unione europea e diritti

Union's Tech-Related Sanctions and Moving Frontiers of the European Integration: Reflections on an Evolving Legal Landscape

Federico Ferri*

1. *Introduction*

One of the most peculiar areas of the external action of the European Union (Union or EU) is the Common and Foreign Security Policy (CFSP).[1] It is well-known that, based on the Treaty on the European

* Assistant Professor in EU Law, Department of Legal Studies, *Alma Mater Studiorum* - University of Bologna.

[1] See more extensively: P. KOUTRAKOS, *The European Union's Common Foreign and Security Policy after Lisbon*, in D. ASHIAGBOR, N. COUNTOURIS, I. LIANOS (eds.), *The European Union after the Treaty of Lisbon*, Cambridge, 2012, p. 185; C. CELLERINO, *Soggettività internazionale e azione esterna dell'Unione europea: fondamento, limiti e funzioni*, Ariccia (Roma), 2015, p. 107; BUTLER, *Constitutional Law of the EU's Common Foreign and Security Policy: Competence and Institutions in External Relations*, Oxford, 2019; R. A. WESSEL, *Common Foreign, Security and Defence Policy*, in R. A. WESSEL, J. LARIK (eds.), *EU External Relations Law: Text,*

Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), the Member States highly influence the EU when it takes action in this field, due to significant constraints resulting from the principle of conferral and because of the persistence of some legacies of the intergovernmental method (which underpinned the former Maastricht Treaty's second pillar). It is right within the CFSP that the Union adopts sanctions, although the expression typically used at the supranational level is "restrictive measures".[2]

For brevity, the Council of the European Union (Council), on the basis of Arts. 29 TEU and 215 TFEU, can impose restrictive measures against third countries, entities or individuals to determine a change in policy or activity by the target(s).[3] In light of objectives set out in Art.

Cases and Materials, Oxford, 2020, p. 283; M. E. BARTOLONI, *La politica estera e di sicurezza comune (PESC)*, in M. E. BARTOLONI, S. POLI (eds.), *L'azione esterna dell'Unione europea*, Napoli, 2021, p. 235; E. GREPPI, *Politica estera e difesa europea*, in M. VELLANO, A. MIGLIO (a cura di), *Sicurezza e difesa comune dell'Unione europea*, Milano, p. 16; L. LONARDO, *EU Common Foreign and Security Policy After Lisbon*, Cham, 2023.

[2] For more considerations on the EU's restrictive measures, see: E. PAASIVIRTA, A. ROSAS, *Sanctions, Countermeasures and Related Actions in the External Relations of the EU: A Search for Legal Frameworks*, in E. CANNIZZARO (ed.), *The European Union as an Actor in International Relations*, Alphen aan den Rijn, 2002, p. 207; I. CAMERON (ed.), *EU Sanctions: Law and Policy Issues Concerning Restrictive Measures*, Antwerp – Portland, 2013; P. J. CARDWELL, *The Legalisation of European Union Foreign Policy and the Use of Sanctions*, in *CYELS,* 2015, p. 287; C. ECKES, *The Law and Practice of EU Sanctions*, in S. BLOCKMANS, P. KOUTRAKOS (eds.), *Research Handbook on the EU's Common Foreign and Security Policy*, Cheltenham – Northampton, 2018, p. 206; A. ALÌ, *The Challenges of a Sanctions Machine: Some Reflections on the Legal Issues of EU Restrictive Measures in the Field of Common Foreign Security Policy*, in L. ANTONIOLLI, BONATTI, C. RUZZA (eds.), *Highs and Lows of European Integration. Sixty Years After the Treaty of Rome*, Cham, 2019, p. 49; S. POLI, *Le misure restrittive autonome dell'Unione europea*, Napoli, 2019; M. SOSSAI, *Sanzioni delle Nazioni Unite e organizzazioni regionali*, Roma, 2020, p. 135; C. BEAUCILLON, *Restrictive Measures As Tools of EU Foreign and Security Policy: Promoting EU Values, from Antiterrorism to Country Sanctions*, in S. MONTALDO, F. COSTAMAGNA, A. MIGLIO (eds.), *EU Law Enforcement. The Evolution of Sanctioning Powers*, London, 2021, p. 187; F. GIUMELLI, F. HOFFMANN, A. KSIĄŻCZAKOVÁ, *The When, What, Where and Why of European Union Sanctions,* in *European Security*, n. 1, 2021, p. 1; J. WOUTERS, F. HOFFMEISTER, G. DE BAERE, T. RAMOPOULOS (eds.), *The law of EU External Relations: Cases, Materials, and Commentary on the EU as an International Legal Actor*, Oxford, 2021, p. 177.

[3] EU's sanctions are adopted following a two-stage procedure. Based on Art. 29 TEU, read in conjunction with 24 TEU, the Council first adopts a decision by unanimity. Then, the Council, acting by a qualified majority on a joint proposal from the High Representative of the Union for Foreign Affairs and Security Policy and the European Commission, adopts, on the basis of Art. 215 TFEU, a regulation setting forth the

21 TEU, the changes sought through these measures should be reflected in conducts compliant with the EU's founding values, enshrined in Art. 2 TEU.[4]

With the passing of time, sanctions have become essential tools of the EU's external action[5] and have progressively acquired a significand binding effectiveness. More than 30 States (plus some non-state actors) are now affected by EU's sanctions, resulting in thousands of individuals and entities being directly subjected to these measures. At the same time, these instruments have become more independent from those adopted at the United Nations (UN) level by the Security Council under Chapter VII of the UN Charter.

One of the most striking facets of this trend is the broadening of the categories of EU's autonomous sanctions, which have been evolving considerably over the last years. The Union is currently resorting to a wide array of restrictive measures, to the point that the state-of-the-art is somewhat chaotic. And although the sanctions introduced by the EU are generally aligned to similar measures of "allied" countries, a certain degree of leeway remains: as an example, it was observed that EU's sanctions, if compared with the ones of the United States (US), are narrower in scope both from the material and territorial points of view.[6]

Among the main thematic fields of the EU's sanctions regimes is technology. After the entry into force of the Lisbon Treaty, many

necessary measures; however, these regulations tend to reproduce the provisions contained in the Council's decisions. Importantly, the regulations adopted under Art. 215 TFEU are not CFSP acts, even though they are complementary to this domain (F. BESTAGNO, *Danni derivanti da misure restrittive in ambito PESC e azioni di responsabilità contro l'UE*, in *EJ*, n. 4, 2020, p. 282).

[4] C. MORVIDUCCI, *Le misure restrittive dell'Unione europea e il diritto internazionale: alcuni aspetti problematic*i, in *EJ*, n. 2, 2019, p. 78. However, the founding values of the EU shall underpin, more in general, the external action of the organization: see in particular: M. CREMONA, *Values in EU Foreign Policy*, in E. SCISO, R. BARATTA, C. MORVIDUCCI (eds.), *I valori dell'Unione europea e l'azione esterna*, Torino, 2016, p. 3; J. WOUTERS, *Enhancing the Rule of Lawin Europe and in the World: Mission Impossible,* in L. M. HINOJOSA-MARTÍNEZ, C. PÉREZ-BERNÁRDEZ (eds.), *Enhancing the Rule of Law in the European Union's External Action*, Cheltenham - Northampton, 2023, p. 18.

[5] Reference can be made to the "EU sanctions map" website (sanctionsmap.eu/#/main).

[6] europarl.europa.eu/RegData/etudes/BRIE/2024/760416/EPRS_BRI(2024)760416_EN.pdf, p. 3. For more information see P. VAN ELSUWEGE, V. SZÉP, *The Revival of Transatlantic Partnership? EU-US Coordination In Sanctions Policy*, in E. FAHEY (ed.), *The Routledge Handbook of Transatlantic Relations*, New York, 2024, p. 81.

restrictive measures were adopted with growing intensity by the EU in the realm of the CFSP to address, in whole or as a matter of priority, technological issues, with an emphasis on those related to digital evolution (hereinafter, "tech-related sanctions"). The main rules concerning these restrictive measures are contained in clauses generally added through amendments to the baseline acts, proving that the EU's focus on tech-related sanctions has been gaining momentum recently.

Even if the EU's tech-related sanctions can differ in scale and impact, they may have the potential to be particularly prejudicial for the development and – at times – the essential needs of the third countries concerned. In particular, since technological progress is one of the primary means of globalization, these measures can undermine the economic capacity of target States in their trade relations worldwide. That is also to be read in the light of the fact that technological development is a thriving ecosystem for the so-called «trade weaponization»[7].

It is thus believed that these tech-related sanctions are worth being analyzed and contextualized, also in order to bring added value to an academic landscape where sanctions keep being quite unexamined as a broader phenomenon of coercion in EU law. Accordingly, the present article aims to explore the main aspects of these measures and to offer legal insights about their placement in pivotal recent evolutionary trajectories of the European integration process.

