Revista Galega de Administración Pública, EGAP
Núm. 65_xaneiro-xuño 2023 | pp. 105-123
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 O sistema multinivel de protección da seguridade pública no ciberespazo. Delimitación da área de investigación

Entre as cuestións problemáticas conectadas co avance do proceso de transición dixital en marcha nos Estados membros na Unión, a tutela da seguridade cibernética ou, mellor dito, da seguridade pública no espazo cibernético, ocupa por suposto un lugar de máxima importancia.

Como é ben sabido, malia que o tema en cuestión se coñeza e discuta desde hai moito tempo[1], os primeiros intentos de responder uniforme e eficaz a nivel interna-

[1] Véxanse, entre outras, a Comunicación da Comisión Europea do 6 de xuño de 2001, *Seguridade das redes e seguridade da información: proposta dun enfoque estratéxico europeo*, COM (2001) 298; a Comunicación da Comisión Europea do 26 de setembro de 2003, *O papel da Administración electrónica para o futuro de Europa*, COM (2003) 567.

cional son recentes, concretamente no ámbito das iniciativas dedicadas á realización do *Digital Single Market*[2].

Con estas actuacións, a Unión quixo consolidar, en particular, unha visión propia estratéxica do ciberespazo, como lugar virtual aberto e seguro para o desenvolvemento das actividades económicas e sociais dos cidadáns europeos, baseada na protección e na fiabilidade dos datos, das redes e dos produtos informáticos presentes no seu interior. Un ámbito de fronteiras indefinidas –«o espazo público máis grande que a humanidade coñecese»[3]– e de potencialidades aínda inexploradas[4], ao que se quere dotar dun nivel elevado de resiliencia a través da aplicación de políticas e medidas homoxéneas, así como a través dun eficiente mecanismo de información de accidentes e de ataques máis relevantes[5].

As directivas xerais dirixidas a desenvolver metodoloxías compartidas de prevención e de xestión do ciber-risco determinaron, no ordenamento italiano, a introdución dun novo sistema organizativo de defensa dos intereses da nación, que ten no Perímetro de Seguridade Cibernética (en diante, PSNC)[6] e na Axencia para a Ciberseguridade Nacional (en diante, ACN)[7] os puntos de referencia esenciais[8].

A arquitectura institucional así definida caracterízase, na actualidade, pola coordinación das accións estratéxicas e pola centralización das competencias administrativas; un sistema que, debido ás peculiaridades que o connotan, resulta en esencia orientado a mitigar o impacto das ameazas informáticas nas infraestruturas e nos

[2] Nesta materia, cfr. a Directiva UE 2016/1148 do Parlamento Europeo e do Consello do 6 de xullo de 2016, Directiva NIS 1, modificada, por último, da Directiva UE 2022/2555 do Parlamento Europeo e do Consello do 14 de decembro de 2022, Directiva NIS 2; as comunicacións conxuntas da Comisión Europea e do alto representante da Unión, respectivamente, do 7 de febreiro de 2013, *Estratexia de ciberseguridade da UE: un ciberespazo aberto e seguro*, JOIN (2013) 1 final, do 13 de setembro de 2017, *Resiliencia, disuasión e defensa: cara a unha ciberseguridade forte na UE*, JOIN (2017) 450 final, e do 16 de decembro de 2020, *A estratexia de ciberseguridade da UE para a década dixital*, JOIN (2020) 18 final; o Regulamento UE 2019/881, do 17 de abril de 2019, *Cybersecurity Act.*

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

[4] Sobre a influencia exercida pola difusión do ciberespazo e das novas tecnoloxías sobre a relectura do concepto de soberanía estatal e sobre a transformación das funcións tradicionais dos Estados, véxanse, 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 a visión estratéxica da Unión relativa ao espazo cibernético, véxanse CENCETTI, C., *Cybersecurity: Unione europea e Italia. Prospettive a confronto*, Nuova Cultura, Roma, 2014, pp. 21 e ss.; CONTALDO, A. e MULA, D. (dirs.), *Cybersecurity Law*, Pacini, Pisa, 2020, pp. 57 e 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 e 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 e ss.; BARONI, M., "Intelligenza artificiale e cybersicurezza in una prospettiva costituzionale", Cerrina Feroni, G., Fontana, C. e Raffiotta, E.C. (dirs.), *AI Anthology*, Il Mulino, Bologna, 2022, pp. 373 e ss.

[6] Instituído polo DL do 21 de setembro de 2019, n. 105, conversión con modificación da Lei do 18 de novembro de 2019, n. 133.

[7] Instituída polo DL do 14 de xuño de 2021, n. 82, conversión con modificación da Lei do 4 de agosto de 2021, n. 109.

[8] Con respecto á fisionomía e ás características da arquitectura italiana en materia de seguridade cibernética, véxanse, *ex multis*, CAROTTI, B., "Sicurezza cibernetica e Stato nazione", *Giornale di Diritto Amministrativo*, n. 5, 2020, pp. 629 e ss.; MELE, S., "Il Perimetro di sicurezza nazionale cibernetica e il nuovo «golden power»", Cassano, G. e Previti, S. (dirs.), *Il diritto di internet nell'era digitale*, Giuffrè, Milano, 2020, pp. 186 e ss.; ATERNO, S., *Sicurezza informatica. Aspetti giuridici e tecnici*, Pacini, Pisa, 2022, pp. 234 e ss.; RENZI, A., "La sicurezza cibernetica: lo stato dell'arte", *Giornale di Diritto Amministrativo*, n. 4, 2021, pp. 538 e 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 e 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 e ss.

servizos considerados de maior importancia para a vida do país[9]. Infraestruturas e servizos que constitúen un verdadeiro "fortín" dotado de bastións pola súa natureza móbiles, concretamente en razón da evolución tecnolóxica, á defensa dos cales non están encargados "incansables soldados con escopetas e canóns", senón enxeñeiros, expertos en *compliance* e máquinas intelixentes[10].

