Transnational Compliance and Legal Responsibility

CEJ
COMPLIANCE ELLIANCE JOURNAL

ISSN 2365-3353
Volume 11 • Number 1
Spring 2025

Compliance Elliance Journal (CEJ)
Volume 11, Number 1, 2025
ISSN: 2365-3353
This version appears in print and online. CEJ is published twice per year, in spring and fall.

Title: Transnational Compliance and Legal Responsibility

Website: www.cej-online.com

E-Mail: info@hendrikschneider.eu

Address:
Taunusstrasse 7
65183 Wiesbaden, Germany

Telephone: +49 611 95008110

Transnational Compliance and Legal Responsibility

TABLE OF CONTENTS

EDITORIAL

Transnational Compliance and Legal Responsibility

In an increasingly interconnected world, legal systems face complex challenges that transcend national borders. This issue of our journal, Transnational Compliance and Legal Responsibility, brings together diverse perspectives on how law interacts with global data flows, economic sanctions, environmental accountability, and the protection of fundamental rights.

From the classification of cash exports under EU sanctions law to the prevention of secondary victimization and the evolving role of compliance in corporate and environmental governance, the contributions highlight the growing importance of legal responsibility in a globalized legal order.

The articles reflect on both doctrinal developments and practical implications, offering critical insight into the future of cross-border legal compliance.

With our best regards,

Michele DeStefano, Konstantina Papathanasiou & Hendrik Schneider
Content Curators of CEJ

CROSS-BORDER TRANSFER OF PERSONAL AND INDUSTRIAL DATA BETWEEN THE EUROPEAN UNION AND CHINA – A COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS AND EXPORT REGULATIONS

Clemens Danda, Tim Robin Kosack, Sofia Kyrampalidou

AUTHORS

The authors are members of the ELSA Team at the DLR Institute for AI Safety and Security in Sankt Augustin, near Cologne. Their research focuses on legal and ethical implications of safety and security risks posed by artificial intelligence across various sectors and technologies.

ABSTRACT

Cross-border data transfers between the European Union and People's Republic of China are crucial for international research, innovation, and international trade. However, navigating the complex regulatory landscapes of those jurisdictions – especially amid their technological competition – poses significant challenges. This Article provides a high-level comparison of personal and industrial data protection, focusing on the general conditions under which transfers are legitimate under EU law. We examine constitutional and statutory data protection laws, export restrictions on industrial data, and cybersecurity requirements for both types of data. Our analysis shows that while China's personal data protection laws are increasingly aligning with European standards in commercial contexts, the risk of interference by administrative bodies remains relevant where national security interests are concerned. The protection of industrial data presents challenges, particularly in IP enforcement, reciprocity in technology transfers, and localization requirements. Nevertheless, maintaining trade relations while safeguarding individual rights and industrial data sovereignty is achievable through thorough risk assessments and the adoption of both conventional and innovative data and cybersecurity strategies.

TABLE OF CONTENTS

I. INTRODUCTION

The People's Republic of China (China) is a potent trade partner of the European Union (EU) in the data sector.[1] At the same time, they find themselves in competition over the development of innovative technologies and the data center industry[2] which contradicts free flow of data.[3] Decisive for adequacy decisions and transfers based on EU Standard Contractual Clauses ("EU SCC") the Article discusses whether the Chinese framework provides essential equivalence from the perspective of EU data protection. Regarding industrial data, we provide a comparative analysis of EU and Chinese export regulations, highlighting Europe's increasing focus on safeguarding its industrial data sovereignty. Additionally, we examine data and cybersecurity frameworks for both personal and industrial data, exploring traditional and innovative technical safeguards that can help mitigate gaps in legal protection. Our study adopts a risk-based approach to cross-border data transfers, emphasizing the need for data exporters to conduct case-by-case risk assessments while considering privacy and IP rights, compensation mechanisms, and technical safeguards.[4] To provide a comprehensive perspective, we also discuss recent EU[5] and Chinese regulatory developments in AI where relevant to the topic.

Personal data make up the majority of data transferred from the EU to China.[6] Different from industrial data, the transfer of personal data is already comprehensively regulated under Chapter V General Data Protection Regulation ("GDPR"). The Court of Justice of the European Union ("CJEU") requires under Art. 45(2) that the level of protection for personal data in the receiving country must be "essentially equivalent" to EU standards.[7] In parallel, depending on future implementing acts of the European Commission ("EC"), cross-border transfers of industrial data related to IP and trade secrets provided by public bodies have to go through a somewhat related essential equivalence test (Art. 5(12) Digital Governance Act ("DGA")[8]. The equivalence test of the GDPR, however, requires a broader assessment of fundamental rights and personal data protection laws, national security policy, and cybersecurity measures of the third country. In this regard, the CJEU[9] and the EC[10] specifically stress access of foreign intelligence services to the data, formal individual rights, and effectiveness of redress by data subjects. In the courts view, there is generally no appropriate protection where the law of the third country permits state interference[11] beyond necessity and proportionality.[12]

[1] UNCTAD, Digital Economy Report (UNCTAD 2021) XV.

[2] Cf. Darcy Pan, 'Storing data on the margins: making state and infrastructure in Southwest China' (2022) 25 Information, Communication & Society 2418.

[3] Cf. Veronica Arroyo et alia, What specific measures could the US, the EU and China take in order to foster and facilitate cross-border data flows? (Sciences Po 2023) 5.

[4] A risk-based approach is also taken under the GDPR Amendment proposed by Draft Christiane Wendehorst, Tentative Academic Discussion Draft (version 1.1) of a Regulation on the protection of personal data in the context of artificial intelligence and the data economy and amending Regulation (EU) 2024/1689 ('AI Data Protection Regulation') 1.

[5] Upcoming amendments of the GDPR for SME's – planned under the 2025 Commission Work Programme – are considered as far as they are published at the time of writing.

[6] Cf. European Union Chamber of Commerce in China (European Chamber), The Impact of China's Data Regulations on European Business (EUCCC 2023) 4.

[7] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2018] ECLI:EU:C:2015:650 ("Schrems I") 52 et seq.

[8] 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).

[9] Cf. Case C-311/18 Facebook Ireland v. Schrems [2020] ECLI:EU:C:2020:559 („Schrems II") 197.

[10] Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, C(2023) 4745 final.

[11] Case C-311/18 *Facebook Ireland v. Schrems* [2020] ECLI:EU:C:2020:559, 126.

[12] Ibid., 174-176.

Where horizontal adequacy is not confirmed, data transfers typically rely on Standard Contractual Clauses under Art. 46(1) GDPR.[13] For example, this approach has been taken by large Chinese tech firms which are now facing recent complaints filed by *Noyb* with multiple European Data Protection Authorities.[14] Art. 46(1) GDPR and Recital 11 and 20 of the SCC Implementing Decision[15] require an investigation of data regulation, case law, independent reports, and practice. However, applying the CJEU's case law mentioned above, the assessment should focus on data subject rights and legal remedies, as well as access by law enforcement and national security authorities.[16] The parties may compensate for uncertainties in legal protection by implementing technical safeguards, in particular cybersecurity measures, and complying with data security principles such as data minimization, anonymization and pseudonymization.[17] Security measures are then again highlighted in the context of the additional exceptional route provided under Art. 49 GDPR, which only enables one-off transfers under appropriate safeguards.[18] Commenting on these routes holistically, the CJEU clarified that a uniform concept of protection applies.[19] Lastly, it should be mentioned, that some Member States restrict transfers of sensitive data to countries that benefit from a adequacy decision, effectively blocking the other two routes.[20]

II. COMPARING PERSONAL DATA PROTECTION FRAMEWORKS

Scholars have expressed doubt whether Chinese constitutional and statutory data law respectively its enforcement aligns with the requirements of essential equivalence test.[21] The European Data Protection Board ("EDPB")[22] argues that China does not guarantee rule of law highlighting that equivalence should not be assessed on the basis of statutory laws alone. This Article, however, follows *Pernot-Leplay's* more nuanced perspective, arguing that China maintains a two-tiered system, were the protection of consumers and companies in civil and commercial matters is stricter compared to scenarios where national security interests are involved.[23] Following this rational, we support the application of a risk-based approach[24] (likelihood of harm*the severity of harm) in the context of the EU SCC,

[13] See Art. 46(2)(c) GDPR.

[14] The complaints against TikTok, AliExpress, SHEIN, Temu, WeChat and Xiaomi can be accessed under Nyob, TikTok, AliExpress, SHEIN & Co surrender Europeans' data to authoritarian China, TikTok, AliExpress, SHEIN & Co surrender Europeans' data to authoritarian China.

[15] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

[16] Case C-311/18 *Facebook Ireland v. Schrems* [2020] ECLI:EU:C:2020:559, para. 103-105.

[17] Case C-311/18 *Facebook Ireland v. Schrems* [2020] ECLI:EU:C:2020:559, para. 133; EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0 (EDPB 2021) 4.

[18] Regarding the third route based on Binding Corporate Rules (Art. 47 GDPR) see EDPB Document Setting Forth a Co-Operation procedure for the approval of Binding Corporate Rules for controllers and processors, 13.3.2025.

[19] Case C-311/18 *Facebook Ireland v. Schrems* [2020] ECLI:EU:C:2020:559, 92.

[20] Cf. § 393 German Social Security Code regarding health data.

[21] Zhang Yueming, 'Processing of Personal Data by Public Authorities in China: Assessing Equivalence for Cross-border Transfers from the EU to China' (2023) 14 *European Journal of Law and Technology* 23; Anja Geller, 'How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective' (2020) 69 *GRUR International* 1191; Shilling Xiao, 'State-Centric Proportionality Analysis in Chinese Administrative Litigation' (2023) 21 *International Journal of Constitutional Law* 461; Carl F. Minzner, 'China's turn against law' (2011) 59 *Am J Comp Law*, 935 et seq.

[22] EDPS, *Government access to data in third countries*, EDPS/2019/02.13 (2019) 12.

[23] Emmanuel Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?' (2020) 8 *Penn State Journal of Law & International Affairs*.

[24] Paul Breitbarth, 'A Risk-Based Approach to International Data Transfers' (2021) 4 *EDPL* 539.

which takes this dichotomy, individual rights protection, and economically feasible technical protection into account (cost/benefit analysis). This approach largely corresponds to the CJEU's uniform concept of protection[25] mentioned above, while simultaneously providing the necessary flexibility to legitimize already established trade relations which carry broader relevance in European security strategies. Arguably, the EC and the EDPB endorse this approach by emphasizing that the implementation of appropriate technical safety measures can legitimize transfers depending on the different risk levels.[26]

A. Fundamental Rights Protection

A thorough investigation first requires a general assessment of the legal system and constitutional framework. The EDPB characterises the Chinese legal system as a "rule of law as rule by law" framework.[27] Whilst Chinese citizens are protected under the Chinese Constitution of 1982 with a comprehensive rights framework[28], the latter does not provide clearly delineated rules for court system that allow to easily challenge administrative regulation and decisions. The ongoing need for a clearer hierarchy of norms renders administrative regulations difficult to be challenged[29] and potentially enables regulators to interpret norms in a more subject than legalistic manner.[30] On a more granular level, there are also technical differences in how administrative action is restricted. As part of the EU fundamental rights framework, Art. 52 Charter of Fundamental Rights of the European Union ("CFR") [31] requires authorities to respect the essence of rights and freedoms and that any interference must be provided by law, be necessary, and proportionate.[32] In contrast, whilst the Chinese Supreme People`s Court as well as the State Council have referenced the principle of proportionality,[33] scholars comment that their interpretation ponders on compliance with statutory law instead of providing a restriction.[34] However, there are certainly efforts and public demands[35] to strengthen formal rule of law to guarantee functionality in matters where national interests are not at risk.[36] For example, the Administrative Punishment Law of 2021 provides basis for the principles of legality fairness, openness, and proportionality (Arts. 4 and 5). In the same sense, Art. 34 PIPL requires necessity where authorities' process personal data.[37]

[25] Case C-311/18 *Facebook Ireland v. Schrems* [2020] ECLI:EU:C:2020:559, 92.

[26] Cf. Recital 6, 16, 20, 21 SCC Implementing Decision; EDPB, Guidelines 01/2025 on Pseudonymisation (2025) 17.

[27] EDPS (n 22) 13.

[28] Constitution of the People's Republic of China of 1982.

[29] Stephanie Balme, *Chine, Les visages de la justice ordinaire* (Science Po 2016) 41 and 45.

[30] Ibid 37.

[31] Charter of Fundamental Rights of the European Union. OJ C 202, 7.6.2016, p. 389–405.

[32] This is specifically relevant for data retention; see Case C-293/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238, 69. The importance of the essence of fundamental rights is again emphasised in Recital 19 SCC Implementing Decision. It should be noted that proportionality as a term is also rarely used in the common law context. This resulted in the term not being used in the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series - No. 225, 5.9.2024 ("CoE AI Framework Convention").

[33] Alec Stone Sweet, Jud Mathews, *Proportionality Balancing and Constitutional Governance A Comparative and Global Approach* (Oxford University Press 2019) 146.

[34] Shilling Xiao, 'State-Centric Proportionality Analysis in Chinese Administrative Litigation' (2023) 21 *International Journal of Constitutional Law* 461.

[35] Stephanie Balme, *Chine, Les visages de la justice ordinaire* (Science Po 2016) 76.

[36] Ibid 25, 79.

[37] Cf. Jamie Horsley, 'China's Revised Administrative Punishments Law: Strengthening Due Process and Implications for Social Credit Enforcement' (Paul Tsai China Center 2021).

Under EU law, privacy and personal data are constitutionally protected under Arts. 7 and 8 CFR. For context, those rights formed the argumentative basis for the recent invalidation of the EU-U.S. Privacy Shield in the CJEU's *Schrems II* decision.[38] Whilst the Chinese Constitution provides individual rights, redress mechanisms, and compensation for illegal interference on the freedom and confidentiality of correspondence and the privacy of the home (Art. 37 et seq), it does not recognise horizontal privacy or personal data rights as such. Some argue that the fundamental right is instead concretized by the Personal Information Protection Law ("PIPL")[39].[40] Personal information is also considered from the perspective of national security.[41] Art. 40 Chinese Constitution permits the examination of correspondence for national security purposes. When read in conjunction with Art. 13(5) PIPL which recognises the "supervision of public opinion" as a basis for data processing, and Art. 12(2) of the Cybersecurity Law ("CSL")[42] which outlines comprehensive prohibitions regarding online activity, achieving essential equivalency under the European Commission's standing policy seems unlikely.[43]

Looking at more specific data privacy topics, the CJEU has emphasised that under Arts. 7, 8, and 47 CFR administrative bodies cannot be granted access to personal data on a generalised basis.[44] Chinese tech firms receive and comply with manyfold requests regarding user data from Chinese public authorities[45] which might be interpreted as granting general access. In parallel, the European Court of Human Rights ("ECtHR") reaffirmed the relevance of protection from back doors to communication services. In the case *Podchasov v. Russia*[46] it held that "legislation providing for the retention of all internet communications of all users, the security services direct access to the data stored without adequate safeguards against abuse and the requirement to decrypt encrypted communications, […] cannot be regarded as necessary in a democratic society."[47] Arguably, the installation of such surveillance technology could be enforced under Arts. 13(5) PIPL, 28, 47 CSL, the Counter-Espionage Law[48], Arts. 50 Network Data Regulation ("NDR")[49], Arts. 62 and 65 of the recently proposed Chinese draft

[38] In Case C-311/18 *Facebook Ireland v. Schrems* [2020] ECLI:EU:C:2020:559, 170 et seq the court ruled that any unauthorised access, retention or use of ordinary or sensitive personal data by public authorities constitutes illegitimate interference and contradicts essential equivalency.

[39] Personal Information Protection Law of the People's Republic of China, 2021.

[40] Chengxin Peng and Guosong Shao, *Privacy and Data Protection Law in China* (Walters Kluwer 2024) Part I § 1.

[41] Xiaowei, Yu, 'The Identifiability Problem in Transnational Privacy Regulation' (2023) 56 *Vanderbilt Journal of Transnational Law* 1329.

[42] Chinese Cybersecurity Law, 2021.

[43] Cf. Stefanie Meyer et alia, 'Untying the Gordian Knot: Legally Compliant Sound Data Collection and Processing for TTS Systems in China' in: Schiffner et alia (eds), *Privacy Symposium 2022. Data Protection Law international Convergence and Compliance with innovative Technologies (DPLICIT)* (Springer 2022) 95 et seq.

[44] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2018] ECLI:EU:C:2015:650, 58, 47, 94.

[45] Nyob, Complaint to the Belgium Data Protection Agency Gegevensbeschermingsautoriteit against Alibaba.com Singapore E-Commerce Private Limited, 16.1.2024; for details see Xiaomi Transparency Report GOVERNMENT REQUESTS FOR USER INFORMATION January 1 – December 31, 2022, p. 4-7, accessible at https://xiaomi.gcs-web.com/static-files/83ae0ea4-2481-4e02-a3e6-75422a8c6df9.

[46] ECHR, *Podchasov v. Russia*, no. 33696/19.

[47] Ibid., [80].

[48] Counter-Espionage Law, 2023.

[49] Regulations on Network Data Security Management, effective January 1, 2025.

for a uniform AI law ("Draft AI Law")[50], or other regulations[51].[52] There is also an ongoing debate regarding a suspected social scoring system in China, which allegedly establishes privacy-invading systems that evaluate individuals based on their personal data and social behavior. Such risks are related to the rights to privacy, dignity and non-discrimination and are subject to the prohibitions in Art. 5(1)(c) of the EU Artificial Intelligence Act ("AIA")[53]. However, leading scholars emphasise that the Chinese system primarily targets severe violations by individuals and companies, with social evaluation initiatives only being implemented locally without endorsement by the central administration.[54]

In summary, considering the uncertainties of horizontal privacy protection, a different understanding of the rule of law and proportionality, the existence of exceptions for state interference, public opinion supervision, and potentially surveillance technologies leads to the conclusion that Chinese Constitutional Law, respectively its enforcement, still faces challenges in light of the CJEU's and the ECtHR's case law. However, considering the aforementioned dichotomy of national and private interests within a risk-based SCC route can be lawful where a thorough assessment of involved national security interests is conducted and technical safeguards mitigate risks. In general, where mostly private or commercial interests are involved, the safety measures can be lowered.[55]

B. Statutory Personal Data Protection Law

The PIPL provides rights regarding personal information, while the update to the Chinese Civil Code[56] provides protection for private information. Recently the Network Data Regulation[57] has brought some iterations and updates to the framework. Before these reforms, it was mainly Chinese criminal law that provided individuals with protection.[58] The PIPL introduces a comprehensive horizontal framework for personal information processing by private and public entities. Although public authorities are covered by the law, the PIPL generally refers to other security laws and their requirements in this context.[59] Some also question whether authorities fall under the definition of data controllers in the PIPL.[60]

The framework therefore primarily corresponds to EU concepts of privacy and data protection in private and commercial matters.[61] Recently, the framework has been extended under the Network Data

[50] Artificial Intelligence Law of the People's Republic of China (Draft for Suggestions from Scholars), 2.6.2024.

[51] Regulation on Internet Security Supervision and Inspection by Public Security Organs, 15.9.2018; cf. Art. 4 Provisions on the Management of Internet Post Comments Services, 17.11.2022

[52] Cf. Jyh-An Lee 'Hacking into China's Cybersecurity Law' (2017) 52 *Wake Forest Law Review* 72.

[53] 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).

[54] Jeremy Daum, 'Far From a Panopticon, Social Credit Focuses on Legal Violations' (2021) *China Brief* 5-9.

[55] Breitbarth (n 21) 539.

[56] The Civil Code of the People's Republic of China, 2021.

[57] Regulations on Network Data Security Management, effective January 1, 2025.

[58] For details see Zhang (n 18) 6.

[59] Section III PIPL.

[60] Graham Greenleaf, 'China's Completed Personal Information Protection Law: Rights Plus Cyber-security' (2021) 20-23 *Privacy Law & Business International Report*, p. 2; cf. Noyb, complaint against Alibaba.com Singapore E-Commerce Private Limited with the Belgium Data Protection Authority (Gegevensbeschermingsautoriteit), 16.1.2024, 12.