The article is divided into two parts. The first part provides an overview of the tech-related sanctions that the EU has been adopting in the field of CFSP (paragraph 2). After providing an overview of the baseline (2.1), the attention is directed towards relevant EU coercive measures affecting the Russian Federation in the context of the aggression perpetrated on Ukraine (2.2), with an emphasis on those aimed at responding to hybrid threats or attacks against the Union (2.3). The second part aspires to anchor the EU's tech-related restrictive measures to the constitutional dimension of the EU legal order, by delving into core transformations that the EU's legal order is currently undergoing (paragraph 3), namely the digital transition (3.1), the pursuit

[7] L. J. ELIASSON, P. GARCIA-DURAN, *EU Trade Policy in Light of a Fragmented Liberal International Order*, in O. COSTA, E. SOLER I LECHA, M. C. VLASKAMP (eds.), *EU Foreign Policy in a Fragmenting International Order*, Cham, 2025, p. 41.

of the so-called European strategic autonomy – and technological sovereignty – (3.2), and the progressive convergence of national security priorities within the supranational security paradigm. In paragraph 4, conclusive remarks are put forward.

A final caveat is in order here, bearing in mind the above: for reasons of consistency, the article does not interrogate the lawfulness of these coercive measures under EU and international law, nor does it venture into technical assessments about their alleged effectiveness.

2. *The steady increase in tech-related sanctions at the Union level*

The EU's tech-related sanctions mainly integrate the category of "economic measures" and primarily amount to restrictions on imports and exports affecting many sectors (e.g., trade, defence, finance, transport, and energy).

These restrictions constitute a structured alternative framework to the imposition of "ordinary" sanctions to individuals and entities somehow operating in various ways in the area of technology, since they often add to arms embargoes, travel bans, and asset freezes.

The initiatives taken in this respect fall within a legal framework that allows the Union to enjoy a wide margin of manoeuvre from a legal point of view, even in the face of the explicit commitment (to be read also under the light of Art. 3, para. 5, TEU)[8] to always respect international law when restrictive measures are adopted and implemented[9] (and leaving aside any reasoning on the autonomy of the EU legal order).[10]

---

[8] This provision runs as follows: «(i)n its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens. It shall contribute to peace, security, the sustainable development of the Earth, solidarity and mutual respect among peoples, free and fair trade, eradication of poverty and the protection of human rights, in particular the rights of the child, as well as to the strict observance and the development of international law, including respect for the principles of the United Nations Charter».

[9] Council of the European Union, Sanctions Guidelines – update, 5664/18, 4 May 2018, point 9.

[10] For comprehensive analyses on this complex topic, see B. CORTESE, *L'ordinamento dell'Unione Europea, tra autocostituzione, collaborazione e autonomia*, Torino, 2018; K. LENAERTS, *The autonomy of European Union Law*, in *DUE*, n. 4, 2018, p. 627; N. NIC SHUIBHNE, *What is the autonomy of EU law, and why does that matter?*, in *NJIL,* n. 1, 2019, p. 9; L. LIONELLO, *L'autonomia dell'ordinamento giuridico*

Chiefly, it is worth recalling the leeway enjoyed by the Council, bearing in mind that these measures are inspired by some core CJEU's findings in the *Rosneft* judgment concerning EU restrictions in response to unprovoked infringement of Ukrainian sovereignty and territorial integrity by the Russian Federation. Here, the Court confirmed that Council has broad discretion in determining both the persons/entities that are to be subject to the restrictive measures (given the wide scope of the aims and objectives of the CFSP) and the type of restrictions to adopt (if they refer to areas which involve the making of political, economic and social choices, and in which complex assessments are to be undertaken).[11]

2.1. *Preliminary overview*

To begin with, four horizontal categories of thematic restrictions now exist, which include human rights, chemical weapons, terrorism, and cyber-attacks. It goes without saying that these cross-cutting topics are increasingly connected with technological issues.

Special attention has to be directed to the cybersecurity domain, due to the establishment, in 2019, of the Cyber Diplomacy Toolbox

dell'Unione Europea. Significato, portata e resistenze alla sua applicazione, Torino, 2024; V. MORENO-LAX, K.S. ZIEGLER, *Autonomy of the EU Legal Order – A General Principle? On the Risks of Normative Functionalism and Selective Constitutionalisation*, in V. MORENO-LAX, P. J. NEUVONEN, K. S. ZIEGLER (eds.), *Research Handbook on General Principles in EU Law Constructing Legal Orders in Europe*, Cheltenham – Northampton, 2022, p. 227; M. KONSTANTINIDIS, *Demystifying Autonomy: Tracing the International Law Origins of the EU Principle of Autonomy,* in *GLJ*, n. 1, 2024, p. 94; C. CONTARTESE, *The Principle of Autonomy in EU External Relations Law*, Padova, 2025.

[11] Judgment of the Court of Justice of 28 March 2017, Case C-72/15, *Rosneft*, paragraphs 88 and 113. On this judgment, see M. GATTI, *Juridiction de la Cour de justice sur les renvois préjudiciels en matière de Politique étrangère et de sécurité commune. A propos de l'arrêt* Rosneft *de la CJUE,* in *AFDI*, 2018, p. 440; L. LONARDO, *Law and Foreign Policy Before the Court: Some Hidden Perils of Rosneft,* in *EP*, n. 2, 2018, p. 547; S. POLI, *The Common Foreign Security Policy after Rosneft: Still Imperfect but Gradually Subject to the Rule of Law. Case C-72/15, The Queen (PJSC Rosneft Oil Company) v. Her Majesty's Treasury, Judgment of the Court of Justice (Grand Chamber), of 28 March 2017, EU:C:2017:236*, in *CMLR*, n. 6, 2017, p. 1799; P. VAN ELSUWEGE, *Securing a Coherent System of Judicial Protection in Relation to Restrictive Measures:* Rosneft, in G. BUTLER, R. A. WESSEL (eds.), U *External Relations Law: The Cases in Context*, Oxford, 2022, p. 881.

(CDT)[12] – to which the Hybrid Toolbox and Foreign Information Manipulation and Interference Toolbox were added – an unprecedented mechanism operating at the EU level as a CFSP instrument.

Under the CDT, sanctions can be adopted in order to better prevent, discourage, deter and respond to malicious behaviour in cyberspace. The CDT is global in scope and mainly entails traditional targeted sanctions, like travel bans and asset freezes towards targets that were found to have perpetrated (or to have been involved in) cyber-attacks. In addition, it is prescribed that no funds or economic resources shall be made available directly or indirectly to or for the benefit of the targeted subjects.[13]

This sanction framework is aimed at affecting persons and entities as the baseline CFSP Decision excludes "incursions" in the area of the attribution of international responsibility.[14] However, since the recent practice of cyberattacks against the EU and the Member States strongly suggests that the perpetrators acted with the support or under the direction of third countries' governments, it was argued that CDT sanctions may be symptomatic – at least to a certain extent – of the indirect attribution of responsibility to States.[15]

Regarding export restrictions, the EU introduced bans on dual-use items,[16] namely goods and technology that can be used for both civilian and military applications. This subject inevitably revives legal

[12] Council Decision (CFSP) 2019/797, of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States; Council Regulation (EU) 2019/796, of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States. See also Commission Recommendation (EU) 2017/1584, of 13 September 2017, on coordinated response to large-scale cybersecurity incidents and crises, C/2017/6100; Council of the European Union, Revised Implementing Guidelines of the Cyber Diplomacy Toolbox, doc. 10289/23, 8 June 2023.

[13] See Art. 5 of Decision (CFSP) 2019/797, cit.

[14] *Ibidem*, Recital 9: «(t)argeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State». See also S. POLI, E. SOMMARIO, *The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions*, in *GLJ*, 2023, p. 522.

[15] Y. MIADZVETSKAYA, R. A. WESSEL, *The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox,* in *EP*, n. 1, 2022, p. 434.

