IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

Compliance institucional y riesgo transnacional digital en la Unión Europea: ¿avanzamos hacia la prevención uniforme?

INSTITUTIONAL COMPLIANCE AND TRANSNATIONAL DIGITAL RISK IN THE EUROPEAN UNION: ARE WE MOVING TOWARDS UNIFORM PREVENTION?

Juan Ignacio Leo-Castela[1]
Profesor Ayudante Doctor. Universidad de Salamanca
leocastela@usal.es 0000-0003-2936-6017

Recibido: 29 de octubre de 2023 | Aceptado: 02 de diciembre de 2023

RESUMEN

En este trabajo se aborda, desde una perspectiva jurídico-económica, la gestión del riesgo transnacional digital por parte de la Unión Europea considerando la importancia creciente del compliance en el ámbito institucional como una herramienta innovadora y de extraordinaria utilidad para la gobernanza global de este riesgo. En este contexto, el trabajo se orienta hacia la búsqueda de respuestas que permitan aportar certidumbre en relación con los posibles avances de la Unión hacia un nuevo modelo de prevención uniforme.

PALABRAS CLAVE

Compliance
Unión Europea
Riesgo transnacional digital

ABSTRACT

This work addresses, from a legal-economic perspective, the European Union transnational digital risk management, considering the growing importance of compliance in the institutional field as an innovative and extraordinarily useful tool for the global risk's governance. In this context, the work is oriented towards the search for answers that allow us to provide certainty in relation to the possible European Union progress towards a new uniform prevention model.

KEYWORDS

Compliance
European Union
Transnational digital risk

1. Profesor Ayudante Doctor acreditado a Contratado Doctor en la Facultad de Derecho de la Universidad de Salamanca, despacho 113. Departamento de Economía Aplicada. Paseo Tomás y Valiente s/n, Campus Unamuno. CP 37007, Salamanca (Salamanca). Investigador en el Centro de Investigación para la Gobernanza Global (CIGG) de la Universidad de Salamanca. La elaboración de este trabajo de investigación se ha realizado en el marco del Proyecto I+D del Ministerio de Ciencia, Innovación y Universidades: "Cumplimiento normativo y protección penal de la Administración Pública".

I. Introducción

La demanda de herramientas idóneas para una adecuada gestión de los riesgos legales ha crecido exponencialmente a medida que la comunidad internacional se ha ido volviendo cada vez más vulnerable frente a los retos y desafíos globales de nuestro tiempo. Nos hallamos inmersos en la llamada "cuarta revolución industrial" (Schwab, 2017). Una revolución marcada por la aceleración digital (pre y post pandemia) y por el auge del "dato" como elemento vertebrador de un nuevo orden social, jurídico y económico[2]. En este contexto, la Unión Europea pretende avanzar hacia la búsqueda de soluciones comunes para la adecuada gestión de los riesgos legales en el panorama comunitario. De manera particular, en relación con aquellos que está propiciando la transformación digital.

El nivel de globalización alcanzado en los últimos años ha traído consigo importantes avances cuyo impacto resulta innegable en términos de bienestar social y progreso. Sin embargo, en la otra cara de la moneda la globalización representa también la necesidad de contar con instrumentos idóneos (cada vez más sofisticados) con los que alcanzar una prevención eficaz y uniforme en ámbitos tan complejos como la delincuencia transnacional, el cambio climático, la protección de los derechos humanos, o la ciberdelincuencia, entre otros[3].

Bajo mi punto de vista el papel de las autoridades comunitarias frente a los retos globales que nos rodean se ha enfocado excesivamente en la producción legislativa de un Derecho cada vez más técnico, indeterminado y complejo cuya aplicación en la práctica no solo resulta tediosa para los operadores jurídicos, sino que a menudo termina frustrando la finalidad de la norma[4]. Si bien es cierto que este afán de la Unión Europea por promulgar normativas en tiempo récord ha estado orientado a la siempre bienintencionada protección de bienes jurídicos expuestos a situaciones de riesgo, no es menos cierto que esta premura ha condicionado en cierta medida la calidad del paraguas jurídico de protección ocasionando alguna que otra gotera. No sería justo obviar que el contexto socioeconómico reciente no ha sido precisamente el más favorable[5] y que, al mismo tiempo, la

2. En este sentido se expresa el *European Data Market study measuring the size and trends of the EU data economy*. Disponible en: https://digital-strategy.ec.europa.eu/en/library/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy. Fecha de última consulta: 24 de agosto de 2023.

3. Estos y otros riesgos globales han sido recopilados por el Eurobarómetro 2022 sobre el futuro de Europa disponible en: https://www.europarl.europa.eu/news/es/press-room/20220119IPR21314/futuro-de-europa-el-cambio-climatico-es-el-mayor-reto-para-la-ue. Fecha de última consulta: 24 de agosto de 2023.

4. En este sentido, la evolución del Derecho digital comunitario resulta tan innegable como la complejidad técnica de algunas de sus normas. Sirva de ejemplo la reciente aprobación del Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo de 31 de mayo de 2023 relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n. º 1093/2010 y (UE) n. º 1095/2010 y las Directivas 2013/36 UE y (UE) 2019/1937. Disponible en: https://www.boe.es/doue/2023/150/L00040-00205.pdf Fecha de última consulta: 24 de agosto de 2023.

5. Según Eurostat la evolución del crecimiento económico de la Unión Europea-27 desde 2020 ha estado realmente muy limitada. La serie histórica completa se encuentra disponible

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

inmediatez con la que a veces se materializan algunos de estos riesgos globales deja muy poco margen de maniobra para que el Derecho comunitario y los mecanismos multilaterales de la Unión (a menudo costosos) puedan desplegar a tiempo su verdadera eficacia. En este contexto debo detenerme un instante a reflexionar sobre la conveniencia de actualizar la configuración tradicional de las normas jurídicas y su capacidad para garantizar el orden y la convivencia social (prevención del daño social) a la luz de este problema que en los últimos tiempos parece estar haciéndose más evidente.

En otras palabras, la producción normativa tradicional respondía a una serie de criterios más o menos satisfactorios que tal vez por inercia (o, sencillamente, por falta de necesidad) se fueron replicando mecánicamente a lo largo del tiempo, pero este planteamiento, a la vista de realidad actual, quizás haya quedado obsoleto. Para comprender mejor este posicionamiento conviene prestar atención al concepto de "sociedades del riesgo" acuñado por Ulrich Beck en pleno apogeo del fenómeno de la globalización a principios de los años noventa (Beck, 1992, 51)[6]. Siguiendo a este autor, los riesgos se definen como la probabilidad de que exista un daño o impacto. En términos agregados cuando hablamos del conjunto de una sociedad, un daño o impacto social. Aunque la opinión de Beck es que su origen puede responder a factores de lo más diverso bajo mi punto de vista y al menos a efectos de cuanto aquí se expone, podríamos dividirlos en dos grandes grupos: aquellos en los que interviene el factor tecnológico y aquellos en los que no.

Siguiendo este razonamiento podría decirse que el hecho de que en los últimos tiempos se hayan incrementado los riesgos (probabilidad de que exista un daño social, entre otras razones, a causa de haber alcanzado un nivel récord de globalización), podría justificar la necesidad de elevar el "listón preventivo" por parte de las autoridades comunitarias para una mejor protección de los bienes jurídicos en juego. Como se verá a lo largo de estas páginas, este planteamiento ya ha calado en la nueva forma de legislar de la Unión Europea modificando, en parte, el paradigma tradicional e incorporando aspectos tan novedosos como la medición de los niveles de riesgo, las evaluaciones de impacto o los mecanismos de compliance (corporativo y/o institucional). De manera particular, cuando se trata prevenir un daño social en ámbitos tan relevantes o con tanta sensibilidad social como los referidos anteriormente[7].

---

en: https://ec.europa.eu/eurostat/databrowser/view/NAMQ_10_GDP__custom_7680558/bookmark/table?lang=en&bookmarkId=a4ce6a9d-7ef1-48f1-a5bf-e23a717fcf75 Fecha de última consulta: 26 de agosto de 2023.

6. El concepto "sociedades del riesgo" fue actualizado por el mismo autor en el año 2009. Con anterioridad a los trabajos de Beck, Simon (1987) describió la gobernanza de la sociedad del riesgo como un "zumbido de circuitos integrados" en el que se interrelacionan diferentes tipos de riesgo (y ésta es precisamente una de las dificultades más importantes para su adecuada gobernanza y gestión. Al otro lado de la doctrina encontramos autores más cercanos en el tiempo como O'Malley (2002) que sostiene que la adecuada gestión del riesgo no es más que una técnica de gobernanza que permite mejorar la eficacia en la sociedad.

7. Véase en este sentido la nota informativa sobre la importancia de las evaluaciones de impacto en los procesos de producción normativa de la Unión Europea, disponible en: https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/impact-assessments_es Fecha de última consulta: 29 de agosto de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

En paralelo, la irrupción de la responsabilidad legal de las personas jurídicas en los ordenamientos internos de cada Estado miembro (ya sea en sede civil, penal, o administrativa) ha modificado la manera de entender la responsabilidad de las organizaciones hacia la sociedad y su entorno. Entre los factores determinantes de este cambio de paradigma no podemos obviar la influencia internacional de organismos tan relevantes como la OCDE o Naciones Unidas que, al margen de la Unión Europea, también han liderado un empuje hacia la consideración de las personas jurídicas como sujetos legalmente responsables[8].

La configuración de todo este nuevo marco legal entorno al nuevo *status* jurídico de las corporaciones y empresas supone la incorporación de importantes obligaciones en materia de buen gobierno corporativo, ética y cumplimiento que han ido calando con mayor o menor protagonismo en las diferentes ramas del Derecho (de manera mayoritaria en el ámbito penal, administrativo y tributario). No solo a nivel interno en los diferentes Estados miembros sino, también en el Derecho comunitario. La puesta en marcha de protocolos y procedimientos normalizados para el control, el registro y el reporte de riesgos ha dejado de ser una cuestión exclusivamente interna de las organizaciones y empresas a partir del momento en que los organismos internacionales han comenzado a considerar su utilidad potencial para la prevención de riesgos transnacionales como los que se expondrán enseguida. Sin embargo, las autoridades nacionales y supranacionales se enfrentan al importante reto de gestionar procesos y flujos de información sensible mediante el empleo de recursos que, desafortunadamente, a menudo resultan escasos. En esta tarea las tecnologías de la información y la comunicación han irrumpido con fuerza desplegando un amplio abanico de bondades entre las que sobresale, sin duda, la agilización y el ahorro de costes. La progresiva digitalización del compliance corporativo e institucional responde precisamente a la necesidad de gestionar los riesgos de la manera más eficiente posible.

