías excede del importe de la indemnización, el demandante deberá compensarlo a la otra parte (art. 9.1.f) Ley 1/2019).

En este caso, lo más razonable es que el actor proponga el valor que se le ha de atribuir a aquellas mercancías, teniendo en consideración su precio en el mercado. Si no hubiere acuerdo entre las partes, no quedará más remedio que acudir a un peritaje para fijarlo.

Si el infractor condenado no cumple con la orden de entregar las mercancías, se deberá instar la correspondiente ejecución, y en ella incluso se podrá dictar una orden de entrada y registro en el lugar donde se encuentre la cosa, para poner al ejecutante en posesión de aquellas merca-

derías. Si fuera preciso, se podrá pedir auxilio a la fuerza pública para ello. Si, por el contrario, se desconoce dónde se encuentra la mercadería, deberán instarse las medidas de localización pertinentes para hallarlas, según lo que ha previsto el art. 701 de la LEC para la ejecución de la entrega de bienes muebles determinados. Lo mismo ocurrirá con la orden de remoción que no se cumple voluntariamente por parte del infractor; al respecto, puede ser necesaria en ejecución la orden de entrada y registro, y una vez removidas las mercaderías, archivos u otros documentos, podrán destruirse por un tercero a costa del infractor ejecutado, en los mismos términos que una ejecución de hacer no personalísimo.

Con todo, hay que tener en cuenta que estas acciones no son en absoluto incompatibles entre sí[9], por lo que se pueden pedir conjuntamente siempre que sean necesarias y proporcionadas.

3.5. Apercibimiento

Un punto clave en la efectividad de las intimaciones es que estas se hagan bajo el apercibimiento de las sanciones que se le pueden imponer al destinatario en caso de que incumpla con su obligación. El apercibimiento tiene una doble función: por un lado, constituye una presión psicológica para el destinatario, ya que se le hace saber las consecuencias que se derivarían de su negativa a cumplir, por lo que en definitiva comporta un incentivo para hacerlo. Por otro lado, es una garantía de seguridad jurídica para el demandante, quien, en caso de incumplimiento por parte del infractor condenado, podrá solicitar de inmediato la aplicación de los apremios correspondientes, sin que este último pueda alegar desconocimiento. Para cumplir los cometidos mencionados, es imprescindible que el tribunal especifique en términos precisos las consecuencias del no cumplimiento. Estudiamos a continuación los dos apremios que podrán formar parte del apercibimiento y su ejecución: la indemnización coercitiva y la responsabilidad penal.

3.6. Apremio económico: la indemnización coercitiva

Si el infractor destinatario de la intimación incumple la obligación impuesta en la misma, el primer apremio será económico y consistirá en el pago de una cantidad de dinero como «indemnización coercitiva». La imposición de este tipo de apremios económicos constituye una novedad importante introducida por la Ley de secretos empresariales, aunque es un mecanismo que ya está vigente en otros ámbitos de nuestro ordenamiento jurídico. Por ejemplo, la Ley de marcas 17/2001 de 7 de diciembre, en su art. 44, prevé que, cuando se condene a la cesación de los actos de violación de una marca, el tribunal fije una indemnización coercitiva de cuantía no inferior a los 600 euros por día transcurrido hasta que se produzca la cesación de la violación[10]. En este ámbito, la jurisprudencia ha establecido en forma explícita que no causa ningún tipo de indefensión el hecho de que en el fallo de la sentencia se fije el importe concreto de la indemnización coercitiva, luego en ejecución de sentencia se fijará el *dies a quo*[11].

Como hemos dicho, la imposición judicial de dicha indemnización coercitiva está dirigida a hacer efectiva la ejecución de las condenas no dinerarias, es decir, busca doblegar la voluntad del infractor, por lo que tendrán una naturaleza coercitiva y no meramente sancionadora[12]. En efecto, el propio legislador las denomina «indemnización

9. En este sentido, Gascón (2018, pág. 1).
10. La doctrina valora positivamente la indemnización coercitiva prevista en el art. 44 de la Ley de marcas, por reforzar la seguridad jurídica y la eficacia de las sentencias judiciales (Castán, 2016). Otros ejemplos de imposición de apremios económicos en el proceso civil español pueden verse en Ruiz de la Fuente (2011, pág. 330).
11. STS 302/2016 de 9 de mayo (RJ 2016\2463); SAP de Valencia de 3 de junio de 2010 (sección 9.ª) 743/2016 de 17 de junio (AC 2016\1452).
12. En el ámbito de la indemnización coercitiva prevista en el art. 44 de la Ley de marcas, la Audiencia Provincial de Alicante se refiere expresamente a la finalidad de aquella, y sostiene: «La indemnización coercitiva tiene como finalidad, una vez que los términos de la condena de cesación de los actos de violación de una marca son claros (...), incitar al ejecutado, que voluntaria y conscientemente los ignora, a respetarlos. Exige, pues, una conducta conscientemente reticente al cumplimiento del fallo condenatorio, en lo que respecta a cesar en los actos de violación de marca ajena», AAP de Alicante (sección 8.ª) 120/2015 de 8 de octubre de 2015 (FJ 2.º). Por su parte, el AAP de Granada (sección 3.ª) 208/2017 de 12 de diciembre, analiza ampliamente la indemnización coercitiva del art. 44 de la Ley de marcas, y sostiene en su fundamento jurídico 4.º): «No estamos en presencia de una multa sancionadora sino de una indemnización coercitiva, fijada

coercitiva». El legislador quiso reforzar con aquella nomenclatura su naturaleza coercitiva y dejar zanjado quién será destinatario de aquella cuantía[13]. Contrariamente a lo que ocurre con las multas que la LEC prevé en ciertos casos similares (por ejemplo, art. 589.3 LEC para la manifestación de bienes del ejecutado, art. 591.2 LEC para la colaboración de terceros en la investigación patrimonial, art. 699 LEC para el incumplimiento del requerimiento de cumplimiento con la sentencia en la ejecución no dineraria), en los que se utiliza el término «multa», la indemnización coercitiva prevista en el art. 9.6 de la Ley 1/2019 está concebida como una indemnización de perjuicios en su naturaleza, por lo que será en beneficio del actor. Es un incentivo muy poderoso para su efectiva exigencia ya que el propio actor se beneficia directamente, lo que contribuye al fin de esta consecuencia, según lo exige la Directiva 2016/943.