[16] For more information see C. CELLERINO, *I beni a duplice uso e la* dual-use technology, in M. VELLANO, A. MIGLIO, *op. cit.*, p. 313.

uncertainties dating back many years, when the nature of EU restrictions on dual-use exports was at the edge of both the Common Commercial Policy (CCP) and CFSP;[17] for this reason, it was assumed that sanctions referring to such items were halfway between commercial rules, foreign policy and security interests.[18] Nowadays, prohibitions of dual-use goods and technology export apply in the context of sanctions regimes against the Democratic People's Republic of North Korea, Iran, and Myanmar, generally on the basis of or in combination with UN Security Council's measures.[19]

Further restrictions – that have progressively become more independent from UN's sanctions – are contained in clauses prohibiting to provide, directly or indirectly, technical assistance, brokering services and other services referring to technological aspects, as well as specific technology and software. The scope and degree of intensity of such prohibitions varies depending on the State against which the measure is directed. Typically, they refer to the content of the Common Military List of the European Union or are related to the provision, manufacture,

[17] See also M. BROMLEY, *The EU Dual-Use Regulation, Cyber-Surveillance, and Human Rights:the Competing Norms and Organised Hypocrisy of EU Export Controls*, in *Defence Studies*, 2023, p. 648. The CJEU, yet long ago, endeavoured to restrict the EU law coverage on dual-use to the realm of common commercial policy (Judgment of the Court of Justice of 17 October 1995, Case C-70/94, *Werner/Bundesrepublik Deutschland*; of 17 October 1995, Case C-83/94, *Leifer e a.*); accordingly, the EU's legislation on dual-use exports was traced back to the scope of this policy.

[18] I. A. COLUSSI, *International Trade Sanctions related to Dual-Use Goods and Technologies*, in *Athens Journal of Law*, n. 4, 2016, p. 249.

[19] The first situation refers to North Korea: see especially Consolidated text of Council Decision (CFSP) 2016/849, of 27 May 2016, concerning restrictive measures against the Democratic People's Republic of Korea and repealing Decision 2013/183/CFSP, Recital 10 and Art. 1(1)c)-d); Consolidated text of Council Regulation (EU) 2017/1509, of 30 August 2017, concerning restrictive measures against the Democratic People's Republic of Korea and repealing Regulation (EC) No 329/2007, Art. 3(2). The second scenario includes, for example, Iran: see Consolidated text of Council Decision of 26 July 2010 concerning restrictive measures against Iran and repealing Common Position 2007/140/CFSP, Recital 9 and Art. 1(1)e); Consolidated text of Council Regulation (EU) No 267/2012, of 23 March 2012, concerning restrictive measures against Iran and repealing Regulation (EU) No 961/2010, especially Annex II. EU-only sanctions concerning dual-use items apply, for instance, to Myanmar: see Council Consolidated text of Decision 2013/184/CFSP, of 22 April 2013, concerning restrictive measures in view of the situation in Myanmar/Burma, Art. 1(a)(1); Consolidated text of Council Regulation (EU) No 401/2013 concerning restrictive measures in view of the situation in Myanmar/Burma and repealing Regulation (EC) No 194/2008, Art. 3a.

maintenance and use of goods included in that list, to any person, entity or body in the target country (or indicated in a dedicated annex to the normative act concerned): this is the case of the legal regimes concerning the situation in Afghanistan,[20] the Democratic Republic of the Congo,[21] the Central African Republic,[22] Somalia,[23] Libya,[24] and Venezuela.[25] Sometimes, instead, the field of application of tech-related sanctions is broader, meaning that it goes beyond the boundaries of the Common Military List and is generally represented by a dedicated Annex (regularly updated) to the applicable act: this is what can be found in the CFSP legal frameworks concerning restrictive measures against the Democratic

[20] Consolidated text of Council Regulation (EU) No 753/2011, of 1 August 2011, concerning restrictive measures directed against certain individuals, groups, undertakings and entities in view of the situation in Afghanistan, Art. 2 (see also Consolidated text of Council Decision 2011/486/CFSP, of 1 August 2011, concerning restrictive measures directed against certain individuals, groups, undertakings and entities in view of the situation in Afghanistan).

[21] Consolidated text of Council Regulation (EC) No 1183/2005, of 18 July 2005, concerning restrictive measures in view of the situation in the Democratic Republic of the Congo, Art. 1a (see also Consolidated text of Council Common Position 2005/440/CFSP, of 13 June 2005, concerning restrictive measures against the Democratic Republic of Congo and repealing Common Position 2002/829/CFSP).

[22] Consolidated text of Council Regulation (EU) No 224/2014, of 10 March 2014, concerning restrictive measures in view of the situation in the Central African Republic, Art. 2 (see also Consolidated text of Council Decision 2013/798/CFSP, of 23 December 2013, concerning restrictive measures against the Central African Republic).

[23] Consolidated text of Council Regulation (EU) No 356/2010, of 26 April 2010, imposing certain specific restrictive measures directed against certain natural or legal persons, entities or bodies, in view of the situation in Somalia, Art. 8 (see also Consolidated text to Council Decision 2010/231/CFSP, of 26 April 2010, concerning restrictive measures against Somalia and repealing Common Position 2009/138/CFSP).

[24] Consolidated text of Council Regulation (EU) 2016/44, of 18 January 2016, concerning restrictive measures in view of the situation in Libya and repealing Regulation (EU) No 204/2011, Art. 3 (see also Consolidated text of Council Decision (CFSP) 2015/1333, of 31 July 2015, concerning restrictive measures in view of the situation in Libya, and repealing Decision 2011/137/CFSP).

[25] Consolidated text of Council Regulation (EU) 2017/2063, of 13 November 2017, concerning restrictive measures in view of the situation in Venezuela, Art. 2 (Council Decision (CFSP) 2017/2074, of 13 November 2017, concerning restrictive measures in view of the situation in Venezuela).

People's Republic of Korea,[26] addressing against certain persons, entities and bodies in Iran,[27] and regarding the situation in Syria.[28]

In certain cases, special attention was paid to specific priorities. To list but a few, restrictions may affect the export of computers and related services,[29] as well as technology or software intended primarily for use in the monitoring or interception of internet or telephone communications[30] or for use in activities connected to the production of selected energy sources (e.g., for the functioning of Iranian nuclear industries or the construction of new electricity power plants in Syria).

2.2. *The latest stage: the case of the Russian Federation*

The trend illustrated above has intensified in the aftermath of the Russian Federation's military illegal and unprovoked aggression against Ukraine since February 2022.[31]

Predictably, that constituted a "stress test" for the CFSP. The scale of the international conflict, the fact that it is taking place in Europe, and the lack of UN-based sanctions against the Russian Federation (due to the veto power that Russia enjoys within the Security Council) led the European Union to adopt a set of unprecedented restrictive measures.[32]

---

[26] Council Regulation (EU) 2017/1509, cit., especially Art. 3.

[27] Council Regulation (EU) No 359/2011, cit., especially Art. 1c.

[28] Consolidated text of Council Regulation (EU) No 36/2012, of 18 January 2012, concerning restrictive measures in view of the situation in Syria and repealing Regulation (EU) No 442/2011, especially Arts. 2a and 3 (see also Consolidated text of Council Decision 2011/782/CFSP, of 1 December 2011, concerning restrictive measures against Syria and repealing Decision 2011/273/CFSP).

[29] This restriction is provided for, safe exceptions, in Council Regulation (EU) 2017/1509 (Democratic People's Republic of Korea), cit., Art. 18.

[30] For example, *Ibidem*, Art. 1b, para. 3; Council Regulation (EU) No 36/2012, cit. (Syria), Art. 4, paras. 2 and 3; Council Regulation (EU) No 401/2013, cit. (Myanmar), Art. 3b, para. 3, Council Regulation (EU) 2017/2063, cit. (Venezuela), Art. 6, para. 3.

[31] It is worth pointing out that since the beginning of the 2022 conflict, the UN General Assembly has taken a clear stand about the existence of a breach of Art. 2(4) of the UN Charter committed by Russia. See Resolution adopted by the General Assembly on 2 March 2022, A/RES/ES-11/1.

[32] See in particular: Consolidated text of Council Decision 2014/145/CFSP, of 17 March 2014, concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine; Consolidated text of Council Regulation (EU) No 269/2014, of 17 March 2014, concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine; Consolidated text of

It has to be specified that the approach chosen by the EU represents an evolution of the CFSP initiatives introduced in 2014 after Russia's illegal annexation of Crimea and Sevastopol.[33] The sanctions adopted by the EU – often in conjunction with like-minded States – range from numerous traditional and individual restrictions to diplomatic and, above all, economic sanctions designed to produce a widespread impact. Indeed, the escalation of the EU's sanctioning powers has been occurring in a scenario characterized by great repercussions on international trade relations[34] and was perceived to coincide with a sort of "economic war".[35]

Council Decision 2014/512/CFSP, of 31 July 2014, concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine; Consolidated text of Council Regulation (EU) No 833/2014, of 31 July 2014, concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine; Consolidated text of Council Decision (CFSP) 2022/266, of 23 February 2022, concerning restrictive measures in response to the illegal recognition, occupation or annexation by the Russian Federation of certain non-government controlled areas of Ukraine; Consolidated text of Council Regulation (EU) 2022/263, of 23 February 2022, concerning restrictive measures in response to the illegal recognition, occupation or annexation by the Russian Federation of certain non-government controlled areas of Ukraine. Some restrictive measures also hit Belarus in response to the support provided to the perpetuation of Russia's aggression.

