Computer Law & Security Review 61 (2026) 106341

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

The Cyber Resilience Act as another brick in the (useless) wall against the spreading of the spyware market in the EU?

Pier Giorgio Chiara [a,#,*], Aljosa Ajanovic [b]

[a] University of Bologna, Department of Law and CIRSFID Alma AI Research Center, Italy
[b] Policy Advisor at European Digital Rights (EDRi), Belgium

ARTICLE INFO

Keywords:
Cyber Resilience Act
EU cybersecurity
Spyware
EU law
Data protection
Fundamental rights

ABSTRACT

The expansion of the spyware market within the European Union reveals a structural contradiction in EU law and policy. While the European Union has strengthened product cybersecurity through the Regulation (EU) 2024/2847 (Cyber Resilience Act, CRA), it continues to tolerate the consolidation of a spyware market benefiting from the internal market legal and economic infrastructure, while inherently exploiting and preserving the very vulnerabilities in products with digital elements that the CRA is intended to reduce. This article examines whether, and to what extent, the Cyber Resilience Act (CRA) can be used to address that contradiction by casting light on three legal challenges. First, can spyware qualify as a product with digital elements within the meaning of the CRA? Second, how far does the Regulation's national security exemption limit that possibility, particularly where spyware is developed, procured, or deployed by state actors? Third, can the CRA's market surveillance and enforcement framework, especially Article 57, realistically be implemented against spyware products that pose significant cybersecurity risks and risks to compliance with Union rules protecting fundamental rights? The article argues that at least some types of spyware fall within the CRA's material scope and that the Regulation may offer a lever for restricting their circulation on the Union market. At the same time, it shows that the CRA's applicability, and above all the practical reach of its enforcement regime, is constrained by expansive national security claims, the opacity surrounding state deployment, and the limited willingness of competent authorities to act in politically sensitive cases. More broadly, it shows why any serious EU response must also turn on a narrower reading of national security exceptions and more credible enforcement structures.

1. Introduction

The shocking revelations around the use of Pegasus spyware have cast a spotlight on the growing threat posed by commercial surveillance technologies. Far from being isolated to authoritarian regimes, the spyware market is rapidly expanding within the European Union itself, either because companies are establishing in EU Member States like Greece, Bulgaria, and Cyprus, or because they are relocating to the EU to benefit from regulatory ambiguity.[1] The surge of this market is fuelled in part by a lucrative vulnerability market, in which software flaws are traded as commodities, often with little transparency.[2] The absence of coordinated vulnerability disclosure frameworks and public bug bounty programs across the EU further compounded the issue, allowing security gaps to be quietly exploited rather than responsibly reported and

* Corresponding author.
E-mail addresses: piergiorgio.chiara2@unibo.it (P.G. Chiara), aljosa.ajanovic@edri.org (A. Ajanovic).

Pier Giorgio Chiara's work was supported by the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union –NextGenerationEU. While the research results are based on a combined effort, Sections 1, 3 and 4 should be attributed to Pier Giorgio Chiara.

[1] European Parliament - Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, Report of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI)) (2023) available at: <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/05-08/REPORTcompromises_EN.pdf>, last accessed 26 March .

[2] O. L. van Daalen et al., 'Export control of cybersurveillance items in the new dual-use regulation: The challenges of applying human rights logic to export control' (2023) 48 Computer Law & Security Review, 1.

https://doi.org/10.1016/j.clsr.2026.106341

Available online 12 May 2026

patched.

Against the background of spyware definitions provided by the US government[3] or the EU, either by ENISA, as endorsed by the EU Parliament PEGA Committee[4] or relevant legislation,[5] for the purpose of this paper, 'spyware' is used as a functional and umbrella term for software that: 1) it is installed or run on a device without the free and informed consent of the user; 2) it compromises the integrity of the device by modifying, temporarily or permanently, one or more elements of the device, internal chips or storage drives; 3) its deployment is primarily facilitated by exploiting existing or created vulnerabilities in digital systems; 4) after installation, its operation (i.e. giving commands) is performed either automatically or remotely; 5) it can be targeted at individuals or groups, or deployed indiscriminately.[6] Compared to the definition provided in the Dual-Use regulation or in the European Media Freedom Act, this paper adopts a more granular analytical category by taking into account technical specifications of modern spyware (e.g., automatic or remote operation; indiscriminate deployment; etc.).

Building on that definition, there is a substantial difference between spyware and traditional means of interception of electronic communications. While law enforcement authorities have long relied on interception measures, such as wiretapping, these tools remain, at least in principle, targeted, functionally limited and subject to strict procedural guarantees. Spyware is fundamentally different from traditional interception because it operates from within the target device, transforming it into a constant and invisible surveillance tool capable of accessing *all* data and functionalities, including information stored on the device and not 'merely' communications in transit. Furthermore, spyware may grant operators the ability not only to extract but also to manipulate data on the infected device, as well as to erase its traces.[7] The potential of spyware to compromise the integrity of the device raises serious concerns not only for confidentiality but also for the integrity of information.[8] By contrast, traditional interception remains external, targeted, and limited in time, place, and communication channels, making it more readily amenable to necessity and proportionality assessments.

As highlighted in the technical analysis of the European Parliament study by Sartor and Loreggia,[9] this novel form of surveillance enables continuous and comprehensive monitoring of a person's digital environment. Spyware deployment and operation also involve a broader ecosystem of actors, not only law enforcement or state authorities, therefore increasing third-party risks of abuse. Thus, spyware poses not only systemic security risks by undermining the integrity of digital infrastructures, but also severe threats to fundamental rights and democratic processes, given proven cases of abuse against journalists, human-rights defenders, political opponents, and civil society.[10]

The invasiveness of *some* of spyware peculiar characteristics, and their difference from traditional means of interception, were partially tackled by the French Constitutional Court, where it ruled that measures allowing, for example, the remote activation of phone cameras and microphones with the potential of recording "in any place… including homes" and even capturing third parties, create a massively intrusive, continuous form of surveillance far beyond wiretaps or physical bugs.[11] Notably, the Court ruled that because remote activation could be used for all offences within organised delinquency or organised crime, and not just the most serious ones, the infringement on the right to private life was disproportionate to the intended goal. Consequently, the contested legislation was found to be contrary to the Constitution.[12]

The novelty and evolving nature of this technology, its fundamental difference to traditional wiretapping when it comes to the potential and far-reaching implications for human rights and due process justifies calls for specific regulatory intervention. This position is defended by EU policymakers, which agreed that "the trade in and use of spyware needs to be regulated strictly[13]", and by EU civil society organisations, which have called repeatedly for the ban on both spyware use and trade.[14] As most EU Member States lack legislation specifically authorising the use of such tools, spyware currently operates within a patchwork of pre-existing legal frameworks that were not designed to address its distinctive features, and that are not being properly enforced to deal with the harms it produces.

This need for regulation must also be understood in light of the rapid evolution of spyware within a broader ecosystem of cyber intrusion capabilities. Initially developed as targeted tools for lawful interception, spyware has increasingly become part of a commercialised and globalised market of "cyber intrusion capabilities," including exploit marketplaces, intrusion-as-a-service models, and privately developed surveillance tools. These capabilities enable remote access to and manipulation of devices without authorisation and are now widely traded across jurisdictions. From 2011 to 2023, at least 74 states reportedly procured commercial spyware, illustrating both the scale of proliferation in its use and the growing role of private actors in supplying such technologies.[15] As argued by Sheniak, "companies now often sell discrete components -such as zero-day exploits, code execution modules, or data extraction capabilities - rather than complete

[3] A broad definition of spyware is provided in the United States' Executive Order 14093, whereby spyware is defined as any software enabling "remote access to a computer, without the consent of the user, administrator, or owner".

[4] Spyware is defined as a type of malware that spies on a users' activities without their knowledge or consent. These spying activities can include key-logging, activity monitoring, and data collection, as well as other forms of data theft. Spyware is usually spread as a trojan, or by exploiting software vulnerabilities. See European Parliament (n 1).

