Revista Galega de Administración Pública, EGAP
Núm. 65_xaneiro-xuño 2023 | pp. 319-337
Santiago de Compostela, 2023
https://doi.org/10.36402/regap.v1i65.5094

ISSN-e: 1132-8371 | ISSN: 1132-8371
Recibido: 04/05/2023 | Aceptado: 01/06/2023

A colaboración entre sector público e privado no sistema de seguridade cibernética: reflexións a partir da estratexia europea e italiana

La colaboración entre sector público y privado en el sistema de seguridad cibernética: reflexiones a partir de la estrategia europea e italiana

Public-private collaboration in the cybersecurity system: reflections from the European and Italian strategy

LUIGI PREVITI
Assistant Professor in Administrative Law
University of Palermo

https://orcid.org/0000-0001-7701-1718

luigi.previti@unipa.it

Resumo: Este estudo aspira a analizar o papel que representa a colaboración entre sector público e privado para alcanzar os obxectivos, nacionais e supranacionais, de tutela da seguridade cibernética, co fin de demostrar como o mellor seguro posible contra os perigos do ciberespazo está representado pola valorización da contribución cognoscitiva e experiencial dos operadores económicos do sector, por un lado, e da contribución dos usuarios da rede, por outro. Mencionadas as recomendacións normativas formuladas ao respecto a nivel europeo, a investigación céntrase na recente estratexia italiana, que parece atribuír, en adhesión ao novo achegamento "*whole of society*", un papel aínda máis activo aos diferentes compoñentes do tecido económico e social do país. Ao final da dita valoración, formúlanse algunhas consideracións conclusivas con respecto ás formas de colaboración entre o sector público e o privado que sería oportuno promover, no noso ordenamento, para aproveitar ao máximo os beneficios que proceden da implementación dunha *governance* compartida en materia de seguridade informática.

Palabras clave: Seguridade cibernética, risco cibernético, xestión compartida, colaboración pública e privada.

Resumen: Este estudio aspira a analizar el papel que juega la colaboración entre sector público y privado para alcanzar los objetivos, nacionales y supranacionales, de tutela de la seguridad cibernética, con el fin de demostrar cómo el mejor seguro posible contra los peligros del ciberespacio está representado por la valorización de la contribución cognoscitiva y experiencial de los operadores económicos del sector, por un lado, y de la contribución de los usuarios de la red, por otro. Mencionadas las recomendaciones normativas formuladas al respecto a nivel europeo, la investigación se centra en la reciente estrategia italiana, que parece atribuir, en adhesión al nuevo acercamiento "***whole of society***", un papel aún más activo a los diferentes componentes del tejido económico y social del país. Al final de dicha valoración, se plantean algunas consideraciones conclusivas con respecto a las formas de colaboración entre el sector público y el privado que sería oportuno promover, en nuestro ordenamiento, para poder aprovechar al máximo los beneficios que proceden de la implementación de una *governance* compartida en materia de seguridad informática.
Palabras clave: Seguridad cibernética, riesgo cibernético, gestión compartida, colaboración pública y privada.

Abstract: The work aims at analysing the role of public-private collaboration in achieving national and supranational cybersecurity objectives, in order to explain that the best possible insurance against the cyberspace threats is represented by the enhancement of knowledge and experience of the economic operators in the ICT sector, on the one hand, and of the contribution of network users, on the other. After having mentioned the normative indications formulated in this regard at European level, the survey focuses on the recent Italian strategy, which seems to assign, in compliance with the new approach "whole of society", a more active role for the various components of society. At the end of the analysis, some concluding remarks are made about the forms of public-private partnership that should be promoted, within our legal system, to fully exploit the benefits of implementing a shared ICT security governance.
Key words: Cyber security, cyber risk, shared management, public and private partnership.

1 El sistema multinivel de protección de la seguridad pública en el ciberespacio. Delimitación del área de investigación

Entre las cuestiones problemáticas conectadas con el avance del proceso de transición digital en marcha en los estados miembros en la Unión, la tutela de la seguridad cibernética, o mejor dicho, de la seguridad pública en el espacio cibernético, ocupa por supuesto un lugar de máxima importancia.

Como es bien sabido, a pesar de que el tema en cuestión se conozca y discuta desde hace mucho tiempo[1], los primeros intentos de responder de modo uniforme y eficaz

[1] Véanse, entre otras, la comunicación de la Comisión Europea de 6 de junio de 2001, ***Seguridad de las redes y seguridad de la información: propuesta de un enfoque estratégico europeo***, COM (2001) 298; la comunicación de la Comisión Europea de 26 de septiembre de 2003, ***El papel de la administración electrónica para el futuro de Europa***, COM (2003) 567.

a nivel internacional son recientes, concretamente en el ámbito de las iniciativas dedicadas a la realización del *Digital Single Market*[2].

Con estas actuaciones la Unión ha querido consolidar, en particular, una visión propia estratégica del ciberespacio, como lugar virtual abierto y seguro para el desarrollo de las actividades económicas y sociales de los ciudadanos europeos, basada en la protección y en la fiabilidad de los datos, de las redes y de los productos informáticos presentes en su interior. Un ámbito de fronteras indefinidas –«el espacio público más grande que la humanidad haya conocido»[3]– y de potencialidades aún inexploradas[4], al que se quiere dotar de un nivel elevado de resiliencia a través de la aplicación de políticas y medidas homogéneas, así como a través de un eficiente mecanismo de información de accidentes y de ataques más relevantes[5].

Las directivas generales dirigidas a desarrollar metodologías compartidas de prevención y de gestión del ciber-riesgo han determinado, en el ordenamiento italiano, la introducción de un nuevo sistema organizativo de defensa de los intereses de la nación, que tiene en el Perímetro de Seguridad Cibernética (en adelante, PSNC)[6] y en la Agencia para la Ciberseguridad Nacional (en adelante, ACN)[7] los puntos de referencia esenciales[8].

La arquitectura institucional así definida se caracteriza, en la actualidad, por la coordinación de las acciones estratégicas y por la centralización de las competencias administrativas; un sistema que, debido a las peculiaridades que lo connotan, resulta

[2] En esta materia, cfr. la Directiva UE 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, Directiva NIS 1, modificada, por último, de la Directiva UE 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, Directiva NIS 2; las comunicaciones conjuntas de la Comisión Europea y del alto representante de la Unión, respectivamente, de 7 de febrero de 2013, *Estrategia de ciberseguridad de la UE: un ciberespacio abierto y seguro*, JOIN (2013) 1 final, de 13 de septiembre de 2017, *Resiliencia, disuasión y defensa: hacia una ciberseguridad fuerte en la UE*, JOIN (2017) 450 final, y de 16 de diciembre de 2020, *La estrategia de ciberseguridad de la UE para la década digital*, JOIN (2020) 18 final; el Reglamento UE 2019/881 de 17 de abril de 2019, *Cybersecurity Act.*

[3] En estos términos, RODOTÀ, S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014, p. 3.

[4] Sobre la influencia ejercitada por la difusión del ciberespacio y de las nuevas tecnologías sobre la relectura del concepto de soberanía estatal y sobre la transformación de las funciones tradicionales de los Estados, véanse, por último, CASINI, L., *Lo Stato nell'era di Google. Frontiere e sfide globali*, Mondadori, Milano, 2020; TORCHIA, L., *Lo Stato digitale. Una introduzione*, Il Mulino, Bologna, 2023.

[5] Sobre la visión estratégica de la Unión relativa al espacio cibernético, véanse CENCETTI, C., *Cybersecurity: Unione europea e Italia. Prospettive a confronto*, Nuova Cultura, Roma, 2014, pp. 21 y ss.; CONTALDO, A. y MULA, D. (dirs.), *Cybersecurity Law*, Pacini, Pisa, 2020, pp. 57 y ss.; KOHLER, C., "The EU Cybersecurity Act and European standard: an introduction to the role of European standardization", *International Cybersecurity Law Review*, n. 1, 2020, pp. 7 y ss.; BASSINI M., "Cybersecurity", Paracampo, M.T. (dir.), *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Giappichelli, Torino, 2021, pp. 319 y ss.; BARONI, M., "Intelligenza artificiale e cybersicurezza in una prospettiva costituzionale", Cerrina Feroni, G., Fontana, C. y Raffiotta, E.C. (dirs.), *AI Anthology*, Il Mulino, Bologna, 2022, pp. 373 y ss.