[61] Pernot-Leplay (n 23) 54 et seq.

Regulation ("NDR")[62] which emphasizes prohibitions regarding illegal data processing (Art. 8), transparency of data handling and again iterate the consent-focused approach of the PIPL (Art. 21 et seq).

1. Personal Data Processing Principles

In alignment with GDPR concepts, Art. 4 PIPL embraces a broad definition of personal data as "all kinds of information, […] related to identified or identifiable natural persons"[63]. Moreover, confidentiality of personal data must be maintained throughout the entire processing lifecycle.[64] Accordingly, the PIPL covers the full data lifecycle[65] including acts of cross-border data transfers. Read together with technical standards[66], the framework includes location information, call logs, browsing history, and metadata ("all human-generated data").[67] Similarity to the GDPR is further underscored by the adoption of a subjective and context-depend approach to identifiability[68] and ongoing nuanced debates on the conditions under which online identifiers – such as IP addresses[69] or Transparency and Consent Strings used in advertising[70] – classify as personal data. The PIPL also provides equivalent processing principles regarding lawfulness, data quality, data accuracy, and cybersecurity.[71] In the context of cross-border transfers, the EDBP[72] specifically highlights purpose limitation, necessity and data minimization as essential. These are all provided for in Arts. 5 and 6 PIPL, the Chinese SCC, and again iterated in Art 34 (4) Draft AI Law and other AI regulations[73] which specifically references necessity, data minimization and lawfulness, as well as in NDR[74]. Finally, the Chinese framework[75] is also formally aligned with Art. 22 GDPR by giving users the right to refuse AI-based decision-making. The protection of human rights in the context of smart courts and automated judgements remains a challenge.[76]

[62] Network Data Regulation, 1.1.2025.

[63] Early Chinese concepts connected dignity and privacy in the sense of "shameful secrets" (*yin-si*).

[64] Art. 5(1)(f) GDPR.

[65] Perry Keller, Li Yang, Tom van Nuenen, *After Third Party Tracking: Regulating the harms of behavioral advertising through data protection* (Kings College 2022) 46.

[66] Cf. Standardization Administration of China (SAC) and State Administration for Market Regulation (SAMR), Standard GB/T 35273-2020 on Information Security Technology - Personal Information Security Specification Art. 3.1.

[67] Xiaowei, Yu, 'The Identifiability Problem in Transnational Privacy Regulation' (2023) 56 *Vanderbilt Journal of Transnational Law* 1333.

[68] According to Xiaowei, Yu, 'The Identifiability Problem in Transnational Privacy Regulation' (2023) 56 *Vanderbilt Journal of Transnational Law* 1333 the context-dependency of the PIPL definition of personal data results from case law, e.g. Beijing internet Court, Case J. 0491 M. C. No. 1, *Ling v BeijingMicrolive Vision Tech. Co., Ltd.* [2018].

[69] See Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779; for China see Chaolin Zhang, Geng Wang, 'Legal Attributes of IP Attribution Information under China's PIPL: Clarification of Identifiability Terminology and Operationalisation of Identifiability Criteria' (2022) *Beijing Law Review* 13;

[70] Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit*, ECLI:EU:C:2024:214.

[71] See Art. 5 et seq PIPL; Art. 19, 22, 39 NDR; Art. 1035 Civil Code; Zhang/Wang, (n. 65) 13.

[72] EDPB (n 22) 11, 45.

[73] Art. 11 Interim Measures for the Management of Generative AI ("Interim Measures"); Art. 4 et seq Several Provisions on Automotive Data Security Management ("Automotive Data Provisions").

[74] Arts. 22(4), 24.

[75] Art. 22 PIPL; Art. 35 Draft AI Law; Art. 42 and 46 Network Data Regulation

[76] Cf. Shi Changqing, Tania Sourdin, Bin Li, 'The Smart Court – A New Pathway to Justice in China? (2021) 12 *International Journal of Court Administration*.

2. Legal Bases for Data Processing

Looking at legal bases for data processing, Art. 13 PIPL offers less leeway compared to the GDPR. It permits processing based on legal consent, contract performance, vital interest of the public or the data subject, news purposes, and where data is already disclosed publicly by the data subject itself. The main difference lies in the absence of a general clause for legitimate interest and the consideration of commercial interests. Instead, consent is repeatedly emphasised as the main legal basis for processing. It is required separately for domestic transfers, purpose change, processing of sensitive data, and cross-border transfer of data.[77] Recently, the courts confirmed the requirement of separate consent where personal data are transferred abroad.[78] Under Art. 15 PIPL, data subjects can also withdraw their consent. Art. 22 NDR additionally prohibits that consent requests cannot be bundled together as well as other misleading designs. In summary, by requiring consent throughout, the PIPL offers individuals more *formal* protection than the GDPR. Legitimate interest under the GDPR provides, in the reading of the CJEU, for "a wide range of interests […], in principle, capable of being regarded as legitimate"[79] under the GDPR. This includes, for example, where the data subjects can reasonably expect data processing for the purpose of direct marketing.[80]

Regarding sensitive personal data, Art. 9(2) GDPR provides a closed list. In contrast, Art. 28 PIPL contains an open-ended list of sensitive data, naming selected examples. As such, the PIPL is more adaptable to new arising forms of sensitive data and challenges created by technological innovation. It also classifies location and bank account data as sensitive personal information, which goes beyond the protection of the GDPR. However, it remains to be determined by the Chinese courts and administrative bodies whether the definition of sensitive data covers racial or ethnic origin, political opinions, philosophical beliefs, genetic data, and sexual orientation. This uncertainty is, however, partly compensated by the horizontal consent approach that already applies to all types of personal data. The same follows from Art. 22(2) NDR which requires separate consent for biometrics, religious beliefs, specific identities, medical health, financial accounts, and geolocation. Regarding the usage of personal data in the AI development context, Chinese law is again stricter compared to EU law. Based on Art. 6 lit. f GDPR, AI developers have to follow the same legitimate interest test and comply with the principle of necessity just as in other contexts. Beyond this flexible balancing test, even training without a legal basis does not necessarily rendered the model illegitimate if the model does not leak personal data ("insignificant likelihood").[81] Art. 10(5) EU AIA permits developers to use sensitive personal data to detect bias in high-risk systems where "strictly necessary". The Chinese Standard Basic Safety Requirements for Generative Artificial Intelligence ("Basic Requirements for GAI")[82] as well as the Interim

[77] Arts. 14, 23, 29, 39 PIPL; Arts. 23 et seq, Art. 21 NDR.

[78] Guangzhou Internet Court, (2022) Yue 0192 Min Chu 6486.

[79] CJEU Case C-26/22 and C-64/22, UF (C-26/22), AB (C-64/22) v Land Hessen, intervener: SCHUFA Holding AG [2023] ECLI:EU:C:2023:958, 76.

[80] CJEU Case C-621/22 *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens* [2024]. ECLI:EU:C:2024:857, 55; cf Rec. 47 GDPR, EDPB, Guidelines 1/2024 on processing of personal data based on Art. 6(1)(f) GDPR Version 1.0, 8.10.2024, p. 30.

[81] EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (2024) 16 and 35.

[82] Art. 5(2)(c) TC260, Basic Safety Requirements for Generative Artificial Intelligence ("Basic Requirements for GAI"), 29.2.2024.

Measures for the Management of Generative AI ("Interim Measures") instead repeat the consent requirement in the AI context[83] and that the usage of user inputs (e.g. prompts) must be subject to opt-outs.[84] Finally, Art. 34 Draft AI leaves the legal bases for AI-related data processing to the PIPL.

In summary, the PIPL offers essentially equivalent protection where it comes to legal bases. It places a strong emphasis on obtaining separate consent for commercial data processing, in particular in the context of cross-border transfers. As Chinese law does not provide a clear-cut exception for AI developers, the protection of data subjects is also greater in this respect. This strict consent approach arguably compensates for ambiguities of the PIPL's definition of sensitive data.

3. Trade in Personal Data

The rules on data trade form the conceptual background for the question of lawfulness of cross-border transfers. Data trade is considered as an act of data processing itself under both EU and Chinese law [85] and permissible if a legal basis applies.[86] However, the details remain vague when consent and legitimate interest are considered. Under EU law, it remains uncertain whether the sale to numerous unknown third parties can be consented to effectively, since such potentially undermines the right to withdraw consent later.[87] Additionally, the also EDPB rejects the processing of data for behavioral advertising purposes based on contractual performance and legitimate interest alone.[88] *Ruschemeier* argues that these guardrails should apply to data trade as such.[89] This position is now supported by the Data Act[90] which highlights economic interests of data subjects. Under these conditions, informed consent appears to be the only viable option. Otherwise personal data could become a *res extra commercium*[91], calling into question segments of already established global data markets.[92] Under Chinese law, the rules on data trade are apparently more straightforward. Domestic data trade and transfers will always require separate consent.[93] Regarding behavioral advertising[94] and algorithmic recommendations[95], however, the data subject apparently only has a right to opt out[96] under Art. 24 PIPL.[97] This could mean that the initial collection of personal data still requires consent, while subsequent algorithmic use must be opted out of. Art. 34 Draft AI Law then again requires consent for commercial

[83] Art. 5(2)(c) and Appendix A.4.e Basic Requirements for GAI, 7(3) Interim Measures.

[84] Art. 7(c) Basic Requirements for GAI.

[85] Art. 4(2) GDPR disclosure by transmission, dissemination or otherwise making available; cf. Art. 4(2) PIPL.

[86] Art. 6 GDPR, Art. 13 PIPL.

[87] Hannah Ruschemeier, 'Data Brokers and European Digital Legislation' (2023) 1 *EDPL* 34.

[88] EDPB, Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR), 27.10.2023, para. 314 et seq.

[89] Ruschemeier (n 87) 33 and 35.

[90] See Art. 1(9) 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 ("Data Act").

[91] Václav Janeček and Gianclaudio Malgieri, 'Commerce in Data and the Dynamically Limited Alienability' (2020) 21 *German Law Journal* 939.

[92] Bart Custers, Gianclaudio Malgieri, 'Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data' (2022) 45 *Computer Law & Security Review*, 11.

[93] Art. 23 PIPL; Art. 12 NDR.

[94] Art. 24 PIPL.

[95] Provisions on the Management of Algorithmic Recommendation in Internet Information Services, effective on 1.3.2022

[96] This should not be confused with the US approach, specifically § 1798. 115 (d) CIV/CCPA, which only provides an opt-out for the onward sale of data.

[97] For more details on behavioral advertisement restrictions under Chinese law see Keller/Yang/van Nuenen (n 65) 33.

AI scoring which potentially overlaps with the notion of behavioral advertising and algorithmic recommendations ("analyze or evaluate an individual's behavioral habits, interests […]"). To summarise, while the PIPL is based on consent as the central legal basis for commercial data processing, EU law is also moving towards this result. We might therefore observe an ongoing convergence of the level of protection in commercial use of data in the EU and China.

4. Secondary Use of Personal Data

Only transfers that align with the original purpose of the data collection are lawful. Secondary use under Art. 6(4) GDPR is only permissible if the new purpose is at least *compatible* with the original purpose. This is to be determined based on factors such as the nature of the uses involved, the context of data collection, consumer expectation, as well as predictable consequences for the data subject and safeguards. *Ruschemeier* notes, that transfers assessments should additionally include the intended use of the receiver of the data[98] – a convincing argument that relates to the full data lifecycle. The data exporter is required to either substantiate compatibility or obtain separate consent for a new purpose. However, the EU is now establishing a new framework for free data flow with the European Health Data Space Regulation ("EHDSP")[99] being the first regulation to provide further details and exceptions for research purposes. Under Art. 14(2) of the PIPL, secondary use constituting a new purpose strictly requires separate consent if consent was the legal basis for the original processing. Since "legitimate interest" is generally not provided under the PIPL, lawful secondary use without separate consent is difficult to achieve. The Chinese scientific community comments that these harsh rules stifle scientific research which often relies on secondary use of (sensitive) data.[100] Whether the more relaxed technical standards[101] provide a sufficient legal basis for research remains questionable. An explicit exception is introduced with already mentioned opt-out clause for behavioral advertising and algorithmic recommendations, which will regularly constitute secondary uses.

The EUs AI Act provides special exceptions for AI developers regarding secondary use of personal data. These rules bring necessary clarification for scientific research under the GDPR.[102] First, Art. 10(5) AIA permits processing of special categories of data for bias detection. This exception should include bias testing where it constitutes secondary use. Second, Art. 59 AIA permits secondary use of personal data for testing of AI systems in regulatory sandboxes where the system relates to substantial public interest. Notably, cross-border and domestic data transfers are not covered here (lit. e). Chinese AI regulation does not provide comparable exceptions for AI training. Art. 5(2)(c)(1) Basic Requirements for GAI and Art. 7(3) Interim Measures instead again require separate consent for the use of personal data for AI training. Arts. 20, 21, 34 Draft AI Law only reference applicable legislation in this regard.

[98] Ruschemeier (n 87) 29.

[99] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance).

[100] Xiaojie Li, Yali Cong, and Ruishuang Liu, 'Research under China's personal information law' (2022) 378 *Science*, 713-715; Yu Yao, Fei Yang, 'Overcoming personal information protection challenges involving real-world data to support public health efforts in China' (2023) 11 *Digital Public Health*.

[101] Art. 5.6(k) and 7.3 Information security technology— Personal information (PI) security specification, GB/T 35273—2020 provide exceptions to consent and a broad understanding of research purposes.

[102] Art. 5(1)(b), Recital 55 (presumed compatibility of secondary use for archiving purposes in the public interest, scientific or historical research purposes or statistical research); Recital 33 (arguably: broad consent for selected areas of research), Art. 5(1) (extension of storage limitation); Art. 9(1)(j) (processing of sensitive data); Art. 89 (e.g. additional safeguards when exceptions are relied upon).

In summary, the Chinese rules on data trade, data transfer, and secondary use of personal data offer essentially equivalent protection compared to the GDPR. While EU law is often vague, the PIPL strictly requires separate consent for most forms of personal data processing including commercial purposes. Arguably, the EU is also moving towards horizontal consent in commercial contexts. Regarding secondary use specifically, the GDPR and the AI Act provide reasonable exceptions for research purposes, which lack under Chinese Law. European developers are specifically allowed to utilise sensitive data for bias detection and re-use personal data for the development of AI systems that benefit the public good. The Chinese AI framework instead iterates consent requirements potentially hampering AI research and development. However, this further solidifies the high formal level of protection for data subjects.

5. Cross-border Transfer Rules

The protection provided by cross-border transfer rules is crucial when potential onward transfers of personal data are concered. Other than Chapter V GDPR, Art. 40 PIPL and Art. 37 CSL, and Chapter IV NDR emphasise national security[103] as well as separate consent as a horizontal privacy measure. Individual rights protection is again considered in the Chinese Standard Contract on Outbound Transfer of Personal Information ("Chinese SCC")[104] which –similar to the GDPR and the EU SCC – require assessment of the receiving countries privacy regulation.[105] Regarding onward transfers specifically, the Chinese SCCs again require separate consent.[106] The separate consent requirement alone may already satisfy GDPR and the EU SCC privacy concepts. It goes beyond 8.1 EU SCC, which narrows the conditions for secondary use to consent, legal claims, and vital interest. However, the EU SCC also require data minimization[107], storage limitation[108], special safeguards for sensitive data,[109] and effective data subject rights and redress.[110] Consequently, the Chinese SCC offer an formaly essentially equivalent protective framework.

Depending on the nature of the data and the exporting entity, cross-border transfers may additionally be subject to security assessments or certification under Chinese national security laws. As explained in more detail in section 3.A., data exports by operators of critical information infrastructures ("CIIs") as well as exporters of important or core data always require a security assessment.[111] Additional localization measures regarding personal data[112] which are neither from CII nor important in nature have been criticised[113] and recently softened[114] by the adoption of the Provisions on Facilitation and Regulation of

[103] For the CSL see Qi Aimin, Shao Guosong, Zheng Wentong, 'Assessing China's Cybersecurity Law' (2018) 34 *Computer Law & Security Review* 1342 et seq.

[104] Standard Contract on Outbound Transfer of Personal Information, 1.6.2023.

[105] See Art. 2(8) and 4(1,2) Chinese SCC.

[106] Compare Art. 3(8) Chinese SCC and Clause 8.7 EU SCC.

[107] Compare Art 2(1) Chinese SCC to Clause 8.3 EU SCC.

[108] Compare Art. 3(5) Chinese SCC and Clause 8.5 EU SCC.

[109] Compare Art. 2(5) Chinese SCC and Clause 8.6 EU SCC.

[110] Compare Art. 5 and 6 Chinese SCC to Clause 10 and 11 EU SCC.

[111] Art. 31 DSL, Art. 37 CSL, and Art. 7(1) Data Flow Provisions, Art. 37 NDR. For example, the Several Provisions on the Management of Automobile Data Security of 1.5.2021 ("Automotive Data Provisions") classify personal data as important.

[112] Cf. CAC, Outbound Data Transfer Security Assessment, effective 7.7. 2022; Noyb, complaint against Alibaba.com Singapore E-Commerce Private Limited with the Belgium Data Protection Authority (Gegevensbeschermingsautoriteit), 16.1.2024, 10.

[113] E.g. Pernot-Leplay (n 23) 52.

[114] Cf. European Chamber (n 4).

Cross-Border Data Flows ("Data Flow Provisions")[115]. The here described principles were later mostly reaffirmed by Art. 35-37 NDR: First, under Art. 4 personal data collected outside of China can be reexported without any specific authorisation. Although well-intentioned, this could introduce risks of unwarranted onward transfers to third countries – the GDPR instead protects personal data regardless of reexport scenarios.[116] Second, Art. 5 (cf. Art. 35 NDR) provides legal bases for cross-border transfers mirroring exceptions provided under Art. 49(1) GDPR: performance of contract, human resources, and emergencies.[117] By omitting legitimate interest like the PIPL and the Chinese SCC, it can generally be said, that the Data Flow Provisions offer high protection to data subjects. Third, Art. 2 (cf. Art. 37 NDR) clarifies that only those personal data are considered as important which are officially declared as such. This is the case, for example, with audiovisual data of individuals' faces, and voices in the automotive sector.[118] Fourth, Art. 6 allows pilot free trade zones to classify data as important. This has been taken up, for example, by the Shanghai Lingang and Tianjiin Zones.[119] The Zones autonomy in this regard is arguably again supported by Art. 35(8) NDR which references other legal authorities. Finally, the Data Flow Provisions loosen up the threshold system for data exports: Art. 5(4) stipulates that non-CII entities, which transfer fewer than 100,000 people's personal information in one year, are exempt from approval. Under Art. 8, non-CIIs transferring personal data of under one million individuals or less than the sensitive personal information of 10.000 individuals can use Chinese SCC or apply for certification. Everything beyond these thresholds triggers a security assessment (Art. 7(2)). Art 35 NDR again iterates these routes and requirements for network operators.

In summary, the Chinese legislator reduced administrative oversight to some degree and updated the SCC to clarify and align its conditions for cross-border transfers with foreign frameworks. Cross-border transfers always require separate consent from the data subject, which balances national security and individual interests to some degree. Export restrictions have been reduced for low-risk scenarios including reexports, administrative tasks, and in terms of numerical thresholds. Since the exceptions of the Data Flow Provisions do not apply to CIIs or important and core data, however, their relevance remains relative and casuistic. IN summary, the combination of somewhat strict export regulations and horizontal consent requirements for data exports offer a high level of formal protection in private and commercial matters.

6. Rights, Redress and International Jurisdiction in Civil Matters

Chapter V GDPR requires that data subjects enjoy data protection rights and have access to justice.[120] As demonstrated in this Chapter, the Chinese framework provides essentially equivalent negative formal rights when it comes to private and commercial matters. Chapter VI PIPL, Chapter VI Civil Code[121], Art. 5 Chinese SCC, and Art. 23 NDR provide simmilar equivalent rights and remedies including the right to withdraw consent, to access and transfer data, as well as to object, complete, or correct false

[115] CAC, the Provisions on Facilitation and Regulation of Cross-Border Data Flows, March 22, 2024.

[116] Art. 3(1) GDPR; Art. 3(8) Chinese SCC only contains onward transfer requirements for the foreign data recipient including separate consent of the data subject (lit. c).