Por la naturaleza jurídica de la indemnización coercitiva y por su configuración legal, esta es acumulable a otras indemnizaciones de perjuicios que pudieran tener lugar a favor del demandante conforme a las normas generales. El propio art. 9.6 de la Ley 1/2019 lo dispone en estos términos. En ningún caso podríamos hablar de una «doble indemnización» pues la indemnización general prevista en el art. 9 g) y 10 de la Ley 1/2019 tendrá lugar cuando el infractor del secreto empresarial haya incurrido en dolo o culpa, y deberá ser adecuada a la lesión realmente sufrida como consecuencia de la infracción. Para fijarla el tribunal tendrá en cuenta el lucro cesante, el enriquecimiento injusto e incluso elementos no económicos, como el daño moral. En cambio, la indemnización coercitiva tiene por finalidad el cumplimiento de la orden judicial, y encuentra su causa en su incumplimiento y no en la propia vulneración del secreto empresarial[14].

---

en sentencia para el caso de incumplimiento de la obligación de cesar en el uso de la marca después del plazo de cumplimiento voluntario, sin que la ley obligue a realizar un examen de la conducta del condenado incumplidor ni un análisis de si su actuación se ha movido en parámetros de buena o mala fe. No debe confundirse las indemnizaciones coercitivas con las "multas coercitivas", reguladas en los arts. 710 y 711 LEC. Las primeras tienen, en principio, una naturaleza "indemnizatoria" y lo que se obtenga por ellas irá a parar al patrimonio del perjudicado. Las segundas, por el contrario, son de naturaleza sancionatoria de carácter público, y, en consecuencia, lo que se ingrese por ellas está destinado a las arcas públicas. Además, la indemnización coercitiva podría ser renunciada por quien tiene que recibirla, cosa que no sucede con las multas, y también podría ser satisfecha de una manera no personalista, lo que con las multas tampoco sucede. Por otra parte, esta indemnización coercitiva se prevé exclusivamente para el caso de condena judicial a la cesación de los actos de violación, y el condenado incumpla el mandato judicial.

No obstante, del art. 44 de la LM parece inducirse que su naturaleza es mixta. Es decir, de una parte tiene una naturaleza indemnizatoria, de modo que, recibida una cantidad por este concepto, el titular del derecho de marca (salvo que acredite un daño mayor) nada podrá pedir en concepto de indemnización de los daños y perjuicios que pueda causarle el uso ilegítimo del signo distintivo después del dictado de la sentencia firme, y ello con independencia de la indemnización de daños y perjuicios a que se refiere el art. 43 de la LM (que procede por los daños causados antes de la sentencia y responde a otros conceptos). Pero, de otra parte, esta indemnización es coercitiva, es decir, punitiva y disuasoria, en el sentido de que, para recibir una cantidad por este concepto, el perjudicado no estará obligado a acreditar daño alguno. Se establece en favor del titular de derecho de marca por una conducta del infractor del derecho de marca en fase ejecutiva, consistente en permanecer en el uso ilegítimo de la marca después de haberse dictado sentencia en su contra prohibiendo dicho uso y ordenándosele el cese en el mismo.

Este tipo de "indemnizaciones" están justificadas por el hecho de que no es infrecuente en estos sectores económicos que los beneficios obtenidos por el infractor sean superiores a los daños que puedan causar a los titulares de los derechos ilegítimamente utilizados. En cualquier caso, su naturaleza indemnizatoria es preponderante con respecto a su naturaleza punitiva-disuasoria, por lo que no es procedente realizar el examen de la conducta del infractor o juicio de culpabilidad que preconiza la parte apelante».

13. Con esto la Ley 1/2019 se diferencia de otros supuestos legales que prevén multas en un proceso civil, en donde explicita que el destinatario de estas será el erario público, por ejemplo en la ejecución de condenas no dinerarias (art. 711.2 LEC).
14. La AAP de Granada (sección 3.ª) 208/2017 de 12 de diciembre, respecto de la indemnización coercitiva del art. 44 de la Ley de marcas, sostiene su incompatibilidad con otras indemnizaciones de la LM o cuanto menos establece límites temporales para una y otra: la sentencia puede indemnizar por daños hasta la sentencia y la indemnización coercitiva será la indemnización para después de la sentencia, sin que quepa otra: «No obstante, del art. 44 de la LM parece inducirse que su naturaleza es mixta. Es decir, de una parte tiene una naturaleza indemnizatoria, de modo que, recibida una cantidad por este concepto, el titular del derecho de marca (salvo que acredite un daño mayor) nada podrá pedir en concepto de indemnización de los daños y perjuicios que pueda causarle el uso ilegítimo del signo distintivo después del dictado de la sentencia firme, y ello con independencia de la indemnización de daños y perjuicios a que se refiere el art. 43 de la LM (que procede por los daños causados antes de la sentencia y responde a otros conceptos)». No cabe realizar la misma interpretación en el ámbito de la Ley de secretos empresariales ya que expresamente se prevé su compatibilidad. Es decir, nada impide que la sentencia disponga una indemnización por lucro cesante que dependa del número de productos vendidos por el demandado, sea antes o después

En cuanto a la cuantía de la indemnización coercitiva, el legislador solo precisa que deberá consistir en una cantidad líquida y que será una cantidad diaria por día transcurrido hasta que se produzca el total cumplimiento. Para fijar la cuantía el tribunal deberá tener en cuenta las circunstancias del caso concreto; al respecto, la ley habla de «adecuada a las circunstancias» (art. 9.6 Ley 1/2019). La Directiva 2016/943 exigía que fuera «proporcionada» y «disuasoria».

Para facilitar la tarea del tribunal, lo ideal hubiera sido que el legislador fuese más preciso, indicando por ejemplo unos criterios concretos y unos parámetros mínimos a partir de los cuales pudiera moverse el tribunal. Por ejemplo, en el caso mencionado de las violaciones a las marcas, la ley sí que establece un límite mínimo: no podrá ser inferior a los 600 euros. En el caso de las obligaciones de hacer o no hacer, la LEC prevé multas mensuales del 20% del valor de la cosa o una multa única del 50% (art. 711.1 LEC). En el caso de acciones de cesación para la defensa de intereses colectivos o difusos, se impondrá una multa que oscilará entre 600 y 60.000 euros por día de retraso en la ejecución de la resolución judicial en el plazo señalado en la sentencia, según la naturaleza y el daño producido y la capacidad económica del condenado (art. 711.2 LEC).

Por lo tanto, el tribunal fijará la cuantía de la indemnización coercitiva líquida y diaria atendiendo a las circunstancias del caso concreto. La falta de mayor detalle en la concreción de los criterios y cuantías mínimas puede suplirse acudiendo a los fines de esta indemnización coercitiva y los propios parámetros que la Ley 1/2019 prevé para las medidas que tiene que adoptar el juez (art. 9.3 Ley 1/2019). La cuantía de la multa debe ser disuasoria para el infractor, es decir, debe tener una cuantía suficiente para que desincentive el incumplimiento de la intimación judicial, por lo que creemos que el tribunal deberá tener en consideración, entre otros aspectos, a la hora de fijarla, el valor del secreto empresarial en cuestión, la entidad o consecuencias del daño provocado para el actor, el comportamiento del infractor y la probabilidad de que este persista en su violación, los intereses de terceros y los generales, pero también la capacidad económica del infractor condenado, que la Ley 1/2019 no menciona, lógico en este ámbito si el fin es disuasorio, y que por lo demás la LEC contempla en ámbitos similares (por ejemplo el art. 711 LEC). Si la cuantía de la indemnización coercitiva no tiene en consideración estos aspectos, perderá su eficacia y no tendrá el carácter «proporcionado» y la fuerza «disuasoria» que le exige la directiva.