[6] Instituido por el DL de 21 de septiembre de 2019, n. 105, conversión con modificación de la Ley de 18 de noviembre de 2019, n. 133.

[7] Instituida por el DL de 14 de junio de 2021, n. 82, conversión con modificación de la Ley de 4 de agosto de 2021, n. 109.

[8] Con respecto a la fisionomía y a las características de la arquitectura italiana en materia de seguridad cibernética, véanse, *ex multis*, CAROTTI, B., "Sicurezza cibernetica e Stato nazione", *Giornale di Diritto Amministrativo*, n. 5, 2020, pp. 629 y ss.; MELE, S., "Il Perimetro di sicurezza nazionale cibernetica e il nuovo «golden power»", Cassano, G. y Previti, S. (dirs.), *Il diritto di internet nell'era digitale*, Giuffrè, Milano, 2020, pp. 186 y ss.; ATERNO, S., *Sicurezza informatica. Aspetti giuridici e tecnici*, Pacini, Pisa, 2022, pp. 234 y ss.; RENZI, A., "La sicurezza cibernetica: lo stato dell'arte", *Giornale di Diritto Amministrativo*, n. 4, 2021, pp. 538 y ss.; SERINI, F., "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021", *Federalismi.it*, n. 12, 2022, pp. 241 y ss.; FORGIONE, I., "Il ruolo strategico dell'Agenzia nazionale per la cybersicurezza nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna", *Diritto amministrativo*, n. 4, 2022, pp. 1113 y ss.

en esencia orientado a mitigar el impacto de las amenazas informáticas en las infraestructuras y en los servicios considerados de mayor importancia para la vida del país[9]. Infraestructuras y servicios que constituyen un verdadero "fortín" dotado de bastiones por su naturaleza móviles, concretamente en razón de la evolución tecnológica, a cuya defensa no están encargados "incansables soldados con escopetas y cañones", sino ingenieros, expertos en *compliance* y máquinas inteligentes[10].

Esta reflexión aspira a poner de manifiesto la importante contribución realizada por el sector empresarial privado para el conseguimiento de los objetivos, nacionales e internacionales[11], de tutela de la seguridad cibernética. Y eso a fin de demostrar como la mejor garantía posible contra los peligros del ciberespacio está representada por el reconocimiento y por la valorización de la contribución cognoscitiva y experiencial de los operadores económicos del sector, por un lado, y del papel colaborativo de los ciudadanos usuarios, por otro.

En los siguientes párrafos se examinarán, por tanto, las principales modalidades con que la valiosa cooperación entre autoridades institucionales y sujetos privados puede cumplirse concretamente, teniendo en consideración, en un primer momento, la categoría de las empresas que operan en el sector de las Tecnologías de la Información y Comunicación (TIC) y de la ciberseguridad, para centrarse después en el papel de cada uno de los usuarios. El análisis propuesto permitirá entender la importancia de la reciente estrategia italiana adoptada en mayo de 2022[12], orientada a atribuir un papel auténticamente activo a los distintos componentes del complejo económico y social del país, de acuerdo con el acercamiento "*whole of society*" que inspira los numerosos actos de orientación de la Unión.

Al final de la investigación, se plantearán unas consideraciones conclusivas con respecto a las formas de partenariado público-privado, que se cree oportuno promover, en nuestro ordenamiento, para poder aprovechar completamente las significativas ventajas que se derivan de la implementación de una *governance* plenamente participante en materia de seguridad informática.

2 Asimetrías informativas, compartición del riesgo y *governance* compartida

La instauración de un sincero y constructivo diálogo entre público y privado en el sector de la ciberseguridad no constituye en absoluto un objetivo de fácil realización.

---

[9] Como señala PARONA, L., "L'istituzione dell'Agenzia per la cybersicurezza nazionale", *Giornale di Diritto Amministrativo*, n. 6, 2021, pp. 709 y ss., spec. 718.

[10] Según la sugestiva y eficaz imagen de URSI, R., "La difesa: tradizione e innovazione", *Diritto Costituzionale*, n. 1, 2022, p. 18.

[11] Sobre la imposibilidad de afrontar y gobernar problemas de orden económico y social que traspasan los límites del Estado, véase, para todos, CASSESE, S., *La crisi dello Stato*, Laterza, Roma-Bari, 2002; CASSESE, S., *Lo spazio giuridico globale*, Laterza, Roma-Bari, 2003.

[12] Cfr. la estrategia de ciberseguridad 2022-2026 y el respectivo plan de implementación de mayo de 2022, localizables en *www.acn.gov.it*, a través de los cuales se adopta un consistente programa de medidas y de inversiones dirigidas a realizar los tres fundamentales objetivos de "desarrollo", "protección" y "respuesta" (se volverá mejor a los puntos 2 y 3).

Las principales razones a partir de una general situación de mutua desconfianza entre los diferentes portadores de interés son ya bien conocidas: por una parte, las autoridades administrativas manifiestan una cierta resistencia a compartir hacia el exterior los datos y las informaciones que atañen a su propia seguridad, temiendo comprometer, de tal forma, su propia imagen institucional; por otra, los operadores económicos, recibiendo solo de vez en cuando adecuados incentivos para la colaboración prestada, prefieren no confiar informaciones reservadas o personales, que los expondrían al riesgo de sufrir acciones legales o de perjudicar su propia reputación en el mercado[13].

Se trata de actitudes que en el pasado han justificado y, en parte aún justifican, el recurso a modelos organizativos y reguladores del tipo *top-down*, que cuentan con la previsión de específicas obligaciones de notificación y de conducta, oportunamente sancionadas a cuenta de las empresas interesadas, en el intento de inducir a estos sujetos a desarrollar comportamientos virtuosos y a prestar las debidas precauciones frente a las numerosas amenazas del ciberespacio[14].

Con el objetivo de superar dichos puntos críticos, las instituciones de la Unión han fomentado, en los últimos años, a través de institutos y modalidades diferentes, una implicación más efectiva de las empresas que ofrecen productos y servicios tecnológicos en el ámbito de los sistemas de seguridad cibernética elaborados por los estados miembros.

La estrategia supranacional, en primer lugar, pasa por fijar principios fundamentales, que se dirigen a los operadores del sector en cuanto coprotagonistas de la calidad del nivel de protección asegurado a las infraestructuras y a los *softwares* presentes en el mercado único.

En este sentido, los productores y los proveedores de las TIC se ven obligados, por un lado, a comercializar exclusivamente bienes y servicios que poseen, desde el momento del proyecto, determinados requisitos de seguridad contra el riesgo de accidentes y de ataques cibernéticos (principio de seguridad *by design*); por otro, los mismos sujetos tienen que asumir, para con los usuarios, un papel de interlocutores privilegiados durante el ciclo completo de vida de los productos, colaborando con el sector público en la gestión de la actividad de vigilancia (principio de responsabilidad tecnológica)[15].

[13] Entre otros, SALES, N.A., "Regulating Cyber-Security", ***Northwestern University Law Review,*** vol. 107, n. 4, 2013, pp. 1549-1550. El dato está confirmado también por el informe del Grupo de coordinación sobre la seguridad cibernética del Banco de Italia, *Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass*, agosto de 2018, localizable en ***www.bancaditalia.it***, donde se subraya que, no obstante el valor estratégico de la participación de las informaciones sobre las amenazas informáticas, las empresas que han sufrido ataques muchas veces son reacias en revelarlos temiendo secuelas reputacionales y están dispuestas a compartir sus propios datos solo en contextos que garantizan confidencialidad y reciprocidad.