[5] Regulation (EU) 2021/821 (Dual-use Regulation) defines at Art. 2, point 20, cyber-surveillance items as "dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems".

[6] EDRi, Spyware and state abuse: the case for an EU-wide ban (2025), 7, available at: <https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/>, last accessed 2 April .

[7] A. Caruso, 'Forensic Analysis of Mobile Spyware: Investigating Security, Vulnerabilities, and Detection Challenges in Android and iOS Platforms' (2024) Master's Degree Thesis in Computer Engineering, Politecnico di Torino, available at: <https://webthesis.biblio.polito.it/33137/> last accessed 10 April .

[8] E. Liu et al., 'No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps' (2023) Proceedings on Privacy Enhancing Technologies Symposium, 1, 218; F. Pierazzi et al., 'A Data-Driven Characterization of Modern Android Spyware' (2020) 11 ACM Transactions on Management Information Systems 1.

[9] G. Sartor and A. Loreggia, 'The impact of Pegasus on fundamental rights and democratic processes' (2023) Study requested by the European Parliament's Committee of Inquiry to investigate the Use of Pegasus and Equivalent Surveillance Spyware (PEGA), available at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf>, last accessed 10 April .

[10] European Parliament Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, recital A.

[11] Conseil Constitutionnel, Décision n° 2023-855 DC du 16 novembre 2023, para. 68, available at: <https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2023-855-dc-du-16-novembre-2023-communique-de-presse> last accessed 03 April .

[12] Ibid., para. 68-69.

[13] European Parliament (n 10), recital 28.

[14] Access Now, ARTICLE 19, Centre for Democracy & Technology Europe (CDT Europe), Civil Liberties Union for Europe (Liberties), EDRi, Privacy International et al., 'Civil Society Joint Statement of the Use of Surveillance Spyware in the EU and Beyond' (2024) available at: <https://ifex.org/wp-content/uploads/2024/09/civil-society-coalition-calls-for-urgent-eu-action-against-spyware-threats.pdf> last accessed 10 April .

[15] S. Herpig, A. Paulus, 'The Pall Mall Process on Cyber Intrusion Capabilities' (2024) Lawfare, available at: <https://www.lawfaremedia.org/article/the-pall-mall-process-on-cyber-intrusion-capabilities> last accessed 10 April .

surveillance solutions".[16] This fragmentation of the spyware supply chain makes "traditional regulatory approaches […] increasingly obsolete".[17] The role of spyware within this fragmented regulatory landscape will be the subject of our analysis.

Against this backdrop, the EU adopted the Regulation (EU) 2024/2847 (Cyber Resilience Act, CRA),[18] which entered into force on 10 December 2024,[19] to strengthen the cybersecurity and resilience of products with digital elements available on the Internal Market and protect consumers and digital (critical) infrastructure from incidents. Here lies a paradox: how can the EU credibly demand rigorous cybersecurity, transparency, and accountability from private actors while some operators, which are often financed or procured by national governments and EU institutions,[20] actively undermine those same principles through spyware production and deployment? The EU Cyber Resilience Act aspires to build a solid 'wall' of cybersecurity, while cracks in that wall are actively carved from within by a tolerated spyware industry with direct, proven links to EU member states themselves.[21]

While recent scholarship has approached spyware primarily through the lenses of export control and dual-use regulation, data protection and privacy, media freedom, and the broader constitutional and international governance of digital surveillance, the CRA has received much less attention as a possible, though indirect, regulatory lever in this field. This article builds on the existing literature but shifts the focus to a different question: whether a product-cybersecurity instrument introducing significant enforcement measures against products presenting significant cybersecurity and fundamental rights risks can constrain the commercial spyware market alongside data processing-focused frameworks.[22]

Bearing this paradox in mind, Section 2 assesses the shortcomings of relevant EU legislation in addressing the trade in and use of spyware products in the EU, and how it is not equipped to deal with the human rights impacts of their use on EU citizens. Then, Section 3 explores whether and to what extent the recently adopted Cyber Resilience Act (CRA) can be leveraged to close the aforementioned paradox by restricting the spyware market in the EU, in particular, by taking into account three legal challenges. The first legal challenge aims to clarify whether and to what extent spyware technologies are 'products with digital elements' (PDE) within the admittedly large scope of the CRA. Building on that, the second legal challenge problematises the national security exemption of the CRA which could cover spyware development, acquisition and use. The third legal challenge hinges on the effectiveness of CRA public enforcement mechanisms in the specific context of the spyware market as products with digital elements which, while compliant with the CRA's cybersecurity requirements, may still trigger investigations by national market surveillance authorities (or the Commission – provided some criteria are met) if they pose significant cybersecurity risks or other risks, such as to the compliance with Union law intended to protect fundamental rights (e.g., the Charter of Fundamental Rights of the EU). These investigations can result in corrective or restrictive measures against the relevant economic operator, including the withdrawal of the product from the EU market. The article concludes that while the CRA should be leveraged to put 'commercial spyware' for private use (i.e. stalkerware or bossware) out of the market, as they indeed pose the aforementioned risks, this would only have a limited impact on the broader commercial spyware market, leaving effectively untouched the more problematic state procurement of such technologies pivoting on national security. We suggest that the concept of national security should be interpreted in a narrower fashion with a view to bring spyware in scope of relevant EU legal acts, such as market-based product safety legislation (e.g., the CRA) and EU data protection law. This human-rights based interpretation of the current legal framework is needed to make the CRA a legal instrument that actually addresses the broader, systemic cybersecurity risks exploited by spyware vendors.

2. Spyware and EU law: addressing a legal gap

2.1. A fragmented framework for trade, procurement and use of spyware

EU law touches the spyware ecosystem in pieces but leaves decisive gaps. On the trade side, the Regulation (EU) 2021/821 (so-called Dual-Use Regulation) controls exports of "cyber-surveillance items" and embeds some human-rights due diligence. In 2024, the Commission issued specific Guidelines[23] on how the Regulation should apply to cyber-surveillance exports and, therefore, to spyware exports. Nevertheless, the Dual-Use Regulation provides only narrow control over spyware exports, as it has not evolved sufficiently to address the multifaceted human rights risks posed to destination countries.[24] More importantly, it applies to exports outside the EU, while inside the Union trade is essentially free, since spyware can circulate between different countries without licences.[25] The 2024 Commission guidelines add little,[26] as they limit scrutiny to vaguely defined "serious" rights violations abroad, rely on exporters' self-assessments, and lack automatic suspension. Enforcement is left to Member States, potentially leading to uneven oversight and weak protection.

On procurement, EU rules primarily govern transparency,

[16] A. Sheniak, 'Bringing technology back into spyware regulations' (2025) 86 Ohio State Law Journal 1, 10.

[17] Ibid.

[18] REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

[19] Although in force, the vast majority of CRA rules will be applicable from 11 December 2027; only the 'notification obligations' pursuant Art. 14 and Chapter IV will apply from 11 September and 11 June respectively.

[20] J. Walraven, 'European Investment Fund financed Israeli spyware company Paragon' (2025) Apache, 1 October 2025, available at: <https://apache.be/2025/10/01/european-investment-fund-eif-financed-israeli-spyware-company-paragon> last accessed 5 March .

[21] S. In't Veld, 'An Inquiry on Spyware in the EU Revealed Abuses by Member States. Now What?' (2025) Digital Front Lines, available at: <https://digitalfrontlines.io/2025/01/31/spyware-regulation-european-commission/> last accessed 5 March .

[22] That is, Regulation (EU) 2016/679 (GDPR), Directive (EU) 2016/680 (LED) and Directive 2002/58/EC (e-Privacy Directive).

[23] European Commission, Commission Recommendation (EU) 2024/2659 of 11 October 2024 on guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council (2024).

[24] M. Kanetake, 'Governing the Global Proliferation of Digital Surveillance Technologies: Lessons from the EU' (2025) in J. Van Dijck, K. van Es, A. Helmond, and F. van der Vlist (eds.) Governing the Digital Society: Platforms, Artificial Intelligence, and Public Values, Taylor & Francis.