[117] The first two scenarios are of high importance for EU companies according to European Chamber (n 4) 4.

[118] Art. 3 Automotive Data Provisions.

[119] IAPP, 'Navigating China's new guidelines for exporting 'important data'' (*IAPP News*, 11.7.2024) <www.iapp.org/news/a/navigating-china-s-new-guidelines-for-exporting-important-data->.

[120] Cf. Recital 2 and 12 SCC Implementing Decision.

[121] Cf. also Art. 23, 24 NDR.

information. Data subjects may also demand deletion of data processed without any legal basis including where consent has been withdrawn, when the processing purpose has been achieved, or when the retention period has expired.[122] A right to explanation and internal complaint mechanisms are provided under Arts. 34, 35, 40 Draft AI Law. In terms of judicial redress, data subjects have formal access to courts and administrative procedures to assert rights and bring liability claims.[123] As far as tortious claims are concerned, Art. 82 GDPR allows for claims regarding immaterial damage, including fear after loss of control,[124] where the defendant acted negligenctly, while Art. 69(2) of the PIPL goes further and provides for claims based on unjust enrichment.[125] Under both Art. 82 GDPR and Art. 69 PIPL Data subjects benefit from a reversal of the burden of prove with regard to the fault of the data handler. Overall, the landscape of formal rights is comprehensive and essentially equivalent.

However, considering Arts. 131 et seq of the Chinese Constitution (see section A.) and court practice, it is not guaranteed that judges are independent and impartial in domestic and international cases from the perspective of European case law.[126] Some argue that due to data export controls by the CAC, data subjects cannot effectively exercise these rights.[127] However, recent case law shows that individual claims by Chinese citizens against larger companies can be successful. In *Huang v Tencent Tech. Co., Ltd.*[128] the Beijing Internet Court decide in favor of a private plaintiff who argued that access to friends lists by other users on WeChat violated his privacy rights. The same accounts for the case *Ling v Beijing Microlive Vision Tech. Co., Ltd.*[129] where the private plaintiff successfully argued, among other things, that geolocation data constitute private information. The Guangzhou Internet Court held that data transfers require separate consent and enforced data deletion and payment of approximately 2,500 EUR.[130] In parallel, public interest lawsuits brought by public prosecutors against larger companies and platforms are also on the rise.[131] Those latter are specifically referenced by Art. 92 AI Draft Law. However, whether foreign individuals enjoy the same protection before Chinese courts remains uncertain given the missing case law.[132] The EDPB remains undecided on the matter[133], whilst Chinese scholars argue in the positive[134] and ask for more nuanced investigation.[135] Where onward transfers from China are concerned, Art. 2.4 Chinese SCC requires the courts to allow data subjects to invoke

[122] Art. 47 PIPL.

[123] Art. 50(2) PIPL, Art. 74 CSL; Art 55 et seq Network Data Regulation.

[124] CJEU Case C-340/21 VB v Natsionalna agentsia za prihodite [2023] ECLI:EU:C:2023:986.

[125] Case C-300/21 *Österreichische Post* [2023] ECLI:EU:C:2023:370.

[126] For details see Yanrong Zhao, 'The Way to Understand the Nature and Extent of Judicial Independence in China' (2019) 6 Asian Journal of Law and Society.

[127] Noyb, complaint against Alibaba.com Singapore E-Commerce Private Limited with the Belgium Data Protection Authority (Gegevensbeschermingsautoriteit), 16.1.2024, 12.

[128] Beijing Internet Court, Case 0491 Min Chu Zi No. 16142, 27 *Huang v. Tencent Technology (Shenzhen) Co., Ltd. and Guangzhou Branch and Tencent Technology (Beijing) Co., Ltd.* [2019].

[129] Beijing Internet Court, Case 0491 Min Chu 6694, 3 *Ling v Beijing Microlive Vision Tech. Co., Ltd., Beijing* [2019].

[130] Guangzhou Internet Court, (2022) Yue 0192 Min Chu 6486.

[131] Hunter Dowart, 'Chinese Data Protection in Transition: A Look at Enforceability of Rights and the Role of Courts' (2022) *Computers, Privacy and Data Protection* <http://dx.doi.org/10.2139/ssrn.4163016> 21 et seq.

[132] Bo Zhao, Jeanne Mifsud Bonnici, 'Protecting EU citizens' personal data in China: a reality or a fantasy' (2016) 24 *International Journal of Law and Information technology*, 149; Noyb, complaint against Alibaba.com Singapore E-Commerce Private Limited with the Belgium Data Protection Authority (Gegevensbeschermingsautoriteit), 16.1.2024, 14.

[133] EDPS (n 22) 13.

[134] Zhang (n 21) 10.

[135] Yanrong (n 126) 151 et seq.

the Chinese SCC as third-party beneficiary rights[136] which should extend to foreign individuals. It should also be noted, that the competence of Chinese courts regarding international cases has been extended under Art. 6(3) Chinese SCC which now mandates their jurisdiction in all cross-border data settings.[137]

Under these conditions effective legal redress of EU citizens is not guaranteed in every case. Instead of presuming protection, data exporters are therefore required to provide data subjects with alternative dispute resolution[138] or compensation mechanisms. This includes, for example, self-executing smart contract and smart enforcement. Following a risk-based approach, transfers can be lawful where sensitive data are not involved and it can reasonably be assumed that affected data subjects can be satisfied by alternative forms of compensation. Monetary compensation is already the de facto outcome where a data transfer infringement resulted in a material or non-material damage.[139]

C. Conclusions on Cross-border Transfer of Personal Data

In view of the potential risk of access of administrative bodies to personal data and the challenges that arise in the context of private law enforcement, the framework still requires changes to be considered if an adequacy decision is sought after.[140] Also, from a perspective of reciprocity, the combination of horizontal consent with strict approval procedures could create a localization effect, constituting a considerable factor in trade relations. However, the emphasis of the PIPL on horizontal and separate consent already provides higher formal protection for commercial settings than the GDPR.[141] Since legitimate (commercial) interest is not recognised as a legal basis for data processing, data subjects are protected from unwanted commercial activities. This comparatively high level of formal protection within private and commercial settings should allow for low-risk cross-border transfers of personal data based on EU SCC.[142] This could be the case, for example, where the data involved are neither sensitive nor related to Chinese national security interests. This typically includes, for example, purely commercial and transactional data related to the fulfillment of cross-border contracts. On the other hand, the transfer of primary raw personal data, e.g. data directly registered by IoT devices, requires detailed risk assessments and risk mitigating safeguards discussed below (pseudo- and anonymization, cybersecurity). In terms of redress and access to justice, low risks can potentially be mitigated by providing (automated) alternative redress and compensatory mechanisms to data subjects.

[136] Cf. Recital 12 SCC Implementing Decision.

[137] Since re-exports of personal data collected outside of mainland China will not require Chinese SCC (Art. 4 Data Flow Provisions), at least those disputes can be subject to diverging jurisdiction clauses agreed upon by the parties. The effect is amplified by the recent introduction of the *general close connection* clause under Chinese private international law, see Art. 276 revised Chinese Civil Procedure Law.

[138] Recital 13 SCC Implementing Decision.

[139] Cf. General Court, T-354/22, *Thomas Bindl v European Commission*, ECLI:EU:T:2025:4.

[140] EDPS (n 19) 14; Pernot-Leplay (n 23) 114.

[141] Sonja Mangold, 'Data Protection Law in Germany, the United States, and China', chapter in: Lars Hornuf, Sonja Mangold, Yayun Yang (eds), *Data Privacy and Crowdsourcing* (Springer 2023) 57.

[142] Breitbarth (n 24) 539.

III. CROSS-BORDER TRANSFER OF INDUSTRIAL DATA

Access to industrial data is directly related to effective development of AI systems in key sectors such as automotive, medical products, or robotics. In this context, restrictions on cross-border data transfer are at the intersection of national security, economic competition, and data sovereignty. The Chinese Cybersecurity Law ("CSL")[143] and the Data Security Law (DSL)[144] are the main instruments addressing cross-border transfer of industrial data. They introduce a tiered approach based on data classification and impact assessments taking national security interests and economic factors into account. For now, the EU takes a more liberal approach to industrial data exports. However, regarding data held by public bodies, the Data Governance Act (DGA) allows the European Commission to adopt stricter rules for data exports in specific sectors. The EU and China have recently launched discussions on new cross-border data flow mechanisms for non-personal data which could result in further easements regarding security approvals.[145]

A. Free Flow of Ordinary Industrial Data

Based on the fundamental right of access to information, the EU wants to ensure free flow of non-personal data including industrial data.[146] In this regard we should mention the Regulation on the free flow of non-personal data[147], the Open Data Directive[148], and the Data Act which are, however, instruments which structure internal European data markets by prohibiting localization measures, regulating specific sectors[149], and granting individuals rights in relation to their economic interests. The DGA is the only EU instrument that provides requirements for the cross-border transfer of industrial data. These rules are, however, restricted to the sharing of data held by public institutions and require relevant individual or economic interests to be concerned – those rules will be the main focus in the following. Otherwise, EU regulation does not restrict the cross-border transfer of ordinary industrial data to third countries.

While Chinese policy advocates for free data flows[150], regulations draw the line at important and core data as well as data held by CIIs. Parallel to the European appraoch, regulations such as the Chinese Draft AI Law[151] primarily envision a domestic free flow of data. However, China recently introduced clarifying and softening export rules in this regard. Art. 3 of the already mentioned Data Flow Provisions clarifies that non-important industrial data from non-CIIs can be exported without any administrative authorization if the data were generated in the context of international trade, academic cooperation,

[143] Chinese Cybersecurity Law, 2021.

[144] Data Security Law, 2021.

[145] EC Directorate-General for Trade, EU and China launch Cross-Border Data Flow Communication Mechanism, (28.9.2024), <https://policy.trade.ec.europa.eu/news/eu-and-china-launch-cross-border-data-flow-communication-mechanism-2024-08-28_en>.

[146] Cf. Recital 5 Directive (EU) 2019/1024.

[147] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

[148] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

[149] See the listed sectors in Annex I Open Data Directive.

[150] Cf. Art. 11 DSL.

[151] Arts. 20, 21 Draft AI Law.

multinational manufacturing, and marketing activities. This exception certainly reduces the tensions and costs within EU-China trade relations. The re-export of industrial data, however, is not expressly privileged by the Data Flow Provisions.

B. Cross-border Transfer Restrictions for Sensitive Industrial Data

There exist manifold restrictions on the cross-border transfer of sensitive industrial data under EU and Chinese law. First, both the EU and China provide specific export controls for technology and data related to civil-military dual use and selected industry sectors such as semiconductors and additive manufacturing. The EUs Dual-Use Regulation[152] regulates cross-border transfer of data-related technology, for example, encryption products in the cyber-surveillance context. While China's export framework traditionally focuse on the prevention of the proliferation of weaponry[153], the ongoing trade war with the U.S. recently let to the adoption of a more comprehensive framework. It requires export licenses for dual use and other technologies or items of national security interest (e.g. minerals for semiconductor and EV production[154]) which includes related industrial data and information.[155] This Article cannot go into the details of this subtopic since our focus is on commercial use of industrial data.

1. EU Export Restrictions

While EU Cybersecurity Regulations stipulate specific data and cybersecurity measures, the DGA introduces cross-border transfer rules for industrial data shared by public sector bodies ("re-used data"). This approach somewhat mirrors the GDPRs essential equivalence test. The focus is on the protection of IP, trade secrets, and otherwise confidential data.[156] Regarding cross-border transfers, re-users are required to implement safeguarding contractual terms on IP and confidentiality protection as well as negotiating trustworthy jurisdiction clauses.[157] In this regard, the EC is empowered to adopt model contractual clauses. Moreover, in cases involving a substantial number of exports, the Commission may require the assessment of essential equivalence of IP rights, enforcement, and judicial redress in the receiving country.[158] In addition, Art. 5(13) DGA introduces the category of highly sensitive non-personal data for sectors such as health, transport, energy, environment, and finance[159] which are related to important public policy objectives and risks of re-identification of individuals. Based on further sectorial regulation, the EC may introduce further cross-border transfer measures such as secure processing environments, limited re-use of data, and restrictions regarding individual re-users and third countries. Arts. 61, 62 EHDSP exemplify such a sectorial regulation for the health data sector referencing risks of reidentification and IP-theft. Finally, both Art 31 DGA and Art. 32 DA require the assessment of international agreements, proportionality, and effective review when courts or administrative

[152] 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.

[153] Cf. BAFA, *Joint EU - Handbook on Export Control of Dual-Use Items in China*.

[154] No. 46 Announcement on Strengthening the Export Control of Relevant Dual-Use Items to the United States, 3.12.2024.

[155] Export Control Law of the People's Republic of China, 17.10.2020; Implemented Export Control Regulation of Dual-Use Items, 1.12.2024.

[156] Art. 5(7, 8) DGA.

[157] Art. 5(10) DGA.

[158] Cf. Art. 5(12) and Recital 21 DGA.

[159] Cf. Recital 24 DGA.

bodies of a third-country request industrial data to be disclosed. Art. 32(3)(f) DA makes explicit reference to withholding data due to national security and defense reasons.

In general, this new approach is aimed at ensuring the protection of sensitive industrial data in the context of transfers to countries which pursue a "market-for-technology" approach typical for (formerly) developing countries such as China. Such contexts create specific risks for intellectual property and trade secrets. For example, foreign companies are often required to closely partner[160] with Chinese companies and to share trade secrets during administrative approval procedures.[161] While recent reforms to competition law and administrative and judicial remedies can mitigate some of the associated risks,[162] the Commission might take action based on these new competences.

2. Overview over Chinese Export Restrictions

Chinese law provides a comprehensive data export regime for industrial data based on data classification and impact assessments. Arts. 31 DSL, 37 CSL,[163] 7(1) Data Flow Provisions[164], and Art 37 NDR specifically emphasis that data collected by CII as well as important or core data are to be stored within China while exports trigger a security assessment with the CAC. As a consequence, foreign and domestic companies in part localise industrial data within China.[165] Arts. 31 CSL and 2 CII Security Regulation[166] closer define relevant CII sectors such as public telecommunications and information services, energy, transportation, technology. They also add sectors where data leakage could gravely harm national security, people's livelihood, or public interest. Given this abstract scope of application, administrative bodies are required to publish additional criteria for each sector and notify stakeholders of their CII status.[167] In 2023, EU companies still needed further clarification on classification criteria[168], having new Chinese criminal rules on espionage and business secrets in mind.[169]

3. The Chinese Data Classification Scheme

Chinese law is first to introduce a comprehensive approach to data exports based on the classification of data and impact assessments. In addition to personal and sensitive data regulated under the PIPL, Art. 21(4) CSL, Art. 21 Data Security Law introduces a three-dimensional classification system for general, important, and core data combined with the dimension of general, serious, and particularly serious impacts on national and individual Chinese interests. Given the challenge to classify data correctly, Art. 2 Data Flow Provisions clarifies for foreign industry stakeholders that data is only considered as

[160] Cf. Jack Nicas et alia, 'Inside Apple's Compromises in China: A Times Investigation' *The New York Times* (17.6.2021) <https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html>.

[161] Jyh-An Lee, 'Forced Technology Transfer in the Case of China' (2020) *Chinese University of Hong Kong*, no. 18.

[162] See Art. 32 for civil and 46(2) for administrative procedures in the PCR Anti-Unfair Competition Law ("AUCL"), 23.4.2019; Art. 8 Network Data Regulation

[163] Jihong Chen, Jiabin Sun, 'Understanding the Chinese Data Security Law' (2021) 2 *Int. Cybersecur. Law Rev.*, 214.

[164] Cf. Maggie Meng, Xingchen Qian, 'China's Data Export Compliance in Law and Practice' *Global Law Office* 10.9.2023.

[165] European Union Chamber of Commerce in China, *European Business in China Business Confidence Survey* (2023) 15.

[166] Regulation on Protection of Security of Critical Information Infrastructure ("CII Security Regulation"), 1.9.2021.

[167] Anna Gamvros, Lianying Wang, 'Am I a CII operator?" – New regulation in China provides more clarity' *dataprotectionreport* (18.8.2021).

[168] European Chamber (n 6) 8.

[169] See Art. 219(1) PRC Criminal Law and Arts. 53 et seq. Anti-espionage Law of the People's Republic of China, 26.3.2023.

important when it is explicitly proclaimed as such.[170] As far as the granular details of the classification methodology are concerned, technical standard such as GB/T 43697-2024[171] provide further detail. It is based, on one hand, on the impact-based approach and, on the other, on the rational that each sector requires further lower-level criteria. Art. 29 et seq NDR then provides further legal basis to classify data, emphasizing catalogs for important data to be introduced by regional administration and industry.

Following these principals, sector-specific regulations have been introduced.[172] For example, the Automotive Data Provisions of 2021[173] classify survey and map data, data on charging networks, and data on traffic volumes as important. In this regard, the European Chamber lobbies for lowering some of the requirements related to cockpit data, operational and business development data, and data classification schemes.[174] Regulations and guidelines governing geographic information data in the context of connected vehicles (such as smart sensors, GPS, and navigation maps) also often mandate a security assessment before any export.[175] In the context of ICT, the Measures for Data Security Management in Industry and Information Technology ("IIT Measures")[176] provide a broad impact-based approach for important and core IT data.[177] The following overview of the IIT Measures serves as an example for typical classification in other schemes[178]: First, General data may be exported where it could cause a minor impact;[179] second, important data involve threats to national or public interest including artificial intelligence development, have a serious impact in the field of industry and information technology, or can cause a major data or production security incident[180]. Core data, finally, are data related to serious threats to politics or economy, a major impact in the field of industry and information technology, or a major harm to industrial production and operations as well as telecommunication networks.[181] The demarcation between those categories is difficult in practice[182] and certainly requires notification and declaration by authorities. Negative data lists issued by Pilot Free Trade Zones such as Shanghai, Beijing and Tianjin also provide details in this regard.[183]

[170] Cf. Arts. 21(3) and 31 DSL.

[171] GB/T 43697-2024 (Rules for data classification and grading).

[172] Cf. Ministry of Finance and CAC, Tentative Measures for Data Security Management of Accounting Firms, 15.3.2024; National Financial Regulatory Administration, Measures for the Data Security Management of Banking and Insurance Institutions, 27.12.2024; Civil Aviation Administration of China, Measures for Civil Aviation Data Management (Draft for Comments), June 2024.

[173] Several Provisions on the Management of Automobile Data Security, 1.5.2021.

[174] European Chamber, European Business in China, Position Paper 2024/2025, 185.

[175] For an overview see Notice of the Ministry of Natural Resources on Strengthening the Administration of Surveying, Mapping and Geoinformation Security of Intelligent Connected Vehicles ("Notice 139").

[176] Ministry of Industry and Information Technology, Measures for Data Security Management in Industry and Information Technology (for Trial Implementation), 1.1.2023.

[177] Art. 8(2) IIT Measures.

[178] Compare the classification systems in Art. 21 DSL; Table F.1 GB/T 43697-2024 (Rules for data classification and grading).

[179] Art. 9(1)) IIT Measures.

[180] Art. 10(1)) IIT Measures.

[181] Art. 11 (1) IIT Measures; cf. Art. 21 DSL definition of core national data.

[182] Sebastian Wiendieck, Li Wang, 'China: New Measures for Data Security Management in Industry and Information Technology (Trial Implementation)' *Roedl & Partner Insights* (11.12023) <https://www.roedl.com/insights/china-data-protection-information-technology-cyber-data-security>.

[183] Barbara Li Sarah Xiong Amaya Zhou, 'Policies relaxing data restrictions adopted in China's free trade zonesHunton Andrews Kurth' *Reed Smith Perpectives* (21.2.2024) <https://www.reedsmith.com/en/perspectives/2024/02/policies-relaxing-data-restrictions-adopted-in-chinas-free-trade-zones>.