[33] However, it should not be forgotten that, in 2014, the EU also adopted restrictive measures against Ukraine, due to the use of violence during the internal crisis experienced by this country at that time. See, for example, C. MASSA, *EU's Restrictive Measures in Ukraine before the CJEU: Taking Stock*, in *EJ*, n. 1, 2021, p. 31.

[34] D. PAUCIULO, *Le misure restrittive del commercio adottate nel contesto del conflitto in Ucraina alla prova del diritto OMC,* in *Quaderni di SIDIBlog*, *2022*, 2023, p. 79.

[35] For an overview of the EU's sanctions regimes against Russia over the last decade, with an emphasis on the post-2022 period, see: F. GIUMELLI, *The Redistributive Impact of Restrictive Measures on EU Members: Winners and Losers from Imposing Sanctions on Russia*, in *JCMS*, n. 5, 2017, p. 1062; C. PORTELA, P. POSPIESZNA, J. SKRZYPCZYŃSKA, D. WALENTEK *Consensus Against all Odds: Explaining the Persistence of EU Sanctions on Russia,* in *JEI*, n. 6, 2021, p. 683; A. ALÌ, *Dalle misure restrittive dell'Unione europea alla "guerra economica" nei confronti della Russia e della Bielorussia a seguito dell'invasione dell'Ucraina*, in *Questione Giustizia*, 2022, p. 42; See more in general L. LONARDO, *Russia's 2022 War Against Ukraine and the Foreign Policy Reaction of the EU: Context, Diplomacy, and Law*, Cham, 2022; P. A. VAN BERGEIJK, *Sanctions Against the Russian War on Ukraine: Lessons from History and Current Prospects*, in *JWT*, n. 4, 2022, p. 571; C. ABLEY, *The Russia Sanctions. The Economic Response to Russia's Invasion of Ukraine*, Cambridge, 2023; A. HORFER, *The EU's 'Massive and Targeted' Sanctions in Response to Russian Aggression, a Contradiction in Terms*, in *CYELS*, 2023, p. 19; K. MEISSNER, C. GRAZIANI, *The transformation and design of EU restrictive measures against Russia,* in *JEI*, n. 3, 2023, p. 377; S. POLI, F. FINELLI, *Context specific and Structural Changes*

Now, with the outbreak of the 2022 conflict, the EU started to increase the volume of comprehensive sanctions alongside (or, sometimes, in lieu of) targeted ("smart") ones. Technology is an indicative element in this respect.

Yet in 2014, the sanctions adopted by the EU also referred to sectors or companies operating in the area of technology. However, these sanctions mainly related to technologies included in the Common Military List and dual-use goods for military application; further limitations were provided for upstream technologies in an attempt to affect the Russian oil industry. From 2022 on, tech-related sanctions adopted by the EU have increased in terms of both quantity and quality.

First of all, it has to be noted that the EU issued a multitude of targeted sanctions against natural and legal persons that play a significant role for Russia's technology, and the addressees of these sanctions operate in fields that go beyond the production and implementation of technologies for the development of energy industries: in particular, these sanctions hit companies active in sectors like military and defence, aviation, shipbuilding, and machine building, but also IT and telecommunications. Part of these restrictions were designed under the CDT.

As for bans on goods and services, the EU established further limitations on trade in advanced dual-use technologies: to give some examples, software for drones or encryption devices, semiconductors, cutting-edge technologies, radio communication technology, and crypto-assets shall no longer be sold or otherwise supplied for use in Russia or to Russian entities.

In addition to this, since the adoption of the first package of sanctions, the EU introduced intensive restrictions on trade and investments connected to important technological sectors. Above all, embargoes were established on many items. Among these are not only technologies applicable to the energy industry (especially oil refining) but also cutting-edge technologies, as well as aviation, space, maritime navigation goods and technologies, plus radio communication technology, IT, electronic, and other goods having the potential to enhance Russia's industrial capacities, including critical technological

in EU Restrictive Measures Adopted in Reaction to Russia's Aggression on Ukraine, in *EJ*, n. 3, 2023, p. 19.

sectors. With these measures, the EU also prohibited certain services such as crypto asset wallets, IT consultancy and legal advice, technical assistance, intellectual property rights and trade secrets related to technology covered by other sanctions.

This trend has become even more pronounced in the last months, as the Council decided to considerably broaden the list of persons, entities, and bodies on which tighter export restrictions regarding strategic technology are imposed in an attempt to affect the technological enhancement of Russia's defence and security sectors; most notably, the list now includes also entities in other third countries which were targeted because of their contribution to Russia through the circumvention of export restrictions.[36]

The restrictive measures discussed in this paragraph may be enhanced through further initiatives. Suffice here to recall the imposition on EU exporters of a new contractual clause, in principle applicable when they intend to sell, supply, transfer, or export to a third country and prohibiting re-exportation to and for use in the Russian Federation of dual-use goods and advanced military technology. Moreover, also prohibitions concerning Russian road transport operators, carriers and vessels may be relevant, especially to further limit the Russian industry in the field of technology.

2.3. *Further developments: reactions against hybrid threats against the EU in the context of the Russia-Ukraine conflict*

The array of CFSP measures against Russia in the context of the current conflict also includes acts aimed at directly protecting the Union's values, fundamental interests, security, independence, and integrity. The restrictive measures adopted to tackle Russian (or Russian-driven) operations against the EU's value system may be seen as

[36] Council Decision (CFSP) 2024/3187, of 16 December 2024, amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine; Council Regulation (EU) 2024/3192, of 16 December 2024, amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

striking examples of what in literature was called «negative democracy promotion».[37]

These sanctions were mainly taken to counter hybrid actions put in place to fracture European society and undermine political decision-making (especially with respect to the well-functioning of the democratic process behind the renewal of the EU's institutional framework). Technology is a relevant element in this context, as many wrongdoings perpetrated by the Russian Federation on European soil consist of hybrid activities, including intimidation, sabotage, subversion, foreign information manipulation and interference, disinformation, and malicious cyber.

For instance, the EU imposed travel bans or asset freezes against natural or legal persons, entities, or bodies that are responsible for, implementing, supporting, or benefitting from actions or policies by the Russian Government that undermine or threaten democracy, the rule of law, stability or security in the Union, or in one or more of its Member States.[38] Other measures have acquired a more pronounced digital dimension, directly aiming at internet infrastructures,[39] due to the need to respond to hybrid threats[40] (e.g. cyber warfare and disinformation strategies) deployed against the Union and its Member States.

A totally new aspect is represented by the EU's sanctions against certain Russian broadcasters and channels.[41] These extraordinary measures determined the suspension of broadcasting activities of outlets directly or indirectly controlled by the Russian State. The ban imposed

[37] P. J. CARDWELL, *Explaining the EU's Legal Obligation for Democracy Promotion: The Case of the EU-Turkey Relationship*, in *EP*, n. 3, 2017, p. 870.

[38] See in particular Council Decision (CFSP) 2024/2643, of 8 October 2024, concerning restrictive measures in view of Russia's destabilising activities; Council Regulation (EU) 2024/2642, of 8 October 2024, concerning restrictive measures in view of Russia's destabilizing activities.

[39] N. TEN OEVER, C. PERARNAUD, J. KRISTOFF, M. MÜLLER, M. RESING, A. FILASTO, C. KANICH, *Sanctions and Infrastructural Ideologies: Assessing the Material Shaping of EU Digital Sovereignty in Response to the War in Ukraine*, in *Policy & Internet*, 11 September 2024, p. 2.

[40] See more in detail L. LONARDO, *EU Law Against Hybrid Threats: A First Assessment*, in *EP*, n. 2, 2021, p. 1075.

[41] The following outlets have been sanctioned so far: Rossiya RTR/RTR Planeta; Rossiya 24/Russia 24; Rossiya 1; Rossiyskaya Gazeta; Spas TV Channel; Sputnik and its subsidiaries; Tsargrad TV Channel; TV Centre International; Voice of Europe; Izvestia; Katehon; New Eastern Outlook; NTV/NTV Mir; Oriental Review; Pervyi Kanal; REN TV; RIA Novosti; Russia Today and its subsidiaries.

by the EU affects all means of transmission and distribution in or directed towards the Member States, including cable, satellite, Internet Protocol TV, platforms, websites and apps.[42] As one can see, the restrictions at stake penetrate inside the Russian telecommunications sector and affect subjects that may play a meaningful role in digital markets.