La cuantía de la indemnización coercitiva deberá ser objeto de discusión en el proceso declarativo y de determinación concreta en la sentencia que contenga la intimación. Esta es la aparente voluntad del legislador que deriva de la configuración que se hace en el art. 9.6 Ley 1/2019. En caso de omisión por error, se podría plantear el posible complemento de la sentencia para llevar a efecto su cumplimiento, según el art. 215 LEC. No parece en cambio que pudiera ser objeto de solicitud de concreción dentro de la propia ejecución.

Si el demandado infractor persiste en su contumacia frente a la intimación[15], la exigencia del apremio económico podrá hacerse efectivo por el demandante mediante la correspondiente demanda de ejecución no dineraria en que se podrá liquidar la cantidad debida como indemnización coercitiva hasta la fecha de la misma demanda, y en ella pedir que la cuantía de la ejecución se amplíe para cubrir los sucesivos incumplimientos de la multa periódica establecida en la sentencia, según lo dispuesto en el art. 578 LEC (art. 9.6 Ley 1/2019), no siendo necesarios nuevos requerimientos[16]. El ejecutante podrá también pedir en la demanda ejecutiva los

de la sentencia, junto con una intimación de cesar en la venta de los productos, con una indemnización coercitiva de tanto por día. Como veremos, esta indemnización coercitiva en la Ley de secretos empresariales se fija según la ley por parámetros que son distintos, aunque pueden coincidir parcialmente con el daño sufrido por el titular del secreto.

15. En el AAP de Alicante 120/2015 de 8 de octubre, el tribunal valora la actitud del condenado a la hora de apreciar la viabilidad de la indemnización coercitiva prevista en el art. 44 de la Ley de marcas, considerando esencial la concurrencia de una «conducta conscientemente reticente al cumplimiento del fallo condenatorio». La audiencia deja sin efecto la indemnización coercitiva en este caso por considerar que la actitud del condenado/ejecutado fue diligente, que no pudo cumplir con el contenido de la orden judicial por razones ajenas a su voluntad y que, además, tuvo una actitud tendente a evitar la producción de perjuicios a la otra parte (titular de la marca).
16. En este sentido se ha manifestado AAP de Granada (sección 3.ª) 208/2017 de 12 de diciembre, en el ámbito de la Ley de marcas: «No cabe establecer la necesidad de un nuevo requerimiento al ejecutado para que cumpla el contenido de la sentencia y en caso negativo proceder a hacer efectiva la indemnización coercitiva, sino que esta cobró virtualidad desde el momento en el que el ejecutado dejó de cumplir los

embargos de garantía con un alcance suficiente para cubrir el importe liquidado y sus sucesivas ampliaciones (art. 700 LEC).

3.7. Apremio personal: la responsabilidad penal

Por otra parte, y a pesar de que la ley no lo dice expresamente, el infractor que ha sido requerido para cumplir con determinada acción o abstención a través de la correspondiente intimación judicial, y que no cumple con el contenido de esta ni se justifica debidamente, podría incurrir en responsabilidad penal por desobediencia a la autoridad, prevista en el art. 556 CP.

Hay que tener en cuenta que la responsabilidad penal en sede civil debe ser el último recurso, sin dejar de reconocer que las medidas personales pueden ofrecer ciertas ventajas, como poder aplicarse a cualquier deudor, con independencia de su titularidad sobre algún bien o su liquidez, por ejemplo. Además, coadyuvan a desarrollar la idea en virtud de la cual el proceso no es solo un instrumento de realización del derecho, sino que también presta un servicio público que debe garantizarse cumpliendo con parámetros de eficacia y rentabilidad[17].

Por lo tanto, si un infractor incumple con la orden judicial contenida en la intimación judicial, primero se le han de aplicar los apremios económicos dispuestos en la ley, esto es, la multa o indemnización coercitiva. Pero si, a pesar de la imposición de dicha multa, esta no es efectiva y el infractor se niega a cumplir y se resiste a realizar lo ordenado en la intimación judicial, entonces se podrá perseguir al contumaz por un delito de desobediencia a la autoridad en sede penal. Esto podrá hacerse simultáneamente a la exigencia del apremio económico; no hay necesidad alguna de optar y no se excluyen ambos tipos de consecuencia.

Ahora bien, como ya apuntábamos anteriormente, para hacer efectiva la responsabilidad penal la jurisprudencia exige que haya existido una orden judicial expresa, terminante y clara, y que se haya puesto en conocimiento del acusado por medio de un requerimiento formal, personal y directo. Además, es necesario que haya una resistencia por parte del requerido a cumplir con lo que se le ordena. En otras palabras, se trata de que exista una verdadera actitud omisiva, pertinaz y clara de resistencia a cumplir con lo ordenado[18].

Por tanto, en caso de falta de cumplimiento voluntario con la resolución judicial, el actor podrá solicitar en la demanda ejecutiva no dineraria que se requiera al deman-

términos del fallo condenatorio en el plazo que se le concedió en la propia sentencia, con independencia de que se le pueda requerir para el cumplimiento de los otros pronunciamientos contenidos en el fallo en el plazo a que se refiere el art. 699 de la LEC» (FJ 2.º).