En vista de todo ello parece razonable reflexionar no solo sobre el papel que está desempeñando la tecnología en la mayor o menor gravedad del riesgo transnacional presente en la Unión Europea si no, al mismo tiempo, también en la gestión que se realiza (tanto a nivel interno en cada Estado miembro como a nivel supranacional) de estos riesgos.

II. El riesgo transnacional digital

2.1. Riesgo transnacional digital y evaluaciones de impacto

Entre las dificultades a las que se enfrenta la Unión Europea a la hora de prevenir y mitigar los riesgos legales que eventualmente pudieran tener un impacto sobre sus

8. Sirvan de ejemplo, entre otros textos internacionales, la Convención para Combatir el Cohecho de Servidores Públicos Extranjeros en Transacciones Comerciales Internacionales de la OCDE. Disponible en: https://www.oecd.org/daf/anti-bribery/convcombatbribery_spanish.pdf; la Convención de Naciones Unidas contra la Corrupción (2004); la Directiva 2008/99/CE del Parlamento Europeo y del Consejo, de 19 de noviembre de 2008, sobre protección del medio ambiente mediante el Derecho penal; o, en el ámbito del *softlaw* las normas ISO 19600, 19601, 19602 e ISO 37001 y 37301 (todas ellas en materia de sistemas de gestión de *compliance* y antisoborno).

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

objetivos e intereses destaca sin duda su carácter transnacional. No en vano, como expondré más adelante, la fragmentación geográfica ha representado tradicionalmente un importante aliado para la delincuencia transnacional. Sin embargo, este viejo problema adquiere un nuevo matiz cuando además del componente transnacional se incorpora el elemento digital. En este sentido no han tardado en ponerse de manifiesto los problemas para atajar la ciberdelincuencia en el espacio transnacional. El uso de recursos informáticos y tecnológicos específicamente diseñados para la mejor (peor) perpetración de actos ilícitos es ya una realidad incontestable cuyo impacto sobre el mercado único y sobre los intereses particulares de los ciudadanos comunitarios hemos podido comprobar, por ejemplo, a propósito del auge de los criptoactivos y de la inseguridad jurídica que propiciaba su desregulación inicial.

Este hecho conduce irremediablemente a que las autoridades e instituciones públicas hayan comenzado a considerar el empleo de la tecnología con la finalidad de combatir de una manera eficaz este tipo de amenazas globales. En este sentido, como se verá a lo largo de las páginas que siguen, el diseño de los mecanismos internacionales de cooperación-prevención ha ido incorporando progresivamente componente tecnológicos y digitales para tratar de acomodarse a la realidad actual. Por un lado, esto nos permite contar con herramientas más sofisticadas (y, probablemente, más eficaces). Sin embargo, por otro lado, no es menos cierto que por la misma razón su utilización se está volviendo cada vez más compleja para los operadores jurídicos y los organismos públicos implicados.

Junto a esta novedad quiero referirme ahora, aunque sea brevemente, a la irrupción del concepto "evaluación de impacto" en el Derecho comunitario y a la importancia que representa no solo a la hora de gobernar y gestionar los riesgos en la Unión Europea sino, muy especialmente, a la hora de afrontar su prevención uniforme. Podría decirse que este concepto aterriza de manera más evidente en el ordenamiento comunitario a partir de la aprobación del Reglamento 2016/679 en materia de protección de datos de carácter personal[9]. Su finalidad esencial no es otra que la de introducir la posibilidad de evaluar, atajar, gestionar, y gobernar a priori situaciones de riesgo mayor que bajo para los derechos de las personas físicas en el ámbito de la protección de sus datos. Cuya vulneración, por cierto, se produce con cada vez más frecuencia en el espacio virtual.

La propia doctrina también se ha referido al concepto como "un proceso o metodología para determinar los riesgos o impactos que una propuesta o proyecto tiene en la privacidad de los individuos, así como para determinar los medios o soluciones para mitigar o evitar dichos riesgos o impactos negativos" (Puyol, 2018, 351). La utilidad de este recurso hace que resulte cuanto menos interesante detenerse a reflexionar sobre su posible incorporación a otras materias en las que, por su especial naturaleza, también resulte conveniente realizar este tipo de evaluaciones previas. Entre otras, el Derecho medioambiental (Quintana *et al*, 2014, 267), el Derecho fiscal y tributario o, como en el caso que nos ocupa, el Derecho digital.

9. Véanse en este sentido el artículo 35 y siguientes del Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Como se verá a continuación la importancia que la Unión Europea le confiere a este instrumento incide de manera directa en la prevención transnacional de cualquier tipo de riesgo en un sentido positivo, esto es, minimizando su daño o impacto social. Conviene tener muy en cuenta que la existencia de riesgos globales que trascienden del ámbito interno tiene un efecto multiplicador sobre el daño social potencialmente asociado y que, en este sentido, toda evaluación previa resultará bienvenida.

Desde este enfoque la Unión Europea parece orientarse hacia la consolidación de una prevención en origen (desde la producción de las normas) fomentando una cultura de prevención a partir de la regulación de una serie de obligaciones previas de vigilancia y control sobre la que edificar toda una arquitectura global para la gobernanza del riesgo. No puede negarse que, al menos en los primeros textos, los enfoques socioeconómico y medioambiental parecen prevalecer sobre el resto. En este punto quiero advertir que el hecho de no considerar su potencial preventivo en otras áreas del Derecho puede hacer que la Unión Europea pierda este tren hacia la configuración de un nuevo modelo de cooperación-prevención. Aún es pronto para saberlo puesto que apenas se ha comenzado con esta andadura y, por tanto, aún no abundan las iniciativas legislativas que incorporan este nuevo enfoque. Pero me atrevería a pronosticar que dada su utilidad preventiva y más allá del posicionamiento que finalmente adopten las autoridades comunitarias el recurso hacia las evaluaciones previas de impacto será una práctica frecuente en la era del dato.

Por otro lado, no quiero dejar de mencionar el hecho de que la producción normativa haya sido casi exclusivamente el único recurso empleado por la Unión Europea en la lucha contra el riesgo transnacional digital. Como se viene indicando la complejidad de esta realidad tiene un claro reflejo en la producción de normas comunitarias cada vez más complejas lo cual ha propiciado la aparición de dos nuevos problemas que se suman a los citados anteriormente. El primero es el relativo a las dificultades propias de su integración en el acervo comunitario. Y el segundo, tanto o más importante, es la sobrecarga de trabajo en la interpretación de estas normas que a la postre ha asumido el Tribunal de Justicia de la Unión Europea (TJUE) como último intérprete y garante de la coherencia entre las diferentes normas que integran el Derecho comunitario.

De manera paralela los intentos del legislador nacional por abordar jurídicamente los riesgos que representa la revolución digital han desencadenado una diarrea legislativa en dos sentidos. El primero a iniciativa propia y, el segundo, por la necesidad de trasponer e integrar en el derecho interno la normativa comunitaria. La crítica que cabe exponer frente a esta nueva realidad pasa de nuevo por recalcar la importancia de pensar antes de legislar. O, dicho en otras palabras, la importancia de evaluar el impacto que tendrá en la comunidad jurídica y en la sociedad general la aprobación de una determinada norma. De manera particular, si su complejidad radica en las dificultades del legislador para tratar de dotar a la sociedad de instrumentos idóneos para la gobernanza de según qué riesgos legales. En consecuencia, nos encontramos frente a un poder judicial cada vez más sobrecargado y ante una sumisión pericial que parece que ya es imparable en la revolución digital.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Quizás la solución pase por un cambio de mentalidad o simplemente por una evolución cultural que nos permita poner en valor la importancia de la valoración apriorística del riesgo digital y su potencial impacto dañino sobre determinados bienes jurídicos dignos de protección. No solo por razones de seguridad jurídica (que también) sino acaso en términos económicos y de bienestar social. En cierta medida la eficacia de las evaluaciones de impacto depende de su contenido y alcance, pero no es menos cierto que existen otros aspectos como su obligatoriedad o su mayor o menor carácter vinculante que quedan a expensas de un legislador que a menudo carece de los conocimientos propios de una ciencia que le puede resultar tan ajena o lejana como la informática, la ingeniería, o la inteligencia artificial. En este sentido quiero subrayar que la importancia que el legislador le confiera a los resultados derivados del proceso de evaluación tiene un impacto directo sobre el diseño de las políticas públicas y el resto de las medidas (no estrictamente legales) con las que se pretenda combatir cada riesgo.

Desde esta perspectiva con este trabajo pretendo abordar la necesidad de avanzar hacia una prevención uniforme del riesgo transnacional digital en la Unión Europea. De entre las múltiples iniciativas puestas en marcha hasta la fecha dirigiré mi análisis a la innovación por la que recientemente parece estar apostado la Unión desde el compliance institucional para el conjunto de los Estados miembros ya que, como trataré de exponer enseguida, parece posicionarse como la herramienta contemporánea más efectiva para esta lucha.

2.2. Riesgo transnacional digital y compliance institucional. La experiencia de la OCDE y sus implicaciones para la Unión Europea

Coincidiendo con el nuevo escenario que dibuja la transformación digital y a propósito del riesgo transnacional digital, las transacciones realizadas *online* por parte de los ciudadanos de la Unión Europea están alcanzado niveles desconocidos hasta la fecha. No solo en sus relaciones comerciales con oferentes y productores comunitarios sino también con terceros países. El modelo tradicional de integración económica también se ha "contaminado" de la nueva realidad digital como ha reconocido la propia Unión Europea en su estrategia para el mercado único digital[10]. La gran pregunta que a mi juicio procede plantearse ahora es si contamos en el plano supranacional con la estructura jurídico-social necesaria para la protección de los ciudadanos comunitarios frente a los riesgos que entraña la extraordinaria expansión de la revolución digital. Bajo mi punto de vista lo ideal sería contar con una herramienta cooperativa multiplataforma desde la que poder gestionar eficazmente cualquier manifestación del riesgo transnacional digital. Quizás, comenzando por los que representan un mayor nivel de peligrosidad o tienen una mayor probabilidad de impactar sobre intereses y objetivos comunes. Entre ellos podemos citar algunos de los típicamente asociados a las conductas propias de las

10. Disponible en: https://eufordigital.eu/discover-eu/eu-digital-single-market/ Fecha de última consulta: 4 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

personas físicas como, por ejemplo, el riesgo de sufrir una estafa en una compra *online*, el riesgo de sufrir una vulneración en la protección de datos de carácter personal, o el riesgo en la formalización de operaciones con criptoactivos en el espacio comunitario. Sin embargo, también resulta interesante atender desde la perspectiva del compliance corporativo al riesgo típicamente asociado a las conductas propias de las personas jurídicas como, por ejemplo, el riesgo de blanqueo de capitales mediante operaciones realizadas en línea, el riesgo de soborno o extorsión en la red, el riesgo de financiación ilegal, etcétera.