Esta reflexión aspira a pór de manifesto a importante contribución realizada polo sector empresarial privado para o logro dos obxectivos, nacionais e internacionais[11], de tutela da seguridade cibernética. E iso co fin de demostrar como a mellor garantía posible contra os perigos do ciberespazo está representada polo recoñecemento e pola valorización da contribución cognoscitiva e experiencial dos operadores económicos do sector, por un lado, e do papel colaborativo dos cidadáns usuarios, por outro.

Nos seguintes parágrafos examinaranse, polo tanto, as principais modalidades con que a valiosa cooperación entre autoridades institucionais e suxeitos privados pode cumprirse concretamente, tendo en consideración, nun primeiro momento, a categoría das empresas que operan no sector das tecnoloxías da información e comunicación (TIC) e da ciberseguridade, para centrarse logo no papel de cada un dos usuarios. A análise proposta permitirá entender a importancia da recente estratexia italiana adoptada en maio de 2022[12], orientada a atribuírlles un papel autenticamente activo aos distintos compoñentes do complexo económico e social do país, de acordo co achegamento "*whole of society*" que inspira os numerosos actos de orientación da Unión.

Ao final da investigación, formularanse unhas consideracións conclusivas con respecto ás formas de partenariado público-privado, que se cre oportuno promover no noso ordenamento para poder aproveitar ao máximo as significativas vantaxes que derivan da implementación dunha *governance* plenamente participante en materia de seguridade informática.

2 Asimetrías informativas, compartición do risco e *governance* compartida

A instauración dun sincero e construtivo diálogo entre público e privado no sector da ciberseguridade non constitúe en absoluto un obxectivo de doada realización.

As principais razóns a partir dunha xeral situación de mutua desconfianza entre os diferentes portadores de interese son xa ben coñecidas: por unha parte, as autoridades administrativas manifestan certa resistencia en compartir cara ao exterior os datos

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

[10] Segundo a suxestiva e eficaz imaxe de URSI, R., "La difesa: tradizione e innovazione", *Diritto Costituzionale*, n. 1, 2022, p. 18.

[11] Sobre a imposibilidade de afrontar e gobernar problemas de orde económica e social que traspasan os límites do Estado, véxase, para todos, CASSESE, S., *La crisi dello Stato*, Laterza, Roma-Bari, 2002; CASSESE, S., *Lo spazio giuridico globale*, Laterza, Roma-Bari, 2003.

[12] Cfr. a estratexia de ciberseguridade 2022-2026 e o respectivo plan de implementación de maio de 2022, localizables en *www.acn.gov.it*, a través dos cales se adopta un consistente programa de medidas e de investimentos dirixidos a realizar os tres fundamentais obxectivos de "desenvolvemento", "protección" e "resposta" (volverase mellor aos puntos 2 e 3).

e as informacións que atinxen á súa propia seguridade, temendo comprometer, de tal forma, a súa propia imaxe institucional; por outra, os operadores económicos, recibindo só de cando en vez axeitados incentivos para a colaboración prestada, prefiren non confiar informacións reservadas ou persoais, que os exporían ao risco de sufrir accións legais ou de prexudicar a súa propia reputación no mercado[13].

Trátase de actitudes que no pasado xustificaron e, en parte aínda xustifican, o recurso a modelos organizativos e reguladores do tipo *top-down*, que contan coa previsión de específicas obrigas de notificación e de conduta, oportunamente sancionadas á conta das empresas interesadas, no intento de inducir estes suxeitos a desenvolver comportamentos virtuosos e a prestar as debidas precaucións fronte ás numerosas ameazas do ciberespazo[14].

Co obxectivo de superar eses puntos críticos, as institucións da Unión fomentaron, nos últimos anos, a través de institutos e modalidades diferentes, unha implicación máis efectiva das empresas que ofrecen produtos e servizos tecnolóxicos no ámbito dos sistemas de seguridade cibernética elaborados polos Estados membros.

A estratexia supranacional, en primeiro lugar, pasa por fixar principios fundamentais, que se dirixen aos operadores do sector en canto coprotagonistas da calidade do nivel de protección asegurado ás infraestruturas e aos *softwares* presentes no mercado único.

Neste sentido, os produtores e os provedores das TIC vense obrigados, por un lado, a comercializar exclusivamente bens e servizos que posúen, desde o momento do proxecto, determinados requisitos de seguridade contra o risco de accidentes e de ataques cibernéticos (principio de seguridade *by design*); por outro, os mesmos suxeitos teñen que asumir, cara aos usuarios, un papel de interlocutores privilexiados durante o ciclo completo de vida dos produtos, colaborando co sector público na xestión da actividade de vixilancia (principio de responsabilidade tecnolóxica)[15].

De aí a previsión dunha serie de desempeños peculiares, que son, entre outros: efectuar revisións periódicas de funcionamento, realizar as actualizacións e revisións necesarias dos *softwares*, eliminar con celeridade as vulnerabilidades informáticas reportadas e garantir un correcto emprego dos datos persoais dos usuarios. Conséguese, en definitiva, a introdución de específicas obrigas de dilixencia reforzada, máis

[13] Entre outros, SALES, N.A., "Regulating Cyber-Security", *Northwestern University Law Review,* vol. 107, n. 4, 2013, pp. 1549-1550. O dato está confirmado tamén polo informe do Grupo de coordinación sobre a seguridade cibernética do Banco de Italia, *Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass*, agosto de 2018, localizable en *www.bancaditalia.it*, onde se subliña que, malia o valor estratéxico da participación das informacións sobre as ameazas informáticas, as empresas que sufriron ataques, moitas veces, son remisas a revelalos temendo secuelas reputacionais e están dispostas a compartir os seus propios datos só en contextos que garantan confidencialidade e reciprocidade.