C. Conclusions on Cross-border Transfers of Industrial Data

In summary, the EU is moving to protect its data sovereignty looking beyond its focus on personal data protection. While the legal framework permits cross-border transfers of private industrial data, the DGA could signal future introduction of safeguards to protect IP, confidential information, and trade secrets where data held by public bodies are involved. However, in the absence of more detailed sectorial rules, exporters can only observe upcoming developments for now. China's regulatory framework instead imposes strict export restrictions on industrial data, with a clear impetus on national security and economic competition. Even though administrative oversight is reduced, the open definitions of PII and sensitive data and recent reforms in espionage and trade secret protection further incentivise companies to localise industrial data.

IV. DATA AND CYBERSECURITY IN CROSS-BORDER DATA TRANSFERS

A. Regulatory Landscape of the EU and China

Stringent technical requirements regarding data security are highly relevant in determining essential equivalence given the rising risks of data breaches around the globe. As such, implementing appropriate data and cybersecurity measures is a fundamental requirement of the GDPR[184] and technical measures are again emphasized in the EU SCC.[185] Where industrial data held by public sector bodies are concerned, also the DGA requires an appropriate level of security.[186] These acts primarily rely on other safety and security regulations, certification mechanisms, and technical standards for details.[187] These include the Cyber Resilience Act ("CRA")[188], the Cybersecurity Act ("CSA")[189], and the Network and Information Systems Directive ("NIS2")[190] which establish rulebooks for the security of storage, devices, networks, and critical infrastructure.

The Cyber Resilience Act regulates products with digital elements extending to standalone software and AI systems. Its Annexes specify comprehensive mid-level requirements and data processing principles for common, important, and critical products. The Cybersecurity Act additionally provides the legal basis for the adoption of voluntary cybersecurity certification schemes for ICT products and processes.[191] Both the CSA and CRA are based on a risk-based self-assessment for low-risk and incentive or require third-party conformity assessment for scenarios where higher risks are involved.[192] Lower-level instruments including harmonized standards, common specifications, and certification schemes

[184] See Arts. 25, 32, 42, 43, 45 (2)(a), 46 GDPR, cf. Case C-311/18 *Facebook Ireland v. Schrems* [2020] ECLI:EU:C:2020:559, 133.

[185] Clause 8.5 EU SCC.

[186] See Art. 5(3), 12(1), 21(4) DGA data. Cf. also Art. 21(4) DGA regarding data altruism organizations.

[187] Recital 78, 81 GDPR refers to the state of the art and certification; see Art. 22(1)(b) DGA. Recital 23 DGA further mentions technical standards, codes of conduct, and certifications as relevant references

[188] 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).

[189] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[190] 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.

[191] Cf. Art. 52 CSA.

[192] Cf. recital 77, Arts. 53 CSA; Recital 45 CRA.

are, however, mostly still under development which incentives adherence to international standards.[193] In this context, the European Union Agency for Cybersecurity (ENISA) proposal for a cybersecurity certification scheme for cloud services (EUCS) sparked controversy regarding server localisation measures for high and high+ security levels. Further tensions with foreign trade partners are related to Art. 24(1) NIS2 which enables EU member states and the EC to require critical infrastructure entities to adopt EUCS-certified ICT solutions .[194]

Following the same governance logic, Art. 51 PIPL and the Chinese SCC[195] outline general cybersecurity duties refering to other instruments for details. Art. 21 CSL introduces mid-level measures for network operators and infrastructure services by updating the Multi-Level Protection Scheme to version 2.0 (MLPS).[196] The latter requires operators to first self-asses risk and impact levels and to implement appropriate cybersecurity measures. The details are specified in technical standards.[197] The MLPS then mandates third-party certification and supervision for its risk-based security levels 2-5. A catalogue additionally specifies which ICT devices specifically require certification. Following a data-based approach, Art. 21 DSL additionally requires appropriate security measures to be implemented depending on the criticality of the data. As a baseline, data handlers are obliged to establish a data security management system and to implement safeguarding technical measures. For critical data and core data, enhanced protection measures must be implemented (Art. 21 DSL).[198] Further emphasis's is given on network infrastructure in Arts. 9 and 30 et seq NDR iterating general network security management duties.

To summarise, the CSL and the DSL establish a framework that aims at ensuring data and cyber security standards comparable to recent EU regulation. The frameworks are similar in terms of their scope of protection and mainly differ in their structural design. Chinese law, however, also follows an impact-based approach considering device, infrastructure, and data classification schemes, while the EU mainly relies on device and infrastructure risk classification. The Chinese framework additionally provides for comprehensive national standards while upcoming EU harmonized standards are still being developed.

B. Technical Measures in Data and Cybersecurity

1. Anonym- and Pseudonymisation

Regarding personal data protection, both systems incentivise and in part require anonymisation of personal data. The frameworks achieve this by excluding non-personal data from the scope of the

[193] ENISA, *Cyber resilience Act Requirements Standards Mapping* (2024), 51; cf. Rec 58, 59, 79 NIS2; 75, 77 CSA; Arts. 18, 19 CRA.

[194] Cf. Charles Helleputte, 'Fewer Clouds on … Cloud: The EU to (Finally) Drop Most Data Localisation Requirements in the EUCS' *Lexology*, 22.9.2023.

[195] Art. 2.5 Chinese SCC, clause 8.5 EU SCC.

[196] DGAP, 'China: MLPS 2.0 - Baseline requirements and practical takeaways for businesses' (One Trust Data Guidance 2022) <www.dataguidance.com/opinion/china-mlps-20-baseline-requirements-and-practical> accessed 14 March 2024.

[197] Cf. GB/T 28448-2019 (Evaluation Requirements) and GB/T 22239-2019 (Baseline for classified protection of cybersecurity).

[198] Art. 30, for example, mandates regular risk assessments for critical information infrastructure operators (CIIO) and immediate reporting of the results to the respective authority bodies.

GDPR[199] respectively the PIPL[200] and requiring anonymisation within more specific regulations (EU[201]; China[202]). In the case of the re-use of personal data, for example, the DGA strictly requires anonymization.[203] This potentially forecasts a potential trend in acknowledging *de facto* loss of control of data subjects despite consent requirements being in place. Compared to EU law, Art. 39 PIPL mandates anonymisation whenever a cross-border transfer cannot be based on separate consent of the data subject.[204] Consequently, there is a double incentive to anonymise since already anonymised non-important data do not trigger a security assessment.

However, many processing purposes depend on non-anonymised data. Both EU[205] and Chinese data regulations[206], SCCs[207], and standards[208] therefore additionally incentivise and in part require pseudonymisation or de-identification[209], which is the process of substituting personal identifiers with a new pseudonym identifier (e.g. by encryption or lookup tables). As an example, Art. 44(3) Proposal EHDS Regulation requires pseudonymisation where anonymisation is not viable. *Yu/Fei* support the adoption of this rule for the Chinese health data space.[210] In this regard, essential equivalence can be argued based on the subjective and context-depended approach to identifiability under both systems.[211] Whilst differences in the understanding of what generally constitutes pseudonymisation may still arise due to the manifold scenarios in data processing, they often remain theoretical in nature.[212] The EDPBs initial strict view, that effective pseudonymisation requires that only the data exporter or a trusted entity based in the EU can hold information that allows for re-identification[213] must be read in context of the EDPBs recent tolerance of pseudonymization as a supplementary measure in data transfers.[214] Overly restrictive measures might result in localization effects comparable to Chinese law.[215] When it comes to AI, the exceptions in Art. 10(5)(a) AIA for bias testing and Art. 59(1)(b) AIA for

[199] Cf. Recital 26 GDPR.

[200] Art. 51 in conjunction with Art. 73(3) PIPL exclude anonymised data from its scope of application (Art. 4 PIPL).

[201] Clause 8.5 EU SCC; Recital 69 AIA (AI lifecycle); Recital 40 CSA (promotion of safe online behavior); Arts. 17(1)(g), 18(4) DA (exceptional need by public entities); Art. 5(3)(a)(i) DGA (anonymization before re-use); Arts. 44(2,3) (access to health data) Proposal EHDS Regulation.

[202] Art. 2(5) Chinese SCC; Arts. 12(1) and 22 Regulations on the Management of Online Data, Art. 42 CSL (condition for transfers by network operators); Art. 11 Interim Measures (usage records); Art. 9 Automotive Data Provisions (processing without consent); Art. 24 NDR (unnecessary data).

[203] Recital 7,8, 15 DGA; Art. 5(3)(a)(i) DGA.

[204] GB/T 35273—2020 requires either de-identification or consent in cross-border transfers.

[205] Clause 8.6 EU SCC; Recital 15 DGA; Art. 18(5), Recital 8, 64 DA; Art. 32, 25, Art. 32(1)(a), Recital 156 GDPR; Art. 44(3) Proposal EHDS Regulation; Recital 61, Art. 10(5) AIA.

[206] Cf. Recital 28, 78 GDPR; Art. 51 PIPL.

[207] Compare Art. 2(5) Chinese SCC and Clause 8.6 EU SCC.

[208] Art. 51(3) PIPL; Art. 6.2 GB/T 35273—2020.

[209] Art. 73(3) PIPL; Art. 2(5) Chinese SCC.

[210] Yu Yao, Fei Yang, 'Overcoming personal information protection challenges involving real-world data to support public health efforts in China' (2023) 11 *Digital Public Health* 4.

[211] See Recital 26 ("reasonably") and 30 GDPR, Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779; for China see Zhang/Wang (n. 65) 13.

[212] Xiaowei, Yu, 'The Identifiability Problem in Transnational Privacy Regulation' (2023) 56 *Vanderbilt Journal of Transnational Law* 1339.

[213] EDPB (n 17), 31.

[214] EDPB, Guidelines 01/2025 on Pseudonymisation (2025) 16.

[215] Cf. GB/T 35273—2020.

secondary use enable the processing of non-anonymised data in the EU. This is not mirrored by Chinese AI regulations[216] which fall in line with the strict horizontal consent approach. In summary, while some differences potentially remain, a high formal standard of data privacy protection is ensured under Chinese law by a combination of strict consent, anonymization and de-identification requirements.

2. Encryption

Encryption is regarded as the essential technical safeguard under both EU[217] and Chinese[218] law. The EU[219] and the ECHR[220] specifically emphasise end-to-end encryption in private communication. Cryptographic algorithms like AES[221], RSA, and the SHA variations are currently the main encryption methods recognised for data transmission in the EU and internationally.[222] China additionally provides its own cryptographic algorithms, mainly the ShāngMì (SM) series (SM2-4,[223] SM9). Encryption is encouraged in China for sensitive personal data,[224] while important and core data must be encrypted.[225] Following criticism in the past, the Chinese Cryptography Law (CL)[226] of 2020 now also permits imports of foreign commercial encryption products with a maximum of 256-bit encryption (Art. 21 CL).[227] EU entities can therefore choose between Western or Chinese algorithms as long as they are guaranteed to provide an equivalent level of protection.[228] This said, potential backdoors and client-side scanning pose a specific challenge with encryption products.[229] Chinese administrative bodies allegedly require access to encryption keys and the installation of backdoors based on Art. 31 CL and Art. 28 CSL.[230] For example, an Apple data center in Guiyang made the headlines when it was allegedly required to store encryption keys on the premises of a partner company.[231] The EC additionally highlights

[216] For standard prohibitions see Art. 11 Interim Measures; Art. 5.2(c) (biometric information) GAIS.

[217] Art. 32(1)(a), Recital 83 GDPR; Clause 8.5 EU SCC; Art. 69 AIA; Recital 40 CSA; Art. 21(2)(h), Recital 98 NIS2; Art. 11, Recital 8, 78 DA; Recital 23 DGA. Art. 21(2) NIS2 mentions cryptography, encryption, and multi-factor authentication.

[218] Art. 2(5) Chinese SCC; Art. 9 Regulations on the Management of Online Data.

[219] Akoh Atadoga, Oluwatoyin Ajoke Farayola, Benjamin Samson Ayinla, Olukunle Oladipupo Amoo, Temitayo Oluwaseun Abrahams, Femi Osasona, 'A Comparative Review of Data Encryption Methods in the USA and Europe' (2024) *5 Computer Science & IT Research Journal* 452.

[220] ECHR, *Podchasov v. Russia*, no. 33696/19; cf. Recital 98 NIS2.

[221] Standardised in ISO/IEC 18033-3.

[222] Akoh Atadoga, et alia, 'A Comparative Review of Data Encryption Methods in the USA and Europe' (2024) *5 Computer Science & IT Research Journal* 448.

[223] Cf. SM 4 is the national standard GM/T 0002-2012 SMA Block Cipher Algorithm.

[224] Art. 51(3) PIPL; Art. 6.3(a) GB/T 35273—2020.

[225] Art. 9(3) Regulations on the Management of Online Data Security, Art. 7 CL.

[226] Cryptography Law of the P.R.C.' (2019).

[227] Frank Pan, Tina Li, 'MOFCOM Issues New Encryption Import Control Effective Immediately' (*Baker McKenzie Blog*, 11.11.2021) <https://sanctionsnews.bakermckenzie.com/mofcom-issues-new-encryption-import-control-effective-immediately/>.

[228] EDPB (n 19) 32; cf. Louise Bergman Martinkauppi et alia, 'On the Design and Performance of Chinese OSCCA-approved Cryptographic Algorithms' (2020) 13th International Conference on Communications (COMM), Bucharest. Foreign encryption can likely not be used for the encryption of important and core data since the CL mentions foreign technology only in the context of commercial encryption under Chapter III.

[229] See an overview of encryption circumventing methods at EU Commission's May 2022 impact assessment report on the draft CSA Regulation, 309.

[230] Lorand Laskai, Adam Segal, 'The Encryption Debate in China: 2021 Update' (2021) *Carnegie Endowment for International Peace*, 31.3.2021.

[231] Cf. Jack Nicas, Raymond Zhong, Daisuke Wakabayashi, 'Inside Apple's Compromises in China: A Times Investigation' *The New York Times* (2021).

future risks arising with post-quantum technology[232] while the US National Institute of Standards and Technology already provides new lattice-based cryptography standards in this regards.[233] However, recent claims of companies of having cracked standard encryption with quantum computing remain unverified.[234] Finally, only selected virtual private networks are currently approved in China, which restricts the available options for lawful cryptographic protection.

3. Innovative Approaches

New data protection and cybersecurity technology promises higher privacy standards. Of particular interest are specifically methods that provide anonym- and pseudonymisation. Recitals 69 AIA and 8 DA specifically reference federated learning as a confidentiality measure in AI development.[235] The approach has been recognised by the German Data Ethics Commission as strengthening data minimization, purpose limitation and privacy by design.[236] In federated learning, sensitive data remains on edge devices while locally trained AI models are transferred to central servers in the form of updates. A related approach is recommended by the EDPB, where transfers of IoT data from edge devices are restricted to locally calculated scores (e.g. in vehicle insurance).[237] However, specific vulnerabilities exist in federated learning and edge devices which allow training data to be extracted from local models.[238] A comprehensive cybersecurity architecture should therefore include homomorphic encryption, differential privacy[239], k-anonymization[240], or multi-party computation[241]. Moreover, innovative digital identity management solutions based on decentralized identifiers (DIDs) provide individuals more selective control over the disclosure of their personal data (Cf. Rec. 7 GDPR).[242] Additionally, smart contract solutions can guarantee execution of claims, where state interference my hinder execution via the court system. All these methods can provide additional protection by adding noise to the data, equalizing data points, obfuscating inputs of individual participants, and localizing computation.[243] Companies may also primarily rely on exporting synthetic data and pre-trained AI models to protect

[232] Commission Recommendation of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography, C(2024) 2393 final.

[233] NIST, Note on post-quantum encryption, Docket No. 240719-0201.

[234] Tanuj Khattar, Noureldin Yosri, A comment on 'Factoring integers with sublinear resources on a superconducting quantum processor' (2023) <https://doi.org/10.48550/arXiv.2212.1237>

[235] Recital 43 Draft EHDSR further mentiones "generalisation, suppression and randomization of personal data".

[236] Data Ethics Commission, *Opinion of the data ethics commission* (Data Ethics Commission 2019) 120.

[237] EDPB, 22. Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications Version 1.0, 2020, 22.

[238] Li et alia, 'A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection' (2021) <https://doi.org/10.48550/arXiv.1907.09693>

[239] Art 29 Data Protection Working Group, 'Opinion 05/2014 on Anonymisation Techniques' (EC 2014) 15 et seq.

[240] EMA, 'Data anonymisation - a key enabler for clinical data sharing Workshop report' EMA/796532/2018, 21.

[241] EDPB (n 19) 33 et seq.

[242] Cf. Alexandra Giannopoulou, 'Data protection compliance challenges for self-sovereign identity' in: J. Prieto et al. (eds.): *BLOCKCHAIN 2020*, *AISC 1238* (2021), 1–10.

[243] Cf. Sophie Stalla-Bourdillon, Alfred Rossi, 'Why a good additional technical safeguard is hard to find A response to the consultation on the EDPB draft recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (2021) EDPB 4 et seq.

anonymity.[244] In this context, federated learning based on differential private synthetic data is one proposed approach.[245] These methods allow for maintaining data-based business relations while lowering risks for personal or otherwise sensitive data.[246] Importantly, these new methods are not prohibited under Chinese law. Instead, Chinese industry[247] and academia consider them as valuable privacy safeguards[248] and are developing their own standards for federated learning as well as multi-party computation solutions.[249] The Chinese administration is not opposed to these developments with technical standards being published on federated learning[250], differential privacy,[251] and multi-party computation[252]. They may arguably even be required in private and commercial settings under Arts. 51(3) PIPL, 21 et seq DSL and the general framework of the MLPS.

As mentioned above, innovative approaches to privacy and confidentiality, especially in the context of AI, require further safety and security research given the known and unknown vulnerabilities such as in model inversion attacks, prompt injection, and jailbreaks.[253] ENISA emphasises that AI development introduces new risks, specifically mentioning vulnerabilities of the open source environment, training data poisoning, adversarial attacks, reverse-engineering of the trained model[254], and low security levels in edge devices.[255] The EDPB[256] and the EDPS[257] already provide first guidance on data confidentiality in the context of AI. The AIA acknowledges these risks by mentioning data poisoning, model poisoning, adversarial attacks, model evasion, confidentiality attacks and model flaws.[258] Art. 10 AIA then translates these risks into data transfer obligations requiring stakeholders to assess the origin of the data[259] and potential biases caused by compromised data.[260] Finally, regarding systemic risks posed by general purpose AI models, Recital 115 AIA mentions model leakage and unsanctioned releases. Looking at Chinese regulation, challenges in the area of AI cybersecurity are not specifically

[244] E.g. Markus Hittmeir, Andreas Ekelhart, Rudolf Mayer, 'Utility and Privacy Assessments of Synthetic Data for Regression Tasks' (2019) IEEE International Conference on Big Data (Big Data).

[245] Charlie Hou et alia, PrE-Text: Training Language Models on Private Federated Data in the Age of LLMs, https://doi.org/10.48550/arXiv.2406.02958 accessed 30 July 2024.

[246] EDPB (n 19) 30.

[247] 'FederatedScope' (GitHub, 28 March 2022) <https://github.com/alibaba/FederatedScope> accessed 26 March 2024.

[248] Yufeng Zhan, et alia, 'A Learning-Based Incentive Mechanism for Federated Learning' (2020) 7 *IEEE*; Xianglong Zhang et alia, 'A Privacy-Preserving and Verifiable Federated Learning Scheme' (2020) *IEEE.*

[249] Rui Ye et alia, 'OpenFedLLM: Training Large Language Models on Decentralised Private Data via Federated Learning' *Cornell University* <https://arxiv.org/abs/2402.06954> accessed 26 March 2024.

[250] AIOSS, Information technology service – Federated learning – Reference architecture, AIOSS-03-2019.

[251] TAF, 'T/TAF 137—2022 Technical requirements for the protection of users' personal information based on differential privacy' (2022).

[252] Cf. Accesswire, 'Technical Requirements and Test Methods for Data Circulation Products based on privacy-preserving multi-party computation' (2021) *Accesswire*, 10.3.2021.

[253] EDPS, *Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems* (2024) 22.

[254] ENISA, *Artificial Intelligence and Cybersecurity Research* (ENISA 2023) 24.

[255] Ibid.

[256] EDPB, *Strategy 2024-2027* (2024).

[257] EDPS (n 223).

[258] Art. 15(5) AIA.

[259] Art. 10(2(b)).