En todas estas modalidades coinciden el elemento transnacional y el elemento digital haciendo que todas estas conductas representen un nivel de riesgo mayor que bajo para la ciudadanía europea. Cualquier gestión eficaz de este tipo de riesgos precisará bajo mi punto de vista de mecanismos idóneos de vigilancia y control global que permitan alcanzar estándares de seguridad aceptables (habida cuenta que el riesgo cero no existe). Estas medidas forman parte de lo que podríamos considerar como compliance institucional o, en otras palabras, mecanismos de cooperación-prevención interinstitucional diseñados para la protección de todos aquellos riesgos que por exceder de las fronteras de un Estado miembro podamos catalogar como transnacionales. Esta idea no se encuentra en el acervo comunitario tradicional y tampoco es exclusiva de la Unión Europea (aunque parece que empieza a aplicarse en algunas de sus estrategias para la gobernanza global). Pero sí podemos identificarla, por ejemplo, en otros organismos internacionales como la OCDE.

La experiencia piloto de la OCDE con la activación en 2019 de su plataforma multilateral de compliance y aseguramiento de riesgos fiscales[11] representa uno de los primeros ejemplos para la gobernanza del riesgo transnacional a partir del compliance, aplicable también en el plano de lo digital. En este caso, en materia fiscal y tributaria. La acción número trece del Proyecto BEPS de la OCDE[12] se orientaba hacia una autoevaluación de riesgos que realizaba la persona jurídica contribuyente haciendo un especial hincapié en la documentación sobre precios de transferencia[13] de acuerdo con el principio de plena competencia (*arm's length principle)* (Keuschnigg y Devereux, 2013, 436). Sin perjuicio de las críticas señaladas por la doctrina a propósito de este modelo y de sus posibles perjuicios en los intercambios intragrupo (Witterndorff, 2010, 343), considero que su potencial disuasorio a la hora de evitar riesgos relacionados con la erosión de la base imponible del impuesto de sociedades resulta satisfactorio. En sintonía con esta iniciativa de

11. OCDE (2019): *International Compliance Assurance Programme* (2019). En línea: http://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/international-compliance-assurance-programme-pilot-handbook-2.0.pdf Fecha de última consulta: 8 de septiembre de 2023.

12. OCDE (2015): *Plan de Acción BEPS*. En línea: https://read.oecd-ilibrary.org/taxation/plan-de-accion-contra-la-erosion-de-la-base-imponible-y-el-traslado-de-beneficios_9789264207813-es#page2 Fecha de última consulta: 8 de septiembre de 2023.

13. Documentación sobre precios de transferencia e informe país por país, Acción 13. Recurso disponible en: https://read.oecd-ilibrary.org/taxation/documentacion-sobre-precios-de-transferencia-e-informe-pais-por-pais-accion-13-informe-final-2015_9789264267909-es#page19 Fecha de última consulta: 8 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

la OCDE la doctrina señala otras de similar naturaleza como las normas internacionales para el control fiscal de empresas extranjeras (*controlled foreign company*, CFC) (Haufler, *et al*, 2018, 31), el diseño de mecanismos para la neutralización de los efectos derivados de instrumentos híbridos, o el proyecto CRS (*Common Reporting Standard*), entre otros (Belmonte, 2016, 103; Vérguez, 2016, 75).

El reflejo de estos instrumentos en la Unión Europea para la gobernanza del riesgo transnacional se ha ido dejando ver poco a poco (sobre todo a partir de la necesidad de gestionar los riesgos fiscales en el plano supranacional) en diferentes textos y Directivas comunitarias que han ido allanando el camino hacia la configuración de un modelo de compliance institucional de cooperación-prevención. Entre otras, podemos citar la Directiva 2014/107/UE del Consejo de 9 de diciembre de 2014[14], o la Directiva (UE) 2018/822 del Consejo, de 25 de mayo del 2018[15]. Ambas en relación con el intercambio automático y obligatorio de información en el ámbito de la fiscalidad en relación con los mecanismos transfronterizos sujetos a comunicación de información.

El éxito en la iniciativa de la OCDE radica en primer lugar en el número de Estados miembro acogidos a su plataforma internacional. Inicialmente, en 2019 contaba con las administraciones tributarias y los grupos empresariales (grandes contribuyentes) de ocho países de la OCDE[16]. Como podrá comprender el lector el éxito en la gestión de un riesgo transnacional es directamente proporcional al número de Estados que participan en el mecanismo propuesto para su adecuada gestión. A la luz de esta experiencia me propongo finalizar este epígrafe analizando algunos de los problemas que estuvieron (y siguen estando) presentes en el diseño y la aplicación de este tipo de plataformas. Pues, como se verá en el siguiente apartado resultan igualmente válidos para cualquier mecanismo de compliance institucional que se proponga en la Unión Europea para la gestión del riesgo transnacional digital.

El primer aspecto controvertido es la siempre temida pérdida de soberanía o de poder decisorio por parte de los Estados adheridos. Este viejo problema (del que es consciente la Unión Europea tal y como se aprecia en su derecho originario) adquiere ahora un nuevo matiz cuando se trata de gestionar los riesgos propios de la revolución digital. Aspectos como las diferencias en el nivel de alfabetización digital entre los diferentes Estados miembros de la Unión Europea[17], el acceso a internet, o las diferentes fuerzas con las que cada Estado se enfrenta a este tipo de riesgo a nivel interno generan asimetrías y desigualdades que comprometen sin duda la prevención uniforme. Para tratar de salvar este obstáculo la Unión cuenta desde hace décadas con mecanismos de cohesión que pretenden precisamente corregir este tipo de desequilibrios territoriales.

14. Directiva 2014/107/UE del Consejo de 9 de diciembre de 2014, disponible en: https://www.boe.es/doue/2014/359/L00001-00029.pdf. Fecha de última consulta: 17 de septiembre de 2023.

15. Directiva (UE) 2018/822 del Consejo, de 25 de mayo del 2018, disponible en: https://www.boe.es/doue/2018/139/L00001-00013.pdf. Fecha de última consulta: 17 de septiembre de 2023.

16. Australia, Canadá, Italia, Japón, Reino Unido, EE. UU., Países Bajos y España.

17. Recogidos entre otros indicadores en el *EU-DESI Index 2022*. Disponible en: https://digital-strategy.ec.europa.eu/es/library/digital-economy-and-society-index-desi-2022 Fecha de última consulta: 17 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Sin embargo, su impacto real sobre la mejora en el desempeño digital de algunas regiones y territorios sigue siendo muy limitado y, en consecuencia, sigue condicionando el acceso de estos ciudadanos al mercado único digital. Como posible solución al temor de la pérdida de soberanía a mi juicio debemos optar por mecanismos complementarios de compliance institucional y nunca sustitutivos de las medidas internas que en cada caso quiera adoptar cada Estado miembro. De tal manera (y este es el reto) que se establezcan criterios claros para aquellos casos de incompatibilidad y/o conflicto siempre en aras de la mejor prevención y/o mitigación posible del riesgo transnacional para el conjunto de los Estados miembros.

A propósito de este problema la doctrina señala que una posible vía para el combate eficaz de los problemas propios de las sociedades del riesgo es la puesta en valor del autogobierno o, si se prefiere, la autogobernanza. Es decir, la posibilidad de establecer políticas públicas que impliquen obligaciones que afecten a comportamientos individuales. Pues, en definitiva, el comportamiento de una sociedad no es más que la agregación de un conjunto de comportamientos individuales (Ericson y Haggerty, 1997, 83). No es menos cierto que estos aspectos, de una u otra manera ya están presentes en buena parte de los modelos de autorregulación regulada que ha ido incorporando el legislador nacional en los diferentes Estados miembros de la Unión Europea desde que se produjo el cambio de siglo. Y, que con independencia de que se hayan llevado por la vía penal, civil, o administrativa, impactan en el comportamiento de organizaciones y empresas que también actúan en el plano internacional.

En segundo lugar, cualquier mecanismo de estas características debe contar necesariamente con incentivos. A pesar de las ventajas derivadas del cumplimiento normativo en cualquiera de sus ámbitos no es menos cierto que existen costes que los Estados y las empresas no siempre están dispuestos a asumir. Entre otros, el coste de coordinar una actuación uniforme entre un conjunto de Estados con diferencias notables entre sí. La dificultad en este caso se nos presenta cuando existen diferencias importantes entre el estándar óptimo de prevención global y el que venía aplicando o pretendía aplicar cada Estado. Este hecho puede acabar obligando a uno o varios países a elevar las condiciones que venía exigiendo en su ámbito interno (shock asimétrico). Al igual que ocurre en el ámbito que nos ocupa existen otros muchos en los que la existencia de regímenes menos estrictos o más beneficiosos actúa como refugio para según qué prácticas o actos ilícitos propiciando la aparición de "focos de riesgo" en un territorio concreto, pero con efectos y consecuencias transnacionales para todos. Son precisamente estos focos los que a menudo nos pueden dificultar el consenso.

El reto en este punto pasa necesariamente por diseñar una plataforma multilateral que resulte atractiva para todos los Estados miembros con independencia de cuál sea su punto de partida. En este punto la Unión Europea se enfrenta al reto de diseñar un sistema de compliance institucional capaz de asumir que los *dispute-prevention efforts* deben ser una prioridad y que la estrategia de pretender una solución demasiado exigente puede acabar desembocando en un incentivo para que aquellos países con peor situación de partida terminen abandonando el proyecto. En relación con todo ello no debemos obviar que la integración de la tecnología y los principios que rigen el funcionamiento electrónico de

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

las relaciones entre particulares y empresas presenta también diferencias notables que pueden estar propiciando la aparición de riesgos digitales potencialmente transnacionales en territorios concretos de la Unión Europea.

III. Compliance, riesgo transnacional y prevención de la delincuencia organizada en la Unión Europea

La estrategia comunitaria para la gobernanza de los riesgos transnacionales se ha centrado tradicionalmente en identificar aquellas actividades en cuyo ámbito pudiera resultar más probable la aparición de estos riesgos para, en un momento posterior, tratar de diseñar e implementar las medidas de vigilancia, monitoreo y control necesarias para alcanzar un determinado nivel de "prevención" y/o "seguridad". En este sentido la traslación de elementos más propios del compliance privado al ámbito público o institucional representa una oportunidad para la adecuada gestión de los riesgos (Nieto y Calatayud, 2015) no solo a nivel interno de cada Estado miembro sino, con cada vez más frecuencia, también en el plano internacional como se aprecia en las políticas públicas de la OCDE o, como se verá a continuación, en la nueva tendencia que parece estar iniciándose en la Unión Europea. Bajo esta premisa aludo al término compliance institucional en referencia a esta maniobra recordando que se trata de un concepto no estrictamente jurídico sino más bien interdisciplinar en el que se combina la ciencia jurídica con otras disciplinas como la economía, la gestión de riesgos, la sociología, o las nuevas tecnologías.