[25] Only those items that are listed under "Annex IV - Very Sensitive Items" of the Dual-Use regulation are subject to licensing when exported from one EU Member State to another. Therefore, the internal market of commercial spyware – which is part of "Annex I – List of Dual-Use Items" - is at the moment a totally free market with no regulations or need for licences.

[26] M. Bromley and G. Maletta, 'Making the most of the EU catch-all control on cyber-surveillance exports' (2024) Sipri, available at: <https://www.sipri.org/commentary/topical-backgrounder/2024/making-most-eu-catch-all-control-cyber-surveillance-exports> last accessed 10 April .

competition and value-for-money; security and secrecy exemptions permit opaque purchasing pathways for offensive tools.[27] This architecture has enabled a thriving commercial market within the EU despite mounting evidence[28] of abuse and chilling effects on rights and democracy. Not only have EU institutions permitted Member States to purchase commercial spyware, but recent investigations have revealed that EU taxpayer money has also reached spyware vendors, including via flagship innovation and security instruments such as Horizon Europe,[29] the European Defence Fund, and the European Investment Bank.[30]

The European Media Freedom Act (EMFA) establishes the most explicit Union-level prohibition on spyware – or, in the wording of the EMFA, 'intrusive surveillance software' – against media actors, but one that is heavily qualified by exceptions. According to Article 4, paragraph 3, letter c EMFA, Member States must not deploy spyware software on any material, including but not limited to digital devices, used by media service providers, their editorial staff or "any persons who, because of their regular or professional relationship with a media service provider or its editorial staff, might have information related to or capable of identifying journalistic sources or confidential communications". However, the general rule prohibiting the deployment of spyware software against media service providers, journalists and their inner circle, suffers from too many exceptions.[31] According to paragraph 5 of Article 4 EMFA, States can deploy spyware against these persons provided that (i) it finds a legal basis in Union or national law; (ii) the criteria of Article 52(1) CFR are fulfilled; (iii) it is justified on a case-by-case basis by an overriding reason of public interest and is proportionate; (iv) it is subject to prior authorisation by a judicial authority or an independent and impartial decision-making authority, and (v) it is carried out for the purpose of investigating serious crimes.

This so-called 'safeguard' risks, due to its broad and interpretable exemptions, is doing more harm than good: rather than setting a model for protecting journalists, it sets the first EU blueprint for how spyware may be lawfully deployed even against them.

2.2. The EU data-protection acquis and its shortcomings

The various spyware scandals have also exposed a fault line in the EU's data protection acquis. While the GDPR, the LED and the e-Privacy Directive (ePD)[32] together form a strong framework,[33] in practice their applicability to spyware remains contested, due to the national security exemption embedded across these regimes. Member States frequently invoke Article 4(2) TEU to argue that such activities fall outside the scope of EU law. As has been noted, the EU legislator lacks competence to regulate national security activities as such.[34]

As the European Parliament's research service observes, "Member States may advocate an interpretation of secondary data protection and privacy laws that excludes Pegasus cases from their application[35]". Similarly, intelligence and security authorities can contend that their activities "escape the purview of both the ePrivacy Directive (ePD) and the Law Enforcement Directive (LED)".[36]

However, this exclusion is not automatic nor absolute. The Court of Justice of the European Union (CJEU) has consistently rejected broad interpretations of national security derogations. In particular, it has clarified that "the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable".[37] Where Member States impose obligations on entities subject to EU law – e.g., electronic communications service providers, or even law enforcement agencies – those measures must comply with EU data protection standards and the Charter of Fundamental Rights. Accordingly, the argument of the inapplicability of data protection rules in relation to spyware deployment under the argument of national security reasons, as if these tools were operated in a vacuum, is hardly acceptable.

This jurisprudence supports a broader constitutional argument: the applicability of EU data protection law should be grounded in primary law. As Tzanou and Vogiatzoglou emphasise, CJEU case law is rooted in the Charter, and Member States must comply with it both when

[27] See Directives 2014/24/EU (Public Procurement Directive) and Directive 2009/81/EC (Defence and Security Procurement Directive)

[28] A. Roussi, 'How Europe became the Wild West of spyware' (2023) Politico, available at: <https://www.politico.eu/article/how-europe-became-wild-west-spyware/> last accessed 10 April ; see also Civicus Lens, Weaponised surveillance: how spyware targets civil society (2025), available at: <https://lens.civicus.org/weaponised-surveillance-how-spyware-targets-civil-society/> last accessed 10 April .

[29] V. Panagiotopoulos, 'Spyware industry pockets EU subsidies while snooping on its citizens' (2025) Follow the money, available at: <https://www.ftm.eu/articles/spyware-industry-eu-subsidies-surveillance-concers> last accessed 11 April .

[30] J. Walraven (n 20).

[31] EDRi, Challenges ahead: European Media Freedom Act falls short in safeguarding journalists and EU fundamental values (2024), https://edri.org/our-work/challenges-ahead-european-media-freedom-act-falls-short-in-safeguarding-journalists-and-eu-fundamental-values/. See also L. Malferrari, 'New and reinforced rights for media service providers under Article 4 European Media Freedom Act' (2025) 1 Rivista Italiana di Informatica e Diritto, 156-166; J. E. Kermer, 'Article 4 of the European Media Freedom Act: a missed opportunity?: assessing its shortcomings in protecting journalistic sources' (2024) in K. Simeonov and M. Yurukova (eds.) Papers from the Eleventh International Scientific Conference of the European Studies Department: the agenda of the new EU institutional cycle, Sofia: Minerva, 192-207.

[32] According to the recital 24 of the ePD, "Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms", which means that the use of spyware and similar tools "should be allowed only for legitimate purposes, with the knowledge of the users concerned". Similarly, the PEGA Committee argued, in its Recital AF, that the use of spyware "constitutes a restriction of the right to protection of terminal equipment" afforded by the ePD.

[33] The GDPR applies to the processing of personal data within its material scope and therefore remains central to private-sector deployment and to public-sector processing outside the specific criminal-law enforcement framework. Directive (EU) 2016/680 applies instead to processing by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Directive 2002/58/EC, as a lex specialis for the electronic communications sector, introduces measures to protect the confidentiality of communications and related traffic and location data. These instruments thus overlap in the broader field of surveillance, but their relevance depends on the actor involved, the purpose pursued and the type of data or communications interference involved.

[34] See, ex multis, D. Korff, Opinion on the Implications of the Exclusion from New Binding European Instruments on the Use of AI in Military, National Security and Transnational Law Enforcement Context (2022), 25, available at: <https://ecnl.org/sites/default/files/2022-10/ECNL%20Opinion%20AI%20national%20security_0.pdf> last accessed 10 April .

[35] European Parliamentary Research Service, Europe's PegasusGate: Countering spyware abuse (2022), 82, available at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf> last accessed 10 April .

[36] Ibid.

[37] CJEU, Judgment of 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier Minister and Others, ECLI:EU:C:2020:791, para 99; see also D. Korff (n 34), 26.

implementing and when derogating from EU law.[38] This Charter-centred approach suggests that fundamental rights constraints persist even in areas of Member State exclusive competence. Indeed, it has been argued that EU fundamental rights standards "could, in principle, be applied to national security agencies".[39] Grounding the scope of EU data protection law in primary law, through a data-subject-centred model, as proposed by Tzanou and Vogiatzoglou, would reduce the risk of the data protection acquis becoming "toothless" in the face of evolving surveillance technologies.

This legal ambiguity generates three interlinked problems that foster a situation of legal uncertainty that is contrary to the general principles of EU law. First, competence disputes arise as Member States invoke national security to assert exclusivity, despite precedents supporting the continued applicability of EU law. Second, the concept of national security remains elastic, with blurred boundaries between national security, public security, and law enforcement. While Member States tend to stretch this notion, the Court of Justice of the European Union has interpreted national security derogations restrictively,[40] refusing to endorse unlimited reliance on this exemption.