[14] Como señalan KESAN, J.P. y HAYES, C.M., "Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals", *Michigan State Law Review*, 2014, pp. 1475 y ss.; BOSSONG, R. y WAGNER, B., "A Typology of Cybersecurity and Public-Private Partnerships in the Context of the European Union", *Crime, Law and Social Change*, n. 67, 2017, pp. 272-273, ellos afirman que «[…] *it is mistaken to assume a general positive impact for all participants of information-sharing exercises. Many actors apparently fear the reputational costs of, or possible liabilities deriving from, breaches of their cybersecurity more than desiring the rather diffuse benefits of strategic threat awareness*».

[15] Sobre el tema, véase TADDEO, M., "Is Cybersecurity a Public Good?", *Minds & Machines*, n. 29, 2019, pp. 351-352.

De ahí la previsión de una serie de desempeños peculiares, que son, entre otros: efectuar revisiones periódicas de funcionamiento, realizar las actualizaciones y revisiones necesarias de los *softwares*, eliminar con celeridad las vulnerabilidades informáticas reportadas y garantizar un correcto empleo de los datos personales de los usuarios. Se consigue, en definitiva, la introducción de específicas obligaciones de diligencia reforzada, más estrictas cuanto más elevados son los riesgos de manipulación de las aplicaciones y de los dispositivos tecnológicos proporcionados en el mercado[16].

El objetivo de construir una arquitectura multinivel eficiente en materia de seguridad cibernética se traduce, en segundo lugar, en la definición de modalidades más estructuradas y duraderas de cooperación entre sector público y sector privado, en condiciones de aprovechar de forma adecuada los conocimientos y las capacidades de análisis de este último, «*that rival those of the world's most sophisticated intelligence agencies, including in the notoriously difficult task of attack attribution*»[17].

Desde esta perspectiva es como se puede entender la institución de algunas sedes privilegiadas de conexión, de matriz europea, como por ejemplo: el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación sobre la Ciberseguridad, que quiere desarrollar los recursos y las competencias de la Unión y reducir su dependencia de terceros países, comprometiendo las energías de los centros nacionales de coordinación (en Italia, el ACN), del mundo de la industria y de la universidad[18]; la Unidad Conjunta para el Ciberespacio (*Joint Cyber Unit*), como plataforma destinada a promover el intercambio de informaciones, buenas prácticas y conocimientos, así como la cooperación entre fuerzas del orden público y de defensa, autoridades civiles y diplomáticas, y sector privado en caso de ataques severos o accidentes transfronterizos[19]; la red de los centros operativos de seguridad (SOC, *Security Operations Center*), como *network* destinado a garantizar una supervisión constante, extendida y en tiempo real de las intrusiones y de las anomalías informáticas en las redes y en los sistemas de diferentes portadores de interés, también a través de la implicación de las PMI de la Unión[20]. Gracias a esta red, en particular, se refuerzan las capacidades de detección, de análisis y de uso compartido de los datos relativos a los ataques *cyber* más peligrosos, permitiendo a las autoridades públicas y a sujetos privados señalar rápidamente amenazas potenciales y en marcha, antes de que estas causen daños irreparables a gran escala.

---

[16] De refuerzo de las obligaciones de diligencia exigibles por parte de los productores y de los proveedores de las nuevas tecnologías hablan, especialmente, la Comunicación conjunta de 13 de septiembre de 2017, ***Resiliencia, disuasión y defensa: hacia una ciberseguridad fuerte para la UE***, cit., pár. 2.2; la Comunicación conjunta de 16 de diciembre de 2020, ***La estrategia de ciberseguridad de la UE para la década digital***, cit., pár. 1.5.

[17] Así, SALES, N.A., "Privatizing Cybersecurity", ***UCLA Law Review,*** vol. 65, n. 3, 2018, p. 632.

[18] Cfr. la normativa UE 2021/887, de 20 de mayo de 2021, que encarga a las redes de los «Centros nacionales de coordinación» la tarea de apoyar al Centro Europeo de Competencia para la Ciberseguridad en la actividad de refuerzo de las capacidades, de los conocimientos y de la competitividad de la Unión en el sector (art. 6 del reglamento).

[19] Cfr. la Comunicación conjunta de 16 de diciembre de 2020, ***La estrategia de ciberseguridad de la UE para la década digital***, cit., pár. 2.1.

[20] Cfr. la Comunicación conjunta de 16 de diciembre de 2020, ***La estrategia de ciberseguridad de la UE para la década digital***, cit., pár. 1.2.

Se trata de organismos e instrumentos que demuestran la madura consciencia, por parte de las instituciones, de la necesidad de establecer una *governance* más participativa para abordar de la mejor manera posible los difíciles desafíos para la seguridad puestos en marcha por la difusión del ciberespacio. Y esto, teniendo en cuenta los importantes beneficios que se pueden obtener de la contribución del mundo empresarial, al menos, bajo una doble perspectiva.

En primer lugar, una interlocución constante entre actores públicos y operadores privados en materia de ciberseguridad fomentaría un intercambio rentable de conocimientos especializados y de soluciones operativas.

En el contexto examinado, de hecho, la creación de un sistema altamente centralizado y unilateral, en presencia de evidentes asimetrías informativas, está destinada a resultar ineficaz: por un lado, la acción capilar de las ciberamenazas y la complejidad de la tecnología en el mercado hacen que las empresas del sector sean los sujetos más cualificados para entender las estrategias de ataque de los *hackers*, para detectar las principales vulnerabilidades escondidas en los *softwares* y para recomendar a las autoridades competentes las contramedidas más apropiadas; por otro, la realización de un circuito de supervisión y de un sistema de alerta distribuido (a.d., *distributed surveillance*), que se basa (también) en la constante actividad de vigilancia realizada por los operadores económicos, puede reducir significativamente las ineficiencias y los costes administrativos soportados por los Estados miembros debido a la protección de la seguridad cibernética nacional[21].

En segundo lugar, la implicación del sector empresarial sería extremadamente importante en la elaboración y en la actualización de los protocolos, de las directrices y de los estándares de seguridad comunes, concretamente en el ámbito de la protección de las infraestructuras y de los servicios considerados "críticos", gestionados, en la mayoría de los casos, por sujetos privados.

Especialmente, la intervención de estos últimos en el proceso de determinación de las políticas y de las medidas vinculantes para todas las partes interesadas (*stakeholders)*, proporcionaría, por supuesto, a las autoridades competentes un soporte técnico valioso[22]; esta forma de colaboración permitiría, además, evitar el riesgo de perseguir ambiciosos objetivos de resiliencia a través de la introducción de cargas y requisitos inadecuados o excesivos, incompatibles con el principio de proporcionalidad y con la perspectiva liberal a preservar en este ámbito[23]. Como parece evidente, empresas y varias entidades hacen frente a amenazas, a vulnerabilidades y a diferentes consecuencias; por consiguiente, una verdadera inclusión de estos sujetos en las sedes

[21] CLARKE, A. y KNAKE, R.K., *Cyber War: The Next Threat to National Security and What To Do About It*, HarperCollins Publishers, New York, 2010, p. 162.

[22] CAPPELLETTI, F. y MARTINO, L., "Achieving robust European cybersecurity through public-private partnerships: approaches and developments", *Elf discussion paper*, n. 4, 2021, spec. pp. 7 y ss.

[23] RAFFIOTTA, E.C., "Cybersecurity regulation in the European Union and the issues of Constitutional Law", *Rivista AIC*, n. 4, 2022, pp. 13-14, que contrapone, al enfoque, en cierta medida, dirigido por el legislador europeo, el modelo liberal adoptado por los Estados Unidos de América. Según el autor, en particular, el paradigma americano, que funciona a nivel federal a través de la *Cybersecurity and Infrastructure Security Agency* (CISA), se caracteriza por «*a voluntary approach, within which there is a synergy between a "light government touch" and a strong empowerment of private entities, including –above all– Big Techs corporations*».

decisorias y consultivas no podría más que fomentar la definición de herramientas parametrizadas con el determinado nivel de riesgo informático, apropiadas para contextos concretos en que operan las empresas y actualizadas con respecto a las innovaciones tecnológicas planteadas.