[14] Como sinalan KESAN, J.P. e HAYES, C.M., "Creating a 'Circle of Trust' to Further Digital Privacy and Cybersecurity Goals", *Michigan State Law Review*, 2014, pp. 1475 e ss.; BOSSONG, R. e 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, eles 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 o tema, véxase TADDEO, M., "Is Cybersecurity a Public Good?", *Minds & Machines*, n. 29, 2019, pp. 351-352.

estritas canto máis elevados son os riscos de manipulación das aplicacións e dos dispositivos tecnolóxicos proporcionados no mercado[16].

O obxectivo de construír unha arquitectura multinivel eficiente en materia de seguridade cibernética tradúcese, en segundo lugar, na definición de modalidades máis estruturadas e duradeiras de cooperación entre sector público e sector privado, en condicións de aproveitar de forma axeitada os coñecementos e as capacidades de análise deste 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 é como se pode entender a institución dalgunhas sedes privilexiadas de conexión, de matriz europea, como por exemplo: o Centro Europeo de Competencia Industrial, Tecnolóxica e de Investigación sobre a Ciberseguridade, que quere desenvolver os recursos e as competencias da Unión e quere reducir a súa dependencia de países terceiros, comprometendo as enerxías dos centros nacionais de coordinación (en Italia, o ACN), do mundo da industria e da universidade[18]; a Unidade Conxunta para o Ciberespazo (*Joint Cyber Unit*), como plataforma destinada a promover o intercambio de informacións, boas prácticas e coñecementos, así como a cooperación entre forzas da orde pública e de defensa, autoridades civís e diplomáticas, e sector privado en caso de severos ataques ou accidentes transfronteirizos[19]; a rede dos centros operativos de seguridade (SOC, *Security Operations Center)*, como *network* destinado a garantir unha supervisión constante, estendida e en tempo real, das intrusións e das anomalías informáticas nas redes e nos sistemas de diferentes portadores de interese, tamén a través da implicación das PMI da Unión[20]. Grazas a esta rede, en particular, refórzanse as capacidades de detección, de análise e de uso compartido dos datos relativos aos ataques *cyber* máis perigosos, permitíndolles ás autoridades públicas e aos suxeitos privados sinalar rapidamente ameazas potenciais e en marcha, antes de que estas causasen danos irreparables a grande escala.

Trátase de organismos e instrumentos que demostran a madura consciencia, por parte das institucións, da necesidade de establecer unha *governance* máis participativa para abordar do mellor xeito posible os difíciles desafíos para a seguridade postos en marcha pola difusión do ciberespazo. E isto, tendo en conta os importantes beneficios que se poden obter da contribución do mundo empresarial, polo menos baixo unha dobre perspectiva.

---

[16] De reforzo das obrigas de dilixencia exixibles por parte dos produtores e dos provedores das novas tecnoloxías falan, especialmente, a Comunicación conxunta do 13 de setembro de 2017, ***Resiliencia, disuasión e defensa: cara a unha ciberseguridade forte para a UE***, cit., par. 2.2; a Comunicación conxunta do 16 de decembro de 2020, ***A estratexia de ciberseguridade da UE para a década dixital***, cit., par. 1.5.

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

[18] Cfr. a normativa UE 2021/887, do 20 de maio de 2021, que lles encarga ás redes dos «Centros nacionais de coordinación» a tarefa de apoiar o Centro Europeo de Competencia para a Ciberseguridade na actividade de reforzo das capacidades, dos coñecementos e da competitividade da Unión no sector (art. 6 do regulamento).

[19] Cfr. a Comunicación conxunta do 16 de decembro de 2020, ***A estratexia de ciberseguridade da UE para a década dixital***, cit., par. 2.1.

[20] Cfr. a Comunicación conxunta do 16 de decembro de 2020, ***A estratexia de ciberseguridade da UE para a década dixital***, cit., par. 1.2.

En primeiro lugar, unha interlocución constante entre actores públicos e operadores privados en materia de ciberseguridade fomentaría un intercambio rendible de coñecementos especializados e de solucións operativas.

No contexto examinado, de feito, a creación dun sistema altamente centralizado e unilateral, en presenza de evidentes asimetrías informativas, está destinada a resultar ineficaz: por un lado, a acción capilar das ciberameazas e a complexidade da tecnoloxía no mercado fan que as empresas do sector sexan os suxeitos máis cualificados para entender as estratexias de ataque dos *hackers*, para detectar as principais vulnerabilidades escondidas nos *softwares* e para recomendarlles ás autoridades competentes as contramedidas máis apropiadas; por outro, a realización dun circuíto de supervisión e dun sistema de alerta distribuído –a.d.– (*distributed surveillance*), que se basea (tamén) na constante actividade de vixilancia realizada polos operadores económicos, pode reducir significativamente as ineficiencias e os custos administrativos soportados polos Estados membros debido á protección da seguridade cibernética nacional[21].

En segundo lugar, a implicación do sector empresarial sería extremadamente importante na elaboración e na actualización dos protocolos, das directrices e dos estándares de seguridade comúns, concretamente no ámbito da protección das infraestruturas e dos servizos considerados "críticos", xestionados, na maioría dos casos, por suxeitos privados.

Especialmente, a intervención destes últimos no proceso de determinación das políticas e das medidas vinculantes para todas as partes interesadas (*stakeholders*), proporcionaríalles, por suposto, ás autoridades competentes un soporte técnico valioso[22]; esta forma de colaboración permitiría, ademais, evitar o risco de perseguir ambiciosos obxectivos de resiliencia a través da introdución de cargas e requisitos inadecuados ou excesivos, incompatibles co principio de proporcionalidade e coa perspectiva liberal a preservar neste ámbito[23]. Como parece evidente, empresas e varias entidades fan fronte a ameazas, a vulnerabilidades e diferentes consecuencias; por conseguinte, unha verdadeira inclusión destes suxeitos nas sedes decisorias e consultivas non podería máis que fomentar a definición de ferramentas parametrizadas co determinado nivel de risco informático, apropiadas para contextos concretos en que operan as empresas e actualizadas con respecto ás innovacións tecnolóxicas formuladas.