These sanctions were primarily intended to tackle disinformation and pro-Russia propaganda during the conflict, which was seen as a widespread threat capable of going beyond the battlefield. Such systematic initiatives have repeatedly and consistently targeted European political parties, especially during election periods, as well as civil society, thereby threatening the functioning of democratic institutions in the Union and its Member States. In this way, the Union clearly showed its aspiration to shield as much as possible freedom of expression and information, not only as the core of Art. 11 of the EU Charter of Fundamental Rights (Charter) but also as a component of its system of values.[43] This remains true even if there is no lack of contrary opinions, based on which such bans could amount to severe restrictions to that same freedom.[44]

The General Court scrutinized this kind of sanctions in a recent judgment, *R T France v Council*.[45] In this case, the applicant sought

[42] However, these media outlets and their staff are not prevented from carrying out activities in the EU that do not involve broadcasting.

[43] That, in turn, echoes one of the main findings of the *Tele2 Sverige* judgment, where the CJEU held that the right to freedom of expression under Art. 11 of the Charter, in the light of its particular importance in any democratic society, «constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded»: Judgment of the Court of Justice of 21 December 2016, Case C-203/15, *Tele2 Sverige AB*, paragraph 93.

[44] See, for example, the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (General Assembly A/77/288, 12 August 2022), where it was argued that «the necessity and proportionality of the ban has been questioned in a region where independent media and fact-checkers are able to challenge disinformation and where other less drastic measures could have been considered». See also D. KORFF, *The EU ban on Russian media: some worrying implications* (available here ianbrown.tech/2024/08/07/the-eu-ban-on-russian-media-some-worrying-implications, 7 August 2024).

[45] Judgment of the General Court of EU of 27 July 2022, Case T-125/22, *R T France v Council of the European Union*. For (different) opinions on this judgment, see S. DE VIDO, *La sentenza del Tribunale nel caso R T France c. Consiglio: la propaganda di guerra e il ruolo di imprese operanti nel settore della radiodiffusione nell'aggressione russa contro l'Ucraina*, in *OIDU*, n. 4, 2022, p. 1086; G. F. LENDVAI, *Media in War: An Overview of the European Restrictions on Russian Media,* in *EP*, n. 3, 2023, p. 1235; L. LONARDO, *Censorship in the EU as a Result of the War in Ukraine. Case*

annulment of acts adopted in the framework of CFSP by claiming the infringement of the rights of defence, freedom of expression and information, conduct a business, and the principle of non-discrimination on the grounds of nationality.[46] The General Court first highlighted the wide margin of manoeuvre to the benefit of the Council in the field of CFSP and noted that the objectives behind the measure at hand could be better pursued at the EU level, instead of based on initiatives taken by national competent authorities. Moreover, in light of the extraordinary context of the case, the General Court balanced the fundamental rights invoked by the applicant (chiefly, freedom of expression) against a pivotal objective of general interest, namely protecting the Union's public order and security, and concluded that, in the framework of Art. 52(1), of the Charter, those limitations – which could only be urgent and compelling in light of the goals to pursue – were lawful. The General Court's judgment, thus, confirms the tight link between restrictive measures aimed at the cessation of a continuous and concerted propaganda activity to the detriment of the Union's civil society and the EU's values, fundamental interests, security, integrity, and public order.

3. *Anchoring tech-related sanctions to the ongoing European Union's metamorphosis process*

The analysis carried out in the previous pages makes the case that the EU has been resorting to tech-related sanctions more frequently and intensely over last years. This trend further confirms the consolidation of the growing leadership position on sanctions that the EU has

T-125/22 RT France v Council, in *ELR*, n. 6, 2023, p. 707; S. POLI, F. FINELLI, *Le misure restrittive russe davanti alla Corte di giustizia dell'Unione europea: le tendenze giurisprudenziali emergenti*, in *DUE*, n. 3, 2023, p. 36; V. SZÉP, R. A. WESSEL, *Balancing Restrictive Measures and Media Freedom:* RT France v. Council, in *CMLR*, n. 5, 2023, p. 1384.

[46] RT France's entire share capital was held by TV Novosti, an autonomous not-for-profit association in the Russian Federation.

progressively acquired;[47] according to some scholars, it may also stimulate the evolution of international law on sanctions.[48]

However, that could beg the question if these are to be seen as stand-alone measures or if they are the expression of a larger pattern. Here, it is argued that the attention paid by the Union to technology in the field of CFSP, especially where the restrictive measures are determined autonomously, is to a large extent in line with some of the main pillars upon which the recent evolution of the European integration process rests. By virtue of the consistency principle, tech-related sanctions can have their proper place in the framework of some pivotal transformations that the European Union is developing also through legal instruments and in the face of multilevel challenges primarily arising in the framework of international relations.

Indeed, there is a gap in terms of technological evolution that is affecting the positioning of the EU on the geopolitical plane at the global level. This gap is particularly evident if one considers very influential States like the US and China; the same goes for powerful private companies, since the main "tech giants" are located outside the EU. In view of this disadvantage, the EU is trying to exploit its legal toolbox to introduce new rules and standards and extend their application as far as possible[49].

Therefore, further remarks are now to be made by considering the sanctions at stake from a broader and constitutionally oriented perspective, having the protection of the internal market, fundamental rights, and the EU's essential interests at its core.

---

[47] P. J. CARDWELL, E. MORET, *The EU, Sanctions and Regional Leadership*, in *European Security*, 2023, p. 1.

[48] See in particular A. M. AMOROSO, *Il contributo delle misure restrittive UE contro la Russia allo sviluppo del diritto internazionale delle sanzioni*, in *DC*, 31 May 2022. The Author explains that if those restrictive measures are lawful *per se*, they can be covered by Art. 41(1) of the 2001 Draft Articles on Responsibility of States for Internationally Wrongful Acts, which prescribes a cooperation duty to bring to an end any serious breach by a State of an obligation arising under a peremptory norm of general international law (*jus cogens*). Instead, if it is assumed that some of these EU's sanctions have – *a priori* and at least in part – the connotations of international law breaches, the action of the Union and its Member States may also have the effect of paving the way for the establishment of a customary rule allowing the lawfulness of countermeasures adopted to react to violations of *erga omnes* obligations.

[49] In this respect, see *inter alia* E. FAHEY, *The European Union as a Digital Trade Actor: The Challenge of Being a Global Leader in Standard-Setting*, in *International Trade Law and Regulation*, 2021, p. 155.

3.1. *The baseline: the Union's digital transition*

The intensification of the EU's regulatory process having technology at its heart is well-known, in particular as regards the digital sector[50]. Multiple initiatives – including strategies – were launched by the EU institutions (notably, the European Commission) to contribute to the digital transition of the Union and to the establishment of rules applicable to emerging technologies[51]. That resulted in the adoption of numerous pieces of legislation in sensitive sectors like privacy and data protection,[52] e-commerce and online platforms,[53] artificial intelligence,[54]

[50] See above all V. PAPAKONSTANTINOU, P. DE HERT, *The Regulation of Digital Technologies in the EU Act-ification, GDPR Mimesis and EU Law Brutality at Play*, Oxon–New York, 2024.

[51] To list but a few: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Market Strategy for Europe*, COM (2015) 192final, 6 May 2015; European Commission, White Paper *On Artificial Intelligence - A European approach to excellence and trust*, COM (2020) 65final, 19 February 2020; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A European strategy for data*, COM (2020) 66final, 19 February 2020; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Shaping Europe's digital future*, COM (2020) 67final, 19 February 2020; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *2030 Digital Compass: the European way for the Digital Decade*, COM (2021) 118final, 9 March 2021.

[52] Regulation (EU) 2022/868 of the European Parliament and of the Council, of 30 May 2022, on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act); Regulation (EU) 2023/2854 of the European Parliament and of the Council, of 13 December 2023, on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828.

[53] Regulation (EU) 2022/2065 of the European Parliament and of the Council, of 19 October 2022, on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act); Regulation (EU) 2022/1925 of the European Parliament and of the Council, of 14 September 2022, on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[54] Regulation (EU) 2024/1689 of the European Parliament and of the Council, of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

dual-use,[55] cybersecurity,[56] and sectoral technologies.[57] This transformation stands out for two characteristic traits of a constitutional nature.

The first is the legal basis. Most of the acts adopted to boost the trend being discussed here are internal market regulations and (to a lesser extent) directives composing a legal framework extensively shaped by the EU; they are therefore harmonization measures based on Art. 114 TFEU. However, it is increasingly evident that the EU legislator is making use (without objections) of this provision in a multitude of scenarios, some of which are at the edge of areas where, according to the founding Treaties, supranational competencies and powers should be limited:[58] the recent set of interventions concerning the development of the European Defence Technological and Industrial Base is a case in point, given its entrenchment in the realm of the internal market.[59]

---

[55] Regulation (EU) 2021/821 of the European Parliament and of the Council, of 20 May 2021, setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast).

[56] Directive (EU) 2022/2555 of the European Parliament and of the Council, of 14 December 2022, on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[57] Regulation (EU) 2023/1781 of the European Parliament and of the Council, of 13 September 2023, establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act); Regulation (EU) 2024/1309 of the European Parliament and of the Council, of 29 April 2024, on measures to reduce the cost of deploying gigabit electronic communications networks, amending Regulation (EU) 2015/2120 and repealing Directive 2014/61/EU (Gigabit Infrastructure Act).