En otras palabras, la promoción de formas más estables y estructuradas de cooperación entre actores públicos y privados permitiría no solo un mayor uso compartido de informaciones, habilidades y buenas prácticas, sino también una deseable participación "desde abajo" al proceso regulatorio, limitando el tradicional enfoque "*command and control*" para fomentar formas de "*enforced self-regulation*"[24]. Como es sabido, también a nivel europeo, "para poder formular eficazmente una política, es preciso entender con claridad la naturaleza y el alcance de los retos. Esto requiere no solo datos estadísticos y económicos fiables y actualizados sobre los incidentes en detrimento de la seguridad informática y sobre los niveles de confianza de los consumidores y de los usuarios, sino también datos actualizados sobre las dimensiones y las tendencias en marcha en el sector de la seguridad de las TIC en Europa"[25].

Estas consideraciones nos llevan inevitablemente a reflexionar sobre el marco institucional de protección de la seguridad cibernética establecido en nuestro ordenamiento, en el cual el intento de reproducir módulos organizativos y operativos, propios del sector *intelligence,* ha determinado un evidente déficit de participación de los operadores económicos del sector[26]. Una elección legislativa que, si se analiza a fondo, resulta llamativa, también si se tiene en cuenta la bien conocida adicción de las administraciones públicas italianas a las capacidades y a las experiencias en el ámbito tecnológico-informático que tiene el sector privado, que ha representado, y aún representa, una de las principales causas de los retrasos registrados por nuestro país en el proceso global de transición digital[27].

Todavía parecen limitadas y genéricas, de hecho, las referencias normativas que tienen en cuenta el valor estratégico de la dinámica cooperativa entre sector público y sector industrial. Se hace referencia, por ejemplo, al art. 7 del DL del 14 de junio de 2021, n. 82, que encarga al ACN la tarea de: "hacer efectivas" las capacidades nacionales de prevención, supervisión, detección, análisis y reacción a los ataques

[24] Respecto a esto, véanse SALES, N.A., "Regulating Cyber-Security", cit., pp. 1554 y ss.; TROPINA, T., "Public-private collaboration: Cybercrime, cybersecurity and nationals' security", Tropina, T. y Callanan, C. (dirs.), ***Self- and Co-regulation in Cybercrime, Cybersecurity and National Security***, Springer, Cham, 2015, pp. 9 y ss.; CAPPELLETTI, F. y MARTINO, L., "Achieving robust European cybersecurity through public-private partnerships", cit., p. 9.

[25] Cfr. la comunicación de la Comisión europea de 31 de mayo de 2006, ***Una estrategia para una sociedad de la información segura. Diálogo, asociación y responsabilización***, COM (2006) 251, pár. 3.2.1., con la que la Comisión ha pedido a ENISA desarrollar una cooperación de confianza con los Estados miembros y las partes interesadas, con el fin de crear un sistema europeo de uso compartido de las informaciones y de alerta, así como de fomentar un espacio adecuado para la recopilación y el análisis de los datos sobre los incidentes y los ataques cibernéticos en la Unión.

[26] Sobre estos perfiles, véanse PARONA, L., "L'istituzione dell'Agenzia per la cybersicurezza nazionale", cit., p. 718; PREVITI, L., "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", ***Federalismi.it***, n. 25, 2022, pp. 81 y ss.

[27] Con respecto al conocido fenómeno del ***digital divide***, véanse, al menos, CASSESE, S., "A Che serve la formazione dei dipendenti pubblici?", ***Politica del diritto,*** 1989, pp. 431 y ss.; DONATI, D., "Digital divide e promozione della diffusione delle ICT", Merloni, F. (dirs.), ***Introduzione all'e-Government***, Giappichelli, Torino, 2005, pp. 209 y ss.; RAMAJOLI, M., "***Quale cultura per l'amministrazione pubblica?***", ***Giornale di Diritto Amministrativo,*** n. 2, 2017, pp. 187 y ss.; SGUEO, G., ***Il divario. I servizi pubblici digitali tra aspettative e realtà***, Egea, Milano, 2022.

informáticos, incluso a través del recurso a iniciativas de colaboración del sector público-privado[28]; de promocionar, a través de la implicación de las universidades y del sistema productivo, el desarrollo de competencias y de capacidades industriales, tecnológicas y científicas[29], incluso en calidad de centro nacional de coordinación, de conformidad con el mencionado art. 6 del reglamento UE 2021/887; de constituir colaboraciones, consorcios, fundaciones o sociedades, con sujetos públicos o privados, para la mejor realización de sus finalidades institucionales[30].

Como se ha señalado, mientras en otros países, como Francia y Alemania, se ha asistido a la creación de organismos específicos, que reúnen a representantes de las administraciones públicas y del mundo empresarial para realizar trabajos de análisis, planificación y elaboración de tendencias normativas en materia de ciberseguridad, en Italia, la colaboración con los privados ha sido, hasta ahora, principalmente de carácter financiero y dirigida al desarrollo de tecnologías e infraestructuras digitales[31].

El marco reglamentario que se acaba de mostrar lleva a acoger con satisfacción las interesantes propuestas contenidas en la reciente estrategia italiana sobre la ciberseguridad 2022-2026 y en el correspondiente plan de implementación de mayo de 2022; a través de estos documentos, además de las necesarias inversiones en el factor "desarrollo", se piensa garantizar una implicación más efectiva en el sector privado en la persecución de los objetivos de "protección", por un lado, y de "respuesta", por otro, hacia las trampas de la dimensión cibernética.

En concreto, en cuanto al primer objetivo, la estrategia y el plan de implementación aspiran a potenciar el sistema nacional de "escrutinio tecnológico", que depende del Centro de Evaluación y Certificación Nacional (CVCN) instituido en el ACN y, en los ámbitos de competencia, depende de los Centros de Evaluación del Ministerio del Interior y de Defensa. Para tal fin, se prevé la introducción de una red de laboratorios acreditados de prueba (a.d. LAP), como sujetos, públicos y privados, llamados a facilitar los procedimientos de certificación de calidad de los recursos (*asset*) tecnológicos utilizados por los sujetos incluidos en el PSNC, y para detectar las correspondientes vulnerabilidades[32].

Al mismo tiempo, las acciones mencionadas destacan la necesidad de aprovechar al máximo las capacidades nacionales de identificación y de respuesta hacia los ciberataques, estableciendo dos formas de colaboración diferentes para los operadores económicos del sector.

La primera, de carácter estructural, se refiere a la implantación de una red de centros sectoriales de análisis y de intercambios de informaciones relevantes (*Information Sharing and Analysis Center*, ISAC) creada para ayudar a las oficinas del

[28] Art. 7, apartado 1, let. n), DL n. 82/2021.

[29] Art. 7, apartado 1, let. r), DL. n. 82/2021.

[30] Art. 7, apartado 1, let. z), DL n. 82/2021.

[31] LAURO, A., "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", *La Rivista Gruppo di Pisa*, n. 3, 2021, pp. 537 y ss.

[32] Sobre esto, se remite a las previsiones del DL de 3 de agosto de 2022, n. 123.

ACN a ofrecer y a difundir buenas prácticas, directrices, avisos de seguridad y recomendaciones dentro del país.

La segunda, de carácter ocasional, contempla la implicación directa de empresas oportunamente calificadas en materia de respuesta ante incidentes (*incident response*), de apoyo en las funciones institucionales del CSIRT Italia, en caso de que se verificase "una cantidad numerosa de ciberincidentes de carácter sistémico". Con ello, Italia demuestra la voluntad de utilizar, junto con adecuadas estrategias de resiliencia, tácticas eficaces de defensa activas (*active defense*), con el propósito de desarrollar, aprovechando múltiples fuentes de datos relevantes y de actores responsables, formas compartidas y rápidas de gestión de crisis y contraataque[33].

Se trata de novedades que se espera implementar aún más, debido a los relevantes efectos disuasorios y preventivos ejercidos por estos instrumentos hacia las operaciones de intrusión y de manipulación realizadas por los criminales informáticos.