Noutras palabras, a promoción de formas máis estables e estruturadas de cooperación entre actores públicos e privados permitiría non só un maior uso compartido

[21] CLARKE, A. e 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. e MARTINO, L., "Achieving robust European cybersecurity through public-private partnerships: approaches and developments", *Elf discussion paper*, n. 4, 2021, spec. pp. 7 e 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 contrapón, ao enfoque, en certa medida, dirixido polo lexislador europeo, o modelo liberal adoptado polos Estados Unidos de América. Segundo o autor, en particular, o paradigma americano, que funciona a nivel federal a través da *Cybersecurity and Infrastructure Security Agency* (CISA), caracterízase 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*».

de informacións, habilidades e boas prácticas, senón tamén unha desexable participación "desde abaixo" ao proceso regulatorio, limitando o tradicional enfoque "*command and control*" para fomentar formas de "*enforced self-regulation*"[24]. Como é sabido, tamén a nivel europeo, "para poder formular eficazmente unha política, cómpre entender con claridade a natureza e o alcance dos retos. Isto require non só datos estatísticos e económicos fiables e actualizados sobre os incidentes en detrimento da seguridade informática e sobre os niveis de confianza dos consumidores e dos usuarios, senón tamén datos actualizados sobre as dimensións e as tendencias en marcha no sector da seguridade das TIC en Europa"[25].

Estas consideracións lévannos inevitablemente a reflexionar sobre o marco institucional de protección da seguridade cibernética, establecido no noso ordenamento, no cal o intento de reproducir módulos organizativos e operativos, propios do sector *intelligence,* determinou un evidente déficit de participación dos operadores económicos do sector[26]. Unha elección lexislativa que, se se analiza a fondo, chama a atención, tamén se se ten en conta a ben coñecida adicción das administracións públicas italianas ás capacidades e ás experiencias no ámbito tecnolóxico-informático que ten o sector privado, que representou, e aínda representa, unha das principais causas dos atrasos rexistrados polo noso país no proceso global de transición dixital[27].

Aínda parecen limitadas e xenéricas, de feito, as referencias normativas que teñen en conta o valor estratéxico da dinámica cooperativa entre sector público e sector industrial. Faise referencia, por exemplo, ao art. 7 do DL do 14 de xuño de 2021, n. 82, que lle encarga ao ACN a tarefa de: "facer efectivos" as capacidades nacionais de prevención, supervisión, detección, análise e reacción aos ataques informáticos, mesmo a través do recurso a iniciativas de colaboración do sector público-privado[28]; de promover, por medio da implicación das universidades e do sistema produtivo, o desenvolvemento de competencias e de capacidades industriais, tecnolóxicas e científicas[29], mesmo en calidade de centro nacional de coordinación, de conformidade co mencionado artigo 6 do regulamento UE 2021/887; de constituír colaboracións,

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

[25] Cfr. a Comunicación da Comisión Europea do 31 de maio de 2006, *Unha estratexia para unha sociedade da información segura. Diálogo, asociación e responsabilización*, COM (2006) 251, par. 3.2.1., coa que a Comisión lle pediu a ENISA desenvolver unha cooperación de confianza cos Estados membros e as partes interesadas, co fin de crear un sistema europeo de uso compartido das informacións e de alerta, así como de fomentar un espazo axeitado para a recompilación e a análise dos datos sobre os incidentes e os ataques cibernéticos na Unión.

[26] Sobre estes perfís, véxanse 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 e ss.

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

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

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

consorcios, fundacións ou sociedades, con suxeitos públicos ou privados, para a mellor realización das súas finalidades institucionais[30].

Como se indicou, mentres noutros países, como Francia e Alemaña, se asistiu á creación de organismos específicos, que reúnen representantes das administracións públicas e do mundo empresarial para realizar traballos de análise, planificación e elaboración de tendencias normativas en materia de ciberseguridade, en Italia, a colaboración cos privados foi, ata agora, principalmente de carácter financeiro e dirixida ao desenvolvemento de tecnoloxías e infraestruturas dixitais[31].

O marco regulamentario que se acaba de indicar leva a acoller con satisfacción as interesantes propostas contidas na recente estratexia italiana sobre a ciberseguridade 2022-2026 e no correspondente plan de implementación de maio de 2022; a través destes documentos, ademais dos necesarios investimentos no factor "desenvolvemento", pénsase garantir unha implicación máis efectiva no sector privado na persecución dos obxectivos de "protección", por un lado, e de "resposta", por outro, cara ás trampas da dimensión cibernética.

En concreto, en canto ao primeiro obxectivo, a estratexia e o plan de implementación aspiran a potenciar o sistema nacional de "escrutinio tecnolóxico", que depende do Centro de Avaliación e Certificación Nacional (CVCN) instituído no ACN, e, nos ámbitos de competencia, depende dos Centros de Avaliación do Ministerio do Interior e de Defensa. Para tal fin, prevese a introdución dunha rede de laboratorios acreditados de proba (a.d. LAP), como suxeitos, públicos e privados, chamados para facilitar os procedementos de certificación de calidade dos recursos (*asset*) tecnolóxicos utilizados polos suxeitos incluídos no PSNC e para detectar as correspondentes vulnerabilidades[32].

Ao mesmo tempo, as accións mencionadas destacan a necesidade de aproveitar ao máximo as capacidades nacionais de identificación e de resposta cara aos ciberataques, establecendo dúas formas diferentes de colaboración para os operadores económicos do sector.