De entre las múltiples actividades que eventualmente pueden dar lugar a la aparición de riesgos transnacionales en la Unión Europea en este trabajo me centraré en una de las que, a mi juicio, resulta más preocupante en el momento actual: la delincuencia organizada. De manera particular atendiendo a sus diferentes manifestaciones en la realidad digital de nuestros días. Como ya anticipaba en el apartado anterior, la adecuada gestión y el tratamiento del riesgo transnacional digital encuentra un importante aliado precisamente en la incorporación de las nuevas tecnologías a las recientes medidas de vigilancia y control que nos ofrece el compliance en el ámbito público.

Debo especificar que a efectos de este trabajo me referiré a dos tipos de estrategias adoptadas por la Unión Europea para la prevención del riesgo asociado a la delincuencia transnacional: *ad intra* y *ad extra*. O si se prefiere en otras palabras: la acción exterior y la acción interior de la Unión. Como trataré de exponer a lo largo de estas páginas esta diferenciación resulta determinante a la hora de seleccionar las medidas preventivas con las que la Unión afronta este reto en uno y otro escenario, de evaluar su idoneidad, y de explorar las posibles sinergias o relaciones de complementariedad que se puedan establecer entre ellas en aras de la máxima aspiración de la Unión: la prevención uniforme. De la misma manera la diferenciación entre ambas resulta también pertinente a la hora de abordar las posibilidades de digitalización que nos ofrece la gestión de este tipo de riesgos en uno y otro escenario.

A lo largo de este trabajo me centraré mayoritariamente en la vertiente *ad intra* de la gestión del riesgo transnacional en la Unión Europea a partir de las diferentes amenazas y

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

desafíos que representa la sociedad digital. En este abordaje me propongo hacer hincapié en la eficacia preventiva de los nuevos elementos de compliance institucional incorporados recientemente por las autoridades comunitarias para tratar de aportar claridad sobre algunos de los interrogantes que considero más relevantes en esta materia. ¿Caminamos verdaderamente hacia una prevención uniforme del riesgo transnacional en el seno interno de la Unión? ¿Estamos ante el diseño de una nueva arquitectura de cooperación-prevención o, por el contrario, nos encontramos más bien ante una mera reformulación estética del modelo anterior? De encontrarnos en el primer escenario, ¿qué significado tienen entonces las nuevas medidas propuestas por las autoridades comunitarias? Y, lo que es más importante aún, ¿hacia dónde nos dirigimos ahora con este nuevo modelo?

3.1. La gestión del riesgo transnacional *ad extra*

Para una mejor comprensión del enfoque propuesto, de su sentido y alcance, conviene también atender siquiera sucintamente a esa otra dimensión exterior en la que la Unión ha desplegado tradicionalmente sus mecanismos para la gobernanza global de este riesgo. En este segundo escenario los esfuerzos de la Unión Europea se han concentrado tradicionalmente en tratar de gobernar, en sentido amplio, cualquier riesgo asociado a la criminalidad transnacional con origen en un territorio extracomunitario cuyo impacto pudiera resultar potencialmente dañino para los intereses de la Unión. En este sentido, la acción preventiva exterior se ha dirigido hacia aquellos países que, a juicio de las autoridades comunitarias, podían representar mayores niveles de riesgo. Destacan en este contexto los diferentes programas y acuerdos de cooperación (cooperación-prevención) suscritos durante los últimos años con América Latina. Por citar algunos ejemplos recientes me referiré, en primer lugar, al Programa de Asistencia contra el Crimen Transnacional Organizado 2017-2022 (en adelante, PAcCTO)[18] cuya finalidad esencial no ha sido otra que la de proporcionar asistencia técnica a los Estados de América Latina incluidos en el programa para la prevención eficaz del crimen organizado.

En mi opinión, desde su suscripción en el año 2017 el programa ha resultado fiel a su propósito y ha cubierto las expectativas. Incluso, como trataré de exponer, arrojando resultados y oportunidades para la cooperación internacional que representan importantes avances en esta materia. Seis años después de su inauguración puede afirmarse que el PAcCTO ha favorecido la cooperación estratégica entre la Unión Europea y América Latina para la prevención del riesgo de delincuencia transnacional. A mayores me gustaría señalar que este marco general de prevención constituye un apoyo importante sobre el que fundamentar cualquier medida de cumplimiento institucional y que también puede resultar especialmente útil cuando se trata de prevenir la vulneración de bienes jurídicos en el espacio virtual.

18. Países incluidos en el PAcCTO: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay, Venezuela.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Es de justicia reseñar que la cooperación policial y judicial se han posicionado como ejes vertebradores del PAcCTO gracias a la implicación de Europol y Eurojust. Como se verá en el siguiente apartado esta cooperación ha sido particularmente estrecha y, al menos bajo mi punto de vista, altamente satisfactoria. Tanto es así que ha permitido la conexión de algunos países de América Latina con otros mecanismos más propios de la gobernanza global de este tipo de riesgos *ad intra*. Aunque esta conexión no se haya materializado al mismo nivel al que rige para los Estados miembros su análisis resulta, a mi modo de ver, bastante interesante desde la perspectiva de la complementariedad entre los instrumentos preventivos *ad intra* y *ad extra* a la que me refería anteriormente. La importancia que representa este análisis justifica su abordaje en el apartado siguiente dedicado a la vertiente *ad intra*.

Como segundo ejemplo quiero referirme un instante al oportuno estrechamiento del cerco que se está produciendo a lo largo de este año 2023 entre la Unión Europea y el Comité Latinoamericano de Seguridad Interior (en adelante, CLASI) para la prevención transatlántica del riesgo de delincuencia transnacional. Con especial atención a la lucha contra el narcotráfico, la trata de seres humanos, el abuso sexual de menores, la corrupción y el blanqueo de capitales, los delitos contra el medio ambiente, el tráfico de armas de fuego, la ciberdelincuencia, o el tráfico ilícito de migrantes. Este nuevo marco de cooperación resulta particularmente interesante cuando se trata de analizar la comisión de estas conductas ilícitas en el espacio virtual.

El acercamiento responde a la misma línea de acción estratégica inaugurada en el PAcCTO y aspira a reforzar la cooperación para la prevención de la delincuencia transnacional mediante el establecimiento de marcos de colaboración permanentes entre la Unión Europea (y sus diferentes organismos y agencias de seguridad y justicia implicados en la gestión de este riesgo; entre ellos, Europol, Eurojust, y Frontex) y América Latina (y sus correspondientes agencias y organismos homólogos; de manera particular, la agencia policial latinoamericana Ameripol). De nuevo, la importancia de analizar este segundo hito histórico se pondrá de manifiesto en el siguiente apartado a propósito del estudio de la vertiente *ad intra* tanto en el plano *online* como *offline* y de sus posibles interacciones con este escenario de acción exterior de la Unión.

Antes de adentrarme en la segunda vertiente quiero referir que si algo caracteriza a esta acción exterior de la Unión es la prevención en origen (presente en ambos ejemplos). Esto es, la importancia de la identificación y la detección temprana de cualquier situación potencialmente dañina a partir de un refuerzo de la vigilancia en origen. Bajo mi punto de vista esta estrategia entronca en cierto modo con la doctrina anglosajona del *Tort Law* o Derecho de daños en la que la apreciación de responsabilidades legales se realiza a partir de la ubicación del origen de un riesgo en la fuente del daño (McBride y Bagshaw, 2008, 30). Si el origen de la responsabilidad es el daño cualquier prevención deberá dirigirse entonces hacia el origen del daño. Como expondré en el apartado dedicado al estudio de los elementos de compliance institucional presentes en la estrategia comunitaria para la prevención del riesgo de delincuencia transnacional, la apreciación (y en su caso la atribución) de responsabilidades penales para el caso de las personas jurídicas, pasa precisamente en este contexto por la adecuación o

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

inadecuación de las medidas internas de vigilancia y control llevadas a cabo para prevenir, reducir o mitigar riesgos legales. Medidas que, a través de los correspondientes sistemas de gestión de compliance, irán dirigidas con más o menos acierto hacia la identificación del riesgo como fuente de origen del daño. En otras palabras, lo habitual es que siguiendo esta teoría en términos generales se trate de orientar cualquier acción preventiva (corporativa o institucional) hacia la circunstancia o actividad concreta generadora del daño alcanzando así lo que se ha dado en llamar la prevención en origen. En este sentido sería razonable que desde la Unión Europea se fomentase la prevención uniforme en origen orientando cada acción preventiva hacia el origen del daño.

3.2. La gestión del riesgo transnacional *ad intra*

De entre las diferentes figuras delictivas que salen a escena cuando hablamos de prevenir el riesgo transnacional en la Unión Europea en este apartado me propongo abordar el asociado al crimen organizado transnacional (especialmente en su vertiente digital) por la importancia creciente que las autoridades comunitarias le han ido confiriendo en los últimos años a la necesidad de articular una red de cooperación-prevención uniforme entre los Estados miembros que optimice los recursos digitales con los que cuenta la Unión.

El interés de la Unión por diseñar una arquitectura eficaz de cooperación-prevención en esta materia se remonta al año 2014, fecha en la que el Consejo de Europa publica el libro blanco sobre el crimen organizado transnacional[19]. En este momento ya se empieza a alertar sobre el impacto de las nuevas tecnologías en la comisión de nuevas modalidades delictivas en la escena transnacional y de la conveniencia de aplicar igualmente los recursos tecnológicos a cualquier estrategia preventiva. Conviene recordar que por aquel entonces la Unión ya estaba inmersa en la preparación de su estrategia para el mercado único digital y que la protección de este mercado y la creación de un espacio virtual de confianza recíproca para oferentes y demandantes precisaba de mecanismos para la prevención de cualquier tipo de riesgo transnacional digital. Bajo esta premisa la importancia de prevenir y gestionar eficazmente este tipo de riesgos se va convirtiendo poco a poco en una prioridad para el correcto funcionamiento del mercado.

La publicación de este libro blanco representa toda una declaración de intenciones por parte de las autoridades comunitarias al incluir, por primera vez, un diagnóstico de situación (fallos y problemas detectados) y un paquete específico de acciones posibles consideradas idóneas para una prevención eficaz y uniforme entre todos los Estados miembros. A mi modo de ver con esta iniciativa el Consejo de Europa hace un llamamiento a los Estados miembros poniendo de manifiesto dos grandes problemas que han dificultado (y que, al menos a mi juicio, continúan dificultando) la gobernanza del riesgo transnacional en el seno interno de la Unión.