17. En este sentido, Armenta Deu (2015, pág. 26).

18. Es reiterada la jurisprudencia del Tribunal Supremo en la que se establece que, para que se configure responsabilidad penal por desobediencia a la autoridad, es necesario que haya existido una orden judicial expresa terminante y clara que informe de las consecuencias de su incumplimiento y que haya sido puesta en conocimiento del destinatario mediante un requerimiento formal personal y directo, a fin de que se pueda acreditar que el destinatario ha tenido conocimiento efectivo de la orden. Además, tiene que haber una resistencia a cumplir con dicha orden. Ver STS 13 de junio de 2000 [RJ 2000\6597], 25 de febrero de 1994 [RJ 1994\566], 13 de diciembre y 16 de marzo de 1993 [RJ 1993\9421 y RJ 1993\2311], y 15 de febrero de 1990 [RJ 1990\1548]); STS de 18 de abril de 1997 [RJ 1997\2991], entre otras. Más recientemente podemos mencionar, por ejemplo, la SAP de Las Palmas (sección 6.ª) 192/2019 de 16 de julio (JUR 2019\264481), en la que el tribunal reconoce que la vía civil (el art. 589 LEC en relación con los arts. 153 y 28.4) permite la notificación por medio de procurador pues no se requiere que la notificación del requerimiento sea personal, si bien ello no presupone que dicha norma despliegue sus efectos igualmente en la vía penal, cuando el delito imputado necesita del cumplimiento de unos requisitos que no se ajustan a los requisitos civiles, siendo reiterada la doctrina y jurisprudencia, que establece que uno de los requisitos imprescindibles es el requerimiento formal, personal y directo, es decir, es necesario un requerimiento personal, en la vía de ejecución en este caso, para poder fundamentar una condena de desobediencia a la autoridad. En el mismo sentido, la SAP de Burgos (sección 1.ª) 32/2020 de 21 de enero (JUR2020\105132) refuerza la importancia del apercibimiento y de la actitud contumaz del incumplidor, sosteniendo que: «En consecuencia, adquiere especial trascendencia en el ámbito penal la existencia de un *apercibimiento previo,* a modo de requerimiento preciso, claro, expreso y terminante de las consecuencias penales que la vulneración del mandato u orden puede generar en el eventual incumplidor. Por otra parte, es preciso para la comisión del delito de desobediencia que haya un mandato persistente y reiterado de modo que frente a él quede de manifiesto una actitud de oposición tenaz y obstinada, que es lo que constituye la esencia de esta infracción penal, unido a la existencia de un dolo específico de escarnecer el principio de autoridad» (FJ 2.º). (La cursiva es nuestra.) Ver también, SAP de Madrid de 11 de febrero de 2003 (JUR2003/200745); SAP de Córdova de 11 de mayo de 2004 (JUR2004/199653); y SAP de Álava de 23 de marzo de 2005 (JUR2004/288236).

dado para que cese en su conducta (art. 699 LEC), bajo el apercibimiento de responsabilidad penal. Podrá y deberá reiterarse el requerimiento dentro de la ejecución a fin de que, de mantenerse el demandado en su conducta, se alcancen los requisitos que exige la jurisprudencia penal para la comisión del delito de desobediencia. Y una vez hecho esto, el actor podrá pedir la deducción de testimonio de los particulares de la ejecución a fin de interponer las correspondientes acciones penales.

4. Conclusiones

El secreto empresarial tiene hoy una nueva regulación sustantiva y procesal. Junto con unas nuevas acciones, que pueden dar lugar a requerimientos, se regulan algunas consecuencias del incumplimiento como es la indemnización coercitiva. La intención del legislador sin duda es buena; sin embargo, como hemos analizado, deja muchos aspectos en el aire, lo que puede poner en jaque su aplicación efectiva.

Es menester mencionar algunos puntos en los que la transposición de la directiva por el legislador español hubiera podido ser mejor.

En primer lugar, se podría haber evitado la dispersión normativa que provoca la utilización de una ley específica para regular las especialidades procesales relativas a la protección del secreto empresarial. Sin duda, las previsiones sobre las intimaciones y sus consecuencias, además de otras normas en la materia, se hubiesen podido incorporar a la LEC para mantener la unidad legislativa procesal, contribuyendo a la seguridad jurídica.

En segundo lugar, el legislador no ha aprovechado todos los avances de la ciencia procesal ya que se ha limitado a regular fragmentariamente algunas consecuencias procesales del incumplimiento de las resoluciones judiciales dirigidas a proteger el secreto empresarial. Ante este panorama, la pretensión del presente artículo ha sido reconstruir la intimación judicial en materia de secretos empresariales, para poder alcanzar los fines de la norma.

En tercer lugar, el legislador, aunque ha optado por una figura como la indemnización coercitiva, dotada de alta eficacia, no ha resuelto todos los problemas a que pueda dar lugar su aplicación, algunos de los cuales ya se han puesto de relieve en ámbitos en que también está prevista. También podría haber contribuido aún más a su efectividad fijando los criterios para su concreción y un importe mínimo, bien por cuantía o porcentaje.

En cuarto lugar, la responsabilidad penal por incumplimiento de la intimación judicial dictada para proteger un secreto empresarial queda sometida a los mismos obstáculos que su exigencia en otros ámbitos. Podría quizá decirse que la sanción prevista por el legislador en este caso no es suficientemente efectiva como exigía la directiva.

En fin, aunque es importante que la ley contemple instrumentos procesales, lo es más que estos se apliquen de forma rápida y efectiva. La intimación judicial es una herramienta legal, disponible, que puede ser muy ágil y económica. Para maximizar su eficacia y garantizar el cumplimiento de las resoluciones judiciales adoptadas en este ámbito, los tribunales deben hacer una aplicación sin vacilaciones, ni dilaciones ni reiteraciones innecesarias. Se trata de garantizar la seguridad jurídica con el fin último de mejorar las condiciones, el marco para el desarrollo y la explotación de la innovación y la transferencia de conocimientos.

Referencias bibliográficas

ARMENTA DEU, T. (2015). «Ejecución y medidas conminativas personales. Un estudio comparado». *Revista de Derecho,* Universidad Católica del Norte (Chile), vol. 22, núm. 2, pág. 23-54 [en línea] http://dx.doi.org/10.4067/S0718-97532015000200002 [Fecha de consulta: 28 de septiembre de 2020].

ARMENTA DEU, T. (2018). «Medidas coercitivas dirigidas a tutelar el desarrollo adecuado del proceso y a colaborar con la justicia. Una aproximación comparada». *Derecho y proceso. Liber amicorum Francisco Ramos Méndez*. Barcelona: Atelier, vol. I, págs. 299-322.

ARROYO APARICIO, A. (2019). «Secretos empresariales en el ordenamiento español, transposición de la Directiva 2016/943». *Revista Aranzadi Doctrinal*, núm. 11, pág. 5.

CASTÁN, A. (2016). «Indemnización coercitiva por incumplimiento de sentencia condenatoria por infracción de una marca comunitaria». Comentario de sentencia [en línea] https://elderecho.com/indemnizacion-coercitiva-por-incumplimiento-de-sentencia-condenatoria-por-infraccion-de-marca-comunitaria [Fecha de consulta: 28 de septiembre de 2020.]

GARCÍA VIDAL, Á. (2019). «Diez cuestiones clave sobre la Ley de secretos empresariales». *Análisis*, pág. 2 [en línea] https://www.gap.com/wp-content/uploads/2019/02/Analisis-Secretos-empresariales_def.pdf [Fecha de consulta: 28 de septiembre de 2020].

GASCÓN, F. (2018). «Hacia una mayor protección jurídica de los secretos empresariales». *Actualidad Jurídica Aranzadi*, núm. 943 (versión electrónica).