[260] Art. 10(2(f, g) and (3)).

addressed on the regulatory level. The Interim Measures[261] and the Draft AI Law[262] mainly reference general cybersecurity requirements which leads to the application of the MLPS. Art. 41 Draft AI Law, however, specifically mentions vulnerabilities and security risks of open-source frameworks and Art. 7(i)(2) of the Basic Requirements for GAI additionally mentions that user's input data must be consistently monitored to prevent denial-of-service, cross-site-scripting, and injection attacks. For now the rules in both jurisdictions only provide a preliminary frameworks which require further development based on scientific research results.

C. Conclusions on Data and Cybersecurity

In summary, both EU and Chinese high-level regulations mandate appropriate cybersecurity measures depending on the associated risk level whilst delegating details to technical standards, lower-level implementing acts, and ultimately the risk assessment of the parties involved. The Chinese cybersecurity framework requires entities to adopt robust measures which guarantees essentially equivalent security in private and commercial matters. At the same, it does not prevent authorities from potentially accessing private and sensitive industrial data. To mitigate medium to high risk scenarios, data exporters should therefore refrain from transferring highly sensitive data or rely on multi-party computation, federated learning, differential privacy, and synthetic industrial data to comply with the requirements of the GDPR and upcoming requirements under the DGA. With regard to future EU regulation, we believe that more emphasis should be placed on innovative approaches to encourage their development and adoption.

V. Final Conclusions

From the viewpoint of the case law of the European Courts, it is unlikely that the Chinese framework will be considered essentially equivalent to a level to allows for an adequacy decision. State influence is an inherent part of the Chinese system of governance and does not align with European privacy concepts. In contrast, we find equivalent legal protection of personal data in private and commercial settings with strict conditions and restrictions regarding the trade, transfer, secondary use, and cross-border transfer of personal data. Hence, where national security interests are not concerned, technical safeguards are provided, and data subjects can be satisfied with alternative compensation, low risk cross-border transfers of non-sensitive personal data appear legitimate from a risk-based perspective. Where higher risks and sensitive personal data are involved, innovative technical measures and anonymization should be considered.

The export of industrial data from the EU remains lawful without authorisation, except where dual-use and sensitive technologies are concerned. However, the DGA now empowers the European Commission to introduce further restrictions on cross-border transfers of re-used data based on future legal acts. In contrast, the Chinese framework already imposes horizontal restrictions on cross-border transfers where critical information infrastructure as well as important and core industrial data are concerned. To ensure a stable flow of data between the EU and China, data exporters need to develop expertise in classifying data according to its sensitivity and potential strategic and economic impact, as well as assessing the appropriateness of conventional and innovative security measures.

[261] Arts. 7(5) and 9.
[262] Art. 22.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

THE CRIMINAL CLASSIFICATION OF CASH EXPORTS TO RUSSIA IN LIGHT OF THE EU SANCTIONS REGULATION AND RECENT CASE LAW

Alicia Althaus

AUTHOR

Alicia Althaus is an attorney specializing in criminal defense, particularly in white-collar and tax criminal law, general criminal law, and compliance, and works at the law firm Traut. She regularly publishes articles on criminal law topics and is currently pursuing a doctorate on a comparative legal topic in the field of criminal law.

TABLE OF CONTENTS

I. INTRODUCTION

Since spring 2022, the EU sanctions imposed on the Russian Federation have led to profound restrictions on economic relations. While the large-scale trade restrictions and financial sanctions against Russian oligarchs have received significant media attention, less prominent measures—such as the ban on cash exports to Russia—have gained increasing importance in criminal law practice.

This article examines the practical implementation and legal classification of this sanction in Germany, focusing in particular on recent case law from courts in Frankfurt. It analyzes the legal consequences for private individuals and critically explores the problematic interpretation of the term "personal use." Against the backdrop of the recent referral by the Higher Regional Court (OLG) of Frankfurt am Main to the European Court of Justice (ECJ), the article also outlines the implications for defense strategies in related criminal proceedings and highlights the need for legal clarification.

II. IMPLEMENTATION IN GERMANY

In Germany, the enforcement of the Russia Regulation (RusslandVO) is primarily carried out through Sections 17 et seq. of the Foreign Trade and Payments Act (Außenwirtschaftsgesetz – AWG) and Sections 80 et seq. of the Foreign Trade and Payments Ordinance (Außenwirtschaftsverordnung – AWV), whereby violations of the regulations are classified as criminal offenses or administrative violations. Particular importance is attached to Section 18 AWG, which defines the criminal consequences of breaches of embargo provisions. The restriction on the export of cash has already led to criminal prosecutions.

A. A Trip from Frankfurt to Russia

Two notable examples of the practical application of these provisions are the judgments of the District Court (Amtsgericht) of Frankfurt am Main.

In the first case, dated January 31, 2023, the defendant was convicted of attempted unauthorized export of banknotes and sentenced to a fine of 90 daily units of €50 each.[1] The case involved a traveler who went to Frankfurt Airport intending to travel via Istanbul to Moscow and further on to Kaliningrad. He was carrying a total of €10,000. According to the traveler, the money was intended to cover travel expenses and an extensive dental treatment planned in Kaliningrad. During a customs check at Frankfurt Airport, customs officers noticed the amount of cash. He was allowed to keep only €500 for travel expenses, and the remaining cash was confiscated.[2]

In the second case[3], the defendant intended to travel from Frankfurt Airport to Istanbul on May 31, 2022, and from there directly onward to Moscow. She was carrying a total of EUR 14,855 and 99,150 rubles. The defendant planned a three-week stay in Russia. The money she was carrying was intended

[1] AG Frankfurt am Main, judgment of 31.1.2023 - 943 Ds 7140 Js 235012/22.

[2] AG Frankfurt am Main, judgment of 31.1.2023 - 943 Ds 7140 Js 235012/22.

[3] AG Frankfurt am Main - 943 Cs 7140 Js 230982/22.

not only to cover travel expenses but primarily to fund three medical treatments in Russia: dental treatment (veneers), hormone therapy at a fertility clinic, and a follow-up treatment after breast surgery at a plastic surgery clinic.[4]
During a customs inspection at the airport security checkpoint, the cash was discovered. The defendant had not made a prior declaration of the planned transport of cash as required under the Cash Control Regulation. As a result, euro banknotes amounting to EUR 13,800 were confiscated, while EUR 1,055 was left to the defendant for personal travel expenses. The defendant did not embark on the trip.[5]

Both cases exhibit significant parallels. In both instances, the individuals involved were travelers who intended to transfer substantial amounts of cash from Frankfurt Airport to Russia. According to the defendants, the cash was in part meant to finance dental treatments in Russia, which were said to be significantly more expensive in Germany. In both inspections, only a small amount of EUR 500 and EUR 1,055 respectively was left to the travelers for personal travel needs. In both proceedings, convictions were made pursuant to § 18(1)(1)(a), § 18(6) of the German Foreign Trade and Payments Act (AWG) in conjunction with Article 5i(1) of the Russia Regulation (RusslandVO).

The key difference lies in the fact that in the first case, the judgment became legally binding, whereas in the second case, the legal question has now been referred to the European Court of Justice (ECJ) for a ruling.[6]

B. Assessment oft the Legal Reasoning

The reasoning of the courts is examined and evaluated below. The interpretation of the regulation as allowing only an upper limit of EUR 500 stands in a certain tension with a FAQ issued by the European Commission. According to this FAQ, funds intended for personal use may be brought in, with the decisive factor being the non-commercial nature of the transaction.[7] However, the District Court of Frankfurt am Main takes its interpretation of the regulation a step further by excluding medical treatments from the exemption under Article 5i(2).[8] Yet, depending on how the regulation is interpreted, medical treatment could indeed be considered a form of personal use.

1. Mistake of Law

The strict interpretation by the District Court of Frankfurt am Main also raises questions regarding the potential for a *mistake of law* (*Verbotsirrtum*) under § 17 of the German Criminal Code (StGB). Supporting the existence of such a mistake is the fact that restrictions on the export of cash by private individuals have received far less public attention than more prominent sanctions against Russian oligarchs. Furthermore, the Russia Regulation (*RusslandVO*) has been amended numerous times since

[4] OLG Frankfurt am Main, judgment of 02.04.2024 - 1 ORs 61/23 Rn. 2.

[5] OLG Frankfurt am Main, judgment of 02.04.2024 - 1 ORs 61/23 Rn. 2.

[6] OLG Frankfurt am Main, judgment of 02.04.2024 - 1 ORs 61/23.

[7] Europäischer Rat und Rat der Europäischen Union, Die Sanktionen der EU gegen Russland im Detail, https://www.consilium.europa.eu/de/policies/sanctions-against-russia-explained/#exportban (Stand: 30.09.2024).

[8] AG Frankfurt am Main, judgment of 31.1.2023 - 943 Ds 7140 Js 235012/22; AG Frankfurt am Main - 943 Cs 7140 Js 230982/22.

its inception[9], which can make it difficult to stay informed about the current legal situation. On the other hand, arguments against recognizing a mistake of law include the fact that the relevant regulations and interpretative guidance are publicly accessible[10], and that there has been broad media coverage of sanctions against Russia in general. The court ultimately followed this latter view in its ruling, classifying the defendant's claim of ignorance regarding the export ban as a mere protective assertion (*Schutzbehauptung*).

Regardless of the question of a mistake of law, the issue of the subjective element of the offense remains a critical point. The subjective element of § 18(1) of the Foreign Trade and Payments Act (AWG) also includes knowledge of the existence of the relevant legal provision. This element will often not be met, particularly in cases where travelers are not fully informed about the specific provisions of the embargo regulations.

2. Personal Use

The correct interpretation of the term "personal use" is problematic for several reasons. While the aforementioned FAQs of the European Commission suggest a distinction between private and commercial use[11], they do not provide an explicit limitation to specific purposes. Although the Local Court of Frankfurt am Main explicitly refers to an average standard of living and excludes luxury expenses[12], it remains unclear what exactly is meant by an "average standard." This ambiguity affects practical aspects such as booking accommodation and transport in Russia, as well as the purchase of souvenirs or food. Average costs can vary significantly depending on region, season, and individual preferences.

Similarly, the interpretation of the term "necessary" in this context is problematic, as the necessity of expenses can vary greatly on a case-by-case basis. The fixed threshold of 500 EUR appears too rigid in light of these considerations. An alternative could be to take orientation from the EU Regulation on Cash Controls (BarmittelVO), which allows for the export of cash up to 10,000 EUR without prior declaration. At first glance, this analogy could be supported by the principle of coherence in EU law, which calls for similar treatment of comparable situations. The Cash Regulation also governs the cross-border movement of economic goods and could thus serve as a reference framework.

However, there are strong counterarguments against a direct and uncritical application: the two regulations pursue fundamentally different objectives. While the Cash Regulation primarily aims to combat money laundering and terrorist financing, the Russia Regulation (RusslandVO) explicitly targets far-reaching economic sanctions – a distinction rightly emphasized by the Frankfurt court in its reasoning.

Nonetheless, one could argue that the significantly higher threshold of 10,000 EUR might better align with the principle of proportionality. It could represent an effective sanctions instrument while avoiding

[9] Note: An overview of how many sanction packages have been adopted can be found on the website of the BAFA (Federal Office for Economic Affairs and Export Control): Restrictive Measures against Russia I. Overview of Sanction Packages, https://www.bafa.de/EN/Foreign_Trade/Export_Control/Embargoes/restrictive_measures_russia/restrictive_measures_russia.html

[10] AG Frankfurt am Main, judgment of 31.1.2023 - 943 Ds 7140 Js 235012/22.

[11] Europäischer Rat und Rat der Europäischen Union, Die Sanktionen der EU gegen Russland im Detail, https://www.consilium.europa.eu/de/policies/sanctions-against-russia-explained/#exportban (Stand: 30.09.2024).

[12] AG Frankfurt am Main, judgment of 31.1.2023 - 943 Ds 7140 Js 235012/22.

disproportionate restrictions on legitimate travel activities of natural persons. Even with differing regulatory purposes, EU legislation should strive for a certain degree of consistency to ensure legal certainty for EU citizens. For travelers, a higher degree of legal clarity would result if the threshold values in cross-border contexts were at least generally harmonized, regardless of the specific regulatory objective.

III. REFERRAL TO THE CJEU – A LEGAL TURNING POINT AHEAD?

The Higher Regional Court (Oberlandesgericht, OLG) of Frankfurt am Main has submitted a preliminary ruling request to the Court of Justice of the European Union (CJEU) regarding the interpretation of Article 5i(2)(a) of Regulation (EU) No 833/2014.[13] Specifically, the question concerns whether the export of euro banknotes to Russia for medical treatments falls under the term "personal use" and is therefore covered by the sanctions exemption.

In the underlying case, the Local Court (Amtsgericht) of Frankfurt am Main convicted the defendant for the attempted unauthorized export of banknotes pursuant to § 18(1)(1)(a), (6) of the German Foreign Trade and Payments Act (AWG) in conjunction with Article 5i(1) of the Russia Regulation. The defendant was sentenced to a fine of 120 daily units of EUR 150 each.[14] In its legal reasoning, the Local Court held that the euro banknotes carried by the defendant for medical treatments in Russia did not fall within the exemption clause of Article 5i(2)(a) of the Russia Regulation. To interpret the term "personal use" in that provision, the court referred—similarly to a previously discussed decision—to the recitals of the Regulation as well as the European Commission's FAQs.[15]

The defendant filed a direct appeal (Sprungrevision), claiming a violation of substantive law.[16] The OLG Frankfurt then saw it necessary to refer a question to the CJEU under Article 267 TFEU. The specific question is:

"Is the export of banknotes denominated in the official currency of a Member State to be regarded as necessary for the personal use of a natural person traveling to Russia within the meaning of Article 5i(2)(a) of Regulation (EU) No 833/2014, if such banknotes are to be used for the purpose of receiving medical treatments in Russia (in this case, dental treatment, hormone therapy at a fertility clinic, and follow-up treatment following a breast surgery at a clinic for plastic surgery)?"[17]

The OLG Frankfurt justifies its referral by noting that the term "personal use" is not further clarified in the Russia Regulation. While the European Commission's FAQs state that a non-commercial character is decisive for determining personal use, they do not specify for which exact purposes the exported banknotes may be used during travel to and within Russia. Similarly, the term "necessary" offers no clear guidance regarding the permissible purposes under the exemption clause.[18]

[13] OLG Frankfurt am Main, judgment of 02.04.2024 - 1 ORs 61/23.

[14] AG Frankfurt am Main - 943 Cs 7140 Js 230982/22.

[15] AG Frankfurt am Main - 943 Cs 7140 Js 230982/22.

[16] OLG Frankfurt am Main, judgment of 02.04.2024 - 1 ORs 61/21 Rn. 12.

[17] OLG Frankfurt am Main, judgment of 02.04.2024 - 1 ORs 61/23.

[18] OLG Frankfurt am Main, judgment of 02.04.2024 - 1 ORs 61/23 Rn. 14 ff.

The referral question submitted by the Higher Regional Court (OLG) of Frankfurt underscores the problem already identified in the discussion of the initial judgment: the term *"personal use"* within the meaning of the Russia Regulation (RusslandVO) is not clearly defined and requires a precise, uniform interpretation. The forthcoming decision by the Court of Justice of the European Union (CJEU) will be pivotal for the criminal prosecution of violations related to the ban on cash exports to Russia.

While the Local Court (Amtsgericht) of Frankfurt applied a very narrow standard in both cases and generally excluded medical treatments from the scope of *personal use*, the OLG's referral raises the legitimate question of whether such a restriction is indeed supported by the wording and objective of the Regulation. In particular, it remains debatable whether personal medical treatments might in fact fall under *personal use*—provided they lack any commercial character and are solely intended for the traveling individual.

The pending CJEU decision will be of significant importance not only for legal practitioners but also for individuals traveling to Russia. It may pave the way for a more differentiated interpretation of which purposes are covered by the exemption clause in Article 5i(2)(a) of the Russia Regulation.

IV. CONCLUSION AND OUTLOOK: A PLEA FOR A PROPORTIONAL INTERPRETATION OF EU SANCTIONS LAW

The recent decisions by the Local Court (Amtsgericht) of Frankfurt am Main concerning the export of cash to Russia reveal significant legal uncertainties for private individuals. The restrictive interpretation of the term “personal use” leads to a criminal assessment that deserves critical scrutiny. While the political objectives of the EU sanctions should not be fundamentally questioned, the current interpretative practice appears disproportionate and potentially incompatible with fundamental rights. Most notably, it poses a serious risk to legal certainty.

The referral by the Higher Regional Court (OLG) of Frankfurt to the CJEU now offers an opportunity for necessary legal clarification and a consistent application of the law across the EU. It is particularly to be hoped that the CJEU will adopt a nuanced approach that better reflects the principle of proportionality. Medical treatments – especially when they serve preventive healthcare – should unquestionably fall under the scope of personal use.

De lege ferenda, a harmonization of threshold values in the context of cross-border cash movements would also be desirable. The divergent provisions between the EU Cash Regulation (BarmittelVO) and the Russia Regulation (RusslandVO) result in avoidable legal uncertainties for EU citizens. Raising the de minimis threshold to the commonly applied limit of EUR 10,000, as used in other regulatory contexts, would not significantly impair the effectiveness of the sanctions but would prevent disproportionate intrusions into the freedoms of private individuals.

Until a final ruling by the CJEU provides clarity, prosecutors and courts should apply Article 5i of the Russia Regulation in strict adherence to the principle of legal certainty, and in cases of doubt, rule in favor of the accused. Particularly in the field of sanctions law – which is marked by high complexity, frequent amendments, and limited public awareness of detailed provisions – the subjective element of the offense should be examined with particular care.

The forthcoming CJEU ruling will make a significant contribution to legal certainty within European sanctions law and could serve as a precedent for the future interpretation of comparable legal provisions.

NAVIGATING CHALLENGES: THE EVOLUTION OF ENVIRONMENTAL CONTROL LEGISLATION

A Cross Country Comparative Study

Luminita Diaconu

AUTHOR

Luminita Diaconu PhD student has been a university lecturer since 1996 with experience in lecturing at many universities from The Republic of Moldova. She has MA in American Studies. (2002) From 2008 Mrs Diaconu has been teaching at the Academy of Economic Studies of Moldova and is a doctoral student at the "Stefan cel Mare" Academy of MIA (Republic of Moldova) She is doing her research in Public Law writing her thesis on Ecological Control.

ABSTRACT

The end of the last century was driven by a huge leap in technological achievement. In a very short time, the humanity was able to capitalize on what nature had placed at its disposal. Precisely because of this, the mankind "forgot" to ensure that the increase in the capacity to exploit natural resources would at the same time secure his future existence. However, as a result of a series of natural disasters, the human being has begun to realize, that the environmental problem is becoming an issue that does not respect the borders between states, but must be tackled at an international, not just a national, level. The protection of the environment is not a separate issue, however, because human health and life on The Earth depend on the solution to this problem. A social, moral and legislative approach to environmental issues has become a vital necessity for the whole earth. The creation of a national regulatory system for environmental control is a vital necessity. Last but not least, such an approach depends on the way and conditions of implementation of environmental control, identified by scientific researches and new legislative approaches. The institution of ecological (environmental) control has a special place in ensuring a correct regulatory process in environmental protection. The elaboration of scientific theories in this field, carried out in parallel with the activity of legislative creation, can and will bring added value to the process of regulating environmental control activities and, as a result, to the entire process of environmental

protection regulation. This paper gives a theoretical analysis of Barriers to Progress: analyzing the development of Environmental Control Laws worldwide.
Key words: ecological control, implementation, worldwide legislation

TABLE OF CONTENTS

I. INTRODUCTION

Although at the legislative level and even at the political-declarative level, we have a coherent approach to the issue of environmental protection, witnessing a positive approach to these issues, we must recognize that both informally, and also in practice, in Moldova, the issue of environmental protection remains a secondary one.