A primeira, de carácter estrutural, refírese á implantación dunha rede de centros sectoriais de análise e de intercambios de informacións relevantes (*Information Sharing and Analysis Center, ISAC*) creada para axudar ás oficinas do ACN a ofrecer e a difundir boas prácticas, directrices, avisos de seguridade e recomendacións dentro do país.

A segunda, de carácter ocasional, contempla a implicación directa de empresas oportunamente cualificadas en materia de resposta ante incidentes (*incident response*), de apoio nas funcións institucionais do CSIRT Italia, en caso de que se verificase "unha cantidade importante de ciberincidentes de carácter sistémico". Con iso, Italia demostra a vontade de utilizar, xunto con axeitadas estratexias de resiliencia, tácticas eficaces de defensa activa (*active defense*), co propósito de desenvolver, aproveitando

[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 e ss.

[32] Sobre isto, remítese ás previsións do DL do 3 de agosto de 2022, n. 123.

múltiples fontes de datos relevantes e de actores responsables, formas compartidas e rápidas de xestión de crise e contraataque[33].

Trátase de novidades que se espera implementar aínda máis, debido aos relevantes efectos disuasorios e preventivos exercidos por estes instrumentos cara ás operacións de intrusión e de manipulación realizadas polos criminais informáticos.

3 Factor humano, cultura da seguridade cibernética e "inmunidade de grupo"

O avance repentino do proceso de informatización das relacións económicas e sociais rexistrado nos últimos anos exixe, sen dúbida, unha reconsideración do papel dos cidadáns usuarios dentro dos sistemas nacionais de protección da ciberseguridade. Esta afirmación pódese demostrar doadamente empezando pola simple consideración das novas ameazas para a seguridade colectiva que derivan da difusión, a nivel internacional, daqueles dispositivos e aparellos, dotados de sensores interconectados e interactivos, que pertencen ao amplo conxunto da *Internet das cousas*: un fenómeno que está determinando, con respecto ao pasado, un aumento vertixinoso das superficies de ataque e o número de obxectivos (*target*) afectados[34]. É posible sacar conclusións análogas poñendo atención na crecente expansión da a.d. economía cibercriminal, que viu florecer co tempo un auténtico mercado en liña (polo xeral, na Internet escura) de produtos e servizos especificamente dirixidos a consumir perigosos ataques informáticos, segundo o concepto de "*crime as a service*"[35].

Trátase de elementos que conducen a reflexionar non só sobre o feito de que os actos de criminalidade informática xa poidan ser perpetrados a prezos moderados por suxeitos particularmente inexpertos na utilización das tecnoloxías[36], senón tamén sobre a urxente necesidade de actuar para mellorar o nivel de alfabetización dixital e conciencia dos usuarios da rede.

---

[33] Sobre o papel estratéxico que xoga a elaboración de axeitadas tácticas de defensa activa, véxanse 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 e ss.

[34] Sobre as novas problemáticas xurídicas relacionadas coa aparición do fenómeno do *Internet of Things,* véxanse WEBER, R.H. e STUDER, E., "Cybersecurity and the Internet of Things: Legal Aspect", *Computer Law & Security Review*, n. 36, 2016, pp. 726 e ss.; RAYES, A. e 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 isto, BRIGHI, R. e 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 a relevancia e as motivacións económicas de organizacións criminais estruturadas como unhas verdadeiras empresas, que ofrecen no mercado *softwares* listos para usar e que non necesitan específicas habilidades informáticas por parte dos compradores. Con respecto ao concepto do "*Crime as a Service*", véxase a interesante análise de PAGANINI, P., "Cybercrime-as-a-Service: EU Perspectives", Martino, L. e Gamal, N. (dirs.), *European Cybersecurity in Context. A Policy-Oriented Comparative Analysis*, Elf study, Brussels, 2022, pp. 67 e ss.

[36] Sobre a criminalidade informática e sobre as problemáticas de dereito penal relacionadas, véxanse para todos AMATO MANGIAMELI, A.C. e SARACENI, G. (dirs.), *I reati informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli, Torino, 2019.

A necesidade de valorar as obrigas e as responsabilidades dos usuarios das infraestruturas e dos sistemas dixitais constitúe desde hai moito tempo un obxectivo das políticas europeas de protección da seguridade informática.

Sobre a cuestión indicouse como a "seguridade das redes e da información é responsabilidade común de todas as partes interesadas, mesmo dos operadores, dos provedores de servizos, dos provedores do *hardware* e do *software*, dos usuarios finais, dos entes públicos e dos gobernos nacionais"[37]; polo tanto, "todos os actores involucrados, sexan autoridades públicas, sector privado ou cada cidadán, deben recoñecer esta responsabilidade compartida, deben activarse para protexerse e, se é necesario, deben garantir unha resposta coordinada para fortalecer a ciberseguridade"[38].

A nivel normativo, non obstante, as recomendacións mencionadas só atoparon unha resposta concreta hai pouco: ao principio, por medio de previsións dirixidas a obrigar os Estados membros a introducir, nas respectivas estratexias nacionais, programas específicos de formación e de actualización profesional[39]; logo, por medio do reforzo das funcións institucionais da Axencia da Unión Europea para a Ciberseguridade (*European Union Agency for Network and Information Security*, en diante ENISA), encargada de promover unha maior conciencia das organizacións públicas, das empresas e dos cidadáns da Unión en materia de ciberseguridade, así como de asesorar os Estados membros nas súas iniciativas de instrución e de sensibilización colectiva[40].