ORTELLS RAMOS, M. (2004). «¿Multas o astricciones? Una indefinición de la Nueva Ejecución Forzosa Española». *Revista Internauta de Práctica Jurídica*, núm. 13, págs. 1-23.

PROTOCOLO DE PROTECCIÓN DEL SECRETO EMPRESARIAL EN LOS JUZGADOS MERCANTILES (2019). Sección de Derecho de la Competencia, Tribunal Mercantil de Barcelona [en línea] https://www.oepm.es/export/sites/oepm/comun/documentos_relacionados/Noticias/2019/2019_11_22_Protocolo_Proteccion_Secreto_Empresarial_en_los_JM.pdf [Fecha de consulta: 28 de septiembre de 2020.]

RUIZ DE LA FUENTE, C. (2011). *Las intimaciones judiciales en el proceso civil.* Barcelona: Atelier.

Cita recomendada

RUIZ DE LA FUENTE, Consuelo (2020). «Las intimaciones judiciales en la Ley de secretos empresariales». *IDP. Revista de Internet, Derecho y Política*, núm. 32 (marzo). UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i32.373743

Sobre la autora

Consuelo Ruiz de la Fuente
consuelo.ruiz.delafuente@uab.cat
Doctora en Derecho, es profesora de Derecho Procesal en la Universidad Autónoma de Barcelona y profesora colaboradora en la Universitat Oberta de Catalunya.

Universitat Oberta de Catalunya

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

www.uoc.edu/idp

ACTUALIDAD NORMATIVA

Novedades legislativas

Jordi Garcia Albero
Profesor de los Estudios de Derecho y Ciencia Política (UOC)

Fecha de publicación: marzo de 2021

Boletín Oficial del Estado (BOE)

Ley Orgánica 1/2020, de 16 de septiembre, sobre la **utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.**
BOE núm. 248, de 17 de septiembre de 2020.
https://www.boe.es/boe/dias/2020/09/17/pdfs/BOE-A-2020-10776.pdf

Ley 3/2020, de 18 de septiembre, **de medidas procesales y organizativas** para hacer frente al **COVID-19** en el ámbito de la **Administración de Justicia.**
BOE núm. 250, de 19 de septiembre de 2020.
https://www.boe.es/boe/dias/2020/09/19/pdfs/BOE-A-2020-10923.pdf

Real Decreto-ley 28/2020, de 22 de septiembre, **de trabajo a distancia.**
BOE núm. 253, de 23 de septiembre de 2020.
https://www.boe.es/boe/dias/2020/09/23/pdfs/BOE-A-2020-11043.pdf

Orden ISM/903/2020, de 24 de septiembre, por la que se regulan las **notificaciones y comunicaciones electrónicas** en el ámbito de la **Administración de la Seguridad Social.**
BOE núm. 258, de 29 de septiembre de 2020.
https://www.boe.es/boe/dias/2020/09/29/pdfs/BOE-A-2020-11359.pdf

Ley 4/2020, de 15 de octubre, del **Impuesto sobre Determinados Servicios Digitales.**
BOE núm. 274, de 16 de octubre de 2020.
https://www.boe.es/boe/dias/2020/10/16/pdfs/BOE-A-2020-12355.pdf

Ley 6/2020, de 11 de noviembre, reguladora de **determinados aspectos de los servicios electrónicos de confianza.**
BOE núm. 298, de 12 de noviembre de 2020.
https://www.boe.es/boe/dias/2020/11/12/pdfs/BOE-A-2020-14046.pdf

Ley 7/2020, de 13 de noviembre, para la **transformación digital del sistema financiero.**
BOE núm. 300, de 13 de noviembre de 2020.
https://www.boe.es/boe/dias/2020/11/14/pdfs/BOE-A-2020-14205.pdf

Real Decreto 43/2021, de 26 de enero, por el que se **desarrolla** el **Real Decreto-ley 12/2018,** de 7 **de septiembre, de seguridad de las redes y sistemas de información.**
BOE núm. 24, de 28 de enero de 2020.
https://www.boe.es/boe/dias/2021/01/28/pdfs/BOE-A-2021-1192.pdf

Diario Oficial de la Unión Europea (DOUE)
Legislación, comunicaciones e informaciones comunitarias

Recomendación (UE) 2020/1307 de la Comisión de **18 de septiembre de 2020** relativa a un **conjunto de instrumentos comunes** de la Unión para reducir el coste del despliegue de redes de muy alta capacidad y **garantizar un acceso al espectro radioeléctrico 5G** oportuno y favorable a la inversión, **a fin de fomentar la conectividad** y ponerla al servicio de la recuperación económica en la Unión tras la crisis de la COVID-19. (C/2020/6270)
DOUE L 305, de 21 de septiembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020H1307&from=ES

Resumen del **Dictamen del Supervisor Europeo de Protección de Datos** sobre la **Estrategia Europea de Datos.** (2020/C 322/04)
DOUE C 322, de 30 de septiembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XX0930(01)&from=ES

Resumen del Dictamen del Supervisor Europeo de Protección de Datos sobre el **Plan de acción** para una política global de la Unión en materia de **prevención del blanqueo de capitales y** de la **financiación del terrorismo.** (2020/C 322/05)
DOUE C 322, de 30 de septiembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XX0930(02)&from=ES

Conclusiones del Consejo «Acceso a la justicia: aprovechar las oportunidades de la digitalización». (2020/C 342 I/01)
DOUE C 342 I, de 14 de octubre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XG1014(01)&from=ES

Reglamento de Ejecución (UE) 2020/1536 del Consejo de 22 de octubre de 2020 por el que se **aplica el Reglamento (UE) 2019/796** relativo a **medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros.**
DOUE C 351 I, de 22 de octubre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020R1536&from=ES

Dictamen del Comité Económico y Social Europeo sobre el **«Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza».** (2020/C 364/12) DOUE C 364, de 28 de octubre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020AE1110&from=ES

Decisión de Ejecución (UE) 2020/1669 de la Comisión **de 10 de noviembre de 2020** relativa a un **proyecto piloto** para la aplicación de determinadas disposiciones de **cooperación administrativa** establecidas en el **Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo,** relativo a **un marco para la libre circulación de datos no personales** en la Unión Europea, mediante el Sistema de Información del Mercado Interior. (C/2020/7658)
DOUE C 377, de 11 de noviembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020D1669&from=ES

Resumen del dictamen del Supervisor Europeo de Protección de Datos sobre el **Libro Blanco** de la Comisión Europea sobre la **inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza.** (2020/C 392/03)
DOUE C 392, de 17 de noviembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XX1117(01)&from=ES