Third, gaps and ambiguities in secondary law, such as the definition of "competent authority" under the Law Enforcement Directive (LED) or the contradiction between recital 24 ePD,[41] (which established that spyware can be used only with the knowledge of the users concerned) and State practice, create enforcement challenges. This has also to do with what has already been observed: spyware is not deployed in a vacuum, but instead, even if its deployment is done under "national security" reasons, it involves authorities, private companies and data-sharing practices that are, indeed, subject to EU law.[42] The consequence is that spyware use labelled as "national security" risk falling through the cracks of EU law. As noted later in the analysis of the CRA, national security carve-outs could exclude state procurement and use of spyware from otherwise applicable Union rules. Yet, as the EPRS confirms, there remain important circumstances in which EU law may apply. Moreover, the cases that have so far come to light largely concern surveillance directed at journalists, activists, opposition figures, and other members of civil society, contexts in which reliance on national security as a blanket justification appears particularly difficult to sustain.

Beyond doctrinal ambiguity, the evolving structure of the spyware market further exposes regulatory shortcomings. The fragmentation of the supply chain, coupled with the transnational nature of the surveillance marketplace, allows vendors and deployers to exploit jurisdictional gaps.[43] Traditional regulatory models, designed around identifiable end-products, struggle to capture distributed and modular surveillance capabilities.

A potential counterargument is that spyware may be used by law enforcement authorities within existing interception frameworks. Yet this argument fails to account for the qualitative and proportionality gap between traditional interception and spyware. As shown in the preceding section, the latter enables systematic, continuous, and covert surveillance at a scale incompatible with core data protection principles, including data minimisation, purpose limitation, and transparency. It is therefore difficult to identify a valid legal basis under the LED or the GDPR (when private actors deploy these software) capable of justifying such practices, particularly in cases involving journalists, activists, or political opponents.

This ambiguity is further compounded by the Commission's own inaction. Despite publicly committing to a communication on spyware's interaction with the data protection acquis in response to the PEGA inquiry's findings, no such initiative has yet been delivered. But as said in a leaked draft of the Commission's own internal document, which has been blocked for more than one year, "national security does not justify spying" [emphasis added],[44] and Member States "cannot exercise their responsibility in a way that undermines the effectiveness of EU law" on data protection and privacy.[45]

In short, the data protection acquis can and should serve as a bulwark against governmental spyware abuse. Many evidenced forms of covert device intrusion, particularly exploit-dependent, large-scale, insufficiently targeted deployments, will face serious difficulty in satisfying the Union's data protection principles of lawfulness, purpose limitation, necessity, proportionality, data minimisation. Furthermore, the more intrusive, opaque and broad the operation, the more difficult it becomes to identify a convincing legal basis under EU data protection law. However, without clearly defining its scope, limiting exceptions, and enforcing the rules effectively, national security will remain the ultimate trump card potentially paving the way towards fundamental rights infringements.

As this section has shown, different Union legal instruments address discrete stages of the spyware lifecycle (i.e., product design, data processing and communications confidentiality, procurement and export) without combining into a coherent framework for exploit-dependent commercial spyware. Besides fragmentation, vendors and deployers benefit from the regulatory infrastructure of the internal market, as disputes over legality are displaced across these legal regimes, most notably through reliance on national-security framing to contest the applicability, scope, or practical enforceability of Union law. It is against that background that the possible contribution of the CRA should be assessed.

3. The CRA and the spyware market: potentials and limitations

Against the background of software that need other digital products vulnerabilities to function, such as spyware, the CRA aims to tackle three problems: i) a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient provision of security updates; ii) an insufficient understanding and access to information by users[46]; and, iii) the lack of a comprehensive legal framework at Union level addressing mandatory cybersecurity requirements for hardware and software products.[47]

In summary,[48] this piece of legislation sets out specific obligations

[38] M. Tzanou and P. Vogiatzoglou, 'National Security and New Forms of Surveillance: From the Data Retention Saga to a Data Subject Centred Approach' (2025) 10 European Papers – A Journal on Law and Integration 3, 817.

[39] H. Hijmans, The European Union as a Guardian of Internet Privacy: The Story of Art 16 TFEU (2016) Springer, 142–143.

[40] European Parliamentary Research Service (n 35), 79. See also M. Tzanou and P. Vogiatzoglou (n 38), 818.

[41] Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.

[42] M. Tzanou and P. Vogiatzoglou (n 38), 819.

[43] A. Lubin, 'Selling Surveillance' (2024) 85 Ohio State Law Journal 809.

[44] A. Roussi, "Curb your snooping, Commission tells EU governments" (2024), available at: <https://www.politico.eu/article/eu-commission-national-security-does-not-justify-spying-document/> last accessed 10 October 2025.

[45] Ibid.

[46] Recital 1, CRA.

[47] Recital 4, CRA.

[48] For a more detailed analysis of the CRA, let us refer to P. G. Chiara, 'Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?' (2025) 16 European Journal of Risk Regulation 2.

for the economic operators involved in the value chain of products with digital elements (PDEs), including manufacturers, bearing the most responsibilities regarding PDEs, importers, distributors, authorised representatives. In line with the principles and mechanisms of EU product safety legislation, the CRA mandates that manufacturers can make PDEs available on the market if they comply with the cybersecurity essential requirements laid down in Annex I CRA.[49] Operators' obligations span throughout the entire life-cycle of PDEs, from the planning, design, development and production phases to the market delivery and maintenance.

Before placing a PDE on the market, manufacturers shall comply with manifold duties, including due diligence, documentation, information and procedural requirements pursuant to Article 13 CRA. Then, manufacturers must demonstrate that PDEs comply with the essential cybersecurity requirements in Annex I by choosing a conformity assessment procedure set out in relevant Annexes to the CRA. Depending on the level of cybersecurity risk, PDEs are divided into categories: important (Class I and II) and critical PDEs must undergo stricter third-party conformity assessment procedures. In line with the New Legislative Framework, PDEs which are in conformity with harmonised standards[50] (translating Annex I requirements into detailed technical specifications), common specifications adopted by the Commission or that are certified under a European cybersecurity scheme pursuant to Regulation (EU) 2019/881 (Cybersecurity Act),[51] are presumed to be in compliance with CRA cybersecurity essential requirements.

The CRA also establishes a market surveillance framework, enabling national authorities or the Commission, if some conditions are met, to take corrective or restrictive measures against non-compliant products, including fines and product withdrawals. Investigations can be launched by the authorities if a product, although compliant with the CRA, can nonetheless pose a significant cybersecurity risk or other risks, including to compliance with obligations under Union or Member States law intended to protect fundamental rights [emphasis added].[52]

This latter point helps shed light on the extent to which the CRA, a product-safety piece of legislation, protects fundamental rights.[53] While the AI Act, arguably the CRA's regulatory sibling,[54] more explicitly hybridises the risk-based and product-safety approaches with a rights-based approach,[55] the CRA does not *explicitly* and *directly* include mechanisms to ensure that PDEs respect fundamental rights, nor does it acknowledge rights to users or, more broadly, individuals affected by, say, exploited vulnerabilities in PDEs. At the same time, as later addressed in Section 3.3, CRA's public enforcement mechanisms empower national market surveillance authorities or, under certain conditions, the Commission, to take corrective or restrictive measures against PDEs which, although compliant with the CRA, pose a risk to compliance with other EU legal acts intended to protect fundamental rights, such as, inter alia, the GDPR. Against the background of these newly introduced cybersecurity rules aiming at managing vulnerabilities and protecting public interests, this section is devoted to assessing whether and to what extent the Cyber Resilience Act can be relied upon to curb the rising spyware market in the EU. To this end, three legal challenges come to the fore. The first hinges on the scope of the CRA: are spyware technologies 'products with digital elements' within the meaning of the Regulation? Related to that, products with digital elements that are exclusively developed or modified for national security or defence purposes are excluded from the scope of the CRA: to what extent does the 'national security and defence exemption' cover the spyware market within the European Union spyware market? Lastly, the effectiveness of CRA's public enforcement mechanisms should be assessed in the specific context of the spyware market and the political reality, as national authorities or the Commission may be lacking the will to confront spyware ecosystems within the EU, especially where Member States themselves are involved as purchasers or users of the technology.