Baixo estas intervencións subxace a constatación do feito de que certo nivel de risco de seguridade se atopa inevitablemente nas modernas sociedades dixitais; «*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 than defense in cyberspace*»[41]. De aquí a necesidade de ver, na implicación directa da sociedade civil, unha formidable arma de prevención dos incidentes e dos ataques informáticos, co intento de desenvolver esa "inmunidade de grupo" indispensable para conter o risco cibernético por debaixo dos niveis admisibles[42].

En concreto, máis alá das alegacións das teorías económicas que consideran a solidez das redes e dos *softwares* como un verdadeiro ben público[43], a introdución de políticas e medidas que teñen o obxectivo de limitar os erros imputables ao a.d.

[37] Cfr. a Resolución do Consello do 18 de decembro de 2009 *Un enfoque cooperativo en materia de seguridade das redes e da información*, 2009/C 321/01, par. 3.

[38] Cfr. a Comunicación conxunta do 7 de febreiro de 2013 *Estratexia de ciberseguridade da UE: un ciberespazo aberto e seguro*, cit., par. 1.2.

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

[40] Art. 4, apartados 7 e 10 do regulamento UE 2019/881. A institución da Axencia realizouse a cargo do Regulamento CE 460/2004, do 10 de marzo 2004.

[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] Véxanse, entre outros, GRADY, M.F. e 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 e ss.; BRIGHI, R. e CHIARA, P.G., "La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione europea", cit., pp. 25 e ss.

"factor humano", permitirían obter vantaxes prácticas, que se aprecian polo menos por unhas razóns tripartitas.

En primeiro lugar, unha maior información á opinión pública con respecto ás principais tipoloxías de ameazas, ás correspondentes modalidades de detección e aos instrumentos de resposta, que a normativa prevé, contribuiría a reducir a eficacia dos ataques menos sofisticados.

Neste sentido, a consolidación de oportunas normas de "hixiene informática", doadas de comprender e replicar mesmo para quen non ten unha preparación especializada (como aquelas relativas aos sistemas de autenticación, ás copias de seguridade e de recuperación ou á instalación de *antivirus* e *firewall*) permitiría deseñar un sistema, se non completamente seguro, si capaz de facer fronte aos perigos do ciberespazo máis comúns e coñecidos[44]. Isto daríalles ás autoridades públicas a posibilidade de concentrar os seus propios recursos cara aos suxeitos máis indefensos, como os usuarios maiores ou moi novos, moitas veces dotados de escasas competencias básicas de informática e, polo tanto, aínda máis expostos ao risco de caer en trampas virtuais dispostas por criminais profesionais.

En segundo lugar, un maior intercambio de boas prácticas (*best practices)* e de directrices de comportamento en liña determinaría un desexable incremento do número das comunicacións e dos avisos por parte dos usuarios.

Esta circunstancia contribuiría non só a establecer unha relación máis directa entre os destinatarios dos ataques e os órganos administrativos encargados da atención e da axuda, senón tamén a proporcionar unha mellor comprensión do nivel de difusión das ameazas e das modalidades de ataque dos *hackers*. Estes últimos, de feito, a través de complexos sistemas de enxeñaría social, destinados a aproveitarse da inxenuidade dos individuos, agora son capaces de introducirse en moitos *servers*, apoderarse deles e afectar a obxectivos (*target*) de considerable relevancia, sen arriscarse a que as autoridades policiais os detecten[45]. Por esta razón, ademais do perfil da seguridade exterior, as modernas estratexias de ciberseguridade deberían prestar especial atención ás vulnerabilidades relacionadas coa seguridade interior[46].

Por último, un apoio económico constante e operativo en favor de iniciativas no ámbito da formación cibernética facilitaría considerablemente a creación dunha verdadeira cultura da seguridade e do risco informático.

Un obxectivo que –malia representar unha das tarefas da ENISA[47] e, por último, da ACN[48], mesmo a través da activación de cursos universitarios específicos e da

---

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

[45] Pénsese no acontecido a algúns xuíces da Corte dei Conti en setembro de 2022. Eles foron vítimas dunha insidiosa operación de suplantación de identidade (*phishing*), que empezou co envío dunha mensaxe, que contiña a solicitude duns datos e ao parecer enviada do teléfono profesional dun compañeiro, ao seu propio móbil. Contestando a mensaxe, os xuíces permitíronlles de feito aos criminais informáticos o acceso aos contactos da súa propia rúbrica e ás súas conversacións de WhatsApp, onde se atopaban 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, par. 1, let. j), Regulamento CE 460/2004, do 10 de marzo de 2004.

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

asignación de bolsas de estudos e de investigación ou doutoramentos[49] – aínda parece lonxe de realizarse plenamente, sobre todo no noso ordenamento.

Ao respecto, téñase en conta que, como afirma o recente informe Censis-*Deepcyber* de abril de 2022[50], o 40 % dos cidadáns italianos permanece indiferente ou non se protexe en absoluto contra os ataques informáticos; segundo esta investigación, ademais, só o 24,3 % dos italianos declara que coñece concretamente o significado da palabra ciberseguridade, mentres que o 58,6 % declara que coñece o tema a grandes trazos e o 17,1 % declara que non sabe que é.

Tamén por estes motivos, no ámbito da nomeada estratexia italiana 2022-2026, se indican expresamente a formación e a promoción da cultura en materia de ciberseguridade como "factores habilitadores" necesarios para o alcance das finalidades de protección, de resposta e de desenvolvemento nela recollidas.

Ao respecto, a dita documentación remarca a exixencia de actuar con dúas principais intervencións.

Por un lado, establécese un programa capilar de educación dixital para todos os niveis de educación escolar, co obxectivo de estimular, nos usuarios máis novos, a elección de boas condutas no espazo cibernético e de desenvolver novas profesionalidades nas carreiras técnico-científicas, mesmo co obxectivo de reducir a distancia relativa ás competencias con respecto doutros países.