El primero de ellos es la fragmentación geográfica y sus consecuencias desde el punto de vista del riesgo ya que, como es sabido, en no pocas ocasiones ha propi-

19. Disponible en: https://rm.coe.int/168070e545. Fecha de última consulta: 21 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

ciado la aparición de focos de riesgo en determinados territorios o regiones que por reunir ciertas características o circunstancias particulares resultan más atractivos para el crimen. Aspecto que desaparece por completo cuando nos movemos en el espacio virtual.

Y, el segundo, es la ausencia de acuerdos multilaterales y de otros mecanismos legales de cooperación-prevención que resulten verdaderamente eficaces en el plano transnacional. Incluyendo, por supuesto, la prevención del riesgo transnacional digital.

3.2.1. ¿Por qué es necesaria una prevención uniforme?

Entre los factores que han alimentado la preocupación de las autoridades comunitarias por alcanzar estándares óptimos de cooperación-prevención en esta materia vale la pena reflexionar un instante sobre su impacto económico. La delincuencia transnacional (*online* y *offline*) a menudo aparece vinculada a la comisión de delitos económicos donde la necesidad de cooperar es, si cabe, aún más intensa cuando además de procesar a los autores se persigue la recuperación de los beneficios derivados de su actividad ilícita.

La localización de estos activos por parte de los autores en diferentes ubicaciones geográficas ha puesto de manifiesto las dificultades reales de la Unión Europea en relación con el comiso y embargo de las ganancias derivadas del crimen organizado transnacional aun cuando estas se materializan en el plano *offline*. De manera similar, cuando nos encontramos en el espacio virtual el rastreo de la actividad delictiva y la búsqueda de estas ganancias precisan de herramientas digitales que nos permitan reconocer la trazabilidad de esos activos.

A propósito de ello me propongo subrayar las consecuencias jurídicas, económicas y sociales que ha desencadenado esta realidad en la última década y realizar un juicio crítico sobre la estrategia comunitaria para su abordaje desde el compliance institucional. Abordaré la primera cuestión a lo largo de este apartado y me dedicaré a la segunda en el apartado siguiente.

Como punto de partida debo advertir que las dificultades a la hora de localizar y recuperar las ganancias procedentes del crimen organizado en el espacio *offline* derivadas de la fragmentación geográfica tienen a su vez un efecto multiplicador que retroalimenta este tipo de delincuencia transnacional. Y que, en ocasiones, fomenta su reingreso en el espacio *online*. Las consecuencias de este tipo de prácticas no son exclusivamente económicas, sino que inciden de manera directa en el comportamiento social y político haciendo del crimen organizado una especie de "colectivo" con capacidad para influir en la sociedad. Como demuestran los informes de INTERPOL[20] en la mayoría de los casos estas ganancias se "invierten" en nuevas actividades delictivas como la corrupción o el propio crimen organizado (revierten en la propia red), nutren

20. Disponibles en: https://www.interpol.int/es/Delitos/Ciberdelincuencia. Fecha de última consulta: 16 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

a otros grupos organizados, financian actos de terrorismo y, en definitiva, fortalecen la delincuencia transnacional.

En este contexto la posibilidad de refugiar estas ganancias en el espacio *online* constituye un aliciente para la ciberdelincuencia que, sin duda, incrementa el riesgo transnacional digital. La Unión Europea, consciente de esta realidad, se ha rearmado modernizando sus técnicas de investigación y fomentando la creación de unidades específicas de ciber vigilancia y la aplicación de recursos informáticos que le permitan identificar el rastro digital de las ganancias económicas derivadas del crimen. En relación con todo ello, en el siguiente apartado expondré las herramientas concretas (jurídicas y extrajurídicas) que recientemente ha incorporado la Unión para su lucha contra el riesgo transnacional digital.

Como segunda derivada y ya en el plano estrictamente económico el fortalecimiento del crimen organizado a partir de este sistema de financiación tiene al menos dos consecuencias directas. La primera es el desequilibrio en la competencia de los diferentes agentes que operan en el mercado global. Y, la segunda, su impacto sobre la economía pública también en términos de confianza y reputación. Este aspecto entronca con la necesidad de alinear cualquier estrategia para la gobernanza del riesgo transnacional asociado a la delincuencia organizada con las políticas públicas comunitarias sobre transparencia y buen gobierno y con otras líneas para la prevención de delitos como la prevención del blanqueo de capitales, los actos de corrupción o el soborno a funcionario público extranjero. Pues, en todos estos casos, se trata de prevenir riesgos contra la administración pública. Y, en todos ellos, puede estar presente directa o indirectamente el componente digital.

A la vista de todo ello se hace aún más necesaria si cabe la búsqueda de nuevas herramientas e instrumentos preventivos multilaterales que nos permitan estar a la altura de este desafío global. Como se verá a continuación, el nuevo modelo de cooperación-prevención diseñado por la Unión Europea combina elementos de compliance institucional con diferentes iniciativas legislativas que representan avances verdaderamente significativos respecto de las herramientas jurídicas tradicionales[21] que si bien han resultado extraordinariamente útiles a mi juicio precisaban ya de un nuevo empuje.

3.2.2. Antecedentes y evolución de la estrategia comunitaria

La respuesta de las autoridades comunitarias frente al desafío global que representa el riesgo transnacional digital ha ido evolucionando desde 2010 hasta nuestros días priorizando una acción conjunta *ad intra* basada en dos ejes fundamentales que podemos considerar prioritarios en el combate de la delincuencia transnacional. El primero de ellos consiste en el establecimiento de mecanismos legales y extralegales para la mejora

21. Entre ellas no quiero dejar de citar el Convenio del Consejo de Europa relativo al blanqueo, seguimiento, embargo y decomiso de los productos del delito y a la financiación del terrorismo de 2005, la Convención UNTOC, o la Convención contra la Corrupción; entre otros.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

en la recuperación de activos procedentes de actividades ilícitas haciendo especial hincapié en la recuperación de los activos digitales. Y, el segundo, consiste en el diseño e implementación de instrumentos multilaterales de cooperación conjunta para la prevención del riesgo transnacional digital.

El primer paso hacia esta nueva dirección lo identifico en los compases previos a la publicación del libro blanco sobre el crimen organizado transnacional del Consejo de Europa en 2014. Concretamente, en los años 2012 y 2013 cuando la Unión puso en marcha por primera vez el llamado ciclo de actuación contra la delincuencia organizada. Podría decirse que este ciclo representa la primera piedra sobre la que, como trataré de exponer, se ha ido edificando toda una política comunitaria para la prevención uniforme del riesgo transnacional. En esta ocasión, asociado al crimen organizado[22].

El principal problema que a mi juicio presenta esta receta de "café para todos" es que la realidad jurídica, económica, digital y social de cada Estado miembro es diferente del resto. Y, por lo tanto, los niveles de riesgo transnacional (digital y no digital) no son homogéneos. En este punto tiene sentido reflexionar un instante sobre dos posibles vías de comprender y aplicar la prevención uniforme.

La primera sería entender que existe prevención uniforme en la aplicación de medidas preventivas globales cuya aplicación se realiza por igual entre y para todos los Estados miembros. Ello aun con independencia de los niveles de riesgo que se presenten en cada uno de ellos. Esta estrategia de máximos nos llevaría quizás que dos Estados con diferentes niveles de riesgo se vieran obligados a aplicar las mismas medidas. Sin embargo, la segunda consistiría en comprender que existe prevención uniforme cuando ante iguales niveles de riesgo se reacciona con las mismas medidas. Este segundo enfoque obliga a que previamente se haya realizado una exhaustiva labor de identificación de riesgos. Aun siendo consciente de que se trata de un camino costoso y seguramente más lento que el anterior bajo mi punto de vista podría resultar más acorde con la realidad socioeconómica actual de los Estados miembros.

A partir de la experiencia adquirida con este ciclo de actuación la Unión Europea da un paso más allá en el año 2021 con la finalidad de mejorar la eficacia de su acción preventiva frente al riesgo transnacional. De esta manera el ciclo de actuación diseñado en 2010 fue reformulado mediante acuerdo del Consejo de 26 de febrero de 2021 pasando a su denominación actual: *European Multidisciplinary Platform Against Criminal Threats* (en adelante EMPACT), o Plataforma Multidisciplinar Europea Contra las Amenazas Delictivas.

Esta plataforma, más actual y por lo tanto más acorde con la realidad social de nuestros días, incorpora novedades metodológicas interesantes para la prevención,

22. La versión inicial de este ciclo se orientó hacia diez figuras delictivas: la ciberdelincuencia, el tráfico de drogas, la facilitación de migración ilegal a la Unión Europea, el robo organizado, la trata de seres humanos, el fraude de impuestos especiales y del operador desapercibido, el tráfico de armas de fuego, la delincuencia medioambiental, las operaciones financieras delictivas, y el fraude documental. Documento disponible en: https://op.europa.eu/en/publication-detail/-/publication/9984824a-7509-448e-8ed8-ea7a54ff5ad6/ Fecha de última consulta: 23 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

el tratamiento y la gestión del riesgo transnacional, también en su versión digital. El nuevo modelo se inspira en cierta medida en la vieja idea del ciclo de *Deming* (PDCA, *Plan-Do-Check-Act*) que ha inspirado el diseño de los sistemas de compliance contemporáneos. A través de esta plataforma se pretende establecer y evaluar prioridades y objetivos de actuación en función de los diferentes niveles de riesgo identificados. Esta nueva política preventiva de la Unión Europea es coherente, como indicaba antes, con la línea seguida por otros organismos internacionales como la OCDE en su plataforma *ICAP*[23]. Y, en este sentido, permite la conexión con la vertiente *ad extra* del riesgo transnacional. La importancia de esta conexión radica en el hecho de que nos encontramos en una economía con niveles récord de globalización y cada día más digitalizada. Por lo tanto, esta evolución de la multilateralidad en el panorama internacional resulta crucial para afrontar con éxito estos desafíos. Tengamos en cuenta que según ha informado recientemente la Comisión Europea el riesgo transnacional asociado al crimen organizado está presente en al menos tres Estados miembros en el 70 de cada 100 casos. Con todo ello, la plataforma EMPACT se encuentra actualmente en el ecuador del marco plurianual 2022-2025[24] y, aunque aún es pronto para evaluar resultados, contamos con algunos indicios interesantes que trataré de exponer a continuación.

Como segunda novedad relevante la plataforma plantea la creación de nuevos servicios de cooperación internacional, inteligencia, y prevención e incorpora nuevas obligaciones de colaboración *ad intra* y *ad extra* para una gestión más eficaz del riesgo transnacional. En este nuevo enfoque está muy presente el daño económico que representa el riesgo transnacional asociado al delito de organización criminal para los ciudadanos y las instituciones europeas. La propia Comisión Europea ha cuantificado los ingresos derivados de la delincuencia organizada en 139.000 millones de euros en 2019. Esta cifra representa el 1% de todo el PIB comunitario y se asocia con una cierta tendencia al alza que, en resumidas cuentas, no es sino la confirmación de que el riesgo transnacional asociado al crimen organizado también está al alza.