[58] As regards the progressive broadening of Art. 114 TFEU's scope of application see *ex multis*: S. WEATHERILL, *The Limits of Legislative Harmonization Ten Years after* Tobacco Advertising*: How the Court's Case Law has become a "Drafting Guide",* in *GLJ*, n. 3, 2011, p. 827; B. DE WITTE, *A competence to protect The Pursuit of Non-Market Aims through Internal Market Legislation*, in P. SYRPIS (ed.), *The Judiciary, the Legislature and the EU Internal Market*, Cambridge, 2012, p. 25; T. M. MOSCHETTA, *Il ravvicinamento delle normative nazionali per il mercato interno. Riflessioni sul sistema delle fonti alla luce dell'art. 114 TFUE*, Bari, 2018; M. KELLERBAUER, *Article 114 TFEU*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Oxford, 2019, p. 1235; D. GALLO, S. POLI, *Enhancing European Technological Sovereignty: The Foreign Investment Screening Regulation and Beyond*, in K. A. ARMSTRONG, J. SCOTT, A. THIES (eds.), *EU External Relations and the Power of Law: Liber Amicorum In Honour of Marise Cremona,* Oxford, 2024, p. 215.

[59] A. MIGLIO, *L'Unione europea e l'"emergenza bellica": verso una politica industriale europea per la difesa*, in P. DE PASQUALE, A. LIGUSTRO (a cura di), *La gestione delle*

The second trait is the increased role of fundamental rights and democratic values in this legal environment, which is destined to breath more life into the text of rights and values-oriented primary law provisions such as Art. 21 TEU. Many of the pieces of legislation adopted to boost the EU's digital transition were elaborated on the assumption that this ambition goes hand in hand with risks for individuals, especially when they are confronted with powerful market operators like certain large-sized platforms. This represents the background of the so-called "European digital constitutionalism".[60] As a result, in the majority of these acts, the essence of the Charter is more visible; moreover, in some cases fundamental rights are part of the scope of the measure concerned or have become parameters against which the legality of the conduct of private subjects shall be checked. At the same time, its impact could be magnified by the action of the Court of Justice, as it happened in landmark fundamental rights judgments (e.g. *Digital Rights Ireland*[61] and *Schrems I*).[62] This process has culminated in the Union's founding values being concretized more effectively.[63]

Well, the increase in tech-related sanctions of various types is to a certain extent combined with the pivotal outcomes stemming from the progressive consolidation of such a regulatory approach. As confirmed by recent studies, with an emphasis on the EU's response to Russian

emergenze nel diritto dell'Unione e nel diritto internazionale. Emergenza energetica, ambientale e bellica, Napoli, 2024, p. 225.

[60] O. POLLICINO (ed.), *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, Oxford, 2021; E. CELESTE, *Digital Constitutionalism. The Role of Internet Bills of Rights*, London, 2022; G. DE GREGORIO, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022.

[61] Judgment of the Court of Justice of 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*: here, the Court declared the invalidity of Directive 2006/24/EC of the European Parliament and of the Council, of 15 March 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[62] Judgment of the Court of Justice of 6 October 2015, Case C-362/14, *Schrems*: with this judgment, the Court declared the invalidity of Commission 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

[63] F. FERRI, *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo*, in *DUE*, n. 2, 2022, p. 277.

aggression on Ukraine, the internal politics of the organization and the distribution of power have been important factors conditioning the definition of autonomous sanctions regimes.[64]

3.2. *The pursuit of the European Strategic Autonomy and Technological Sovereignty*

Notwithstanding the centrality of Art. 114 TFEU, the Union is promoting the goals concerning its digital transition also beyond the internal market sphere in order to exercise a considerable global role. This is all the more true if one looks at the matter as a whole through the paradigms of the European strategic autonomy[65] and technological sovereignty.[66]

Even if these expressions have not been conceptualized in a clear and uniform way at the EU level,[67] it can be affirmed that the latter is one of the pillars of the former and that, overall, this approach has been pioneered to make the Union fit to better preserve its interests and values worldwide.

---

[64] E. SANUS, S. AKGÜL-AÇIKMEŞE, H. EMRAH KARAOGUZ, *The EU's Autonomous Sanctions Against Russia in 2014 Versus 2022: How Does the Bureaucratic Politics Model Bring in the Institutional 'Balance of Power' Within the EU?,* in *JCMS*, n. 5, 2024, p. 1278.

[65] See *amplius* M. KOPPA, *The Evolution of the Common Security and Defence Policy. Critical Junctures and the Quest for EU Strategic Autonomy*, Cham, 2022.

[66] This expression is often used as a synonym for "digital sovereignty".

[67] N. HELWIG, V. SINKKONEN, *Strategic Autonomy and the EU as a Global Actor: The Evolution, Debate and Theory of a Contested Term,* in *EFALR*, 2022, p. 1; S. POLI, E. FAHEY, *The Strengthening of the European Technological Sovereignty and its Legal bases in the Treaties,* in *EJ*, n. 2, 2022, p. 147; D. BROEDERS, F. CRISTIANO, M. KAMINSKA, *In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions*, in *JCMS*, n. 5, 2023, p. 1261; P. DE PASQUALE, F. FERRARO, *L'autonomia strategica dell'Unione europea: dalla difesa…alla politica commerciale c'è ancora tanta strada da fare*, in *DPCE*, n. 2, 2023, p. V; J. CARVER, *More Bark than Bite? European Digital Sovereignty Discourse and Changes to the European Union's External Relations Policy*, in *Journal of European Public Policy*, n. 8, 2023, p. 2250; A. MIGLIO, G. PEROTTO, L. GROSSIO, *I meccanismi di finanziamento del settore difesa nell'Unione europea e il loro contributo al rafforzamento dell'autonomia strategica*, in *Centro Studi sul Federalismo*, January 2024, p. 9, csfederalismo.it/it/pubblicazioni/research-paper/imeccanismi-di-finanziamento-del-settore-difesa-nellunione-europea-e-il-loro-contributo-alrafforzamento-dellautonomia-strategica.

The increased supranational interventionism in the governance of technology[68] is instrumental to enable the Union to reach a sectoral leadership and a higher degree of independence[69] ahead of these purposes. Just to give an example, it is no coincidence that some the legislative acts epitomizing the digital transition of the EU were designed with a view to increasing the potential of the territorial extension[70] of some key rules and standards (e.g., the GDPR, the Regulations composing the Digital Services Package, and the Artificial Intelligence Act).[71]

For sure, also the EU's external action matters. It is in this perspective, first of all, that the EU intends to recalibrate its trade policy by adjusting the "physiognomy" of the CCP. The baseline idea is that «the EU can only succeed in its digital transformation if it builds its digital agenda in an outward-looking manner, taking full account of a global environment that is increasingly, fiercely competitive and sometimes challenging the EU's values-based approach to digitalisation».[72] These priorities were underscored also by the Council of the EU.[73]

But there is more, since the Union is also trying to mainstream key prerogatives of its digital transition throughout its existing foreign and

[68] See S. HEIDEBRECHT, *From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance*, in *JIMS*, n. 1, 2024, p. 205.

[69] For further considerations, see the *Special Focus on EU Strategic Autonomy and Technological Sovereignty*, edited by C. BEAUCILLON, S. POLI, 2023.

[70] It appears more appropriate to use this expression in lieu of the term "extraterritoriality". See J. SCOTT, *Extraterritoriality and Territorial Extension in EU Law*, in *AJCL*, n. 1, 2014, p. 87.

[71] See, for instance, H. SHEIKH, *European Digital Sovereignty: A Layered Approach,* in *Digital Society*, 2022, p. 20; M. BURRI, K. KUGLER, *Regulatory Autonomy in Digital Trade Agreements*, in *JIEL*, n. 3, 2024, p. 399; M. MÜLLER, M. C. KETTEMANN, *European Approaches to the Regulation of Digital Technologies*, in H. WERTHNER, C. GHEZZI, J. KRAMER, J. NIDA-RÜMELIN, B. NUSEIBEH, E. PREM, A. STANGER (eds.), *Introduction to Digital Humanism. A Textbook*, Cham, 2024, p. 623; M. ŠONKOVÁ, *Brussels Effect Reloaded? The European Union's Digital Services Act and the Artificial Intelligence Act*, in *EU Diplomacy Papers*, n. 4, 2024, p. 1.

[72] Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, *Trade Policy Review - An Open, Sustainable and Assertive Trade Policy*, COM (2021) 66final, 18 February 2021, p. 14.