Por outro lado, a estratexia propón a organización de cursos de formación especializada adecuados e de actualizacións profesionais, dirixidos aos empregados das administracións públicas e aos dos entes privados, grandes ou pequenos, con especial atención aos que ocupan posicións apicais. A estas últimas, de feito, corresponderalles establecer eficaces plans de xestión interior do risco cibernético e proporcionar axeitados mecanismos de mitigación e de aviso, mesmo a través de operacións de autoavaliación do seu propio nivel de exposición.

Está claro que a efectiva realización destes obxectivos, dirixidos a reducir os descoidos e os erros máis comúns dos operadores e dos usuarios da dimensión cibernética, implicará custos elevados; non obstante, se é certo que o elo máis débil da cadea de seguridade está representado xusto polo factor humano, entón "non facer nada tería custos moito máis elevados"[51].

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

[50] Cfr. o informe Censis-*Deepcyber*, do 22 de abril de 2022, *Il valore della cybersecurity*, dispoñible en *www.censis.it*. Aos datos contidos neste informe hai que lles engadir aqueles referidos na edición do 2022 do Índice europeo de dixitalización da economía e da sociedade (*Digital Economy and Society Index*, DESI), que coloca Italia na posición 18 e, polo que se refire ao capital humano, na posición 25 entre os 27 Estados membros, posto que só o 46 % dos cidadáns italianos de entre os 16 e os 74 anos ten polo menos coñecementos dixitais básicos.

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

4 Patróns de colaboración entre sector público e privado e perspectivas de *iure condendo*

Nos parágrafos anteriores púxose en evidencia a necesidade de promover unha maior colaboración entre público e privado nos sistemas nacionais de seguridade cibernética, como medida fundamental de prevención e de reacción ante o significativo aumento dos incidentes e dos ataques informáticos rexistrados a nivel mundial.

Como se sinalou, o logro deste resultado está completamente avalado polas recentes directrices europeas en temas de ciberseguridade, que implican todos os compoñentes da sociedade na construción dunha "Unión da seguridade verdadeira e eficaz"[52], que se basea en instrumentos, coñecementos e actitudes, comúns e compartidos, impulsados mesmo pola mencionada directiva UE 2022/2555, a.d. directiva NIS 2[53].

Para poder aproveitar ao máximo os mencionados beneficios que proceden da actuación do achegamento "*whole of society*" de matriz supranacional –cuxo valor xa é recoñecido mesmo no ordenamento xurídico italiano– parece importante actuar, en particular, en dous aspectos problemáticos fundamentais.

En primeiro lugar, unha vez recoñecido que «o dereito do risco perfila patróns relacionais baseados máis que en mecanismos de "*command and control*" ou total "autoadministración" privada, na integración e na cooperación entre público e privado»[54], non parece posible deixar a aplicación do novo paradigma exclusivamente en mans da mera adhesión voluntaria dos suxeitos interesados. En cambio, sobre todo na fase de experimentación das novas propostas, sería necesario fixar con que modalidades e en que límites a colaboración debe realizarse. Iso implica, por exemplo, a conclusión de acordos contractuais destinados a aclarar os incentivos económicos, a repartición dos riscos, as condicións de privacidade e as cláusulas de exención das responsabilidades para as empresas do sector[55].

---

[52] Cfr. a Comunicación da Comisión Europea do 24 de xullo de 2020, *Estratexia da UE para a Unión pola Seguridade*, COM (2020) 605 final, par. 3, onde se reafirma que: «[...] a cooperación co sector privado é fundamental, tanto máis que a industria conta cunha parte importante da infraestrutura dixital e non dixital indispensable para loitar de forma eficaz contra a criminalidade e o terrorismo. Igualmente, cada individuo pode achegar a súa contribución, creando por exemplo competencias e conciencia para combater a criminalidade informática ou a desinformación».

[53] A nova acción intervén para aclarar e ampliar o alcance da anterior disposición UE 2016/1148, e, desde o punto de vista subxectivo, facendo referencia á detección dos suxeitos involucrados na cadea de xestión do risco cibernético, e, desde o punto de vista obxectivo, facendo referencia ás obrigas de aviso e de seguridade. É interesante sinalar, por un lado, como a Comisión Europea expresamente cualificara os entes da Administración pública, central e rexional (agás os que desenvolven as súas actividades «nos sectores da seguridade nacional, da seguridade pública, de defensa, mesmo a prevención, a investigación, a comprobación e a persecución dos crimes»), como suxeitos que operan en sectores "de alta criticidade", e, por outro, como a mesma Comisión ampliase o ámbito de aplicación da disposición mesmo ás PMI, en caso de que estas últimas se consideren esenciais para a vida económica e social dun Estado membro.

[54] Sobre isto, BARONE, A., *Il diritto del rischio*, Giuffrè, Milano, 2006, pp. 64 e ss.

[55] Sobre o tema, véxanse BOSSONG, R. e WAGNER, B., "A Typology of Cybersecurity and Public-Private Partnerships in the Context of the European Union", cit., p. 284, que subliñan 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*».

Dito doutro xeito, se 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 outro «*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 a importancia da cooperación nos sectores da investigación e da innovación –obxecto, non por casualidade, do primeiro acordo de colaboración estipulado nesta materia en sede europea[57]–, a atención do lexislador nacional debería dirixirse aínda máis a regulamentar formas máis estables e articuladas de colaboración.