En tercer lugar, la metodología propuesta en esta plataforma se basa en un modelo secuencial en cuatro pasos que aspira a servir como marco global para la cooperación-prevención *ad intra*. Al análisis crítico de este modelo me dedicaré en el apartado siguiente.

23. Acceso al documento para el desarrollo completo de la plataforma *ICAP* de la OCDE disponible en: http://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/international-compliance-assurance-programme-pilot-handbook-2.0.pdf Fecha de última consulta: 17 de septiembre de 2023.

24. Prioridades EMPACT 2022-2025 disponibles en: https://www.consilium.europa.eu/es/press/press-releases/2021/05/26/fight-against-organised-crime-council-sets-out-10-priorities-for-the-next-4-years/ Fecha de última consulta: 17 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

3.2.3. Breve análisis de la plataforma comunitaria EMPACT desde la perspectiva del compliance institucional. ¿Un recurso útil para la gestión del riesgo transnacional DIGITAL?

En relación con la idoneidad del modelo contenido en la plataforma comunitaria para la prevención del riesgo transnacional asociado al crimen organizado dedicaré este apartado al análisis de su eficacia en el espacio *online* a partir de los elementos de compliance institucional que identifico en su configuración. A lo largo de esta exposición me propongo realizar algunas aportaciones desde la crítica constructiva sobre aquellos aspectos en los que considero que existe algún margen para la mejora.

La primera podríamos localizarla en la fase del modelo dedicada a la elaboración de políticas. Este elemento resulta clave en cualquier sistema de gestión de compliance por su utilidad para la prevención de cualquier tipo de riesgo. Tomando como base la segunda interpretación del concepto de prevención uniforme a la que me referí anteriormente la identificación previa de diferentes niveles de riesgo (en diferentes territorios y/o Estados) puede acabar determinando la eficacia de cualquier medida preventiva. En otras palabras, la elaboración de políticas requiere siempre de una evaluación previa del riesgo. Sin embargo, al menos sobre el papel, no parece que en el diseño originario de esta plataforma se le haya conferido esta relevancia a la identificación previa del riesgo como elemento clave de la elaboración de políticas. Bajo mi punto de vista resultaría conveniente que, al menos en la práctica, se incorporase este enfoque ya que puede resultar particularmente útil en el espacio virtual. Por otro lado, el hecho de que no se le haya conferido esta importancia a la gestión apriorística del riesgo en la fase de elaboración de políticas resulta cuanto menos chocante con la intención del propio Consejo de hacer de esta fase una herramienta útil para la evaluación de amenazas de delincuencia organizada en sentido amplio respecto de cualquier riesgo potencialmente dañino para la Unión Europea. De hecho, las figuras delictivas comprendidas en el ámbito de actuación de la plataforma tienen una extraordinaria capacidad para transformarse, como ocurre con cada vez más frecuencia, al confluir elementos digitales o informáticos en la comisión del delito. El hecho de que puedan intervenir estos elementos justificaría, a mi modo de ver, no solo un enfoque más centrado en el riesgo sino también más centrado en la revisión periódica y en la actualización de los diferentes niveles de riesgo. En consecuencia, los controles internos y las medidas de compliance institucional de la Unión deberían acomodarse con relativa rapidez a cualquier cambio identificado en los niveles de riesgo.

Por último, este hecho podría comprometer la efectividad de las evaluaciones de impacto que analizamos anteriormente. Una de las debilidades de cualquier modelo secuencial es precisamente su incapacidad para adaptarse con rapidez a los cambios. La aparición de nuevos riesgos no detectados o la modificación de los ya existentes puede comprometer el resto de las etapas del ciclo. En este sentido se echa en falta quizás un compromiso menos tibio de las autoridades comunitarias con la acomodación del modelo a la realidad digital de nuestros días. Digo menos tibio porque, en honor a la verdad, debe reconocerse que la implicación de EUROPOL en la cooperación entre

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Estados miembros para la detección temprana de riesgos ha sido creciente desde el año 2021. Y, a mayores, el sistema prevé el reporte de informes periódicos desde EUROPOL al Consejo.

En segundo lugar, procedería reflexionar ahora a propósito de la primera interpretación del concepto de prevención uniforme referido anteriormente en relación con los planes estratégicos plurianuales previstos por este modelo. También llamados *General Multi-Annual Strategic Plan* (en adelante, G-MASP). En pocas palabras, se trata de una planificación de metas horizontales comunes (el Consejo se refiere a ellas como *Common Horizontal Strategic Goals*, CHSG) en las que todo parece indicar que se ha optado de nuevo por una receta de café para todos.

De nuevo aflora la cuestión de qué ocurre cuando en uno o varios Estados o regiones de la Unión Europea se presentan niveles particulares de riesgo (nacional y/o transnacional) que precisen de medidas concretas o que no puedan prevenirse, mitigarse, o gestionarse con la receta global. Las CHSG podrían haber previsto esta situación, pero es posible que la reacción que contemplen no sea la más adecuada para ese país o región en concreto. En otras palabras, la cauterización de ese punto caliente podría requerir de medidas complementarias o independientes de las previstas por el plan general y, bajo mi punto de vista, esta posibilidad debería estar incluida con mayor nitidez en la estrategia comunitaria. No como un incentivo hacia la inequidad horizontal (aspecto que habrá que trabajar aparte) pero sí como una posible solución frente a los casos concretos. La previsión de esta posibilidad no tendría por qué comprometer, al menos no necesariamente, la uniformidad de la prevención. Pues, al preverse para situaciones concretas que eventualmente pudieran presentarse en el conjunto de los países incluidos en la plataforma, procedería su aplicación para cualquiera de ellas con independencia del factor geográfico. De la misma manera sería recomendable buscar la complementariedad entre la plataforma EMPACT y las medidas internas que en cada caso pudiera haber previsto cada Estado miembro respetando siempre los principios que rigen las relaciones entre las competencias nacionales y supranacionales en la Unión Europea.

En tercer lugar, la plataforma incorpora un comité bautizado como "de cooperación operacional y seguridad interna" (COSI, *Committee on Operational Cooperation on Internal Security*) para una mejor prevención de la delincuencia transnacional en las diez áreas seleccionadas como prioritarias[25]. Como se puede observar en la mayoría de estas áreas existe la posibilidad de toparnos con conductas y riesgos en el espacio virtual. En este sentido el recurso hacia redes seguras para el intercambio de información entre Estados miembros y hacia las autoridades comunitarias se hace inevitable. Este hecho ha impulsado, como trataré de exponer en el apartado siguiente, algunas iniciativas legislativas en la Unión Europea para adecuar nuestro marco jurídico a las nuevas necesidades de intercambio de información que ha puesto de manifiesto nuestra realidad digital. La red europea SIENA opera en este contexto como un recurso digital coadyuvante en la

25. Acceso al documento completo (con descripción de las áreas) de la estrategia de prevención EU-EMPACT 2022-2025 disponible en: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact Fecha de última consulta: 21 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

prevención del riesgo transnacional. Sin embargo, en no pocas ocasiones desafortunadamente la configuración de estas redes y la redacción de estas normas presenta vulnerabilidades y riesgos que comentaré más adelante y que también pueden condicionar la gestión del riesgo transnacional en la Unión.

En cuarto lugar, me detendré en la necesidad de evaluar de manera independiente e imparcial el funcionamiento general del modelo. Este es un aspecto que a menudo sobresale en cualquier sistema de gestión de compliance corporativo y que en el plano institucional aparece, bajo mi punto de vista, con menor intensidad. Posiblemente la envergadura del modelo, el volumen de información y las características del riesgo al que nos enfrentamos en el plano supranacional puedan explicar en alguna medida el porqué de este hecho. Lo cierto es que en la plataforma que nos ocupa se menciona este aspecto sucintamente por parte de las autoridades comunitarias, pero al menos bajo mi óptica, no se concreta nítidamente la manera de llevarlo a la práctica y esta es quizás la crítica más evidente.

IV. Hacia un modelo de compliance institucional para la prevención (¿uniforme?) del riesgo transnacional digital en la Unión Europea

A partir del análisis previo procede adentrarse ahora en los elementos de compliance institucional presentes en las diferentes herramientas jurídicas y extrajurídicas con las que cuenta hasta la fecha la Unión Europea para la prevención del riesgo transnacional (incluida su versión digital).

Para una mejor comprensión de cuanto se expone a continuación procede acotar siquiera sucintamente el concepto de riesgo transnacional digital sin perjuicio de cuanto ya se ha ido avanzando al respecto en las páginas precedentes. La coincidencia de estos tres elementos en este concepto responde a la necesidad de delimitar una realidad que sin apellidos podríamos considerar infinita. Si comenzamos por el primer elemento lo cierto es que en relación con el acervo comunitario puede generar la misma sensación que tenemos cuando se nos presenta en casa una visita inesperada. Las referencias hacia el concepto de riesgo no resultan precisamente abundantes en el derecho comunitario (salvo en alguna que otra regulación sectorial) precisamente por la dificultad conceptual que representa. No en vano se trata de un concepto interdisciplinar.

Sin embargo, la evolución del Derecho digital en la Unión Europea ha impulsado su incorporación en cada vez más textos normativos desde una perspectiva basada en el fenómeno anglosajón del *risk management* o la gestión de riesgos[26]. Al menos hasta el momento en ninguno de los textos legales que ha ido aprobando y proponiendo la Unión se especifica con claridad qué debe entenderse por "riesgo". Sin embargo, si acudimos a las fuentes de *softlaw* encontramos que el estándar ISO 37301:2021 sobre sistemas de

26. En este sentido discurren, por ejemplo, las nuevas directivas propuestas en materia de ciberseguridad, resiliencia y protección frente a ciberataques de la Unión Europea que se analizarán en seguida.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

gestión de compliance (requisitos con orientación para su uso) define el riesgo como el "efecto de la incertidumbre sobre los objetivos"[27]. Siguiendo esta definición la cuestión espacial me aboca a emplear el adjetivo transnacional para acotar este efecto a este espacio geográfico concreto (con todas sus connotaciones en el panorama comunitario) en contraposición, por ejemplo, a otros efectos que pudiera tener la incertidumbre en cualquier otro escenario. De la misma manera el adjetivo digital. Así, en definitiva, bajo la óptica que aquí se propone se encontrarían comprendidos en el concepto de riesgo transnacional digital todos aquellos efectos de la incertidumbre en los que concurra el elemento digital y que pudieran manifestarse más allá de las fronteras de cada Estado miembro. Sin ánimo de ahondar más en esta cuestión terminológica por el momento y sin obviar su interés académico tomaré como válida esta delimitación del concepto tan brevemente esbozada únicamente a los efectos de cuanto se pretende con este apartado.