3 Factor humano, cultura de la seguridad cibernética e "inmunidad de grupo"

El avance repentino del proceso de informatización de las relaciones económicas y sociales registrado en los últimos años exige sin duda un replanteamiento del papel de los ciudadanos usuarios dentro de los sistemas nacionales de protección de la ciberseguridad. Esta afirmación se puede demostrar fácilmente empezando por la simple consideración de las nuevas amenazas para la seguridad colectiva que se derivan de la difusión, a nivel internacional, de aquellos dispositivos y aparatos, dotados de sensores interconectados e interactivos, que pertenecen al amplio conjunto de la *Internet de las cosas*: un fenómeno que está determinando, con respecto al pasado, un aumento vertiginoso de las superficies de ataque y el número de objetivos (*target*) afectados[34]. Es posible sacar conclusiones análogas prestando atención a la creciente expansión de la a.d. economía cibercriminal, que ha visto florecer con el tiempo un auténtico mercado en línea (por lo general, en la internet oscura) de productos y servicios específicamente dirigidos a consumir peligrosos ataques informáticos, acorde con el concepto de "*Crime as a Service*"[35].

---

[33] Sobre el papel estratégico que juega la elaboración de adecuadas tácticas de defensa activa, véanse GORI, U., "Nuovi approcci alla sicurezza cibernetica: la diplomazia preventiva come strumento di difesa attiva", Gori, U. (dir.), *Cyber Warfare 2018. Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche*, Franco Angeli, Milano, 2019, pp. 17 y ss.

[34] Sobre las nuevas problemáticas jurídicas relacionadas con la aparición del fenómeno del *Internet of Things,* véanse WEBER, R.H. y STUDER, E., "Cybersecurity and the Internet of Things: Legal Aspect", *Computer Law & Security Review*, n. 36, 2016, pp. 726 y ss.; RAYES, A. y SALAM, S., *Internet of Things: from Hype to Reality*, Springer, Cham, 2019; DE NARDIS, L., *The Internet in Everything. Freedom and Security in a World with No Off Switch*, Yale University Press, New Haven, 2020; NOTO LA DIEGA, G., *Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies*, Routledge, Londra, 2022.

[35] Sobre esto, BRIGHI, R. y CHIARA, P.G., "La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione europea", *Federalismi.it*, n. 21, 2021, p. 21, que destacan la relevancia y las motivaciones económicas de organizaciones criminales estructuradas como unas verdaderas empresas, que ofrecen en el mercado *softwares* listos para usar y que no necesitan específicas habilidades informáticas por parte de los compradores. Con respecto al concepto del "*Crime as a Service*", véase el interesante análisis de PAGANINI, P., "Cybercrime-as-a-Service: EU Perspectives", Martino, L. y Gamal, N. (dirs.), *European Cybersecurity in Context. A Policy-Oriented Comparative Analysis*, Elf study, Brussels, 2022, pp. 67 y ss.

Se trata de elementos que conducen a reflexionar no solo sobre el hecho de que los actos de criminalidad informática ya se puedan perpetrar a precios moderados por sujetos particularmente inexpertos en la utilización de las tecnologías[36], sino también sobre la apremiante necesidad de actuar para mejorar el nivel de alfabetización digital y conciencia de los usuarios de la red.

La necesidad de valorar las obligaciones y las responsabilidades de los usuarios de las infraestructuras y de los sistemas digitales constituye desde hace mucho tiempo un objetivo de las políticas europeas de protección de la seguridad informática.

Sobre esta cuestión se ha señalado cómo la "seguridad de las redes y de la información es responsabilidad común de todas las partes interesadas, incluso de los operadores, los proveedores de servicios, los proveedores del *hardware* y del *software*, los usuarios finales, los entes públicos y los gobiernos nacionales"[37]; por tanto, "todos los actores involucrados, sean autoridades públicas, sector privado o cada ciudadano, deben reconocer esta responsabilidad compartida, deben activarse para protegerse y, si es necesario, deben garantizar una respuesta coordinada para fortalecer la ciberseguridad"[38].

A nivel normativo, sin embargo, las recomendaciones mencionadas solo han encontrado una concreta respuesta hace poco: al principio, por medio de previsiones dirigidas a obligar a los Estados miembros a introducir, en las respectivas estrategias nacionales, programas específicos de formación y de actualización profesional[39]; después, a través del refuerzo de las funciones institucionales de la Agencia de la Unión Europea para la Ciberseguridad (*European Union Agency for Network and Information Security*, en adelante ENISA), encargada de promover una mayor conciencia de las organizaciones públicas, de las empresas y de los ciudadanos de la Unión en materia de ciberseguridad, así como de asesorar a los Estados miembros en sus iniciativas de instrucción y de sensibilización colectiva[40].

Bajo estas intervenciones subyace la constatación del hecho de que cierto nivel de riesgo de seguridad se encuentra inevitablemente en las modernas sociedades digitales; «*some intrusions can be prevented or mitigated but others cannot, and any defensive scheme is necessarily imperfect. This is so because offense is much less costly*

[36] Sobre la criminalidad informática y sobre las problemáticas de derecho penal relacionadas, véanse para todos AMATO MANGIAMELI, A.C. y SARACENI, G. (dirs.), *I reati informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli, Torino, 2019.

[37] Cfr. la Resolución del Consejo de 18 de diciembre de 2009 *Un enfoque cooperativo en materia de seguridad de las redes y de la información*, 2009/C 321/01, pár. 3.

[38] Cfr. la Comunicación conjunta de 7 de febrero de 2013 *Estrategia de ciberseguridad de la UE: un ciberespacio abierto y seguro*, cit., pár. 1.2.

[39] Art. 7, apartado 1, let. d), directiva NIS 1.

[40] Art. 4, apartados 7 y 10 reglamento UE 2019/881. La institución de la Agencia se ha realizado a cargo del Reglamento CE 460/2004, de 10 de marzo 2004.

than defense in cyberspace»[41]. De ahí la necesidad de ver, en la implicación directa de la sociedad civil, una formidable arma de prevención de los incidentes y de los ataques informáticos, con el intento de desarrollar esa "inmunidad de grupo" indispensable para contener el riesgo cibernético por debajo de los niveles admisibles[42].

En concreto, más allá de las alegaciones de las teorías económicas que consideran la solidez de las redes y de los *softwares* como un verdadero bien público[43], la introducción de políticas y medidas que tienen el objetivo de limitar los errores imputables al a.d. "factor humano", permitirían obtener ventajas prácticas, que se aprecian al menos por unas razones tripartitas.

En primer lugar, una mayor información a la opinión pública con respecto a las principales tipologías de amenazas, a las correspondientes modalidades de detección y a los instrumentos de respuesta que la normativa prevé, contribuiría a reducir la eficacia de los ataques menos sofisticados.

En este sentido, la consolidación de oportunas normas de "higiene informática", fáciles de comprender y replicar incluso para quien no tiene una preparación especializada (como aquellas relativas a los sistemas de autenticación, a las copias de seguridad y de recuperación, o a la instalación de *antivirus* y *firewall*), permitiría diseñar un sistema, si no completamente seguro, sí capaz de hacer frente a los peligros del ciberespacio más comunes y conocidos[44]. Esto daría a las autoridades públicas la posibilidad de concentrar sus propios recursos hacia los sujetos más indefensos, como los usuarios mayores o muy jóvenes, muchas veces dotados de escasas competencias básicas de informática y, por tanto, aún más expuestos al riesgo de caer en trampas virtuales dispuestas por criminales profesionales.

En segundo lugar, un mayor intercambio de buenas prácticas (*best practices)* y de directrices de comportamiento *online* determinaría un deseable incremento del número de las comunicaciones y de los avisos por parte de los usuarios.

Esta circunstancia contribuiría no solo a establecer una relación más directa entre los destinatarios de los ataques y los órganos administrativos encargados de la atención y la ayuda, sino también a proporcionar una mejor comprensión del nivel de difusión de las amenazas y de las modalidades de ataque de los *hackers*. Estos últimos, de hecho, a través de complejos sistemas de ingeniería social, destinados a aprovecharse de la ingenuidad de los individuos, ahora son capaces de introducirse en muchos *servers*, apoderarse de ellos y afectar a objetivos (*target*) de considerable

[41] SALES, N.A., "Regulating Cyber-Security", cit., p. 1545.