In an attempt to explain and justify such an approach, we note that researchers in the field are sounding the alarm, in most cases the emphasis is on the quality of the rules, not on the implementation element[1]. The problems associated with the development of environmental control legislation around the world are many and interrelated, reflecting the complex challenges of environmental protection. A major problem is regulatory inconsistency, where different countries adopt different regulations, making it difficult to implement uniform environmental control standards. In addition, a lack of financial and human resources to enforce existing laws limits the effectiveness of enforcement agencies, resulting in inadequate monitoring of environmental practices. Low awareness of the importance of environmental protection among the general public and policy makers also contributes to the stagnation of legislative progress. These problems underline the need for closer international co-operation and harmonization of environmental legislation to address global environmental challenges. In many countries, environmental legislation is often fragmented and poorly enforced, resulting in ineffective protection of ecosystems. For example, air, soil and water pollution remains a major problem, and legislation does not adequately address the root causes of these problems. In addition, there is a lack of harmonization between different national and international regulations, which hampers global environmental control efforts. This situation is exacerbated by economic interests that prioritize industrial development over environmental protection.

II. BARRIERS FOR IMPLEMENTATION

We have to recognize that the cause of such a situation, is the people who have to implement the environmental regulations. It is not uncommon for us to find out, that the rules are good, but they are poorly implemented.

Thus, although some authors[2] point to the quality of the rules governing the use and protection of environmental resources, we should also focus our attention on the question of the quality of the implementation of these rules.

For these reasons, we realize and argue that the introduction of systems of mechanisms that would lead to the streamlining of the process of implementation of environmental control regulations in the area of environmental use and protection would ensure the implementation of the system of environmental control regulations and provide an optimal level of environmental protection, regardless of the quality of the regulatory norms.

A large part of the burden in this respect falls on the (environmental) control institution.

[1] M.Neagu, Legal liability in environmental law, The Transilvania University Annals no. 10/2007, p. 268.

[2] M.Duțu, Dreptul mediului [Environmental law], C.H.Beck Publishing House, Bucharest, 2007, p. 283.

To this end, we propose to carry out a comprehensive study of the legislation on environmental control, in particular to clarify the main issues in this field in order to identify existing problems and ways of solving them.

In our view, the starting point in this respect is to study the content, character and structure of the environmental control system, as well as the mechanism of application of control levers, and through these studies to identify the existing shortcomings in this area.

III. ANALYZING THE DEVELOPMENT OF ENVIRONMENTAL CONTROL LAWS WORLDWIDE

It must be recognized that although there are many scientific studies in the area of "state control", however, in the area of "environmental control" we find only tangentially scientific studies, related to the non-systematic approach to the problems in the field of environmental control.

All existing scientific research in this paper deals tangentially with the issue of environmental control. Although the topics related to environmental law began to be addressed with insistence only in the sixth decade of the last century, however, the issue that directly concerns ecological control, although being recognized as important, has not been the subject of a separate study in the Republic of Moldova.

However, this does not apply to the Russian Federation and Ukraine, since, until the break-up of the Soviet Union, we were part of the same conceptual system of law, it was difficult to break away from the old perceptions of the Soviet system of regulating the relations of ecological control, and it is still quite important how things developed in all the countries of the former Soviet Union.

Among the authors who left their scientific mark in absolutely all countries of the former Soviet Union were Prof. V. Petrov, Prof. B. Erofeev, Prof. S. Bogoliubov, Prof. M. Brinciuk and others. One of the notable Russian scientists who wrote about ecological control is Alexei A. Zheleznov. Viktor A. Karpov and other scientists in the field of ecology have also contributed to studies on ecological management and environmental protection.

For example, the contribution of Professor B. Erofeev,[3] in whose work - *Экологическое право России*, we can trace the main references referring to the principles and rules of implementation of ecological control, as well as its types. Of special interest is the researcher's approach to the district or “oblasti” ecological control.

We should also mention Prof. M. Brinciuk [4], who has given his opinion on the clarification of concepts and terms used in legislative acts in this field in the Russian Federation. Thus, in his research we find explanations and interpretations of such categories as "environment", "favourable environment", "environmental protection", "ecological system", "ecological control requirements", "ecological behaviour", "ecological safety", etc.

In the same context, the approaches of Mr. S. Bogoliubov,[5] who refers to the need to develop a concept for the development of environmental legislation.

[3] B. Erofeev, in whose work - Экологическое право России,(Москва, 2000. 448 p.)

[4] Бринчук М. М. Экологическое право. Москва: Юристь, 1998, 684 с.

[5] Боголюбов С. А. Экологическое право. Учебник для вузов. Москва: НОРМА, 1998. 434 с.

A similar concern can be found in the environmental control doctrine of Ukraine, where the idea of the need to unify the system of environmental regulation, including the establishment of a separate regime for the majority of institutions regulating environmental law, has recently been increasingly popularized. Academician Yu. S. Shemoshchukenko, addressing the given problem, notes the necessity of achieving institutional systematization of the branch.

In the same sense, we refer to the achievements in this field of another Ukrainian researcher - N. A. Orlov, who puts forward some ideas that may cause discussion and controversy. Thus, according to the researcher, there is a need for a single code of laws containing norms-principles that would extend their action to all categories of institutions applicable to ensuring environmental protection.

Furthermore, studying the Romanian doctrine, we note a multitude of authors, but also - approaches. and valuable ideas. Different aspects of the subject of our study have been approached by different researchers, among whom we mention Prof. E. Lupan, Prof. M. Duțu, Prof. D. Marinescu, Prof. Șt. Tașcă; L. Dogaru; O. Popovici and others.

Professor E. Lupan, one of the founders of the discipline of environmental law in Romania, in his works on environmental law, published in 1997, 1998, 1999, 2000 and 2009, addressed the importance of the environmental control mechanism in solving environmental protection tasks.

The Romanian researcher, Prof. M. Duțu,[6] recognized as one of the current promoters of environmental law in Romania, in his numerous publications, especially in recent years, has managed to present a fairly accessible picture of the content and essence of environmental control. In his numerous works, especially those published in recent years (e.g. "Environmental Law", "Environmental Law Treaty", the author provides a detailed analysis of the evolution of the legal protection of the environment in Romania, highlighting the legislative changes from the previous to the current regime and their consequences. An important aspect that the researcher emphasizes is the period and conditions of Romania's pre-accession to the European Union, a period that significantly influenced the development of environmental legislation.

According to the author, the process of aligning Romanian legislation with the acquis communautaire in the field of the environment, which involved the transposition of some 90 European legal acts into more than 120 national regulations, has had a significant impact. In particular, Mr Duțu[7] draws attention to some negative practices observed in this sector, such as: the adoption of the requirements of European directives through subsequent normative acts (government decisions and ministerial decrees); the automatic and full adoption of Community regulations without taking into account existing national regulations; the repeal of the Framework Law on Environmental Protection No. 137/1995 and the adoption of the Emergency Ordinance No. 195/2005, a moment perceived as a political gesture confirming the intention to join the EU, rather than as a well-founded and necessary normative act. However, the EESC believes that this ordinance is essentially transitional in nature and fits into the logic of the development of environmental legislation and the context of the pre-accession period.

[6] M,Dutu "Environmental Law" - University Course, Bucharest, 2007, (482 p.)

[7] M.Duțu, Dreptul mediului [Environmental law], C.H.Beck Publishing House, Bucharest, 2007, p. 283.

Another interesting researcher is Gh. Iancu[8], who in his work entitled *Fundamental Rights and Environmental Protection*. examines in detail the relationship between fundamental human rights and environmental protection.

He argues, that environmental protection is essentially about respecting the rights of others by preventing the degradation or destruction of the environment in which people live. Any form of environmental degradation or destruction can be caused by the abuse of rights by individuals. The central concept promoted by the researcher focuses on the constitutional recognition and enshrinement of the fundamental right to a healthy environment and the establishment of legal liability for its violation. In addition to the in-depth, interdisciplinary and complex nature of the work, we believe that it proposes an innovative principle and objective for environmental law as a whole, namely respect for human rights. Thus, respect for these rights will facilitate effective environmental protection, and protection of the environment will also ensure respect for certain fundamental human rights.

Of course, in spite of the fact that these works comprise, for the most part, a didactic material for the use of students, the authors nevertheless present distinct opinions on different notions, concepts and institutions of environmental control in environmental law, views on the character and effectiveness of environmental control regulations in the field.

At the same time, environmental monitoring has been a focus of scientific and legislative efforts in Europe since the mid-20th century. Scientists have played a key role in policy development, providing empirical evidence, underpinning regulatory frameworks for air quality, water protection, waste management and biodiversity conservation. This paragraph reviews the contributions of key European scientists who have influenced environmental legislation, highlighting their research and its impact on environmental policy-making.

It should be noted at the outset that environmental legislation in Europe has developed in response to scientific discoveries and growing concerns about pollution, resource depletion and climate change. Scientific research has provided the basis for legislation aimed at reducing environmental damage and promoting sustainability. We seek to analyze the contributions of some notable European scientists whose work has shaped European environmental governance.

Among world pioneers in environmental science, we can name the following authors:

- *Vladimir Vernadsky* (1863-1945) Although of Russian origin, Vernadsky's concept of the biosphere had a lasting influence on European environmental thinking. His work laid the foundations for modern ecosystem studies and influenced sustainable development policies in Europe, notably through UNESCO's *Man and the Biosphere* program.

- *Arne Næss* (1912-2009). Norwegian philosopher and ecologist Arne Næss introduced the concept of deep ecology, advocating a holistic approach to environmental protection. His influence extended into European legal frameworks, particularly in the development of sustainability-oriented policies within the European Union (EU).

[8] Ghe. Iancu, Dreptuirile fundamentale și protecția mediului [Fundamental rights and environmental protection], Publishing House of the Independent Official Gazette of Romania, Bucharest, 1998, p. 267.

- *Svante Arrhenius* (1859-1927) made a scientific contribution to European environmental policies. Arrhenius, a Swedish scientist, was one of the first to quantify the greenhouse effect, laying the foundations for climate change legislation. His research provided the scientific basis for EU policies to combat climate change, such as the 2005 EU Emissions Trading Scheme (ETS) and subsequent carbon reduction strategies.

- *Bert Bolin* (1925-2007.Swedish meteorologist, Bolin was one of the founders of the IPCC. His work on atmospheric carbon dioxide has played a crucial role in international climate policies, including those adopted by the EU to reduce emissions.

- *Tim Lenton* (b. 1973). Lenton, a British climatologist, has worked extensively on climate tipping points, warning of irreversible environmental change. His research has influenced EU policies on climate resilience and adaptation strategies.

- *Hans Joachim Schellnhuber* (b. 1950) German physicist and climatologist, Schellnhuber pioneered work on climate risk assessment and planetary boundaries. His research directly influenced EU policies, including the European Climate Change Act.

- *Syukuro Manabe* (b. 1931) Although born in Japan, Manabe's collaborations with European scientists have been instrumental in improving climate projections. His work has influenced EU adaptation policies and risk assessments for extreme weather events.

These scholars have made valuable contributions to the development and implementation of environmental law in Europe.[9]

At the same time several US authors have significantly influenced the field of law and science

1. *Rachel Carson*, Ph.D., USA - Often considered a pioneer, her seminal work *Silent Spring* (1962) catalyzed the modern environmental movement by highlighting the dangers of pesticides, especially DDT, and their environmental impacts. Carson's plea for science-based environmental policy continues to resonate today, marking her as a seminal figure in environmental law discourse According to the editors of Discover magazine in 2006, *Silent Spring* was named one of the 25 best science books of all time.

2. *Daniel Bodansky*, PhD, USA - A prominent scholar in the field of international environmental law, Bodansky's work[10] focuses on climate change and governance frameworks. His contributions to understanding the legal mechanisms underlying international agreements, such as the Paris Agreement, have been instrumental in shaping contemporary environmental policy.[11]

3. *Oliver Houck*, Ph.D., USA - Known for his compelling stories and legal expertise, Houck is the author of influential texts exploring the intersection between law and environmental activism. His case studies illustrate how ordinary citizens can harness legal frameworks to challenge environmentally harmful corporate practices.

[9] PRIEUR M., Droit de l'environnement, Dalloz, 1991.

[10] Lovelock, J. (1979). Gaia: A New Look at Life on Earth. Oxford University Press.

[11] Bodansky, Daniel. "The Legitimacy of International Governance: A Coming Challenge for International Environmental Law?" American Journal of International Law 93, no. 3 (1999): 596–624.

4. *Arden Rowell and Kenworthey Bilz* USA - Their collaborative paper, *The Psychology of Environmental Law*, examines how psychological principles can improve legal frameworks for pollution control and ecosystem management. This interdisciplinary approach has opened new avenues for integrating behavioral sciences into environmental law.

5**.** *Rob Fischman*, Ph.D., USA - As a leader in environmental law education, Fischman's research emphasizes the importance of scientific knowledge in developing effective environmental policies. His recent publications contribute to our understanding of the role of law in addressing contemporary environmental challenges.

At the same time, if we are to refer to the issue of ecological control, several scientists and researchers have written directly referring to the regulation and management of ecosystems to maintain stability, biodiversity and sustainability, including:

1) *Howard Odum* (1924-2002) was a pioneer in systems ecology, which examines energy flows and control mechanisms within ecosystems. His book *Environment, Power, and Society* (1971) examines how ecosystems regulate themselves and how human intervention can influence these processes. Odum's work is fundamental to our understanding of ecosystem self-regulation and ecological control mechanisms through feedback loops.

2) *Eugene Odum's* book *Fundamentals of Ecology* (1953), a leading ecologist, introduces ecological principles that deal with ecological control, stability and resilience. He emphasized the importance of homeostasis in ecosystems, in which natural processes regulate environmental conditions.

3) *C.S. Holling* (1930-2019) - Crawford Stanley (C.S.) Holling was a key figure in the field of ecological control through his resilience theory and adaptive management framework. Holling developed resilience theory, which explores how ecosystems absorb disturbances while maintaining their function. His adaptive management framework suggests that ecological control should be flexible, allowing for natural feedbacks from the system. His contributions focus on how ecosystems absorb disturbances while maintaining function, emphasizing the dynamic and non-linear nature of ecological control. The key contributions to ecological control are in his paper *Resilience and Stability of Ecological Systems* (1973) Holling distinguished between engineering stability (returning to equilibrium) and ecological resilience (absorbing change while maintaining essential functions). This idea transformed ecological control from a rigid, equilibrium-oriented perspective to a more flexible, adaptive one. Holling argued that ecosystems should be managed using feedback loops, adjusting policies based on real-time ecological responses rather than fixed rules. This approach recognizes uncertainty and change as inherent to ecological control. In his paper *Panarchy Theory* -Dl Holling explains how ecological and social systems interact at different scales, showing how disturbances in one part of the system, can lead to transformations in others. He also suggests multiple control mechanisms at different levels, rather than a single, top-down approach.

Mr. Holling's impact on ecological control is that he shifted the view of ecosystems from static equilibrium to adaptive cycles that include growth, collapse and reorganization. He inspired modern ecosystem-based management and climate change adaptation strategies.

4) *Paul R. Ehrlich* (b. 1932) - In *The Population Bomb* (1968), Ehrlich addresses the impact of human population growth on ecological control and resource management. His later work emphasizes biodiversity conservation as a method of ecological control.

5) *Fritjof Capra* (b. 1939) is a physicist and systems thinker who applies systems theory to ecological control, emphasizing interconnectedness and self-regulating processes. His work integrates biology, cybernetics and complexity science to explain ecological balance. Key contributions to ecological control are outlined in the key paper *The Web of Life* (1996), where Capra describes nature as a self-organizing system in which ecological control results from interdependent relationships rather than centralized regulation. In contrast to traditional models of ecological control, that rely on linear cause-effect relationships, Capra emphasizes the networked feedback loops that stabilize ecosystems. Example: A forest ecosystem is self-controlled through nutrient cycling, predator-borer dynamics, and climatic interactions. Capra argues that human interventions should align with natural control mechanisms, rather than impose mechanistic, top-down controls that disrupt self-regulating systems. Capra's book *The Web of Life* (1996) explains how ecological control is maintained through interconnected natural systems. He applies systems theory to ecosystems, showing how different environmental factors regulate and control each other.

6) *Elinor Ostrom* (1933-2012) - Ostrom's economic and political approach to ecological control is presented in *Governing the Commons* (1990). The author analyzes how local communities effectively manage ecosystems without top-down regulation.

7) *James Lovelock* (1919-2022) - Lovelock's *Gaia Hypothesis* (1979) suggests that the Earth functions as a self-regulating system in which ecological control occurs naturally. His work has influenced climate change policies and ecological management strategies.[12]

These authors represent only a fraction of those shaping the dialog around ecological control, reflecting a diverse range of methodologies and theoretical frameworks that continue to evolve in response to global environmental problems. [13]

Eventually, the main topics covered in the literature on ecological control were:

- Self-control: How ecosystems maintain equilibrium through natural feedback loops (e.g. predator-prey relationships).
- Resilience: How ecosystems adapt to disturbances by maintaining their function (Holling).
- Sustainability: Managing human impacts to allow ecological processes to continue (Ostrom, Ehrlich).
- Ecological engineering: Designing human interventions to work with nature rather than against it (Odum).

It is imperative to mention, that, a particular role in European legislation has been played by scientific institutions such as:

- Intergovernmental Panel on Climate Change (IPCC) Although global in scope, the IPCC reports have had a major impact on EU legislation, in particular the European Green Deal and climate change mitigation policies. European scientists, including Bert Bolin and Jean Jouzel, have played important

[12] Lovelock, J. (1979). Gaia: A New Look at Life on Earth. Oxford University Press.

[13] Schellnhuber, H. J. (1999). 'Earth System' Analysis and the Second Copernican Revolution. Nature.

roles in the development of these reports. Established in 1994, the EEA has played a crucial role in translating scientific findings into policy recommendations. It monitors environmental trends, provides input for legislation and supports sustainability initiatives across the EU.

- The Joint Research Center (JRC) JRC, the EU's science service, carries out research that underpins environmental regulation, such as air quality standards, climate change adaptation measures and waste management policies.

- Potsdam Institute for Climate Impact Research (PIK) Based in Germany, PIK is one of Europe's leading climate research institutes. It has provided scientific assessments that influence EU policy decisions on emission targets and climate change adaptation.

- Tyndall Center for Climate Change Research Based in the UK, the Tyndall Center has been instrumental in providing research on climate change mitigation, renewable energy transitions and adaptation strategies, that have influenced European climate policies.

At the same time, we would like to mention that the most effective pollution prevention measures adopted by countries with advanced environmental legislation include a range of strategies and regulations aimed at protecting the environment and reducing the impact of economic activities on it. Among them are the following:

1. Promoting clean energy: Switching from fossil fuels to renewable energy sources such as solar, wind and hydropower is key to reducing greenhouse gas emissions and air pollution.

2. Stringent emission regulations: Implementing stringent standards for industrial emissions and motor vehicles contributes to reducing air pollution. Advanced countries encourage the use of electric and low-emission vehicles.

3. Waste management: Separate collection, recycling and composting are important measures to reduce the amount of waste going to landfill. Pilot projects for organic waste management have demonstrated their effectiveness in this respect.

4. Biodiversity protection legislation: Measures aimed at conserving ecosystems and protecting endangered species help maintain a healthy environment by reducing the impact of pollution on biodiversity.

5. Environmental education: Public awareness campaigns and environmental education are essential to change citizens' behavior and promote sustainable practices.

6. Precautionary Principle: This principle requires that actions that may harm the environment should be avoided until sufficient evidence of their safety is obtained, which helps to prevent pollution before it becomes a problem.[14]

[14] LARSSON Marie-Louise, The law of environmental damage – Liability and reparation, Kluwer International, 1999

IV. CONCLUSIONS

Scientific research has played a key role in the development of global environmental legislation.[15] Pioneers in environmental science have provided essential data and frameworks for policy makers. The contributions of scientists, have laid the foundations for policies on climate change, air and water pollution and biodiversity loss. As environmental challenges evolve, continued collaboration between scientists and legislators remains essential for effective environmental governance. Environmental protection has, for several decades now, been both the subject of extensive environmental control regulations and a frequent topic of scientific research. The increase in environmental problems and the continuous degradation of environmental factors have aroused the interest of specialists, especially with regard to the quality of environmental legislation and the effectiveness of its implementation. These measures, implemented in a coherent and integrated way, can lead to a significant reduction in pollution and a healthier environment for future generations. Therefore, in generalizing the above, we would like to emphasize once again the valuable contribution of all the listed researchers to the development of the issue of environmental control. Their achievements represent a significant value and theoretical-scientific benchmarks for the improvement of environmental legislation of the Republic of Moldova.