3.1. *Spyware as a product with digital elements*

The CRA applies to "products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network".[56] Within the meaning of 'product with digital elements' (PDEs) fall not only hardware products but also software, including software components which are placed on the market separately.[57] Furthermore, CRA's extensive cybersecurity requirements and obligations also extend to PDEs' remote data processing solutions, meaning data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions.[58] Also, free and open-source software (FOSS) falls within the scope of the CRA, provided that it is made available on the market, that is, supplied for distribution or use in the course of a commercial activity,[59] given the dramatic impacts on the entire supply chain following security attacks on open-source components (e.g., Log4Shell, XZ Utils).[60]

[49] Art. 6, CRA.

[50] In accordance with Regulation (EU) No 1025/2012, the presumption of conformity with harmonised legislation is provided by harmonised standards, that is, technical standards drafted by European Standardisation Organisations based on a Commission's request to satisfy the essential requirements of relevant legislation and the reference of which is published on the Official Journal of the EU.

[51] The Commission will specify, via delegated acts, under which conditions the European cybersecurity certification schemes can be used to demonstrate conformity with the CRA essential requirements.

[52] Art. 57(1), CRA. Other fundamental values protected by the CRA vis-à-vis compliant products include: i) the health or safety of persons; (ii) the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by NIS2 essential entities; or (iii) other aspects of public interest protection.

[53] The CRA indirectly upholds fundamental rights and freedoms since more secure and resilient products with digital elements will minimise risks to fundamental rights, including the right to privacy, protection of personal data, or freedom of expression.

[54] C. Goanta, 'Regulatory Siblings: The Unfair Commercial Practices Directive Roots and the AI Act' in I. Graef and B. van Der Sloot (eds.), The Legal Consistency of Technology Regulation in Europe (2024), London, Hart Publishing, 84.

[55] T. Evas, 'The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI' (2024) 1 AIRe – Journal of AI Law and Regulation, 98; M. Almada, N. Petit, 'The EU AI Act: between the rock of product safety and the hard place of fundamental rights' (2025) 62 Common Market Law Review 1.

[56] Art. 2(1), CRA.

[57] The broadening of the notion of 'product' to include software in the CRA is aligned with other EU legal acts, such as Directive (EU) 2024/2853 on liability for defective products and repealing Council Directive 85/374/EEC.

[58] Art. 3, point 2, CRA. Therefore, not all software-as-a-service (e.g., cloud computing) fall within the scope of the CRA. The CRA does not apply, e.g., to a cloud service whose design falls outside the responsibility of the manufacturer of a PDE, or to a website that does not support the functionalities of a PDE. Afterall, the cybersecurity aspects of SaaS are already regulated by Directive (EU) 2022/2555 (NIS2).

[59] Recital 18, CRA.

[60] L. Colonna, 'The End of Open Source? Regulating Open Source under the Cyber Resilience Act and the New Product Liability Directive' (2025) 56 Computer Law & Security Review, 4–5; J. Tridgell, 'Open or Closing Doors? The Influence of 'Digital Sovereignty' in the EU's Cybersecurity Strategy on Cybersecurity of Open-Source Software (2025) 56 Computer Law & Security Review.

In light of the definition of spyware given in the Introduction, it should be assessed whether spyware falls within the scope of the CRA. Three elements are relevant for determining the applicability of the Regulation to spyware. First, the nature of spyware, i.e. *what* spyware *is*; second, the capabilities of spyware, i.e. *what* spyware *does*; third, the commercial relationships underlying the EU spyware market, i.e. *how* and *to whom* spyware is sold.

According to our definition, spyware is a software product. Art. 3(1) of the CRA clarifies that the notion of PDEs is as broad as to cover software products. Inasmuch as the 'ontological criterion' is concerned, it can preliminarily be concluded that spyware *prima facie* meets the definition of "product with digital elements".

To fall within the scope of the CRA, PDEs' intended purpose or reasonably foreseeable use must include a direct or indirect logical or physical data connection to a device or network.[61] To perform its functionalities, which are predominantly performed remotely, spyware software needs a logical data connection to a network, such as the Internet. This notwithstanding, a physical connection (e.g., USB access) is however possible, although implausible given the most common attack scenarios involving spyware. The 'data connection requirement' is indeed inherent in spyware's design and operation.

Lastly, the CRA applies to PDEs that are made available on the market. In the context of a market, such as that of spyware, mainly characterised by covered procurement, it is necessary to clarify the extent to which spyware is 'made available on the market' if purchased by governments. Recital 15 of the CRA unsurprisingly aligns with the definition provided for in Art. 2(1) of Regulation (EC) No 765/2008 and clarifies that PDEs are made available on the market if they are "supplied for distribution or use on the Union market in the course of a commercial activity". The two distinctive elements of the definition are i) the supply for use, *prima facie*, regardless of the type of buyer or user; ii) the commercial nature of the transaction. All in all, a contract between a private company and a government can fall under "making available" if the commercial and functional criteria are met.

Against this backdrop, a paradox may arise where the CRA would ensure that spyware products are designed and developed in a more secure and resilient manner, and offer greater guarantees (and fewer risks) to their "consumers", for example, state actors. This consideration leads us to the second legal challenge. Thus, the so-called 'national security' exemption set out in Art. 2(7) CRA would most likely prevent the application of the CRA to most spyware technologies made available to the EU market.

3.2. The national security exemption

Unsurprisingly,[62] the CRA contains an exclusion provision according to which products with digital elements "developed or modified exclusively for national security or defence purposes" are not included in the scope of the regulation.[63] While a blanket exception of *all* spyware products would be contrary to the law, there remains a significant grey area. Member States' governments and state security apparatus, as well as their private providers, can claim that spyware PDEs fall outside the remit of EU law, including the CRA, insofar as the intended purpose of the spyware software is *exclusively* linked to national security or defence activities. Accordingly, if a manufacturer can prove that spyware was developed exclusively for national security or defence purposes, it is irrelevant, for the purpose of excluding it from the scope of the CRA, whether the spyware is deployed by a government or security agency or by private individuals or companies.[64]

In any case, this interpretation of the CRA's national security clause will likely lead to problematic consequences, particularly vis-à-vis States' procurement of spyware. It risks encouraging an overly broad application of the notion of national security, a sole responsibility of Member States under EU primary law.[65] According to the case-law of the Court of Justice of the European Union, "although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law".[66]

National security, therefore, does not give Member States a blank check to bypass EU law. The question, then, is how narrowly the national security purposes should be defined.[67] In the settled case-law of the CJEU, the notion of national security has a more restricted scope than public security and serious crime, encompassing "the prevention and punishment of activities capable of *seriously destabilising the fundamental constitutional, political, economic or social structures of a country* and, in particular, of *directly threatening* society, the population or the State itself, such as terrorist activities [emphasis added]".[68] National security threats can be distinguished from those pertaining to public security (or serious crime) essentially by their nature and particular seriousness.[69] In other words, national security is affected when a nation's fundamental interests are harmed or threatened, thus having a much more restricted scope than public security.

The notion of national security found in *La Quadrature du Net* is directly quoted by the Commission in its 'Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)'.[70] Interestingly, the Commission goes on specifying the 'exclusively' criterion relating to the national security exemption pursuant Article 2(3) AI Act: "if an AI system placed on the market, put into service or used for military, defence or national security purposes is used (temporarily or permanently) for other purposes, such as for civilian or humanitarian purposes, law enforcement or public security purposes, that system will fall within the scope of the AI Act".[71] Given that the wording of Article 2(3), second subparagraph, of the AI

[61] Art. 2(1), CRA.