Ao respecto, cabe destacar como a ENISA invitou varias veces os Estados membros a investir nesta dirección, identificando, en particular, catro paradigmas principais xa presentes en Europa[58]: I) o *Institucional PPP,* destinado a garantir a protección de institucións e infraestruturas críticas a través dunha cooperación a longo prazo entre os interesados, que se cumpre, por exemplo, no desenvolvemento de actividades de soporte operativo, de análise de datos, de elaboración de boas prácticas, de control dos estándares de seguridade e doutros servizos[59]; II) o *Goal-oriented PPP*, destinado a promover a cultura da seguridade informática nos Estados membros a través da constitución de centros e de grupos de intercambio de coñecementos e de solucións prácticas sobre argumentos concretos[60]; III) o *Service outsourcing PPP*, útil para presentar *ás* autoridades públicas competentes as problemáticas cibernéticas máis importantes nun sector empresarial específico e a suxerir, por conseguinte, os oportunos actos normativos e de orientación que deben adoptarse para solucionalas[61]; o *Hybrid PPP*, que constitúe unha combinación do primeiro e do terceiro patrón, moitas veces utilizado para deixar en mans de entes privados cualificadas funcións e tarefas que as mesmas institucións nacionais non están á altura de exercer, como as inherentes ás actividades de aviso e de resposta en caso de ataques cibernéticos[62].

A elección do patrón de colaboración que se debe implementar déixase, en realidade, a cada Estado membro, posto que «*there is no universal, simple solution that applies*

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

[57] Trátase do Acordo de cooperación público-privada sobre a ciberseguridade do 5 de xullo de 2016, promovido pola Comunicación da Comisión Europea do 6 de maio de 2015, *Estratexia para o mercado único dixital en Europa,* COM (2015) 192 final, par. 3.4., con que se instaurou unha cooperación máis estable entre suxeitos diferentes, públicos e privados, interesados en promover a investigación e a innovación no ámbito cibernético, promover a industria europea da seguridade informática e introducir solucións innovadoras e fiables (produtos, servizos e *software* TIC) nalgúns sectores estratéxicos da Unión (*i.e.*, enerxía, sanidade, transportes, finanzas). En concreto, o acordo recibiu un investimento por parte da Unión Europea, no marco do programa Horizonte 2020, de 450 millóns de euros, mentres os investimentos dos operadores do mercado da ciberseguridade, representados pola Organización Europea para a Seguridade Informática (ECSO), foron tres veces maiores, para un total de aproximadamente 1,8 miles de millóns entre o 2016 e 2020.

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

[59] Trátase do patrón difundido en Estonia e en Polonia.

[60] Trátase do patrón presente en España, Reino Unido, Luxemburgo, Holanda, Austria e Eslovaquia.

[61] Trátase do patrón que se atopa en Alemaña e en Austria.

[62] Patrón presente, por exemplo, na República Checa.

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].

Tendo en conta estas consideracións, é posible destacar a exixencia de introducir sucesivas fases e modalidades de implicación da clase privada-empresarial no ámbito da arquitectura italiana de tutela da seguridade cibernética, en especial na determinación das políticas, dos procedementos, dos estándares, das medidas e contramedidas máis importantes na materia[64].

Parecen inadecuadas para asegurar este obxectivo, de feito, as previsións normativas actualmente vixentes, que contemplan a mera participación sen dereito de voto ás reunións do Núcleo para a Ciberseguridade dos «suxeitos públicos ou privados eventualmente interesados» en situacións de crise de natureza cibernética[65] e que deixan en mans do ACN a tarefa de establecer «cun regulamento propio» os niveis mínimos de seguridade, de capacidade de elaboración, de aforro enerxético e de fiabilidade das infraestruturas dixitais da Administración pública[66], ademais de promover, en xeral, a creación de actuacións de colaboración.

De aí a contraproba do feito de que, a pesar da retórica da transición dixital, aínda poida ser difícil para un Estado esa «confesión de fracaso»[67] ao regulamentar e tutelar con autonomía e con recursos propios a seguridade pública no ciberespazo.

Bibliografía

AMATO MANGIAMELI, A.C. e 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. e Raffiotta, E.C. (dirs.), *AI Anthology*, Il Mulino, Bologna, 2022.

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

[64] Sobre a necesidade de promover, na Unión, un sistema de ciberseguridade aberto á participación e á colaboración dos actores privados, mesmo co fin de facilitar o alcance do obxectivo n. 16 da Axenda ONU 2030 para o Desenvolvemento Sostible, dedicado á promoción de sociedades pacíficas e inclusivas, así como á construción de institucións responsables e eficaces a todos niveis, véxanse 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] Artigo 10, apartado 3, DL n. 82/2021. O Núcleo para a ciberseguridade (en orixe, Núcleo para a Seguridade Cibernética) foi implantado polo DPCM n. 66/2013, co fin de coordinar a acción de todos os suxeitos involucrados na preparación e na xestión das situacións de crise e activar os eventuais procedementos de alerta e de resposta. Desde 2021 o Núcleo opera na Axencia Nacional para a Ciberseguridade.

[66] Artigo 33-*septies*, apartado 4, DL do 18 de outubro de 2012, n. 179, conversión con modificación da Lei do 17 de decembro de 2012, n. 221.

[67] MONTI, A., "Internet e ordine pubblico", Cassano, G. e Previti, S. (dirs.), *Il diritto di internet nell'era digitale*, Giuffrè, Milano, 2020, p. 75. Sobre as inevitables dificultades que os poderes públicos atopen en regulamentar as conexións e relacións humanas que teñen lugar no espazo virtual, véxanse, por último, MANNONI, S. e 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.

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

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

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. e PARISI, F., *Law and Economics of Cybersecurity*, Cambridge University Press, Cambridge, 2005.
KESAN, J.P. e 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. e STAZI, G., *Sovranità.com. Potere pubblico e privato ai tempi del cybers-pazio*, Editoriale scientifica, Napoli, 2021.
MELE, S., "Il Perimetro di sicurezza nazionale cibernetica e il nuovo «golden power»", Cassano, G. e 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. e 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. e 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. e 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. e 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. e 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. e Perri, P. (dirs.), *Tecnologia e diritto*, vol. III, Giuffrè, Milano, 2019.