Exposición de motivos del Consejo: Posición (UE) 12/2020 del Consejo en primera lectura **con vistas a la adopción del Reglamento del Parlamento Europeo y del Consejo** relativo a la **cooperación** entre los órganos jurisdiccionales de los Estados miembros en el ámbito de la **obtención de pruebas en materia civil o mercantil.** (versión refundida) (2020/C 405/01)
DOUE C 405, de 26 de noviembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020AG0012(02)&from=ES

Posición (UE) 12/2020 del Consejo en primera lectura **con vistas a la adopción del Reglamento del Parlamento Europeo y del Consejo** relativo a la cooperación entre los **órganos jurisdiccionales** de los Estados miembros en el ámbito de la **obtención de pruebas en materia civil o mercantil** (versión refundida). (2020/C 405/01)
DOUE C 405, de 26 de noviembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020AG0012(01)&from=ES

Reglamento (UE) 2020/1783 del Parlamento Europeo y del Consejo de 25 de noviembre de 2020 relativo a la **cooperación** entre los **órganos jurisdiccionales de los Estados miembros** en el ámbito de la **obtención de pruebas en materia civil o mercantil (versión refundida).**
DOUE L 405, de 2 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020R1783&from=ES

Reglamento (UE) 2020/1784 del Parlamento Europeo y del Consejo de 25 de noviembre de 2020 relativo a la **notificación y traslado** en los Estados miembros de **documentos judiciales y extrajudiciales en materia civil o mercantil (versión refundida).**
DOUE L 405, de 2 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020R1784&from=ES

Conclusiones del Consejo sobre la **ciberseguridad de los dispositivos conectados.** (2020/C 427/04)
DOUE C 427, de 10 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XG1210(01)&from=ES

Dictamen del Comité Económico y Social Europeo sobre **«El mercado único digital: tendencias y perspectivas para las pymes».** (Dictamen de iniciativa) (EESC 2017/01768)
DOUE C 429, de 11 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017IE1768&from=ES

Dictamen del Comité Económico y Social Europeo sobre **«La minería digital en Europa: nuevas soluciones para la producción sostenible de materias primas».** (Dictamen de iniciativa) (EESC 2020/01559)
DOUE C 429, de 11 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020IE1559&from=ES

Dictamen del Comité Económico y Social Europeo sobre **«Trabajo digno en la economía de plataformas».** (Dictamen exploratorio) (EESC 2020/01859)
DOUE C 429, de 11 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020AE1859&from=ES

Dictamen del Comité Económico y Social Europeo sobre la **«Digitalización y sostenibilidad – Situación actual y necesidad de intervenir desde una perspectiva de la sociedad civil».** (Dictamen exploratorio) (EESC 2020/01918)
DOUE C 429, de 11 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020AE1918&from=ES

Dictamen del Comité Económico y Social Europeo **sobre la «Comunicación** de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones **– Despliegue seguro de la 5G en la UE – Aplicación de la caja de herramientas de la UE».** (EESC 2020/00956)
DOUE C 429, de 11 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020AE0956&from=ES

Dictamen del Comité Económico y Social Europeo **sobre la «Comunicación** de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones – **Una Estrategia Europea de Datos».** (EESC 2020/01042)
DOUE C 429, de 11 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020AE1042&from=ES

Dictamen del Comité Europeo de las Regiones – **Una estrategia para el futuro digital de Europa y una estrategia europea de datos.** (COR 2020/02354)
DOUE C 440, de 18 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020IR2354&from=ES

Dictamen del Comité Europeo de las Regiones – **Libro Blanco sobre la inteligencia artificial – Un enfoque europeo orientado a la excelencia y la confianza.** (COR 2020/02014)
DOUE C 440, de 18 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020IR2014&from=ES

Recomendación (UE) 2020/2245 de la Comisión de 18 de diciembre de 2020 relativa a los mercados pertinentes de **productos y servicios dentro del sector de las comunicaciones electrónicas que pueden ser objeto de regulación ex ante de conformidad** con la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo por la que se establece **el Código Europeo de las Comunicaciones Electrónicas.** (C/2020/8750)
DOUE L 440, de 29 de diciembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020H2245&from=ES

Dictamen del Comité Económico y Social Europeo **sobre la propuesta de Reglamento** del Parlamento Europeo y del Consejo por el que se **establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE** del Parlamento Europeo y del Consejo en lo que **respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra el abuso sexual de menores en línea.** (EESC 2020/04192)
DOUE C 10, de 11 de enero de 2021.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020AE4192&from=ES

Decisión de Ejecución (UE) 2021/27 de la Comisión de 7 de enero de 2021 sobre la solicitud de registro de la **iniciativa ciudadana europea titulada «Iniciativa de la sociedad civil para la prohibición de las prácticas de vigilancia biométrica masiva».** (C/2021/32)
DOUE L 13, de 15 de enero de 2021.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32021D0027&from=ES

Dictamen del Comité Europeo de las Regiones – **Reforzar la gobernanza local y la democracia representativa mediante nuevas herramientas de tecnología digital.** (COR 2020/00830)
DOUE C 37, de 2 de febrero de 2021.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020IR0830&from=ES

Reglamento de Ejecución (UE) 2021/133 de la Comisión de 4 de febrero de 2021 por el que se establecen las normas de **desarrollo del Reglamento de Ejecución (UE) 2018/858** del Parlamento Europeo y del Consejo en lo que respecta al **formato y la estructura básicos,** así como a los **medios de intercambio de los datos del certificado de conformidad en formato electrónico.** (C/2021/459)
DOUE L 42, de 5 de febrero de 2021.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32021R0133&from=ES

Jordi Garcia Albero
Profesor de los Estudios de Derecho y Ciencia Política (UOC)

‹https://dx.doi.org/10.7238/idp.v0i31.3263›

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

https://idp.uoc.edu

ACTUALIDAD JURÍDICA

Jurisprudencia

Patricia Escribano
Profesora ayudante doctora
Universitat Jaume I

Fecha de publicación: marzo de 2021

Sentencia del Tribunal de Justicia de la Unión Europea (Sala Sexta) de 8 de octubre de 2020

Caso EU contra PE Digital GmbH

El presente litigio tiene como objeto el derecho de desistimiento en relación con el suministro de un contenido digital que no se presta en un soporte material. En concreto, la interpretación de los artículos 2.11[1]; 14 apartado 3[2], y 16 letra m)[3] de la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo.