[62] As seen in Section 2, many other provisions of EU (digital) law exclude national security activities from their scope: see e.g., Art. 2(2) GDPR, read in conjunction with recital 16; Art. 1(3) e-Privacy Directive; Art. 2(3) AI Act; Art. 2 (6-7), NIS2 Directive; etc.

[63] Art. 2(7), CRA.

[64] In the context of the national security exclusion provisions of the e-Privacy Directive, the CJEU ruled that it is necessary to draw a distinction according to who was carrying out the data processing operation concerned: "all operations processing personal data carried out by providers of electronic communications services fall within the scope of that directive". See CJEU, Judgment of 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier Minister and Others, ECLI:EU:C:2020:791, para. 101.

[65] Art. 4(2), TEU.

[66] CJEU, Judgment of 6 October 2020, Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, ECLI:EU:C:2020:790, para. 44; see also La Quadrature du Net and Others v. Premier Minister and Others, para. 99.

[67] In its Opinion to the La Quadrature du Net Case, the Advocate General Campos Sanchez-Bordona held that the range of public authority activities concerning national security, that are exempt from the general regime governing the processing of personal data, must be interpreted narrowly: Opinion of A.G. Campos Sanchez-Bordona, delivered on 15 January 2020, Joined Cases C-511/18 and C-512/18, La Quadrature du Net and Others v. Premier Minister and Others, ECLI:EU:C:2020:6, para. 80).

[68] La Quadrature du Net and Others v. Premier Minister and Others, para. 135.

[69] Ibid., para. 136.

[70] European Commission, Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) (2025), para. 23.

[71] Ibid., para. 24. See also E. Biber, 'A Close Reading of the European Commission's Guidelines on Prohibited Artificial Intelligence Practices: A Powerful Reflection of the European Approach to AI' (2025) 2 AIRe – Journal of AI Law and Regulation 3, 267.

Act and Article 2(7) of the CRA is essentially the same, the legal reasoning presented by the Commission in the "Guidelines on Prohibited AI Practices" should also be applied to interpret the CRA's 'national security exemption', to ensure uniform and consistent application of EU law. Accordingly, spyware that are used for both public security and national security purposes fall within the scope of the CRA.[72]

The objective of safeguarding national security can justify measures entailing serious interferences with fundamental rights, provided that Article 52(1) of the Charter requirements are met. As noted by Sartor and Loreggia in their report requested by the EU Parliament's PEGA Committee, spyware in general, and Pegasus in particular, fail to satisfy the Charter's and ECHR's rigorous conditions of legitimacy, legality, necessity, balancing, and consistency with democracy to restrict fundamental rights in carrying out national security activities.[73] The PEGA Committee not only shed light on the absence of a solid legal framework,[74] including safeguards and oversight against spyware abuse in most EU countries,[75] but also raised concerns on the unjustified invocation of 'national security' to justify the deployment and use of spyware and to ensure absolute secrecy and lack of accountability.[76]

What is sure is that, when it comes to State deployment of spyware, the CRA would nonetheless apply to spyware PDEs which are *not exclusively* developed for national security purposes, regardless of who is the actor deploying it. First, this exclusion should require demonstrable exclusive national security application, not a vague declaration by the companies and countries, and secondly, all spyware tools used against civil society, journalists, political opponents, or designed to be used in the course of "regular" criminal investigations, should not fall under this exclusion.

It is also clear that privately used spyware technologies, that is, available of-the-shelf to the general public, would fall under the CRA's scope. These tools are oftentimes disguised under the label of 'parental control', used by private individuals in the context of intimate relationships with a view to monitoring (and exerting control) over another individual (so-called 'stalkerware'),[77] or can also be deployed by employers to spy on their employees, in what is known as 'bossware'.[78] These software are not merely harmful when misused; they pose systemic cybersecurity threats to all users. Their core functionality depends on deception, concealment and exploitation of device vulnerabilities in order to remain undetected by the person being surveilled. In other words, they operate by deliberately undermining the security and integrity of devices, the very opposite of what the CRA seeks to ensure. A product that is designed to remain hidden from its user, to obfuscate its presence, or to disable protective mechanisms such as antivirus detection or OS permission prompts is by definition incompatible with the principle of "cyber resilience". Furthermore, clear anti-abuse safeguards (e.g., prohibit default configurations of commercial spyware that enable deceit and secret surveillance; require explicit and informed consent from all monitored parties; facilitate removal from all those failing to respect these principles) and proactive market surveillance should be established specifically for these dangerous PDEs.

The Recital corresponding to the national security exemption laid down in Article 2(7) CRA adds that Member States are encouraged to ensure the same or a higher level of protection for those products as for those falling within the scope of this Regulation.[79] As seen above, the CRA aims to achieve an *adequate* level of *cybersecurity* protection. The risks mainly tackled by the CRA are, therefore, cybersecurity risks. However, as shown in greater detail in the next section, PDEs – even if compliant with the CRA – can nevertheless pose other risks, such as compliance with national or Union law intended to protect fundamental rights.

3.3. Public enforcement

The market surveillance authority designated by each Member State for implementing and enforcing the CRA may carry out an assessment of a product with digital elements regarding its compliance with the essential requirements of the regulation if it has sufficient grounds to consider that such a product presents a significant cybersecurity risk, also taking into account non-technical risk factors.

If, following the investigation, the product is found to be non-compliant, the authority shall request the economic operator to adopt the appropriate corrective measures. In case the economic operator fails to cooperate, the authority adopts appropriate provisional restrictive measures (e.g., prohibition or limitation of availability, withdrawal, or recall). These measures become final if no objections are raised by the Commission or the other Member States within three months of receiving the notification from the initiating authority.[80]

After carrying out the aforementioned investigation, the authority may still identify a significant cybersecurity risk or, inter alia, a 'risk to compliance with obligations under Union or national law protecting fundamental rights', even if the product is deemed compliant with the regulation.[81] In such a case, the relevant economic operator is required to take the necessary corrective measures within the time limit set by the authority, which shall notify the Commission and the other Member States of the measures taken.

It is important to underline the Commission's power to 'prompt' the assessment by the competent national authorities if it has grounds to believe that a product, although compliant with the CRA, presents the aforementioned risks. As in the Union-level procedure concerning non-compliant products under Article 56, the Commission may carry out the risk assessment in place of the national authorities, with the support of ENISA, provided that: i) there are circumstances justifying immediate intervention to preserve the proper functioning of the internal market; ii) no effective measures have been taken by the competent national authority; iii) the Commission has sufficient grounds to believe that the product continues to pose risks to these fundamental values; and iv) it informs the concerned national authorities.[82] The Commission may then impose a corrective or restrictive measure at the Union level.[83]

Against this background, we can envisage a scenario where a spyware product, falling within the scope of the regulation and thus not covered by the national security exemption as addressed above (e.g., 'stalkerware or spyware also used for law enforcement or public security

[72] In the context of the AI Act, see M. Tzanou and P. Vogiatzoglou (n 38), 816.
[73] G. Sartor and A. Loreggia (n 9), 55.
[74] Spyware and similar hacking-technologies cannot be assimilated to traditional interception techniques used by law enforcement, which are regulated by national and supranational instruments, due to the capacity of the former to collect a larger body of information as it grants complete and unrestricted access to the targeted device: see EDPS, Preliminary Remarks on Modern Spyware (2022), 3-4, available at: <https://www.edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en>, last accessed 14 April ; G. Sartor and A. Loreggia (n 9), 21-22.
[75] European Parliament Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP)), paras. U-V.
[76] Ibid., para. 42.
[77] National Cybersecurity Alliance, 'What to know about stalkerware' (2023), available at: <https://www.staysafeonline.org/articles/what-to-know-about-stalkerware> last accessed 10 October 2025.
[78] L. Munn, 'Expansive and Invasive: Mapping the "Bossware" Used to Monitor Workers' (2024) 22 Surveillance & Society 2; D. Brantes Ferreira, E. A. Bromova, 'The Bossware Era and the e-Panopticon: Current Technologies and Legal Challenges' (2025) Industrial Law Journal.
[79] Recital 26, CRA.
[80] Art. 54, CRA.
[81] Art. 57(1), CRA.
[82] Art. 57(7), CRA.
[83] Art. 57(8), CRA.

purposes'), and the processes put in place by the manufacturer are in compliance with CRA's essential requirements. The horizontal cybersecurity essential requirements of Annex I CRA concern the (cyber)security properties of the product *itself* (Part I) and the management of vulnerabilities *affecting the product* (Part II), while paying limited attention to the broader risks that the product with digital elements may pose to the cybersecurity of other systems or devices. Particularly, spyware inherently leverage vulnerabilities in other PEDs.