[73] Council Conclusions on Digital Diplomacy, 10526/23, 19 June 2023.

security policy.[74] In this regard, it should not be forgotten that, even if the current Union's vision of strategic autonomy is (or should be) certainly broader than the original model, this concept first appeared in EU's documents concerning the external security of the organization and was immediately connected with technology; in fact, focusing on the Common Security and Defence Policy and Europe's defence industry, the European Council stated that «Europe needs a more integrated, sustainable, innovative and competitive defence technological and industrial base (…) to develop and sustain defence capabilities. This can also enhance its strategic autonomy and its ability to act with partners».[75]

Furthermore, in the 2022 Strategic Compass for Security and Defence it is possible to find other interesting indications.[76] This strategy refers a number of times to technology and postulates the implementation of an integrated approach to security characterized by the combination of diplomatic and economic instruments, «including (…) sanctions regimes». It also expresses the intention to enhance the EU's strategic autonomy and its ability to work with partners to safeguard its values and interests.

More in general, the European Commission recently placed the improvement of the implementation and enforcement of EU's sanctions regimes at the heart of a strategy for reinforcing strategic autonomy in core macro-economic and financial fields, including sectors closely related to technology.[77] But the fact is that restrictive measures, if used wisely, are supposed to be useful to maintain the Union's capacity to act

---

[74] For example, R. A. WESSEL, *European Law and Cyberspace*, in N. TSAGOURIAS, R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham Northampton, 2021, p. 507.

[75] European Council, Conclusion of 19 and 20 December 2013, EUCO 217/13, especially point 16.

[76] *A Strategic Compass for Security and Defence. For a European Union that Protects its Citizens, Values and Interests and Contributes to International Peace And Security*, especially pp. 14, 23 and 25. This strategy was deemed innovative from a theoretical point of view, but practically unfit in the face of the main current challenges: see M. VELLANO, *La guerra in Ucraina e le conseguenti decisioni dell'Unione europea in materia di sicurezza e difesa comune,* in *DUE*, n. 1, 2022, p. 130.

[77] Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, *The European Economic and Financial System: Fostering Openness, Strength and Resilience*, COM (2021) 32final, 19 January 2021.

independently to protect its values and interests under the umbrella of strategic autonomy;[78] in fact, the EU's sanctioning powers can fashion strategic autonomy as much as this goal defines sanctions.[79]

As one can see, there is a clear link between the proper definition and application of tech-related sanctions and the EU's interests referring to new prerogatives of the development of the internal market, also in light of the evolving challenges for fundamental rights and founding values. Specifically, having all the Member States aligned is a preliminary condition to increase the EU's credibility as a regulatory power worldwide and to preserve the integrity and the level playing field of an internal market underpinned by the essence of the Charter of fundamental rights. These restrictive measures, thus, concur to pinpoint distinctive elements of a theory illustrated in the literature and referring to the EU's (self-proclaimed) strategic autonomy and technological sovereignty; indeed, they consolidate the idea of «an axiological subordination of the substantive values of Articles 2 and 3(5) TEU to the meta-rationale of security»,[80] with the EU's internal market on the background.

3.3. *Towards a (more) supranational security*

The extension of the abovementioned priorities for the sake of strategic autonomy – and, accordingly, the "mantra" of technologic sovereignty – partly overlaps with a further transformation. The reference is to the progressive convergence of the essence of both national and EU security, due to the escalations of widespread hybrid attacks against Europe. This also applies to cyber threats originating from the context of battlefields located outside the Union, as with the Russia-Ukraine war.

More to the point, the need to preserve primary interests of the EU, like the cornerstones of the fundamental rights and founding values protection systems as well as those of (the digital version of) the internal

[78] E. VAN DEN ABEELE, *Towards a New Paradigm in Open Strategic Autonomy?* in *Working Paper*, 2021, p. 46.
[79] L. LONARDO, V. SZÉP, *The Use of Sanctions to Achieve EU Strategic Autonomy: Restrictive Measures, the Blocking Statute and the Anti-Coercion Instrument,* in *EFALR*, n. 4, 2023, p. 363.
[80] *Ivi*, pp. 374-376.

market, has been determining a reshaping of the EU-Member States security nexus. Despite the seemingly insurmountable demarcation lines drawn in the EU's founding Treaties – in particular, in the national security clause contained in Art. 4(2) TEU – with respect to national/supranational security prerogatives,[81] European security now tends to be considered «indivisible», bearing in mind that «any challenge to the European security order affects the security of the EU and its Member States».[82]

That is step-by-step shaping a less member state-driven scenario characterized by the increment of the Commission's weight,[83] also as regards the definition of the strategic interests under Art. 26(1) TEU. In this situation, the Union can exercise a more assertive capacity to strengthen supranational competences to the detriment of Member States' prerogatives.[84] In consequence, it was convincingly argued that a

[81] In this respect, C. NOTA, *Il futuro della PESC tra autonomia strategica e sovranità nazionale*, in *Quaderni AISDUE*, n. 3, 2024, p. 12. However, the introduction of this clause was considered to be quite limited, as it cannot be invoked by Member States to exclude the applicability of the law of the EU. The content of the clause at stake is thus to be interpreted under the light of the other principles enshrined in that same article. The Court has already clarified the matter. See in particular Judgment of the Court of Justice of 6 October 2020, Joined Cases C-511/18, C-512/18, C-520/18, *La Quadrature du Net*, paragraph 99: «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». For more insights on this issue see L. AZOULAI, *The "Retained Powers" Formula in the Case Law of the European Court of Justice: EU Law As Total Law?*, in *EJLS*, 2011, p. 192; G. DI FEDERICO, *L'identità nazionale degli Stati membri nel diritto dell'Unione europea: natura e portata dell'art. 4, par. 2, TUE*, Napoli, 2017, p. 156; G. DI FEDERICO, *Il ruolo dell'art. 4, par. 2, TUE nella soluzione dei conflitti interordinamentali*, in *QC*, n. 2, 2019, p. 337; F. FERRARO, *Brevi note sulla competenza esclusiva degli Stati membri in materia di sicurezza nazionale*, in AA.VV. (a cura di), *Temi e questioni di diritto dell'Unione europea. Scritti offerti a Claudia Morviducci*, Bari, 2019, p. 27; F. CASOLARI, *Leale cooperazione tra Stati membri e Unione europea: studio sulla partecipazione all'Unione al tempo delle crisi*, Napoli, 2020, p. 203.

[82] Council conclusions on the European security situation, 5591/22, 24 January 2022, p. 2. It should be noted that the Member States' representatives sitting in the Council clarified this position before the beginning of Russian invasion of Ukraine.

[83] C. PORTELA, *Sanctions and the Geopolitical Commission: The War over Ukraine and the Transformation of EU Governance*, in *EP,* n. 3, 2024, p. 1125.

[84] F. CASOLARI, *EU Sanctions Policy: A Legal Apprisal in Light of the EU's Strategic Autonomy Doctrine*, in G. ADINOLFI, A. LANG, C. RAGNI (eds.), *Sanctions by and Against International Organizations. Common Issues and Current Developments*, Cambridge, 2024, p. 47.

sort of «buffer zone» has emerged which is characterized by a «hybridization» of multilevel competences and instruments in security matters.[85]

Such goalposts moving is leading to the draining of security concerns in multiple sectors of different EU's policy areas, also due to the fact that European security is an inescapable precondition for sustainable growth, as confirmed in Mario Draghi's Report on "The Future of European Competitiveness".[86]

The recent institutional practice helps to understand the acceleration of the security paradigm shift at the EU level. The European Council's Strategic Agenda 2024-2029 revolves around European security[87] and affirms that the Union and the Member States will take the necessary responsibility for their security and defence, mobilizing the necessary instruments to ensure the EU's lead in addressing global challenges and championing international law and institutions; in the Agenda, there is a clear focus on the link between this ambition, the EU's economic base, and the digital transition of the organization. A similar approach was endorsed by the Polish Presidency of the Council of the EU.[88] Furthermore, among the principal guidelines of the "Von der Leyen II" Commission is "A new era for European Defence and Security". The new composition of the institution stands out for the presence of policy areas like "Tech Sovereignty, Security and Democracy" and "Trade and Economic Security". And the recent White Paper for "European Defence Readiness 2030" anticipates that, with a view to reducing dependencies and ensuring the security of supply, the EU will initiate a

[85] In this respect, F. CASOLARI, *Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine: The EU-Member States Security Nexus Revisited*, in *EFALR*, n. 4, 2023, p. 323.

[86] The report is available here: commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059.

[87] The text of the Agenda is available here: consilium.europa.eu/media/yxrc05pz/sn02167en24_web.pdf.