Partiendo entonces de esta definición procede ahora realizar la aproximación hacia el impulso del compliance institucional previsto por la reciente regulación de la Unión Europea en materia de Derecho digital y prevención de ciberamenazas. Por cuestiones de espacio me centraré en el paquete formado por las siguientes cuatro normas comunitarias: (1) El Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 20 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. o 526/2013 («Reglamento sobre la Ciberseguridad»)[28]. (2) La propuesta de Reglamento de Ciberresiliencia de la Comisión Europea de 15 de septiembre de 2022[29]. (3) La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (en adelante, Directiva SRI 1)[30]. (4) La Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a

27. La propia norma ISO 37301:2021 aclara sobre la base de este concepto cuatro elementos que nos permiten delimitar su alcance. En ese sentido se indica que un efecto es "una desviación de lo esperado ya sea positiva o negativa". La incertidumbre es "el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o su probabilidad". Seguidamente se indica que "con frecuencia el riesgo se caracteriza por referencia a eventos potenciales (como se define en la Guía ISO 73) y consecuencias (como se define en la Guía ISO 73), o a una combinación de estos". Por último, se añade que "con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluidos los cambios de las circunstancias) y la "probabilidad" (como se define en la Guía ISO 73) asociada de que ocurra".

28. Texto completo del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 20 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. o 526/2013 («Reglamento sobre la Ciberseguridad») disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881 Fecha de última consulta: 29 de septiembre de 2023.

29. Versión en castellano disponible en: https://data.consilium.europa.eu/doc/document/ST-12429-2022-INIT/es/pdf Fecha de última consulta: 29 de septiembre de 2023.

30. Texto completo de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (en adelante, Directiva SRI 2)[31].

Comenzando por el Reglamento 2019/881 lo primero que debo advertir es que establece una serie de competencias, obligaciones y facultades en materia de ciberseguridad y prevención de riesgos digitales para la ENISA (Agencia de la Unión Europea para la ciberseguridad)[32] con una doble finalidad. La primera es garantizar un estándar óptimo de ciberseguridad y ciberresiliencia en el conjunto de la Unión Europea y, la segunda, proteger el mercado interior. Se establece así la existencia de un órgano autónomo (institución pública) con competencias propias al que la Unión Europea le confía la máxima autoridad en esta materia.

Como primer aspecto relevante el Reglamento define el concepto de incidente (artículo 2.6) por remisión a la Directiva SRI 1 que se comentará a continuación (artículo 4.7) como "todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información". Podríamos analizar las semejanzas entre este concepto y el concepto de riesgo referido en la norma ISO 37307:2021 y citado anteriormente si no fuera porque la misma Directiva SRI 1 incorpora en su artículo 4.9 su propio concepto de riesgo y lo define como "toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información". De nuevo la posibilidad de identificar el riesgo en términos razonables es lo que nos permite diferenciarlo de otras categorías jurídicas como el incidente. Como es sabido la Directiva SRI 1 fue derogada en 2022 por la Directiva SRI 2 en la que, a propósito de los conceptos de riesgo e incidente sorprenden algunas diferencias notables en relación con la Directiva SRI 1[33]. En mi opinión estas diferencias nos dan buena muestra de la evolución digital sufrida en la Unión Europea durante esos seis años y de cómo el dato pasa a ubicarse ahora en el centro de la regulación de la prevención de incidentes y riesgos relacionados con la ciberseguridad. Este aspecto ha propiciado el refuerzo de ENISA cuyas funciones en materia de compliance y control interno representan un claro avance institucional hacia la prevención uniforme.

redes y sistemas de información en la Unión (Directiva SRI 1) disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148 Fecha de última consulta: 29 de septiembre de 2023.

31. Texto completo de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022L2555&qid=1689114036076 Fecha de última consulta: 29 de septiembre de 2023.

32. Sitio web oficial ENISA: https://www.enisa.europa.eu/about-enisa/about/es

33. En la Directiva SRI 2 se define el incidente como: "todo hecho que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por sistemas de redes y de información o accesibles a través de ellos". En la misma Directiva SRI 2 se define el riesgo como: "la posible pérdida o perturbación causada por un incidente expresada como una combinación de la magnitud de tal pérdida o perturbación y la probabilidad de que se produzca tal incidente".

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

El Reglamento se centra en la labor de ENISA y le atribuye competencias concretas en relación con los incidentes y su gestión. De manera particular en dos sentidos: la detección de incidentes y la asistencia y apoyo a los Estados miembros para su gestión. Así su función de vigilancia y control se basa fundamentalmente en un modelo de cooperación *ad intra* y se combina con una acción exterior (acaso más discreta) de manera muy similar a los sistemas de gestión de compliance corporativos referidos en la norma ISO 37307:2021. De manera complementaria a la labor de la ENISA el Reglamento refuerza el papel de la red CSIRT[34] en la Unión Europea. Conviene recordar que esta red tiene como finalidad principal el establecimiento de equipos nacionales en cada Estado miembro para responder frente a posibles incidentes y analizar los riesgos que se produzcan en el espacio virtual. En segunda instancia, la red CSIRT alerta sobre estos riesgos facilitando su detección temprana en otros Estados miembros (componente transnacional) y aportando soluciones para mitigar sus efectos desde su propia experiencia[35]. En este sentido nos encontramos ante otro elemento institucional de compliance que también sale reforzado tras la aprobación del Reglamento comunitario.

Por lo que respecta a la Directiva SRI 1 de 2016, su análisis nos puede resultar interesante como predecesora de la Directiva SRI 2 que la deroga y rige desde 2022. Ya se ha referido que se orientaba a la consecución de un determinado nivel de seguridad en las redes y sistemas de información de la Unión y en este sentido incorpora elementos interesantes como el concepto de incidente, el concepto de riesgo, o la creación de la red CSIRT (nacional y supranacional). El establecimiento de obligaciones de cooperación nacional e internacional en esta Directiva resulta clave para comprender la estructura de compliance y ciberseguridad institucional que se persigue en ella. En pocas palabras, la Directiva articula una suerte de colaboración entre las autoridades comunitarias, ENISA, y la red CSIRT orientada a la detección temprana de cualquier efecto perturbador significativo en el mercado interior. De esta manera la prevención del riesgo transnacional digital encuentra un importante aliado en la acción encomendada a los equipos de respuesta a incidentes de seguridad cuya labor, como refería anteriormente, se ha visto reforzada con el Reglamento (UE) 2019/881. Con esta estrategia la Unión afronta la prevención del riesgo transnacional digital desde una doble perspectiva. En primer lugar, fomentando la creación de nuevos organismos e instituciones con perfiles profesionales especializados en el campo de la informática, la ciberseguridad y la gestión de información sensible. Y, en segundo lugar, dotando a estos órganos de competencias en materia de vigilancia, supervisión, reporte y control interno del riesgo asociado a los incidentes de seguridad en la red. Esta estrategia representa un avance significativo en términos de compliance y seguridad institucional en un campo, el del Derecho digital, donde esta demanda era una de las asignaturas pendientes del legislador.

34. De las siglas en inglés *Computer Security Incident Response Teams*. La regulación de esta red se encuentra en el artículo 1.2.c) y en el artículo 9 de la Directiva SRI 1.

35. En el caso de España, en el año 2022 existían más de una docena de equipos integrados en la red CSIRT dependientes directamente del Ministerio de Transformación Digital.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

Abordando ya por el último el caso de la Directiva SRI 2 de 2022 se observa que esta tendencia continúa al alza. En primer lugar, la Directiva reformula los conceptos clásicos de riesgo e incidente presentes en la Directiva SRI 1 a partir de un nuevo elemento clave: el dato. En este sentido se habla por primera vez de autenticidad, integridad y confidencialidad de los datos para referirse al concepto de incidente (y cuasiincidente) cuando éstas se vean comprometidas. Y para referirse también al concepto de riesgo al hacerlo depender de la existencia de un incidente. La Directiva hereda la regulación de la red CSIRT que ya introdujo la SRI 1 y, sobre esta base, añade una serie de obligaciones y competencias en materia de prevención de riesgos (artículo 11) muy centradas en la cooperación transnacional de los Estados miembros. En otras palabras, en la aspiración de alcanzar una cierta prevención uniforme.

En este camino hacia la creación de nuevos organismos e instituciones para dotarlos de competencias en materia de vigilancia, control y gestión de riesgos, la Directiva SRI 2 crea en su artículo 16 la red europea de organizaciones de enlace para las crisis de ciberseguridad, en adelante EU-CyCLONe. Sorprende que ni la Directiva SRI 1, ni la SRI 2, ni el Reglamento (UE) 2019/881 hayan definido qué debe entenderse por crisis de ciberseguridad. La aproximación teórica más cercana a este concepto la encontramos en la Recomendación (UE) 2017/1584 de la Comisión de 13 de septiembre de 2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala[36]. Sin embargo, la Directiva SRI 2 establece la obligación de que cada Estado miembro designe a una autoridad nacional competente para gestionar estas crisis (artículo 9).

Para finalizar, me referiré brevemente al capítulo IV de la Directiva SRI 2 sobre medidas para la gestión de los riesgos de ciberseguridad y obligaciones de notificación. Este capítulo establece todo un paquete de medidas que bajo mi punto de vista resultan perfectamente aplicables a la gobernanza *ad intra* del riesgo transnacional digital en la Unión. En él concurren entre otros elementos interesantes de compliance institucional, la obligación de monitorear, reportar y notificar cualquier tipo de riesgo en el sentido indicado por la Directiva SRI 2, la evaluación coordinada y conjunta de esos riesgos, el recurso hacia la certificación de esquemas de ciberseguridad, o la normalización. El hecho de que la Unión haya decidido por fin incorporar una regulación de estas características responde a mi modo de ver a dos factores fundamentales. El primero, la utilidad práctica que incorporan este tipo de medidas de cumplimiento normativo, prevención y seguridad. En su mayoría, presentes ya en el derecho interno de los Estados miembros a propósito de la responsabilidad legal de las personas jurídicas y de otros aspectos jurídicos afines a ella. Este hecho facilita, en este momento, su regulación comunitaria con una terminología y unos procedimientos ciertamente similares. Y, el segundo, la envergadura del desafío digital al que nos enfrentamos cuando se trata de abordar este tipo

36. Recomendación (UE) 2017/1584 de la Comisión de 13 de septiembre de 2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017H1584 Fecha de última consulta: 30 de septiembre de 2023.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

de riesgos más allá de las fronteras nacionales. La conjunción de ambos factores hace de la Directiva SRI 2 un instrumento jurídico necesario, pero al mismo tiempo, al menos a mi juicio, insuficiente.