One notable exception is the requirement to "minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks".[84] However, such a requirement remains limited in scope and effect. First, manufacturers can indicate, on the basis of the cybersecurity risk assessment carried out in the design phase, that a particular essential requirement of Annex I, part I is not applicable to the product in question.[85] Second, and more importantly, that requirement addresses only the availability property,[86] whereas in contexts such as spyware, the integrity and confidentiality of systems and data[87] are often the most critically affected. This narrow focus underscores a broader shortcoming: the CRA's essential requirements are predominantly inward-looking and largely neglect the relational dimension, that is, the systemic and interdependent nature of cybersecurity risks stemming from interactions among multiple products, networks, and threat environments.

While the product may comply with CRA's requirements, spyware products *inherently* pose both significant cybersecurity risks and risks to the compliance with Union's obligations intended to protect fundamental rights. We have addressed earlier the case of stalkerware, making the case of the threats posed by it. Commercial spyware used by states also presents significant cybersecurity risks because it compromises systems' integrity, usually by leveraging so-called 'zero-day' vulnerabilities[88] and through 'zero-click' attacks,[89] to gain complete and unrestricted access to a system or device, thus targeting systems and data integrity and confidentiality – two core principles of the so-called CIA (confidentiality, integrity and availability) triad of network and information security, now included in the broader concept of cybersecurity.[90]

Instead of responsibly reporting and patching vulnerabilities, spyware vendors - and, at times, the States procuring their services - choose to weaponise them, keeping millions of users, including public institutions, permanently exposed.[91] Even more alarming is the scale at which commercial spyware vendors sustain the vulnerabilities market. According to Google's Threat Analysis Group, 20 out of 25 zero-day vulnerabilities identified in 2023 were used by commercial spyware vendors.[92] This stunning figure demonstrates that such vendors are primary drivers of exploit demand, incentivising a global trade in insecurity. The result is a failure of the cybersecurity market: rather than strengthening the Union's cyber resilience, commercial spyware vendors create a permanent incentive to keep systems vulnerable. With the CRA, the EU wants to provide security for products with digital elements, but without removing the biggest drivers of such insecurity, this legislation might miss the point.

Besides cybersecurity risks, spyware also presents risks to compliance with the Union's fundamental rights law when it comes to its use. As seen in the previous section, the practice of device hacking is hardly compatible with EU law rules aiming at protecting fundamental rights, such as the EU Charter of Fundamental Rights. Many rights and principles are impacted by spyware: the rights of private life and data protection (Arts. 7 and 8); freedom of expression and information, including the freedom of the media, if journalists are targeted by hacking technologies (Art. 11); freedom of assembly and association (Art. 12), including the freedom to join political parties, where targets are members of opposing political parties (Art. 12(2)); the right to non-discrimination (Art. 21), etc.

As addressed in the previous section, Charter's rights and freedoms can be lawfully restricted, say, for national security purposes, provided that such limitations satisfy the principles of legality (each limitation must be provided for by law and respect the essence of those rights and freedoms) and proportionality (limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others).[93] However, as noted by Sartor and Loreggia, spyware in general, and Pegasus in particular, can hardly be reconciled with the above-mentioned requirements: first, these hacking tools have been deployed in contexts unrelated to national security; second, the use has often occurred outside an adequate legal framework, enabling forms of pervasive surveillance that are disproportionate to the objectives pursued; third, the objectives pursued could have been achieved through less intrusive means; fourth, the resulting interference with individual rights and democratic processes appears, in many cases, to outweigh any purported security benefits.[94]

As mentioned above, Article 57 CRA precisely contemplates this scenario. This enforcement procedure could be levelled against spyware PDEs by national market surveillance authorities or the Commission, if the conditions set out in paragraphs 6 and 7 of Article 57 CRA are fulfilled. As a result, corrective or restrictive measures can be established by the initiating authority, including requiring the products with digital elements concerned to be withdrawn from the market, or recalled, within a reasonable period, commensurate with the nature of the risk. If the procedure is initiated by the Commission, then the enforcement measures, adopted via implementing acts, would have effect in the Union.[95]

Therefore, for both the effects of the vulnerability market that fuel spyware vendors in global cybersecurity, and the fundamental rights impacts of its deployment by states, a coherent and teleological interpretation of the law leads us to conclude that spyware can fall under the CRA, and CRA enforcement mechanisms can be activated against those PDEs.

At the same time, it cannot be ignored that the aforementioned procedure is subject to the political-institutional capacity of the relevant authority to initiate the investigation and, eventually, adopt enforcement measures. Thus, the CRA does not require MSAs to be independent.

[84] Annex I, Part I, point 2, letter (i), CRA.

[85] Art. 13(3), CRA.

[86] The US NIST defines availability as the property of ensuring timely and reliable access to and use of information. Similarly, ENISA defines it as the property of being accessible and usable on demand by an authorized entity.

[87] Integrity is defined by the NIST as the property of guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity, while confidentiality aims at preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

[88] A 'zero-day vulnerability' is a security flaw that has not yet been fixed as it is unknown to the entity responsible for developing the software or to security researchers.

[89] A hacking attack that does not require any action by the user to be triggered.

[90] See ex multis M. Veale and I. Brown, 'Cybersecurity' (2020) 9 Internet Policy Review 4.

[91] EDRi (n 6).

[92] S. Smalley, 'Commercial spyware on the agenda as UN Security Council members meet' (2024) The Record, available at: <https://therecord.media/commercial-spyware-meeting-un-security-council-members> last accessed 5 October 2025.

[93] Art. 52(1), Charter of Fundamental Rights of the European Union.

[94] G. Sartor and A. Loreggia (n 9), 55.

[95] Art. 57(9), CRA.

Most of them, in fact, are governmental agencies.[96] It is therefore unlikely that market-surveillance authorities investigate a (spyware) product, under Article 57 CRA procedure, that may have been procured or licensed by the government they depend on or by the same state apparatus of which it forms part.

Against the background of the institutional proximity between cybersecurity governance and the wider state security agencies, national MSAs might rely on cooperation from the very state apparatus whose use of spyware is at issue. Accordingly, the PEGA final report places great emphasis on the role of independent authorities (particularly, data protection supervisory authorities) in tackling spyware abuses.[97] A partial solution could involve amending the CRA to include a right to lodge a complaint with a market surveillance authority, similar to Art. 85 AI Act, which explicitly requires MSAs to consider complaints submitted by individuals or legal persons about alleged infringements for the purpose of conducting market surveillance activities. A logic that is also present in Article 57(1)(f) GDPR, under which Supervisory Authorities are *explicitly* required to handle data subjects complaints.[98]

Instead, Art. 52(11) CRA mandates MSAs only to inform consumers where to submit complaints; this obligation is limited to consumers, making its scope narrower than that of Art. 85 AI Act. Moreover, it does not *explicitly* require MSAs to consider consumer complaints when deciding on their activities. Instead, it refers to Art. 11 Regulation (EU) 2019/1020, where consumer complaints are listed among various factors MSAs must take into account, following a risk-based approach, when deciding on which activities to perform.[99] The proposed amendment would strengthen the legal standard and create consistency with the neighbour's legal framework.