1. Hace referencia a la definición de «contenido digital» como «los datos producidos y suministrados en formato digital».
2. Obligaciones del consumidor en caso de desistimiento: «3. Cuando un consumidor ejerza el derecho de desistimiento tras haber realizado una solicitud de conformidad con lo dispuesto en el artículo 7, apartado 3, o en el artículo 8, apartado 8, el consumidor abonará al comerciante un importe proporcional a la parte ya prestada del servicio en el momento en que el consumidor haya informado al comerciante del ejercicio del derecho de desistimiento, en relación con el objeto total del contrato. El importe proporcional que habrá de abonar el consumidor al comerciante se calculará sobre la base del precio total acordado en el contrato. En caso de que el precio total sea excesivo, el importe proporcional se calculará sobre la base del valor de mercado de la parte ya prestada del servicio».
3. «Excepciones al derecho de desistimiento: Los Estados miembros no incluirán el derecho de desistimiento contemplado en los artículos 9 a 15 en los contratos a distancia y los contratos celebrados fuera del establecimiento que se refieran a: m) el suministro de contenido digital que no se preste en un soporte material cuando la ejecución haya comenzado con el previo consentimiento expreso del consumidor y con el conocimiento por su parte de que en consecuencia pierde su derecho de desistimiento.»

Hechos

Los hechos que dan lugar al conflicto son los siguientes: PE Digital es una empresa alemana que se dedica a la búsqueda de pareja. Para ello, a sus usuarios les ofrece dos modalidades de suscripción: la gratuita y la prémium. Esta última es de pago y tiene una duración de seis, doce y veinticuatro meses en función de los intereses del usuario. Lo que permite es que este tipo de suscriptores puedan ponerse en contacto con otros usuarios prémium e intercambiar mensajes e imágenes. Incluye lo que denominan «garantía de contacto», es decir, que se pueda establecer un número de contactos con otros usuarios. Tal y como dispone el párrafo 13 de la sentencia, «se considera contacto cualquier respuesta leída por el usuario en cuestión a un mensaje que él haya enviado, así como todo mensaje recibido por el usuario tras el cual haya leído e intercambiado al menos dos mensajes con otro usuario».

Después de darse de alta, cada persona recibe una serie de sugerencias de pareja, como consecuencia de la realización de un test de personalidad. Por lo que respecta a los usuarios de la web por un período de doce meses, «esta selección ya representa casi la mitad de todas las sugerencias de pareja suministradas al suscriptor durante el período contractual» (párrafo 15). Además, reciben el resultado del test mediante un «informe de evaluación de la personalidad» de cincuenta páginas, que pueden adquirir como una forma de prestación parcial mediante el pago de una cantidad.

E. U. celebra el 4 de noviembre de 2018 un contrato de suscripción prémium por doce meses, pagando, a tal efecto, algo más de 520 euros. No obstante, esta cantidad era muy superior de lo que se le estaba cobrando a otros usuarios por el mismo tipo de contrato que tenía ella. PE Digital le informa a E. U. de su derecho de desistimiento, la cual responde que la empresa ha de empezar a prestar el servicio del contrato antes de que finalice tal plazo. E. U. desiste del contrato cuatro días después y la empresa le cobra un importe de casi cuatrocientos euros, motivo por el cual la usuaria demanda a la empresa ante el Tribunal Civil y Penal de Hamburgo, solicitando la devolución de todos los pagos realizados.

Cuestiones prejudiciales

Debido a la complejidad del contrato, y en virtud de la Directiva 2011/83, así como el art. 357 apartado 8 del Código Civil alemán, el tribunal suspende el procedimiento y plantea al TJUE cuatro cuestiones prejudiciales:

1. Citamos textualmente: «¿Debe interpretarse el art. 14, apartado 3 de la Directiva (...), habida cuenta de su considerando 50[4], en el sentido de que, en el caso de un contrato en virtud del cual no ha de

4. «(50) Por un lado, el consumidor debe poder disfrutar del derecho de desistimiento aun cuando haya solicitado la prestación de los servicios antes de que finalice el período de desistimiento. Por otro lado, si el consumidor ejerce su derecho de desistimiento, el comerciante debe tener garantías de que se le va a pagar convenientemente el servicio que ha prestado. El cálculo del importe proporcionado debe basarse en el precio acordado en el contrato, a menos que el consumidor demuestre que el precio total es ya de por sí desproporcionado, en cuyo caso el importe a pagar se calculará sobre la base del valor de mercado del servicio prestado. El valor de mercado se debe establecer comparando el precio de un servicio equivalente prestado por otros comerciantes en el momento de la celebración del contrato. Por lo tanto, el consumidor debe solicitar de forma expresa la prestación del servicio antes de que finalice el plazo de desistimiento mediante una solicitud expresa y, en el caso de un contrato celebrado fuera del establecimiento mercantil, deberá hacerlo en un soporte duradero. Del mismo modo, el comerciante debe informar al consumidor, utilizando un soporte duradero, de toda obligación de abonar la parte proporcional del coste de los servicios ya prestados. En el caso de contratos que tengan por objeto bienes y servicios, las normas previstas en la presente Directiva sobre la devolución de bienes deben aplicarse a los elementos relativos a los bienes y el régimen de compensación se aplicará a los elementos relativos a los servicios.»

realizarse una prestación única, sino que ha de prestarse un servicio global compuesto por varias prestaciones parciales, el importe proporcional a la parte ya prestada del servicio en el momento en que el consumidor haya informado al comerciante del ejercicio del derecho de desistimiento, en relación con el objeto total del contrato, a pagar por el consumidor, debe calcularse exclusivamente pro rata temporis, cuando el consumidor paga por el servicio global pro rata temporis, pero las prestaciones parciales se realizan en momentos diferentes?»

2. «¿Debe interpretarse el mismo precepto de forma que el importe proporcional a la parte ya prestada del servicio en el momento en que el consumidor haya informado al comerciante del ejercicio del derecho de desistimiento, en relación con el objeto total del contrato, que debe pagar el consumidor, también debe calcularse únicamente pro rata temporis cuando una prestación (parcial) se realiza de forma continuada pero esta tiene mayor o menor valor para el consumidor al inicio de la duración contractual?»

3. «¿Deben interpretarse el art. 2, punto 11, de la Directiva 2011/83 y el art. 2, punto 1, de la Directiva (UE) 2019/770 (LCEur 2019, 836) del Parlamento Europeo y del Consejo, de 20 de mayo de 2019 [relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales (DO 2019, L 136, pág. 1)], en el sentido de que también pueden ser «contenidos digitales», en razón del art. 2, punto 11, de la Directiva 2011/83 y del art. 2, punto 1, de la Directiva 2019/770, aquellos ficheros suministrados como prestación parcial en el marco de un servicio global prestado principalmente como «servicio digital» en el sentido del art. 2, punto 2, de la Directiva 2019/770, lo que tiene como consecuencia que el comerciante puede lograr la extinción del derecho de desistimiento con arreglo al art. 16, letra m) de la Directiva 2011/83 en cuanto a la prestación parcial, pero que el consumidor, en caso de que el comerciante no lo consiga, podría desistir del contrato en su conjunto y en virtud del art. 14, apartado 4, letra b), inciso ii), de la Directiva 2011/83 (LCEur 2011, 1.901), no tendría que pagar ninguna compensación por dicha prestación parcial?»