[42] MONTESSORO, P.L., "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", *Istituzioni del Federalismo*, n. 3, 2019, pp. 784-785.

[43] Véanse, entre otros, GRADY, M.F. y PARISI, F., *Law and Economics of Cybersecurity*, Cambridge University Press, Cambridge, 2005; ROSENZWEIG, P., *Cyber Warfare: How Conflict in Cyberspace is Challenging America and Changing the World*, Praeger Press, Westport, 2012; TADDEO, M., "Is Cybersecurity a Public Good?", cit., pp. 350 y ss.; BRIGHI, R. y CHIARA, P.G., "La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione europea", cit., pp. 25 y ss.

[44] ZICCARDI, G., "La cybersecurity nel quadro tecnologico (e politico) attuale", Ziccardi, G. y Perri, P. (dirs.), *Tecnologia e diritto*, vol. III, Giuffrè, Milano, 2019, p. 210.

relevancia sin arriesgarse a que las autoridades policiales los detecten[45]. Por esta razón, además del perfil de la seguridad exterior, las modernas estrategias de ciberseguridad deberían prestar especial atención a las vulnerabilidades relacionadas con la seguridad interior[46].

Por último, un apoyo económico constante y operativo en favor de iniciativas en el ámbito de la formación cibernética facilitaría considerablemente la creación de una verdadera cultura de la seguridad y del riesgo informático.

Un objetivo que –aunque represente una de las tareas de la ENISA[47] y, por último, de la ACN[48], incluso a través de la activación de cursos universitarios específicos y de la asignación de becas de estudios y de investigación o doctorados[49]– aún parece lejos de realizarse plenamente, sobre todo en nuestro ordenamiento.

Al respecto téngase en cuenta que, como afirma el reciente informe Censis-*Deepcyber* de abril de 2022[50], el 40 % de los ciudadanos italianos permanece indiferente o no se protege en absoluto contra los ataques informáticos; según esta investigación, además, solo el 24,3 % de los italianos declara que conoce concretamente el significado de la palabra ciberseguridad, mientras que el 58,6 % declara que conoce el tema a grandes rasgos y el 17,1 % declara que no sabe qué es.

También por estos motivos, en el ámbito de la mencionada estrategia italiana 2022-2026, se indican expresamente la formación y la promoción de la cultura en materia de ciberseguridad como "factores habilitadores" necesarios para el alcance de las finalidades de protección, de respuesta y de desarrollo en ella contempladas.

Al respecto, dicha documentación remarca la exigencia de actuar con dos principales intervenciones.

Por un lado, se establece un programa capilar de educación digital para todos los niveles de educación escolar, con el objetivo de estimular en los usuarios más jóvenes la elección de buenas conductas en el espacio cibernético y de desarrollar nuevas profesionalidades en las carreras técnico-científicas, incluso con el objetivo de reducir la distancia relativa a las competencias con respecto de otros países.

Por otro lado, la estrategia plantea la organización de cursos de formación especializada adecuados y de actualizaciones profesionales, dirigidos a los dependientes empleados de las administraciones públicas y a los de los entes privados, grandes o

[45] Piénsese en lo ocurrido a algunos jueces de la Corte dei Conti en septiembre de 2022. Ellos fueron víctimas de una insidiosa operación de suplantación de identidad (*phishing),* que empezó con el envío de un mensaje, que contenía la solicitud de unos datos y al parecer enviado del teléfono profesional de un compañero, a su propio móvil. Contestando al mensaje, los jueces permitieron de hecho a los criminales informáticos el acceso a los contactos de su propia rúbrica y a sus conversaciones de WhatsApp, donde se encontraban documentos reservados.

[46] A este respecto, DE VERGOTTINI, G., "Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata", *Rivista Aic*, n. 4, 2019, p. 77.

[47] Art. 3, pár. 1, let. j), Reglamento CE 460/2004, de 10 de marzo de 2004.

[48] Art. 7, apartado 1, let. u), DL n. 82/2021.

[49] Art. 7, apartado 1, let. v), DL n. 82/2021.

[50] Cfr. el informe Censis-*Deepcyber,* de 22 de abril de 2022, *Il valore della cybersecurity*, disponible en *www.censis.it.* A los datos contenidos en este informe hay que añadir aquellos referidos en la edición del 2022 del Índice europeo de digitalización de la economía y de la sociedad (*Digital Economy and Society Index*, DESI), que coloca Italia en la posición 18 y, por lo que se refiere al capital humano, en la posición 25 entre los 27 Estados miembros, puesto que solo el 46 % de los ciudadanos italianos de entre los 16 y los 74 años tiene al menos conocimientos digitales básicos.

pequeños, con especial atención a los que ocupan posiciones apicales. A estas últimas, de hecho, les corresponderá establecer eficaces planes de gestión interior del riesgo cibernético y proporcionar los adecuados mecanismos de mitigación y de aviso, incluso a través de operaciones de autoevaluación de su propio nivel de exposición.

Está claro que la efectiva realización de estos objetivos, dirigidos a reducir los descuidos y los errores más comunes de los operadores y de los usuarios de la dimensión cibernética, conllevará costes elevados; sin embargo, si es cierto que el eslabón más débil de la cadena de seguridad está representado justo por el factor humano, entonces "no hacer nada tendría costes mucho más elevados"[51].

4 Patrones de colaboración entre sector público y privado y perspectivas de *iure condendo*

En los párrafos anteriores se ha puesto en evidencia la necesidad de promover una mayor colaboración entre el sector público y el privado en los sistemas nacionales de seguridad cibernética, como medida fundamental de prevención y de reacción ante el significativo aumento de los incidentes y de los ataques informáticos registrados a nivel mundial.

Como se ha señalado, el logro de este resultado está completamente respaldado por las recientes directrices europeas en temas de ciberseguridad, que implican a todos los componentes de la sociedad en la construcción de "una Unión de la seguridad verdadera y eficaz"[52], que se basa en instrumentos, conocimientos y actitudes, comunes y compartidos, impulsados incluso por la mencionada directiva UE 2022/2555, a.d. directiva NIS 2[53].

Para poder aprovechar al máximo los mencionados beneficios que proceden de la actuación del acercamiento "*whole of society*" de matriz supranacional –cuyo valor ya es reconocido incluso en el ordenamiento jurídico italiano– parece importante actuar, en particular, en dos aspectos problemáticos fundamentales.

En primer lugar, una vez reconocido que «el derecho del riesgo perfila patrones relacionales basados más que en mecanismos de "*command and control*" o total "autoadministración" privada, en la integración y en la cooperación entre público y

[51] GORI, U., "Lo spazio cibernetico tra esigenze di sicurezza nazionale e tutela delle libertà individuali", *Informazioni difesa*, supl. n. 6, 2014, p. 21.

[52] Cfr. la Comunicación de la Comisión Europea de 24 de julio de 2020, *Estrategia de la UE para la Unión por la Seguridad*, COM (2020) 605 final, pár. 3, donde se reafirma que: «[…] la cooperación con el sector privado es fundamental, tanto más que la industria cuenta con una parte importante de la infraestructura digital y no digital indispensable para luchar de forma eficaz contra la criminalidad y el terrorismo. Igualmente, cada individuo puede aportar su contribución, creando por ejemplo competencias y conciencia para combatir la criminalidad informática o la desinformación».

[53] La nueva acción interviene para aclarar y ampliar el alcance de la anterior disposición UE 2016/1148, y desde el punto de vista subjetivo, haciendo referencia a la detección de los sujetos involucrados en la cadena de gestión del riesgo cibernético y, desde el punto de vista objetivo, haciendo referencia a las obligaciones de aviso y de seguridad. Es interesante señalar, por un lado, cómo la Comisión europea haya expresamente calificado los entes de la Administración pública, central y regional (excepto los que desarrollan sus actividades «en los sectores de la seguridad nacional, de la seguridad pública, de la defensa, incluso la prevención, la investigación, la comprobación y la persecución de los crímenes»), como sujetos que operan en sectores "de alta criticidad" y, por otro, como la misma Comisión haya ampliado el ámbito de aplicación de la disposición incluso a las PMI, en caso de que estas últimas se consideren esenciales para la vida económica y social de un Estado miembro.

privado»[54], no parece posible dejar la aplicación del nuevo paradigma exclusivamente en manos de la mera adhesión voluntaria de los sujetos interesados. En cambio, sobre todo en la fase de experimentación de las nuevas propuestas, sería necesario fijar con qué modalidades y en qué límites la colaboración debe realizarse. Eso implica, por ejemplo, la conclusión de acuerdos contractuales destinados a aclarar los incentivos económicos, el reparto de los riesgos, las condiciones de privacidad y las cláusulas de exención de las responsabilidades para las empresas del sector[55].