[15] DANDACHI Amira, La Convention sur la protection de l´environnement par le droit pénal, RJE, no. 3, 2003.

THE PREVENTION OF SECONDARY VICTIMIZATION

Implementation of Mendez principles

Aura Marcela Preda

AUTHOR

Dr. Aura Marcela Preda is teaching Criminology and Criminal Executional Law at a private university, "Spiru Haret" University (Faculty of Law, Bucharest) since 1999, and she is senior researcher at the Legal Research Institute of Romanian Academy, since 2006. She is a member at The International Association of French-Speaking Criminologists, member at European Society of Criminology - Victimology working group, also was member of MC for Romania at Cost Action CA 18121-Cultures of Victimology:understanding processes of victimization across Europe (2019-2023), Cost Action CA 22106 - Migrant Disaster Victim Identification (MDVI) (2023-) and Cost Action CA 22128 Establishing Networks to Implement the Principles on Effective Interviewing for Investigations (IMPLEMENDEZ), (2024-) In Romania, she is a vice-president of the Romanian Society of Criminology and Forensic, also the president of the Romanian Society of Victimology (created in 2022). She has worked in the field of domestic violence (national survey, 2006-2008) and during the last decade, her research has focused on gender-based violence, human trafficking, the crime/victimization `s prevention, secondary victimization, difficulties in probation services, the rights of convicted persons.

TABLE OF CONTENTS

I. INTRODUCTION

Sometimes the victims experience a double victimization: one from the aggressor (primary victimization), the second one comes from the representatives of public authorities with whom they come into contact (secondary victimization). Various ways of preventing both forms of victimization have been proposed, but I will insist on one of them that refers to the prevention of secondary victimization by implementing the Mendez`s principles.

The six Mendez`s principles will be applied by professionals involved in interviewing to suspect/perpetrator, witnesses and victims, adults or children, in order to assure the efficacity and accuracy of the information gathering.

So, this article tryes to show wich ares the benefits of a properly implementation of Mendez principles for provide the efficient interviews.

II. THE CONCEPTUAL DELIMITATIONS

The father of this concept is considered to be Symonds M., but he speaks about t*he "second injury"* to victims of violent acts .His approach involves:

(1) self-hate and shame as the key in posttraumatic distress;
(2) the *ordinary professional attitudes* of those who are supposed to help often intensify the traumatized person's self-hate and shame, wich is called *"second injury"*;
(3) to counteract the self-hate and the shame, *the professional* must adopt a much more active attitude and behavior.[1]

Secondary victimization (also known as post crime victimization or double victimization) refers to further victim-blaming by criminal justice authorities following a report of an original victimization.
Different other definitions used in literature[2] are the following:

- victims' post-crime experiences with institutions such as medical staff, justice and the law enforcement systems, or their employers
- additional trauma experienced by rape victims due to victim blaming or otherwise insensitive responses within the criminal justice system
- problems at all stages of the victims` interaction with the representatives of criminal justice system.
- victims are injured once by the crime and then a second time by criminal justice authorities.

As we can notice, all these behaviors refer to insensitive, victim-blaming treatment, and negative victim experiences at various stages of the legal process that often result in greater feelings of trauma. However, most of the available research on secondary victimization has focused on criminal justice authorities (police, prosecutors, judges).

[1] Martin Symonds, The "second injury" to victims of violent acts. 1980 (https://pubmed.ncbi.nlm.nih.gov/20212437/).
[2] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6994185/

For this reason the professionals termed secondary victimization as institutionalized victimization. Most apparently, it occurs within the criminal justice system and results from intrusive or inappropriate conduct investigation by police officers or other criminal justice professionals. Still, secondary victimization may be the byproduct of interaction with other entities: *school personnel* may disclosure abused child; doctors may not acknowledge signs of domestic abuse, etc. Even *organizations* such as victim services, victim compensation systems, refugee services and mental health institutions may implement policies and procedures that could lead to secondary victimization.[3]

Hence, through the improper attitudes/reactions faced by the victim from the criminal justice system, public authorities or *NGO`s*, *neighbours, media (*if they find themselves in the media spotlight, victims become a vulnerable target).

Sometimes, the police convince victims that without the assistance of a lawyer any effective action is not possible and inform them that their chances of finding the perpetrator are minimal, so they discourage them from reporting a crime.[4]

Others signs of secondary victimization could be:
- delays times for trials to begin – it takes too long to start a trial
- the lengthy duration of the process – unreasonable time during the trial
- poor/lack of communication
- the communication is misaligned with victims' needs
- demanding proofs for establishing their credibility
- victim-blaming
- disbelief of victim/survivor testimonies
- inadequate police investigations
- frequent 'no further action' outcomes, low charge, prosecution and conviction rates,
- requirements for sharing intimate personal details
- juridical language can be confusing and threatening

III. THE LEGAL FRAMEWORK ON THE SECONDERY VICTIMIZATION

A. International Regulations

One of the first documents regarding this topic containing such considerations and recommendation since 1985 is the UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power.

In recognition of this term, a lot of international protocols and standards call on states to ensure measures in order to protect complainers and avoid their re-traumatization. As an example, the UN General Assembly, through, the Declaration on the Elimination of Violence against Women from 20th December 1993, requires States based on *Art.4* to ensure that: "*…the re-victimization of women does not occur because of laws insensitive to gender considerations, enforcement practices or other interventions."*[5]

[3]https://victim-support.eu/wp-content/files_mf/1673427018NationalFrameworkforComprehensiveVictimSupportcompressed.pdf

[4] https://www.semanticscholar.org/paper/Empowering-the-Victims-of-Crime%3A-A-Real-Goal-of-the-KlausBuczkowski/bdb54f0020f79a5cc4d422a8e9631838782344be

[5] https://www.ohchr.org/en/instruments-mechanisms/instruments/declaration-elimination-violence-against-women

B. European Regulation

As regard the European legislation, we will reffer at some european directives and to the Instanbul Convention.

A lot of provizions on this matter are included in Recommendation of the Council of Europe concerning the position of the in the framework of criminal law and procedure.

As about some European directives in this regard, we will briefly analyze some of them relating with crime victims. For example, *Directive 2011/99/EU on the European Protection Order (EPO) in criminal matters.* (JO-L 338) The directive allows victims of violence, especially domestic violence and harassment, to continue to benefit from protection against perpetrators when they move to another EU country. In order to issue a European protection order, there must be a national protection measure in force in that EU country that imposes one or more of the following prohibitions or restrictions on the person who poses a danger[6] in order to avoid secondary victimization in other countries:

- prohibition to move to certain places or defined areas where the protected person resides or visits;
- a prohibition or regulation of contact, in any form, with the protected person, including by telephone, by electronic means or by regular mail, by fax or any other means;
- a prohibition or regulation of approaching the protected person at a distance smaller than that provided for.

Another directive refers to very vulnerable crime victims, such as victims of human trafficking, namely Directive 2011/36/EU of the European Parliament and of the Council of April 5, 2011, on preventing and combating human trafficking and protecting its victims, replacing Framework Decision 2002/629/JHA of the Council. The Directive establishes minimum rules on the definition of offences and criminal sanctions in the field of human trafficking.

The directive also introduces common provisions, taking into account the gender perspective, to ensure better ways to avoid secondary victimization and prevention of this category of crimes and better protection of their victims. The Directive mentions that human trafficking is a gender-differentiated phenomenon, with men and women often being trafficked for different purposes. For this reason, assistance and support measures should also be gender-differentiated where appropriate.

Triggers may differ depending on the sectors involved, such as human trafficking in the sex industry or labor exploitation, such as construction work, agriculture or domestic servitude. (JO-L 101)

The last European Directive concerning victims` rights is Directive 2012/ 29/EU of the European Parliament and the Council of October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA. Named the Victims' Rights Directive, this normative act provides in *Para.53-63* and *art. 5, 9, 19, 20, 22,23, 25 a lot of rules during the penal procedure interaction with different types of professionals in order to avoid secondary victimization or revictimization or retaliation.*[7]

Also, t*he Council of Europe Convention* on Preventing and Combating Violence Against Women (the Istanbul Convention) from November 2014, specifies that :

[6] https://eur-lex.europa.eu/RO/legal-content/summary/european-protection-order-supporting-crime

[7] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:115:0001:0011:EN:PDF

- *"all measures to provide protection and support to victims should be with the aim of preventing secondary victimization "* ,
- *" Parties shall ensure that measures taken pursuant to this chapter shall:..... – aim at avoiding secondary victimization"*; according with Chapter IV – Protection and support, Article 18 – General obligations par.3

The main causes[8] identified in this normative act are:

- repeated exposure of the victim to the perpetrator
- repeated interrogation about the same facts,
- the use of inappropriate language,
- unintentionally insensitive comments made by all those who come into contact with victims,
- insensitive media reporting of cases.
- social rejections and insensitivities to acknowledging trauma or violence

IV. PRINCIPLES OF MENDEZ

The Principles of Effective Interviewing for Investigations and Information Gathering, also known as the Mendez Principles, is a document developed by international experts that provides a concrete alternative to coercive interrogation methods (currently available in 11 languages)[9].

The document is built on six principles. These are:

- Effective interviewing is instructed by science, law and ethics.
- Effective interviewing is a comprehensive process for gathering accurate and reliable information while implementing associated legal safeguards.
- Effective interviewing requires identifying and addressing the needs of interviewees in situations of vulnerability.
- Effective interviewing is a professional undertaking that requires specific training.
- Effective interviewing requires transparent and accountable institutions.
- The implementation of effective interviewing requires robust national measures.

These principles are also called the Mendez Principles to honor the former UN Special Rapporteur on Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Juan E. Méndez.[10] The document grew from a thematic report submitted by Prof. Méndez to the United Nations (UN) General

[8] https://www.google.com/search?q=causes+of+secondary+victimization&oq=causes+of+secondary+victimization+&aqs=chrome..69i57j0i22i30l2.10073j0j7&sourceid=chrome&ie=UTF-8

[9] https://interviewingprinciples.com/#comp-179e548ce41

[10] Méndez, Juan E. (August 2016). "UN Docs A/71/298". undocs.org. Retrieved 2024-04-11 and https://en.wikipedia.org/wiki/Juan_E._M%C3%A9ndez

Assembly in 2016 calling for the development of international standards for interviews based on scientific research, legal safeguards and ethical principles.[11] The Mendez Principles represent the realization of that call.[12]

The Principles respond to the persistent challenge of torture and ill-treatment during investigations and intelligence gathering, including in situations of armed conflict or public emergency, despite an extensive international legal framework prohibiting such practices. They build on a vast scientific literature that establishes rapport-based, non-coercive interviewing techniques as the most effective means of gathering accurate and reliable information. They also draw on extensive literature underscoring the ineffectiveness and counter-productive property of torture and abuse.

The Mendez Principles seek to transform how authorities question detainees and conduct interviews across a range of straightforward and complex scenarios. They are applicable to all interviews conducted by authorities, including police, intelligence, military, immigration and customs officers, and related administrative bodies. They cover interviews with suspects, witnesses, victims, and other persons of interest.

The global consortium of experts who crafted the text came from various fields, including law enforcement, psychology, national security, military, intelligence gathering, human rights, and criminology. By operationalizing the presumption of innocence, the Principles contribute to more just, safe, and inclusive societies, aligning with the UN Sustainable Development Goals.

Formally, the document has six sections, each addressing one of the six principles for effective interviewing. Each section consists of advice, counsel, and practical steps to be taken.

Principle 1 – On Foundations

This initial Principle establishes the groundwork for effective interviewing practices with three critical pillars: scientific foundations, legal grounds, and widely accepted professional ethics. Together, these components provide the basis for ensuring that interviews are conducted in a manner that upholds all the central elements at stake.

Principle 2 – On Practice

The second Principle outlines a process for conducting interviews, prioritizing the collection of accurate and reliable information. It underscores the importance of legal safeguards, ensuring a non-coercive environment before the interview, establishing and maintaining rapport during the interview, and conducting assessment and analysis at the interview's conclusion.

[11] Ibidem

[12] Méndez, Juan E.; Drummond, Vanessa (2021-06-01). "The Méndez Principles: A New Standard for Effective Interviewing by Police and Others, While Respecting Human Rights". Just Security. Retrieved 2024-04-11 și Barela, Steven J.; Fallon, Mark (2021-06-01). "The Méndez Principles: Leadership to Transform Interrogation via Science, Law, and Ethics". Just Security, Retrieved 2024-04-11

Principle 3 – On Vulnerabilities

Recognizing the inherent power imbalance that all interviewees face, this Principle highlights the interview as a situation of vulnerability. It also provides guidance on addressing situations of heightened vulnerability and offers a framework for assessing and mitigating potential risks during interviews.

Principle 4 – On Training

Effective interviewing relies on well-trained professionals. It emphasizes the need to train interviewers and promote continuous professional development to ensure that interviewers are able conduct effective interviews.

Principle 5 – On Accountability

Accountability is a cornerstone of effective interviewing practice. This Principle outlines institutional procedures and review mechanisms, effective record-keeping, prevention and reporting of misconduct, external oversight and independent monitoring, as well as processes for handling complaints, conducting investigations, and providing redress and reparations when necessary.

Principle 6 – On Implementation

The final Principle focuses on application within domestic legal frameworks. It addresses institutional culture and capacity, the role of judicial authorities, and the dissemination of these Principles to ensure their widespread adoption and consistent application.

Effective interviewers adhere to the highest ethical standards, guided by professional regulations and codes of ethics that outline the purpose, values, and expected conduct.[13] These ethical principles govern all aspects of an official's duties, including interviews, in accordance with international legal obligations. Commitment to ethical interviewing prevails even in situations of intense pressure, such as limited time or demands for immediate results. Interviewers, exercising their authority while upholding the law, strive to achieve ethical outcomes that can withstand ethical, judicial, and public scrutiny.

Professional codes of ethics for law enforcement officials underscore the significance of respect, fairness, and honesty as the fundamental pillars of all interviews. Officials are also required to wield state authority in a lawful, fair, and responsible manner at all times. Any illicit action performed in an official capacity constitutes an abuse of power.

Interviewers bear an ethical duty to employ the most effective methods available that safeguard the rights and dignity of interviewees while preserving the integrity of the process. Likewise, they have an obligation to abstain from coercive tactics, as these methods not only inflict harm on interviewees but also compromise the goal of acquiring accurate information.

[13] UN General Assembly, Code of conduct for law enforcement officials, A/RES/34/169, (5 February 1980), also International Association of Chiefs of Police (IACP), Law Enforcement Code of Ethics, October 1957, also Southern African Regional Police Chiefs Co-operation Organisation (SARPCCO), Harare Resolution on the SARPCCO Code of Conduct for Police Officials, 31 August 2001 and Council of Europe, The European Code of Police Ethics, (19 September 2001)

V. CONCLUSIONS

Sumarising here are some correlations that looks obvious, between secondary victimization and the Mendez Principles:

1. Dignity and Respect:
   - Secondary victimization: Victims may experience disrespect or stigmatization when interacting with law enforcement or the legal system, exacerbating their trauma.
   - Mendez Principles: Emphasize the right to be treated with dignity and respect, regardless of legal status or accusation.
2. Fair Trial and Due Process:
   - Secondary victimization: Victims may face insensitivity or disbelief from authorities, affecting their ability to participate effectively in legal proceedings.
   - Mendez Principles: Advocate for fair trial rights, including the presumption of innocence, access to legal representation, and the right to challenge evidence.
3. Protection from Harm:
   - Secondary victimization: Victims may feel vulnerable or exposed to further harm when their privacy or safety is compromised during legal processes.
   - Mendez Principles: Stress the obligation of authorities to protect individuals in custody from any form of harm or abuse.
4. Access to Support Services:
   - Secondary victimization: Victims often lack adequate support services to address their emotional, psychological, and practical needs after victimization.
   - Mendez Principles: Highlight the importance of access to medical care, counseling, and other support services for individuals deprived of their liberty.
5. Non-Discrimination:
   - Secondary victimization: Victims from marginalized groups may face additional discrimination or bias during interactions with the criminal justice system.
   - Mendez Principles: Prohibit discrimination based on race, ethnicity, gender, religion, or any other status, ensuring equal treatment and protection for all individuals.

These correlations illustrate how the Mendez Principles align with efforts to mitigate secondary victimization and uphold the rights and dignity of all individuals, including victims of crime.

RECONCEPTUALIZING ENVIRONMENTAL LIABILITY

The Impact of the Preventive Action Principle

Grigore Ardelean and Luminita Diaconu

AUTHORS

Grigore Ardelean PhD in law, is an associate professor at "Stefan Cel Mare" Academy of The Ministry of Internal Affairs (Republic of Moldova). Lecturing at The Department of Private Law, author of textbooks and articles, mainly specialized in public and private law.

Luminita Diaconu PhD student has been a university lecturer since 1996 with experience in lecturing at many universities from The Republic of Moldova. She has MA in American Studies. (2002) From 2008 Mrs Diaconu has been teaching at the Academy of Economic Studies of Moldova and is a doctoral student at the "Stefan cel Mare" Academy of MIA (Republic of Moldova) She is doing her research in Public Law writing her thesis on Ecological Control.

ABSTRACT

The foundation of any regulatory framework is predicated on a set of guiding principles that serve as the cornerstone for the legislator in establishing the overarching vision and rationale that governs societal governance. Beyond these general principles, there exists a necessity for principles that are specific to each respective domain, thereby ensuring a nuanced and comprehensive regulatory framework.

In the context of environmental concerns, the unique characteristics of environmental harm and the intricate nature of determining liability have given rise to a compelling need for the introduction of novel principles that underpin the concept of preventive liability. This paradigm shift has the potential to significantly transform the prevailing understanding of environmental liability. Furthermore, while certain existing environmental protection mechanisms are modelled on European legislation, they lack a legally established principle as their foundation. This paper thus

aims to provide a first doctrinal approach to the need for a legal enshrinement of the principle of preventive action of environmental liability.

***Keywords**: environment, principles, legal rules, prevention, preventive liability, damage, protection mechanisms, environmental liability*

TABLE OF CONTENTS

I. INTRODUCTION

As with any type of regulation, the institution of environmental liability requires the establishment of principles in the form of guidelines, guiding ideas, with the aim of consolidating legal mechanisms that are as effective as possible and capable of ensuring maximum effectiveness in resolving problems concerning the applicability of this particular category of liability. In addition to these observations, it is imperative to acknowledge that the specific nature of environmental damage is exhibiting novel trends in its manifestations and means of propagation. Moreover, it is almost impossible to make reparation in kind. Consequently, the emphasis must be placed on action to prevent damage, including the acts that cause damage, and, as a result, on liability, which is difficult to enforce in environmental matters. However, the principles that underpin reparatory liability are not very effective in the process of regulating environmental liability, since reparation is difficult and sometimes impossible. The environmental liability regime is therefore to be reshaped by getting rid of the current traditionalism and resorting to anticipatory measures – a kind of 'pre-liability', applicable even before damage occurs.

The methods and materials applied in the study process belong to the most diverse category, being used the most effective methods in the field of legal research, among which we list: the method of analysis, the method of synthesis, the method of deduction, the systemic method, the historical method, the comparative method, as well as the empirical method.

II. RESULTS AND DISCUSSIONS.

The ensuing discourse is predicated on the findings and deliberations that have been meticulously obtained. In order to achieve the pre-determined objective, it is imperative to commence from the premise that the principle of preventive action of environmental liability should be accorded the highest priority within the framework of future regulations. This principle should serve as the foundational basis for the establishment of other principles and a novel concept of regulation for this distinct form of liability. The 'polluter pays' principle, which underlies the law on payment for pollution, is instrumental in this regard. It facilitates the possibility of providing compensation in advance through taxes, thereby fulfilling a preventive function of liability for future damage. Furthermore, the precautionary principle also reinforces the principle of preventive action of liability. Article 6 of the Water Law explicitly states that in instances where there is a risk of significant or irreversible harm to water resources, the absence of complete scientific certainty cannot be employed as a justification for the avoidance of necessary measures. Therefore, we note that this principle also requires anticipatory action, even if it is not known with certainty that some activities are causing harm or if they are generating harm, the extent and nature of the harm is not known, and the failure to take these measures should constitute grounds for liability and not their effect, i.e. the harm.[1]

Moreover, the state's obligation to guarantee the right to a healthy environment necessarily implies the establishment of new categories of obligations, the breach of which should constitute grounds for environmental liability. In this sense, our idea finds support in the Romanian doctrine, according to which, failure to comply with the obligations established for the protection of the environment must constitute a fact that gives rise to liability for failure to comply with the constitutional and legal duty to protect and improve the environment.[2]

[1] Directiva 2004/35/CE a Parlamentului European și a Consiliului din 21 aprilie 2004 privind răspunderea pentru mediu în legătură cu prevenirea și repararea daunelor aduse mediului [European Directive].