4. Si el art. 14 apartado tercero de la Directiva 2011/83 debe interpretarse, según el considerando 50, en el sentido de que el precio total que se acuerda de forma contractual para un servicio es «excesivo» en el sentido del art. 14, apartado tercero, tercera frase de la Directiva 2011/83, si es superior de forma significativa al precio total pactado con otro consumidor por un servicio del mismo contenido, que presta el mismo comerciante, durante el mismo período contractual y bajo las mismas condiciones generales.

Resolución de las cuestiones prejudiciales

En relación con la primera y segunda de las cuestiones, parte de considerar que el contrato controvertido no establecía ninguna prestación separable de la prestación principal. De este modo, el art. 14 apartado tercero de la Directiva 2011/83 debe interpretarse del siguiente modo:

– Para calcular el importe proporcional que el consumidor debe pagar al comerciante cuando haya solicitado de forma expresa, que la ejecución del contrato inicie durante el período de desistimiento, desistiendo del mismo, se debe tomar, en principio, como referencia el precio acordado en dicho contrato para su objeto total y calcular el importe adeudado pro rata temporis. Si el contrato que se celebra prevé que alguna prestación se ha de llevar a cabo de forma íntegra, por separado, desde que se inicia el contrato a un precio que deberá abonarse separadamente, se deberá tener en cuenta el precio total que se haya establecido para esa prestación al calcular el importe adeudado al comerciante, en función de lo establecido en el art. 14, apartado 3 de la Directiva.

En lo atinente a la cuarta cuestión, es decir, qué criterios han de aplicarse para considerar si el precio total es excesivo según el art. 14 apartado tercero, el TJUE establece que:

– Hay que tener en cuenta el precio del servicio que se ha ofrecido por el comerciante a otros consumidores en las mismas condiciones, y los servicios equivalentes prestados por otros comerciantes en el momento en que se celebre el contrato.

Por último, y en lo que atañe a la tercera cuestión, se ha de determinar la consecuencia (a efectos del importe que ha de abonar el consumidor al comerciante), es decir, el hecho de que una de las prestaciones del contrato celebrado tenga por objeto el suministro de contenido digital que no se presta en soporte material (en el caso, el informe de evaluación de la personalidad). En este supuesto, el consumidor no puede ejercitar el derecho de desistimiento en virtud del art. 16, letra m) de la Directiva. El TJUE manifiesta que este precepto ha de interpretarse de forma estricta; de este modo, el servicio que presta PE Digital no puede considerarse, como tal, suministro de «contenido digital», en relación con dicho precepto. Del mismo modo que el informe de evaluación de personalidad tampoco puede entenderse englobado en tal excepción. En consecuencia, el art. 16, m) de la Directiva, en relación con el art. 2, apartado 11, ha de interpretarse de forma que la elaboración –por parte de una web que se dedica a la búsqueda de pareja– de un informe de evaluación de la personalidad no constituye suministro de «contenido digital».

Sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1.ª) de 25 de septiembre de 2020

En este caso, se analiza la retirada de datos personales en el buscador de Google. El actor presenta una reclamación ante Google solicitando la retirada de sus datos personales y su fotografía contenida en un blog, en relación con diez URL. El buscador accede al blog interno de modo que los usuarios que entraran no vieran esa información, sino un aviso de censura. Sin embargo, buscando desde Estados Unidos o España (pero modificando la IP como si se estuviera en Estados Unidos), se podía acceder a sus datos personales en cuatro páginas web. El demandante presentó una reclamación ante la Agencia Española de Protección de Datos solicitando que se bloquearan las URL cuando las búsquedas se realizaran en España «utilizando la funcionalidad de Google que permite al buscador geolocalizar la búsqueda en EE. UU., a pesar de encontrarse el usuario que realiza la búsqueda en España».

La AEPD desestima la pretensión al considerar que «el uso de sistemas técnicos que eludan los sistemas de geolocalización de dicha entidad y que simulen que las búsquedas se realizan en Estados Unidos, no justifican la aplicación extraterritorial de la normativa española y europea en materia de protección de datos y la restricción de la libertad de expresión en un ámbito territorial ajeno al de la Unión Europea». Hemos de precisar que, para resolver el caso, se había de aplicar normativa que, a día de hoy, se encuentra derogada, como es la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Con independencia de este hecho, la Audiencia Nacional hace referencia también a la nueva normativa que se aplicaría y trae a colación la STJUE de 24 de septiembre de 2019 para resolver el caso.

Lo que debe realizar la Audiencia Nacional es una ponderación entre los derechos del interesado relativos a su vida privada y la protección de datos personales, y el derecho a la libertad de información, a fin de determinar si se han de bloquear las URL objeto de litigio, cuando las búsquedas se efectúen en España utilizando la aplicación de Google que permite geolocalizar en Estados Unidos. El tribunal

analiza los derechos en cuestión, de forma pormenorizada, mediante las sentencias del Tribunal Constitucional, la STJUE de 13 de marzo de 2014 que resuelve un proceso similar y las directrices del Grupo de Trabajo del 29 en materia de derecho al olvido.

Como conclusión, considera que los datos contenidos en las páginas web son comentarios relacionados con la vida privada del actor que no tienen interés público y, además, datan de 2008, así que estima la pretensión del actor de bloquear en Google las cuatro URL «para la búsqueda de los datos personales del recurrente, cuando las búsquedas se realicen en España, en el uso de una funcionalidad aplicable en Google, que permite al buscador geolocalizar la búsqueda en EE. UU., a pesar de encontrarse el usuario que realiza la búsqueda en España».

Lo que desestima la AN es la pretensión del actor de eliminar el aviso de retirada de los contenidos publicado por Google, en relación con las cuatro URL. En los enlaces constaba el siguiente texto: «Entrada no disponible. Como respuesta a un requerimiento legal enviado a Google, hemos eliminado esta entrada. Puedes consultar más información sobre la solicitud en LumenDatabase.org». El demandante consideró que, aunque la información por la que se realizó el bloqueo estuviera anonimizada, podía ser relacionada con una de las cuatro páginas web. Google modificó el enlace para que este solo dirigiera a Lumen, en la que nada se decía sobre el actor. Por tanto, esta segunda pretensión no fue estimada.

Cita recomendada

ESCRIBANO, Patricia (2021). «Jurisprudencia». IDP. Revista de Internet, Derecho y Política, núm. 32. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i32.378904

Sobre la autora

Patricia Escribano
Profesora ayudante doctora
Universitat Jaume I

Universitat Oberta de Catalunya