Dicho de otro modo, si por un lado «*computer hygiene and basic cybersecurity arrangements should become part of the everyday skills of any internet user, and in the corporate environment cybersecurity should become an overall management challenge, requiring a holistic risk-management approach*», por otro «*it is thus clear that new conceptual approaches to cybersecurity are required to make the behaviour of all players in this market more incentive-compatible*»[56].

En segundo lugar, estando clara la importancia de la cooperación en los sectores de la investigación y de la innovación –objeto, no por casualidad, del primer acuerdo de colaboración estipulado en esta materia en sede europea[57]– la atención del legislador nacional debería dirigirse todavía más a reglamentar formas más estables y articuladas de colaboración.

Al respecto cabe destacar como la ENISA ha invitado varias veces a los Estados miembros a invertir en esta dirección, identificando, en particular, cuatro paradigmas principales ya presentes en Europa[58]: I) el *Institucional PPP*, destinado a garantizar la protección de instituciones e infraestructuras críticas a través de una cooperación a largo plazo entre los interesados, que se cumple, por ejemplo, en el desarrollo de actividades de soporte operativo, de análisis de datos, de elaboración de buenas prácticas, de control de los estándares de seguridad y de otros servicios[59]; II) el *Goal-oriented PPP*, destinado a promover la cultura de la seguridad informática en los Estados miembros a través de la constitución de centros y de grupos de intercambio

[54] Sobre el tema, BARONE, A., *Il diritto del rischio*, Giuffrè, Milano, 2006, pp. 64 y ss.

[55] En cuanto a esto, véanse BOSSONG, R. y WAGNER, B., "A Typology of Cybersecurity and Public-Private Partnerships in the Context of the European Union", cit., p. 284, que subrayan que: «*In the area of cybersecurity, other forms of risks and responsibilities beyond timely construction or reliable service provision have to be considered. Governments are also increasingly able to exert pressure to obtain "voluntary" cooperation from business […]. But when dealing with new or advanced cyber threats, public actors often enter these partnerships as the weaker partner, reliant on specialised IT companies to define the level of vulnerability and appropriate countermeasures*».

[56] Así, PUPILLO, L., "EU Cybersecurity and the Paradox of Progress", *CEPS policy insights*, n. 6, 2018, p. 3.

[57] Se trata del Acuerdo de cooperación público-privada sobre la ciberseguridad de 5 de julio de 2016, promovido por la Comunicación de la Comisión Europea de 6 de mayo de 2015, *Estrategia para el mercado único digital en Europa*, COM (2015) 192 final, pár. 3.4., con que se ha instaurado una cooperación más estable entre sujetos diferentes, públicos y privados, interesados en promocionar la investigación y la innovación en el ámbito cibernético, promover la industria europea de la seguridad informática e introducir soluciones innovadoras y fiables (productos, servicios y *software* TIC) en algunos sectores estratégicos de la Unión (*i.e.*, energía, sanidad, transportes, finanzas). En concreto, el acuerdo ha recibido una inversión por parte de la Unión Europea, en el marco del programa Horizonte 2020, de 450 millones de euros, mientras las inversiones de los operadores del mercado de la ciberseguridad, representadas por la Organización Europea para la seguridad informática (ECSO), han sido tres veces mayores, para un total de aproximadamente 1,8 millardos entre el 2016 y 2020.

[58] Cfr. ENISA, *Public Private Partnerships (PPP). Cooperative models*, noviembre de 2017, pár. 3 y ss. (Acceso web: consultable en *www.enisa.europa.eu*).

[59] Se trata del patrón difundido en Estonia y en Polonia.

de conocimientos y de soluciones prácticas sobre argumentos concretos[60]; III) el *Service outsourcing PPP*, útil para presentar a las autoridades públicas competentes las problemáticas cibernéticas más importantes en un sector empresarial específico y a sugerir, por consiguiente, los oportunos actos normativos y de orientación que deben adoptarse para solucionarlas[61]; el *Hybrid PPP*, que constituye una combinación del primero y del tercer patrón, muchas veces utilizado para dejar en manos de entes privados cualificadas funciones y tareas que las mismas instituciones nacionales no están a la altura de ejercer, como las inherentes a las actividades de aviso y de respuesta en caso de ataques cibernéticos[62].

La elección del patrón de colaboración que se debe implementar se deja, en realidad, a cada Estado miembro, puesto que «*there is no universal, simple solution that applies to all the nations for creating and developing PPP. It is rather a national issue, connected with the culture and the way how the whole political and economic system works*»[63].

Teniendo en cuenta estas consideraciones, es posible destacar la exigencia de introducir sucesivas fases y modalidades de implicación de la clase privada-empresarial en el ámbito de la arquitectura italiana de tutela de la seguridad cibernética, en especial, en la determinación de las políticas, de los procedimientos, de los estándares, de las medidas y contramedidas más importantes en la materia[64].

Parecen inadecuadas para asegurar este objetivo, de hecho, las previsiones normativas actualmente vigentes, que contemplan la mera participación sin derecho de voto a las reuniones del Núcleo para la Ciberseguridad de los «sujetos públicos o privados eventualmente interesados» en situaciones de crisis de naturaleza cibernética[65] y que dejan en manos del ACN la tarea de establecer «con un reglamento propio» los niveles mínimos de seguridad, de capacidad de elaboración, de ahorro energético y de fiabilidad de las infraestructuras digitales de la Administración pública[66], además de promover, en general, la creación de actuaciones de colaboración.

---

60 Se trata del patrón presente en España, Reino Unido, Luxemburgo, Holanda, Austria e Eslovaquia.

61 Se trata del patrón que se encuentra en Alemania y en Austria.

62 Patrón presente, por ejemplo, en República Checa.

63 Cfr. ENISA, *Public Private Partnerships (PPP). Cooperative models*, cit., pár. 3.

64 Sobre la necesidad de promover, en la Unión, un sistema de ciberseguridad abierto a la participación y a la colaboración de los actores privados, incluso con el fin de facilitar el alcance del objetivo n. 16 de la Agenda ONU 2030 para el Desarrollo Sostenible, dedicado a la promoción de sociedades pacíficas e inclusivas, así como a la construcción de instituciones responsables y eficaces a todos niveles, véanse ROSSA, S., "Administrative Law Reflections on Cybersecurity, and on its Institutional Actors, in the European Union and Italy", *Italian Journal of Public Law*, n. 2, 2022, pp. 449-450.

65 Art. 10, apartado 3, DL n. 82/2021. El Núcleo para la ciberseguridad (en origen, Núcleo para la Seguridad Cibernética) ha sido implantado por el DPCM n. 66/2013, con el fin de coordinar la acción de todos los sujetos involucrados en la preparación y en la gestión de las situaciones de crisis y activar los eventuales procedimientos de alerta y de respuesta. Desde 2021 el Núcleo opera en la Agencia Nacional para la Ciberseguridad.

66 Art. 33-*septies*, apartado 4, DL de 18 de octubre de 2012, n. 179, conversión con modificación de la Ley de 17 de diciembre de 2012, n. 221.

De ahí la contraprueba del hecho de que, a pesar de la retórica de la transición digital, aún pueda ser difícil para un Estado esa «confesión de fracaso»[67] al reglamentar y tutelar con autonomía y con recursos propios la seguridad pública en el ciberespacio.

Bibliografía

AMATO MANGIAMELI, A.C. y SARACENI, G. (dirs.), *I reati informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli, Torino, 2019.