[88] See the Programme of the Polish Presidency of the Council of the European Union, launched early in 2025 under the motto "Security, Europe!", and available here polish-presidency.consilium.europa.eu/media/zkcno325/programme-of-the-polish-presidency-of-the-council-of-the-european-union.pdf.

long-term effort to address the issue of restrictions that are imposed on third-country technologies.[89]

An emblematic manifestation of this evolution is the strategy on economic security launched in June 2023 by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy.[90] The strategy is underpinned by a risk-based approach, which largely relates to the protection of the EU's core strategic critical infrastructure and technologies. Risks to the EU's economic security will be identified and assessed by the European Commission collectively with EU Member States. This process will be dynamic, continuous and carried out within clearly defined parameters.

However, it is pointed out that some risks are both evolving rapidly and merging with national security concerns, also referring to numerous technological issues. In addition, the Commission and the High Representative announced their intention to explore, in their respective competences, the targeted use of CFSP instruments to enhance EU economic security. Interestingly, the document concludes as follows: «(i)n an interconnected world, no country can act alone to ensure its economic security. In today's world, Member States' economic and national security interests, vulnerabilities and responses can rarely be seen or identified in isolation from those of other Member States or those of the Union as a whole. Individual Member State's interests are inextricably linked to the proper functioning of the internal market, the integrity of the EU trade policy and the security interests of the EU as a whole».[91]

All in all, it is fair to expect that the steady "securitization" of the EU's economy will lead to a more suitable operating environment for the imposition of more frequent and diversified restrictive measures, like those addressed in this work. For sure, the Union's tech-related sanctions can make a remarkable impact on crucial economic sectors of the third countries addressed time after time, thereby contributing to meeting

[89] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint White Paper for European Defence Readiness 2030*, JOIN (2025) 120final, 19 March 2025 (p. 14).
[90] Joint Communication To The European Parliament, the European Council and the Council *on "European Economic Security Strategy"*, JOIN (2023) 20final, 20 June 2023.
[91] *Ivi*, p. 14.

urgent needs related to supranational security, particularly with a view to impeding the ability of the sanctioned States to start or continue a conflict, as it happened in the case of the Russian Federation.

4. *Conclusive remarks*

Tech-related sanctions adopted in the framework of the CFSP have progressively become more frequent, widespread, and intensive. The Russia-Ukraine conflict has exacerbated this trend.

The evolution of the approach behind these coercive measures shows that the EU's extensive focus on technology in the domain of the internal market, and through the prisms of fundamental rights and founding values, has clearly been manifesting also in the external dimension, in particular for the pursuit of the European strategic autonomy and technological sovereignty. The expansion of the paradigm of supranational security is a core driver in this respect. In light of the above, tech-related sanctions could contribute to the emergence of a more consistent concept "common defence" at the EU level (whose development, as recently pointed out, mainly depends on the "creativity" of the Member States)[92] and the strengthening of the nexus between the CFSP and the CCP.[93]

Bearing in mind the theoretical and practical difficulty of bringing about a fair balance between the needs of the European Union and those of the Member States under a unitary constitutional pattern,[94] this perspective should still orient the elaboration of some Member States' strategic interests, which have long disregarded the EU's needs in terms of technological development in the fields of security and defence.[95] Indeed, the idea is that the integration process has not weakened

[92] C. CELLERINO, *La difesa europea dinanzi alla guerra in Ucraina tra "autonomia strategica" e vincoli strutturali: quali prospettive per la Difesa comune?*, in *Quaderni AISDUE*, n. 2, 2022, p. 23.

[93] See also J. G. OLMEDO, *The Legality of EU Sanctions under International Investment Agreements*, in *EFRLR*, 2023, p. 95. For considerations developed from a different angle, see A. OTT, G. VAN DER LOO, *The Nexus between the CCP and the CFSP: Achieving Foreign Policy Goals through Trade Restrictions and Market Access*, in S. BLOCKMANS, P. KOUTRAKOS (eds.), *op. cit.*, p. 230.

[94] In this respect, see E. CANNIZZARO, *Le relazioni esterne dell'Unione europea: verso un paradigma unitario?,* in *DUE*, n. 2, 2007, p. 237.

[95] In this respect, see F. MUNARI, *La politica di sicurezza e difesa comune nell'Unione: il tempo delle scelte,* in *EJ*, n. 3, 2024, p. 228.

Member States' ability to protect national interests, but has, if anything, enabled them to bring those interests into a system allowing all participants to benefit from the European perspective – in a spirit of mutual and sincere cooperation.[96] This is all the more true having account of the fact that, since Art. 21 TEU does not clearly distinguish values from interests, these two concepts overlap to a large extent, to the point that values could be seen as long-term interests.[97]

It is believed that the EU's approach to tech-related sanctions is part of a legal framework where the governance of security issues that also touch upon trade is being increasingly "centralized",[98] and where a growing geopolitical and technocratic Union[99] is proving more able to affect mechanisms traditionally inspired to the intergovernmental method. These measures may also contribute to fostering the spirit of interstate solidarity and to unleashing the potential of the coordinating role that the Union could exercise through the CFSP during international crises.[100]

More in general, tech-related sanctions partly express some kind of an emerging Union's statecraft in a context characterized by a broad fragmentation of the liberal international order that has inevitably changed the EU's foreign policy agenda and made its actorness harder to achieve.[101] In particular, tech-related sanctions are likely to end up being significant instruments for the reshaping of Union's relations with the wider world (to use the words of Art. 3(5) TEU), especially through

---

[96] F. CASOLARI, *Per una vera Unione di diritto: cinque priorità per l'ordinamento giuridico dell'Unione Europea*, in *federalismi.it*, n. 9, 2025, p. XIV.
[97] A. ROSAS, *EU Restrictive Measures against Third States: Value Imperialism, Futile Gesture Politics or Extravaganza of Judicial Control?,* in *DUE*, n. 4, 2016, p. 641.
[98] T. PERIŠIN, S. KOPLEWICZ, *The Nexus between the CCP and the CFSP*, in M. HAHN, G. VAN DER LOO (eds.), *Law and Practice of the Common Commercial Policy. The first 10 years after the Treaty of Lisbon*, Leiden – Boston, 2020, p. 414.
[99] A. PINTSCH, M. RABINOVYCH, *Geopolitical and Technocratic: EU International Actorness and Russia's War Against Ukraine*, in *Foundation Robert Schuman – Policy Paper – European Issues*, n° 657, 21 February 2023, available here old.robert-schuman.eu//en/doc/questions-d-europe/qe-657-en.pdf).
[100] For a general perspective on these aspects, see A. PAU, *The Solidarity Principle in the Context of the CFSP: The Adoption of Restrictive Measures as an Expression of Solidarity?*, in E. KASSOTI, N. IDRIZ (eds.), *The Principle of Solidarity. International and EU Law Perspectives*, The Hague, 2023, p. 237.
[101] O. COSTA, E. BARBÉ, *A Moving Target. EU Actorness and the Russian Invasion of Ukraine,* in *JEI*, n. 3, 2023, p. 435.

the consolidation of a more unitary role of the EU itself in the realm of security and on the international plane.

Time will tell if the intertwining of the evolving approach to sanctions and the major challenges of the European integration in the areas of the internal market and the protection of fundamental rights and values will make the Union something more akin to a security actor. However, the phenomenon discussed in the present work suggests that the new legal order of international law theorized in *Van Gend en Loos*[102] seems to be at an existential crossroad.

[102] Judgment of the Court of Justice of 5 February 1963, Case 16/62, *Van Gend en Loos*, paragraph 12.

ABSTRACT (ita)

Il fattore tecnologico è sempre più importante nell'approccio dell'Unione europea alle misure restrittive adottate nell'ambito della politica estera e di sicurezza comune. In virtù di ciò, con il presente articolo ci si propone di analizzare il quadro giuridico dell'Unione relativo alle sanzioni che prendono di mira aspetti strettamente collegati all'evoluzione tecnologica, con un'enfasi specifica sulla risposta all'aggressione della Russia all'Ucraina. Si procederà altresì alla contestualizzazione del fenomeno in una dimensione più ampia, a sua volta riconducibile alle trasformazioni del diritto UE di fronte a sfide di impatto costituzionale: la transizione tecnologica dell'Unione, la ricerca di una autonomia strategica e di una sovranità tecnologica europee, il progressivo rafforzamento del paradigma della sicurezza sovranazionale.

ABSTRACT (eng)

Technological factor is increasingly important in the Union's approach to restrictive measures taken under the Common Foreign and Security Policy. By virtue of this, the purpose of the present article is to analyze the EU legal framework for sanctions targeting aspects closely related to technological developments, with a specific emphasis on the EU response to Russia's aggression against Ukraine. An attempt will also be made to contextualize the phenomenon in a broader dimension, which in turn can be traced to the transformations of EU law in the face of challenges of constitutional impact: the Union's digital transition, the quest for European strategic autonomy and technological sovereignty, and the progressive strengthening of the supranational security paradigm.