A short-term alternative, pending the negotiation of such an amendment, would be for the Commission to issue guidelines on complaints clarifying that MSAs should take into account information submitted by individuals or legal persons with a view to triggering investigations. A different, more technical path for reducing the risk of abuse would be for the Commission to request ENISA to prepare a European cybersecurity certification scheme (ECCS) specifically addressing spyware PDEs by incorporating technical safeguards against misuse.[100] Since certification under the Cybersecurity Act is, in principle, voluntary,[101] the Commission could then assess whether such a scheme should be rendered mandatory for specific categories of spyware.[102] Here too, however, political resistance from Member States is likely, both during the preparation of the ECCS, particularly within the European Certification Group,[103] and later in the consultation process supporting the Commission assessment of whether the relevant ICT products should be made subject to a mandatory scheme.[104]

Similarly, in scenarios where the Commission decides to evaluate a spyware as a product with digital elements posing relevant risks under Art. 57 CRA procedure, while the risk of proximity between the investigative authority and state agencies deploying spyware would be significantly mitigated (if not eliminated altogether), the action of the Commission still remains conditioned by national security carve-outs and, notably, by Member States' control over the examination procedure in the context of implementing acts deciding on enforcement measures. Article 57(9) CRA measures are adopted by implementing act under the examination procedure in Article 62(2), which refers to Article 5 Regulation (EU) 182/2011: this framework provides that such committees are composed of Member State representatives and the opinions are delivered by qualified majority. If the product under scrutiny is 'politically sensitive' because Member States themselves are purchasers and deployers, as in the case of spyware, it is very likely that, even if the Commission decides to act against such PDEs, it will face intergovernmental pressure.[105]

4. Conclusion

The article has identified a paradox in EU (digital) law: while hardware and software products made available on the Internal Market are, in principle, subject to baseline and comprehensive cybersecurity requirements, spyware products – whose design and operation are structurally at odds with the rationale and objectives of those rules – remain, to a significant extent, tolerated within the Union. The same inconsistency is reflected in the EU's trade regime.[106] Although the Dual-Use Regulation affords a measure of protection to persons outside the EU by controlling exports of cyber-surveillance items, no comparable protection is offered to individuals within the Union, where the placing on the market and circulation of spyware remain largely unregulated.

Against this backdrop, our analysis shows that the Cyber Resilience Act (CRA) can, in fact, be leveraged to contrast the spread of spyware within the EU, despite the challenges posed by the 'national security exemption' of the Regulation, similar to other relevant pieces of EU legislation. The CRA applies to spyware PDEs that are not exclusively developed for national security purposes, regardless of who deploys them. As such, spyware must comply with CRA's cybersecurity essential requirements, including minimising any negative impact on the availability of services provided by other PDEs. Furthermore, spyware manufacturers are required to adhere to the manifold obligations set out in Article 13 CRA. Most importantly, though, national Market Surveillance Authorities, or the Commission under specific circumstances, can benefit from the enforcement powers and mechanisms provided by the CRA to take spyware out of the EU market provided – as it is indeed the case - that spyware presents significant cybersecurity risks *and* a risk to compliance with obligations under Union or national law intended to protect fundamental rights, such as the Charter (EU primary law) or the GDPR (EU secondary law).

National security activities can justify restrictions of fundamental

[96] For example, this is the case of Germany's Federal Office for Information Security (BSI - Bundesamt für Sicherheit in der Informationstechnik); France's National Agency of Information Systems Security (ANSSI - Agence nationale de la sécurité des systèmes d'information); Italy's National Cybersecurity Agency (ANC - Agenzia per la Cybersicurezza Nazionale).

[97] European Parliament - Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (n 1), paras. 177; 198.

[98] The Court of Justice has clarified that supervisory authorities must deal with data subjects' complaints with all due diligence: Case C.311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, EU:C:2020:559, §109; Joined Cases C-26/22 and C-64/22, UF, AB, v Land Hessen, ECLI:EU:C:2023:958, §56; Case C-768/21, TR v Land Hessen, ECLI:EU:C:2024:785, §32.

[99] Art. 11(3), Regulation (EU) 2019/1020.

[100] Art. 49, Regulation (EU) 2019/881.

[101] Art. 56(2), Regulation (EU) 2019/881

[102] Art. 56(3), Regulation (EU) 2019/881.

[103] Pursuant to Art. 62 of Regulation (EU) 2019/881, the European Cybersecurity Certification Group is composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities.

[104] Art. 56(3)(c), Regulation (EU) 2019/881.

[105] A.H. Türk, 'Legislative, Delegated Acts, Comitology and Interinstitutional Conundrum in EU Law – Configuring EU Normative Spaces' (2020) 26 European Law Journal 415.

[106] Similarly, MEP Sophie in t Veld noted that "the EU may appear to be operating under a double standard with regard to digital threats to democracy: while the Commission is determined to fight attacks on democracy from the outside, when a threat to democracy comes from the governments of EU member states, it suddenly considers that the defence of European democracy is no longer a European matter but a matter for the Member States": J. Rankin, Dutch MEP says illegal spyware 'a grave threat to democracy' (2022) The Guardian.

rights and be used by national authorities to escape the scope of relevant instruments of EU law, not limited to the CRA (e.g., EU data protection acquis). However, as stressed by the Court of Justice, the mere fact that a national security measure has been implemented does not render EU law inapplicable. It is crucial therefore to establish clear limits on the concept of national security. A core tenet of the rule of law implies putting in place guarantees safeguarding the individual's rights against interference by executive authorities; normally, the judiciary, offering independence and impartiality, is best placed to strike a balance between the serious interference of the individual's rights and the lawful aims (i.e., uphold national security) pursued.[107] The assessment of the national court needs to be contextual, that is, depending on "the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by national law".[108] These are the criteria courts rely on to determine whether the legal framework under scrutiny is of a quality to keep the interference to what is "necessary in a democratic society".

In light of the *prima facie* incompatibility of spyware with the EU legal order & democratic values, as claimed by the EDPS,[109] several civil society associations – such as EDRi – proposed an EU-wide ban on spyware.[110] Another scenario might be a *moratorium,* as the one proposed by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression David Kaye.[111] As convincingly put by Sartor and Loreggia, "the very existence of widespread abuses in the deployment of a device-hacking system could justify the suspension of their use until all technological, legal, or organisational issues that have enabled such abuses have been satisfactorily addressed. A global, albeit provisional, ban on device-hacking would undoubtedly be the most effective way to prevent the widespread abuses we have witnessed".[112]

All in all, it remains to be seen whether the CRA will be remembered as a successful regulatory measure directed at designing and developing more cyber-secure and cyber-resilient devices and protocols and thus as a 'dam' against the infuriating flood of mass surveillance tools undermining civil liberties and rights, or just another box-checking compliance exercise.[113] Nevertheless, the CRA will only serve as a true facilitator of fundamental rights and liberties, as inter alia claimed by the Commission when the proposal was published, if national authorities or the Commission show the political will to enforce it against surveillance software undermining other products' and Europe's global cybersecurity.

Declaration of competing interest

The authors confirm that they do not have any conflict of interest.

Data availability

No data was used for the research described in the article.

[107] ECtHR, Klass and Others v. Germany [Plenary] App. No. 5029/71, 6 September 1978, para. 50-55; ECtHR, Weber and Saravia v. Germany, App. No. 54934/00, para. 106.

[108] ECtHR, Roman Zakharov v. Russia [GC] App. No. 47143/06, 4 December 2015, para. 232. See M. Cole and A. Vandendriessche, 'From Digital Rights Ireland and Schrems in Luxembourg to Zakharow and Szabo/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance' (2021) 2 European Data Protection Law Review 1; P. G. Chiara, 'Statutory Requirements for Communications Service Providers to Decrypt Online Communications Impair the Essence of Article 8 ECHR' (2024) 10 European Data Protection Law Review 3.

[109] EDPS (n 74), 9.

[110] EDRi (n 6).

[111] D. Kaye, 'The impact of spyware on fundamental rights' (2022) Testimony to the PEGA Committee of the European Parliament.

[112] G. Sartor and A. Loreggia (n 9), 59.

[113] F. Teichmann and B. Sergi, 'The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem' (2025) 59 Computer Law & Security Review, 6.