ATERNO, S., *Sicurezza informatica. Aspetti giuridici e tecnici*, Pacini, Pisa, 2022.

BARONE, A., *Il diritto del rischio*, Giuffrè, Milano, 2006.

BARONI, M., "Intelligenza artificiale e cybersicurezza in una prospettiva costituzionale", Cerrina Feroni, G., Fontana, C. y Raffiotta, E.C. (dirs.), *AI Anthology*, Il Mulino, Bologna, 2022.

BASSINI, M., "Cybersecurity", Paracampo, M.T. (dir.), *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Giappichelli, Torino, 2021.

BETZU, M., *I baroni del digitale*, Editoriale scientifica, Napoli, 2022.

BOSSONG, R. y WAGNER, B., "A Typology of Cybersecurity and Public-Private Partnerships in the Context of the European Union", *Crime, Law and Social Change*, n. 67, 2017.

BRIGHI, R. y CHIARA, P.G., "La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione europea", *Federalismi.it*, n. 21, 2021.

CAPPELLETTI, F. y MARTINO, L., "Achieving robust European cybersecurity through public-private partnerships: approaches and developments", *Elf discussion paper*, n. 4, 2021.

CAROTTI, B., "Sicurezza cibernetica e Stato nazione", *Giornale di Diritto Amministrativo*, n. 5, 2020.

CASINI, L., *Lo Stato nell'era di Google. Frontiere e sfide globali*, Mondadori, Milano, 2020.

CASSESE, S., "A Che serve la formazione dei dipendenti pubblici?", *Politica del diritto*, 1989.

CASSESE, S., *La crisi dello Stato*, Laterza, Roma-Bari, 2002.

CASSESE, S., *Lo spazio giuridico globale*, Laterza, Roma-Bari, 2003.

CENCETTI, C., *Cybersecurity: Unione europea e Italia. Prospettive a confronto*, Nuova Cultura, Roma, 2014.

CLARKE, A. y KNAKE, R.K., *Cyber War: The Next Threat to National Security and What To Do About It*, HarperCollins Publishers, New York, 2010.

CONTALDO, A. y MULA, D. (dirs.), *Cybersecurity Law*, Pacini, Pisa, 2020.

[67] MONTI, A., "Internet e ordine pubblico", Cassano, G. y Previti, S. (dirs.), *Il diritto di internet nell'era digitale*, Giuffrè, Milano, 2020, p. 75. Sobre las inevitables dificultades que los poderes públicos encuentren al reglamentar las conexiones y relaciones humanas que tienen lugar en el espacio virtual, véanse, por último, MANNONI, S. y STAZI, G., *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Editoriale scientifica, Napoli, 2021; BETZU, M., *I baroni del digitale*, Editoriale scientifica, Napoli, 2022.

DE NARDIS, L., *The Internet in Everything. Freedom and Security in a World with No Off Switch*, Yale University Press, New Haven, 2020.

DE VERGOTTINI, G., "Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata", *Rivista Aic*, n. 4, 2019.

DONATI, D., "Digital divide e promozione della diffusione delle ICT", Merloni, F. (dirs.), *Introduzione all'e-Government*, Giappichelli, Torino, 2005.

ENISA, *Public Private Partnerships (PPP). Cooperative models*, noviembre 2017. Acceso web: *www.enisa.europa.eu*.

FORGIONE, I., "Il ruolo strategico dell'Agenzia nazionale per la cybersicurezza nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna", *Diritto amministrativo*, n. 4, 2022.

GORI, U., "Lo spazio cibernetico tra esigenze di sicurezza nazionale e tutela delle libertà individuali", *Informazioni difesa*, supl. n. 6, 2014.

GORI, U., "Nuovi approcci alla sicurezza cibernetica: la diplomazia preventiva come strumento di difesa attiva", Gori, U. (dir.), *Cyber Warfare 2018. Dalla difesa passiva alla risposta attiva: efficacia e legittimità della risposta attiva alle minacce cibernetiche*, Franco Angeli, Milano, 2019.

GRADY, M.F. y PARISI, F., *Law and Economics of Cybersecurity*, Cambridge University Press, Cambridge, 2005.

KESAN, J.P. y HAYES, C.M., "Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals", *Michigan State Law Review*, 2014.

KOHLER, C., "The EU Cybersecurity Act and European standard: an introduction to the role of European standardization", *International Cybersecurity Law Review*, n. 1, 2020.

LAURO, A., "Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione", *La Rivista Gruppo di Pisa*, n. 3, 2021.

MANNONI, S. y STAZI, G., *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Editoriale scientifica, Napoli, 2021.

MELE, S., "Il Perimetro di sicurezza nazionale cibernetica e il nuovo «golden power»", Cassano, G. y Previti, S. (dirs.), *Il diritto di internet nell'era digitale*, Giuffrè, Milano, 2020.

MONTESSORO, P.L., "Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale", *Istituzioni del Federalismo*, n. 3, 2019.

MONTI, A., "Internet e ordine pubblico", Cassano, G. y Previti, S. (dirs.), *Il diritto di internet nell'era digitale*, Giuffrè, Milano, 2020.

NOTO LA DIEGA, G., *Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies*, Routledge, Londra, 2022.

PAGANINI, P., "Cybercrime-as-a-Service: EU Perspectives", Martino, L. y Gamal, N. (dirs.), *European Cybersecurity in Context. A Policy-Oriented Comparative Analysis*, Elf study, Brussels, 2022.

PARONA, L., "L'istituzione dell'Agenzia per la cybersicurezza nazionale", *Giornale di Diritto Amministrativo*, n. 6, 2021.

PREVITI, L., "Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico", *Federalismi.it*, n. 25, 2022.
PUPILLO, L., "EU Cybersecurity and the Paradox of Progress", *CEPS policy insights*, n. 6, 2018.
RAFFIOTTA, E.C., "Cybersecurity regulation in the European Union and the issues of Constitutional Law", *Rivista AIC*, n. 4, 2022.
RAMAJOLI, M., "*Quale cultura per l'amministrazione pubblica?*", *Giornale di Diritto Amministrativo*, n. 2, 2017.
RAYES, A. y SALAM, S., *Internet of Things: from Hype to Reality*, Springer, Cham, 2019.
RENZI, A., "La sicurezza cibernetica: lo stato dell'arte", *Giornale di Diritto Amministrativo*, n. 4, 2021.
RODOTÀ, S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014.
ROSSA, S., "Administrative Law Reflections on Cybersecurity, and on its Institutional Actors, in the European Union and Italy", *Italian Journal of Public Law*, n. 2, 2022.
ROSENZWEIG, P., *Cyber Warfare: How Conflict in Cyberspace is Challenging America and Changing the World*, Praeger Press, Westport, 2012.
SALES, N.A., "Regulating Cyber-Security", *Northwestern University Law Review,* vol. 107, n. 4, 2013.
SALES, N.A., "Privatizing Cybersecurity", *UCLA Law Review,* vol. 65, n. 3, 2018.
SERINI, F., "La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021", *Federalismi.it*, n. 12, 2022.
SGUEO, G., *Il divario. I servizi pubblici digitali tra aspettative e realtà*, Egea, Milano, 2022.
TADDEO, M., "Is Cybersecurity a Public Good?", *Minds & Machines*, n. 29, 2019.
TORCHIA, L., *Lo Stato digitale. Una introduzione*, Il Mulino, Bologna, 2023.
TROPINA, T., "Public-private collaboration: Cybercrime, cybersecurity and nationals' security", Tropina, T. y Callanan, C. (dirs.), *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*, Springer, Cham, 2015.
URSI, R., "La difesa: tradizione e innovazione", *Diritto Costituzionale*, n. 1, 2022.
WEBER, R.H. y STUDER, E., "Cybersecurity and the Internet of Things: Legal Aspect", *Computer Law & Security Review*, n. 36, 2016.
ZICCARDI, G., "La cybersecurity nel quadro tecnologico (e politico) attuale", Ziccardi, G. y Perri, P. (dirs.), *Tecnologia e diritto*, vol. III, Giuffrè, Milano, 2019.