V. Conclusiones

Del análisis realizado a lo largo de estas páginas se extrae como primera idea fundamental que la realidad digital de nuestros días ha superado cualquier expectativa del legislador nacional y comunitario. La aparición y propagación del riesgo digital a lo largo y ancho de la Unión Europea constituye hoy un desafío de primer orden que coloca a la ciencia jurídica en una posición realmente comprometida. En primer lugar, porque se demandan respuestas cada vez más rápidas y eficaces para tratar de regular jurídicamente una realidad cada día más cambiante y volátil; aspecto que de por sí resulta difícil de conciliar con los procesos legislativos comunitarios que a menudo precisan de consensos y tramitaciones realmente lentas. Y, segundo lugar, porque la complejidad de la materia objeto de regulación está tecnificando el Derecho comunitario hasta extremos inimaginables. Incorporando, con cada vez más frecuencia, conceptos y razonamientos más propios de otras disciplinas como la ingeniería informática, la gestión de riesgos, la economía, o la inteligencia artificial. Este hecho dificulta la aplicación y la interpretación de este nuevo Derecho comunitario por parte de todos los operadores jurídicos e introduce la posibilidad de que esta dificultad termine frustrando la finalidad de estas normas.

En segundo lugar, podemos concluir que la Unión Europea es consciente de esta realidad y ha apostado claramente por evolucionar su Derecho en este sentido. Prueba de ello son los diferentes Reglamentos y Directivas comunitarios aprobados en los últimos años en materias tan novedosas como la ciberseguridad, los criptoactivos, o la protección del denunciante de infracciones del Derecho de la Unión. Sin embargo, la magnitud del desafío global al que nos enfrentamos no se conforma con una respuesta jurídica. Si no que, bajo mi punto de vista, precisa también de una reacción comunitaria que, sin apartarse del poder legislativo, incorpore jurídica o extra jurídicamente elementos eficaces e idóneos para la gobernanza y la gestión de estos riesgos. Es aquí donde la traslación de mecanismos de compliance (diseñados inicialmente para el sector privado) hacia el ámbito de las instituciones públicas adquiere un nuevo sentido.

En tercer lugar, el riesgo transnacional digital se caracteriza por representar una amenaza global que en mi opinión sólo se podrá combatir con éxito desde una actuación que ya no puede ser únicamente conjunta o cooperativa, sino que además debe ser necesariamente uniforme. Esta exigencia choca de manera frontal con las características propias de cada Estado miembro y con la indiscutible disparidad entre los recursos y riesgos que existen en cada territorio. No quiero decir con ello que los Estados miembros deban afrontar este reto desde una misma posición de partida, pero sí que al menos se avance de manera más significativa hacia la corrección de las posibles desigualdades entre ellos en aras de una mayor uniformidad preventiva tal y como ya se

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

hace, por cierto, en otros ámbitos comunitarios donde podemos identificar fácilmente las bondades de los mecanismos de cohesión.

En cuarto lugar y en relación con lo anterior, en honor a la verdad debe reconocerse tras todo lo expuesto que existen importantes avances en materia de cooperación para la prevención del riesgo transnacional en la Unión y que si por algo se caracteriza este nuevo rumbo es por el compromiso de las autoridades comunitarias con el diseño de una respuesta común más transversal y acorde con la realidad que vivimos. Sin embargo, hablar en este momento de prevención uniforme me resulta un ejercicio un tanto forzado. En primer lugar, porque los niveles de prevención alcanzados internamente en cada Estado miembro siguen estando condicionados por la mayor o menor eficacia de su Derecho interno en la lucha frente a este tipo de riesgos. En segundo lugar, porque bajo mi punto de vista la corrección de esta disparidad no puede alcanzarse exclusivamente desde el Derecho, sino que precisa de otros cambios culturales, sociales y económicos en los que ya se está trabajando tanto a nivel interno como desde la Unión Europea. Y, en tercer y último lugar, porque los recursos económicos, técnicos y materiales de los que se dispone en relación con este desafío son limitados y, a la luz de los hechos, podríamos decir que insuficientes.

En quinto y último lugar, la prevención del riesgo transnacional digital (y no digital) no puede afrontarse desde un posicionamiento exclusivamente jurídico. La complejidad de este reto demanda la aplicación de herramientas interdisciplinares y la implicación de las autoridades comunitarias, pero también de las nacionales en cada Estado miembro. En este contexto el compliance institucional entra en escena como un recurso innovador e interesante que puede resultar extraordinariamente útil en ambos planos cuya finalidad no es otra que la de completar esa laguna allá donde el Derecho no puede llegar aportando soluciones desde la gestión y la gobernanza del riesgo que pasan, necesariamente, por tres ejes principales. Un cambio en la cultura y en la manera tradicional de entender la prevención (que quizás fuera válida en otros momentos o contextos históricos de la Unión pero que a todas luces ha quedado obsoleta frente a la realidad actual), la implicación del legislador nacional y comunitario pero también del resto de los poderes públicos para la mejor aplicación posible de sus mecanismos e instrumentos; y, por último, la colaboración eficaz entre todas las partes interesadas (agentes sociales, sector privado, fuerzas y cuerpos de seguridad, autoridades supranacionales, poderes públicos, *policy makers* y sociedad civil) en la implementación y el seguimiento de todos los recursos a su alcance.

Bibliografía

Agencia Europea para la ciberseguridad (2023). Reporte anual en materia de ciberseguridad. Recuperado el 7 de septiembre de 2023 de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

BECK, U. (1992). *Risk Society: Towards a New Modernity*. (London: Sage).

BECK, U. (2009). "Critical theory of world risk society: a cosmopolitan vision". *Constellations*, vol. 16, n. º 1.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

BELMONTE, P. (2016). "El nuevo estándar global de intercambio automático de información sobre cuentas financieras de la OCDE ("*CRS, Common Reporting Standard*"): estructura y funcionamiento. Aplicación del mismo en la Unión Europea: Directiva 2014/107/UE del Consejo de 9 de diciembre de 2014". *Crónica tributaria*, Vol. 159 (103-130).

Comisión Europea (2017). Report Study. *European Data Market study measuring the size and trends of the EU data economy*. Recuperado el 7 de septiembre de 2023 de https://digital-strategy.ec.europa.eu/en/library/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy

CONSEJO DE EUROPA (2014). Libro blanco sobre el crimen organizado transnacional.

Directiva (UE) 2018/822 del Consejo, de 25 de mayo del 2018, que modifica la Directiva 2011/16/UE por lo que se refiere al intercambio automático y obligatorio de información en el ámbito de la fiscalidad en relación con los mecanismos transfronterizos sujetos a comunicación de información. Recuperado el 16 de septiembre de 2023 de https://www.boe.es/doue/2018/139/L00001-00013.pdf

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148.

Directiva 2008/99/CE del Parlamento Europeo y del Consejo, de 19 de noviembre de 2008, sobre protección del medio ambiente mediante el Derecho penal.

ERICSON, R. V., y HAGGERTY, K. D. (1997). Policing the risk society. (London: Clarendon Press).

EU4Digital (2021). EU Digital Strategy. Recuperado el 13 de septiembre de 2023 de https://eufordigital.eu/discover-eu/eu-digital-single-market/

HAUFLER, A., MARDAN, M., y SCHINDLER, D. (2018). "Double tax discrimination to attract FDI and fight profit shifting: The role of CFC rules". *Journal of International Economics*, Vol. 114 (25-43).

INTERPOL (2023). La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad. Recuperado el 11 de septiembre de 2023 de https://www.interpol.int/es/Delitos/Ciberdelincuencia

ISO (2021). Norma ISO 37301:2021 sobre Sistemas de gestión del compliance. Requisitos con orientación para su uso.

KEUSCHNIGG, C., y DEVEREUX, M. (2013). "The arm's length principle and distortions to multinational firm organization". *Journal of International Economics*, Vol. 89, n. º 2 (432-440).

MCBRIDE, N., y BAGSHAW, R. (2008). *Tort law*. (London: Pearson Education).

NIETO, A. y CALATAYUD, M. (2015). *Public Compliance: Prevención de la corrupción en administraciones públicas y partidos políticos* (Vol. 13). Ediciones de la Universidad de Castilla La Mancha.

NACIONES UNIDAS (2004). Convención de Naciones Unidas contra la Corrupción. Recuperado el 21 de septiembre de 2023 de https://www.unodc.org/pdf/corruption/publications_unodc_convention-s.pdf

O'MALLEY, P. (2002). Risk societies and the government of crime. In *Dangerous offenders* (pp. 27-44). Routledge.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09

OCDE (1997). Convención para Combatir el Cohecho de Servidores Públicos Extranjeros en Transacciones Comerciales Internacionales de la OCDE. Recuperado el 23 de septiembre de 2023 de https://www.oecd.org/daf/anti-bribery/convcombatbribery_spanish.pdf

OCDE (2015). *Plan de Acción BEPS*. Recuperado el 17 de septiembre de 2023 de https://read.oecd-ilibrary.org/taxation/plan-de-accion-contra-la-erosion-de-la-base-imponible-y-el-traslado-de-beneficios_9789264207813-es#page2

OCDE (2019). *International Compliance Assurance Programme* (2019). Recuperado el 17 de septiembre de 2023 de http://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/international-compliance-assurance-programme-pilot-handbook-2.0.pdf

PUYOL, J. (2018). El Modelo de Evaluación de Riesgos en la Protección de Datos EIPD/PIA's. (Valencia: Tirant lo Blanch).

QUINTANA, T. y CASARES, A. (2014). *Evaluación de Impacto Ambiental y Evaluación Estratégica*. (Valencia: Tirant lo Blanch).

Recomendación (UE) 2017/1584 de la Comisión de 13 de septiembre de 2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala.

Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 20 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. o 526/2013 («Reglamento sobre la Ciberseguridad»).

Reglamento 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

SCHWAB, K. (2017). *The fourth industrial revolution*. (New York: Crown Business Publishing).

SIMON, J. (1987). The Emergence of a Risk Society-Insurance, Law, and the State. *Socialist Review*, (95), 60-89.

VÉRGEZ, J. (2016). "Alcance de la acción 2 del plan BEPS: recomendaciones relativas al diseño de las medidas nacionales y los tratados fiscales para neutralizar los efectos de los acuerdos de desajuste híbrido". *Fórum fiscal: la revista tributaria de Álava, Bizkaia y Gipuzkoa*, n. º 217 (75-88).

WITTENDORFF, J. (2010). *Transfer pricing and the arm's length principle in international tax law* (Vol. 35). Netherlands: Kluwer Law International BV.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 181-209
ISSN 2444-8478 • http://doi.org/10.12795/IESTSCIENTIA.2023.i02.09