[2] Duțu, M. (2014). Un nou model de responsabilitate: răspunderea pentru viitor. Perspectiva de mediu. Pandectele române, 8, 24.

It is inevitable that such an approach will lead to a paradigm shift in environmental liability from traditional liability to preventive liability. In the given context, liability for environmental damage should fulfil a preventive function, as is also the case in some instances of the application of classical liability. However, according to some opinions identified in the specialist literature, the classic preventive function of liability must also be specifically manifested in the field of environmental protection, in particular through the role played by the civil court. To illustrate this point, it can be noted that the utilization of ordinary-law procedural mechanisms enables the judicial authority to mandate the cessation of any unlawful act of pollution, thereby ensuring that the deleterious situation does not persist or materialize. Nevertheless, as asserted by the French doctrine, in such instances, the judge is effectively implementing the very essence of the principle of prevention. However, it is imperative to recognize that the relative nature of the judgment constitutes the primary constraint on the preventive role of the law of civil liability in environmental matters.

In a different order of ideas, the legal nature of the damage for salvage has no legal support in the absence of the enshrinement of the principle of preventive action in environmental liability. Compensation for environmental damage is essentially the cost incurred by an individual in connection with measures to prevent possible environmental damage (e.g. the construction of a protective wall, a canal around a private residence, etc.), which is imminent and unavoidable and which may in the future result from industrial activities. The following article will set out details of this new type of damage in an attempt to demonstrate its connection with the principle of preventive action in environmental liability.

It is acknowledged that this approach may be subject to initial criticism; however, it presents a number of advantageous prospects in the current era of guarantees, with the objective of condemning any reprehensible conduct in favor of the environmental well-being of future generations. To this end, the principles underpinning both classical civil liability and environmental liability are to be integrated into a single system of principles which, through their interaction and mutual support, will underpin the legal regime of the principle of preventive action as a specific principle of environmental liability, applicable to both ascertained and possible environmental damage[3].

Consequently, on the basis of this principle, in the case of potentially polluting acts, regardless of whether or not they have caused damage, environmental liability may be invoked, especially that which anticipates damage or liability for damage not yet ascertained.

As previously mentioned, contemporary environmental doctrine is engaged in a discourse surrounding numerous mechanisms for holding the polluter accountable, underpinned by the principle of preventive action. However, this principle has not been explicitly codified in legislation. Positive liability, which does not encompass damages, is also founded on the principle of prevention, if not of the damage, then at least of the inability to identify the perpetrator. Strict liability is predicated on the notion of the risk of the impossibility of identifying the person responsible for the restoration of the environment and guaranteeing the performance of the obligation to repair. Some economic and financial instruments for environmental protection are also based on the principle of preventive action, such as the idea of compulsory environmental liability insurance and the impunity of setting up private funds on behalf of polluters.

[3] Duțu, M. (1993). Dreptul mediului. București: Gamian.

It is evident from an observational standpoint that while environmental legislation does not explicitly support the notion of preventive action of environmental liability through other general principles, environmental protection mechanisms, or new categories of damage (rescue damage, loss of opportunity), it does not legally enshrine this principle in the text of the framework law (Law No. 1515/1993). Consequently, the legislator lacks a legally substantiated point of reference when formulating rules of a preventive nature or even those referring to uncertain risks of damage, which are indispensable for environmental protection. In the following section, an analysis will be conducted on the essence of the principle of prevention of environmental damage in contrast to the principle of preventive action of environmental liability, with a view to demonstrating the correlation and difference between them. The correlation of the principle of preventive action of environmental liability with the precautionary principle, as well as with other institutions of environmental law, such as the principle of anticipatory economic-financial instruments of environmental protection and the mechanism of compensation for new types of damage, will also be demonstrated.

Confluence of the preventive action principle of environmental liability with other principles of environmental law (prevention principle, precautionary principle, conservation principle). The precautionary principle in relation to the preventive action principle of environmental liability.

Although at first glance the principle of prevention of environmental damage would seem to express meanings in common with the principle of preventive action of environmental liability, although they also share common features, they should be viewed from different perspectives. What they have in common is that the prevention of damage has the direct effect of avoiding environmental liability, since there is no damage - a prerequisite for triggering liability to pay compensation. However, it should be borne in mind that, in environmental matters, liability may also be imposed in the absence of damage, i.e. for an act that has not yet caused damage, or where the damage is not yet detectable or the causal link between the act and the damage is difficult to quantify and prove. In other words, the principle of prevention of damage is a general principle which obliges the necessary actions to prevent damage, and is transposed into the rules concerning the environmental friendliness of production processes, the assessment of the risk and negative impact of certain activities on the environment, the planning and public consultation of any activities or projects, etc.).

Conversely, the principle of preventive liability aims to forestall liability for potential environmental damage, thereby enabling its application prior to the occurrence of certain consequences on the environment (e.g. the imposition of pollution taxes on the import of plastic materials before they are placed on the market or become waste; compensation for damage suffered by private individuals when bearing the costs of self-protection; the establishment of guarantee funds on behalf of polluters, the application in advance of economic and financial instruments for environmental protection, the application of guarantee fees for the return of packaging, etc.). The principle of preventive action of liability is, therefore, directly aimed at anticipating environmental liability, being a special principle applicable in the process of accountability in the action of each individual imposed and directed towards ensuring environmental protection.
In the context of the legislative situation pertaining to the principle of prevention, it is observed that the relevant legislation (Article 3, paragraph c) of Law no. 1515/1993)[4] makes only cursory and ambiguous reference to the principle, and It is stated in the context of the responsibility of all natural and legal persons for damage caused to the environment; prevention, limitation, combating pollution, as well as recovery of damage caused to the environment and its components on behalf of natural and legal persons who have admitted (even unconsciously or negligently) the damage.

[4] Duțu, M. (2010). Dreptul mediului (ediția a III-a). București: C.H. BECK.

Within this paradigm, it is imperative to delineate and differentiate the import of both principles across disparate texts, notwithstanding the feasibility of their integration within a singular norm, as exemplified by the following: Every individual has a duty to avert environmental degradation and to assume the consequences of liability, even in circumstances where the damage has not yet materialized or cannot be ascertained due to its unique propagation and quantification.

III. THE PRECAUTIONARY PRINCIPLE AND THE PRINCIPLE OF PREVENTIVE ACTION OF ENVIRONMENTAL LIABILITY.

As previously stated, the law may require the implementation of additional measures by an individual whose activities may have a negative impact on the environment, in accordance with the precautionary principle. These measures are intended to prevent damage, even in the absence of sufficient scientific data regarding the potential nature of future damage or its detectability. The same principle may also be invoked to mandate the implementation of environmental protection measures by the potential polluter, at their own expense, with the aim of encouraging more cautious behavior with regard to the environmental components of their activities. In this manner, the legislator may establish liability for failure to comply with all precautionary conditions, even in the absence of any identified damage. In other words, a party cannot rely on the absence of damage to claim exemption from liability, particularly when it has failed to implement all the prescribed measures designed to protect the environment. This principle thus establishes a legal foundation that enables the anticipation of environmental liability, thereby preventing the circumvention of responsibility or uncertainties that could otherwise compromise the process of accountability under the conventional framework of liability.

Thus, originally established to warn and impose the need to consider prudence when making decisions with a negative impact on the environment, the precautionary principle has asserted itself throughout its existence, albeit a relatively short one, by shaping and founding new concepts in the field of environmental responsibility. However, as it is also argued, the debates so far have failed to establish an exact and unique meaning of the principle, which can be interpreted either as an attitude of reasonable prudence, which does not necessarily imply the search for liability, or as a new basis for liability in an uncertain universe.[5]

As mentioned in other papers[6], the precautionary principle is often confused with the principle of prevention, although the latter becomes applicable to certain risks, while the precautionary principle is intended to require measures to be taken from the moment of detection of uncertain risks of occurrence, but which by their potentiality and irreversibility may generate certain more specific damage in the ascertainment, assessment and repair because of the lack of knowledge even in the scientific field. The precautionary principle, which originated in Western law and is situated between the principle of prevention and the principle of compensation for damage, is a fairly favorable alternative for those who carry out economic activities with an impact on the environment, who would prefer to bear certain costs in exchange for ceasing these activities, which would make it possible to manage the lesser-known risk of damage or even to promptly repair the damage to the environment with potential repercussions for the individual.

[5] Duțu, M., & Duțu, A. (2015). Răspunderea în dreptul mediului. București: Editura Academiei Române.

[6] Diaconu, L. Environmental control and fiscal policy. Theory and Applied Fiscal Policy (p. 86). Ed.Peter Lang Group.

In certain countries, the legislative basis for the principle of preventive action of liability is established through the provisions of civil law. For instance, in the legislation of the Russian Federation, the principle of prevention of future damage, as outlined in paragraph 1 of Article 1065 of the Civil Code of the Russian Federation, stipulates that the potential for future harm may serve as a foundation for initiating legal action aimed at prohibiting activities that pose such a risk. In such circumstances, as outlined in Russian doctrine, the application of preventive sanctions is permissible in instances where there is a potential for future harm, which is not associated with any tortious obligation.[7] Furthermore, Article 2000 of the Civil Code of the Republic of Moldova stipulates that the threat of future damage constitutes sufficient grounds for the prohibition of acts that may engender such a threat.

Thus, the precautionary principle, being exclusively intended to make environmental protection measures more effective, has gradually been adapted and applied in order to strengthen the legal framework necessary for the process of preventing future risks, uncertain but plausible potentiality, and more recently, the doctrine is trying to base on this principle, the regime of liability applied in anticipation for the damage to be caused in the future.

However, as also stated[8], the precautionary principle is one of anticipation, the damage has not occurred and the possibility of its occurrence is not indisputably proven, nor is it demonstrable. Now a legal reality, although still contested by some, the precautionary principle is an expression of liability based on uncertainty, a liability without object, but which has paradoxically become established not only in doctrine but also in positive law. This principle covers, in fact, any attitude adopted with a view to initiating or permitting an activity which gives rise to a reasonable assumption that it may pose a danger to the environment or human health. Therefore, the conduct of public authorities which have authorized an activity with a negative impact without taking account of the possible risks, or of the person who benefits from such an authorization but fails to take adequate measures to prevent harm, is an element of that liability.

In conclusion, the codification of the principle of preventive action of environmental liability in the text of the law, in addition to the demonstrated effectiveness in preventing damage by imposing specific preventive measures from the moment the risk is recognized, would also have certain advantages in terms of assessing and proving the causal link between the act and the possible damage.

Firstly, the issue of assessing harm is rendered moot by the recognition that quantification is of no practical use, given that the objective is not to compensate a victim, but to regulate or prohibit an activity or action that poses a risk, the occurrence of which could potentially inflict incalculable damage.[9]
Secondly, the direction of the process and the burden of proof will be reversed, as is rightly considered. At present, the person who estimates that they have suffered damage is responsible for proving that there are no future risks arising from their activity which could be legally pursued. In the event that the action is upheld, the reverse will be true.[10]

[7] Țeruș, I. (2024). Instrumente juridico-financiare de protecție a mediului în cadrul activității economice [Doctoral thesis]. Chișinău.
[8] Nicolau, I. (2010). Aspecte privind responsabilitatea pentru daune ecologice în legislația franceză. Legea şi viaţa, 11, 39.
[9] Mîrzac (Mititelu), D. (2010). Principiul precauției. Legea şi viaţa, 2, 27-33.
[10] Brun, P. (2005). Responsabilité civile extracontractuelle. Paris: Litec.

IV. THE PRINCIPLE OF NATURE CONSERVATION AND THE PRINCIPLE OF PREVENTIVE ACTION OF ENVIRONMENTAL LIABILITY.

One of the objectives of environmental protection is to preserve the components of the environment for future generations. This implies the need to preserve their quantity and quality by acting before they are destroyed, taking into account the irreversibility of many of them. In order to support the realization and enhancement of the conservation principle, the principle of preventive action of empowerment must also be implemented, in the context of the fact that the doctrine today confidently argues that preference should be given in environmental policies to preventive and active rather than corrective and reactive strategies.[11]

The compatibility of the principle of preventive action of environmental liability with the legal essence of certain categories of environmental damage (salvage damage, development damage, loss of opportunity) is also examined. The concept of preventive environmental liability entails the mitigation of damage in order to avert the potential for ecological degradation.

Essentially, salvage damages represent the financial obligations undertaken by an individual or entity to avert and eliminate the threat of potential environmental harm. It is important to note that the legislator has included the rule that expressly provides for liability for preventive expenses in the Civil Code during its modernization (art. 2027 CC). *This rule stipulates that an individual who has reasonably incurred expenses or other damage with the aim of preventing imminent harm or limiting the size or severity of the damage suffered is entitled to reimbursement from the person who would have been liable if the damage had occurred*.

This rule thus implements the principle of preventive action liability, a liability which applies in advance once it becomes necessary to incur costs in connection with the prevention of damage, constituting a preventive liability, with possible application also to liability for damage where it could not have been avoided by preventive measures.

Indeed, the actions taken by an individual who is aware of the imminent threat to their own interests often necessitate the assumption of financial responsibility by the party who, through their actions, has engendered a risk of pollution, thereby incurring financial losses. Conversely, if an individual engages in an activity that has an impact on the environment and thereby creates a risk for others, they become obligated to implement measures to contain and prevent potential damage to the environment. In the event that the obligated party fails to implement the requisite measures, the aggrieved party is nevertheless entitled to undertake preventive measures, at their own expense, in lieu of the obligated party.[12]

Among other things, the principle of preventive action in environmental liability makes it possible to widen the circle of liable parties. We are referring to the fact that the injured party could also bring an administrative action against the environmental authority which, despite having been informed by the owner of the polluting source of the imminent threat of damage, has not taken the measures required by law in this respect and is therefore guilty of accepting that environmental damage has occurred. Moreover, pursuant to Article 25 para. 1 of the Romanian O.U.G. No. 68/2007, the person affected or likely to be affected by an environmental damage may apply to the competent administrative conten-

[11] Glingan, O. Pierderea unei şanse prin prisma condiţiilor răspunderii civile. Retrieved from https://dreptmd.wordpress.com

[12] Diaconu, M., & Diaconu, L. (2024). Environmental control and the fiscal performance policy. Revista națională de drept, 1, 76.

tious court to challenge, from a procedural or substantive point of view, the acts, decisions or omissions of the competent authorities. In this way, the injured party could request that the competent authority responsible for authorizing the damage be designated as the person responsible for remedying the damage, and that this authority could subsequently claim from the economic operator, by way of recourse, payment of the costs resulting from the remedial action taken by the competent authority.

Future damage - a category of damage giving rise to the right to environmental liability in a prior context. The need to intervene at the stage when it is necessary to prevent the full extent of the damage, makes it necessary to consider an incipient damage, not yet detectable, as a future damage, which gives rise to the right to take legal action, either to stop the damaging activity, to limit the incipient damage or to compensate for the expenses necessary to prevent future damage.

In order to do so, it is necessary to analyze in detail the essence of future damage, which is a special category of damage consisting in the future effect of the environmental damage caused by acts of pollution. As we have already pointed out when writing other works, for a long time the doctrine, but also the case law, in order to be considered and to be entitled to compensation, has for this category of damage, for a long time, imposed the certainty of future occurrence as a condition.

However, now that the precautionary principle has been enshrined at European level in environmental matters, the doctrine is redirecting its research towards considering and compensating for future damage, even in the presence of uncertainties as to its future occurrence and assessment. In this respect, the emergence of a new type of environmental damage, specific in terms of its future effects, known as "development damage"[13], is becoming increasingly urgent.

Loss of opportunity - a model of damage involving a preventive action of liability. Although its true meaning has not yet been discovered, the loss of an opportunity, as a negative effect of the damage, implies the loss of an advantage from which the person could benefit in the future. Now, in French doctrine, through the analysis of the decisions of the Court of Cassation, the loss of opportunity is considered as an element of the damage to be compensated whenever the disappearance of the possibility of favorable events is established, even if the realization of the opportunity is never certain.

Thus, we undoubtedly consider that, in addition to the damage to environmental factors caused by destruction, contamination or pollution, the adverse effect of such damage is, of course, also aimed at depriving the person of the opportunity to enjoy a healthy and ecologically balanced environment. Yes, today there are still sceptics about this category of damage, noting that the possible benefit is not considered certain, but in the context of the modernization of the Moldovan Civil Code, the legislator has expressly enshrined this new category of damage in para. 4 of Article 19, taking into account the certainty of the chance and not the possible benefit. Now, according to the rule, the loss of chance is compensable only if it consists in the actual and certain disappearance of a favorable eventuality. The extent of this loss corresponds to the chance lost and cannot be equal to the advantage that would have resulted from the chance if it had materialized.

Thus, according to some authors, approaching the issue of loss of chance from the perspective of civil law, it is considered that the loss of a chance has legal relevance only when it occurs as a result of culpable conduct of another person, which interferes with the normal course of events and thus leads

[13] Boutonenet, M. (2008). Le contract et le droit de l'environnement. Revue trimestrielle de droit civil, 1, 79.

to the disappearance of the possibility of a favorable event expected by the victim, materialized either in a gain or in the avoidance of a loss. Moreover, the consideration of such a sui generis injury is also a benefit for the victims, who may thus benefit from compensation for part of the loss suffered. The authors [14] are of the same opinion, arguing that the acceptance and promotion of this theory of environmental damage liability would benefit in particular the victim of an environmental personal injury caused, for example, by inhaling or ingesting a toxic substance produced by industrial plants, such as asbestos or dioxin. In such cases, the term "loss of a chance of recovery or survival" will no longer be "loss of a chance of not falling ill".

V. DEVELOPMENT DAMAGE SUPPORTED BY THE PREVENTIVE ACTION PRINCIPLE OF ENVIRONMENTAL LIABILITY.

As we find in the specialized literature, development damage appears as an application of the precautionary principle, and according to us also of the principle of preventive action, which responds to the obligation of security subsequent to objective liability and justifies risk-based civil liability. The damage in question is as yet undecidable, but can be assessed by the courts from the angle of contract law and tort liability. Similarly, it is considered that the liability of the system should be borne by those whose activity generates the risks. Anyone who participates in the creation of a risk must bear the consequences. Therefore, even if at the time of carrying out activities with an impact on the environment no environmental damage is detected, the person who benefits from these activities will be liable to pay compensation for the risk to which subjects who do not carry out such activities are exposed (strict liability), but in certain circumstances not attributable to them bear the subsequent consequences (damage) of any damage to the environment.[15]

The Romanian authors rightly argue that such jurisprudence could pave the way for the promotion of liability for endangering another person by creating a new, managed risk, which some present as a newly created fact [8, p. 443]. In this respect, it is also considered that, in order to give rise to a right to compensation, it is sufficient that the damage is substantially caused by these acts, since the person who carries out a certain activity must assume the risks, and all the more so if the activity carried out is a source of profit for him. Profit and risk must be combined in the same patrimony.[16]

Nevertheless, we believe that the application of environmental liability for development damage cannot take place without the legal enshrinement of the principle of preventive action of environmental liability, which would explain the idea of legal action in the circumstances of the identification of obstacles to development caused by certain activities that, in principle, have not yet caused quantifiable patrimonial damage.

VI. INFLUENCE OF THE PRINCIPLE OF PREVENTIVE ACTION OF ENVIRONMENTAL LIABILITY WITH SOME ANTICIPATORY ECONOMIC-FINANCIAL MECHANISMS OF ENVIRONMENTAL PROTECTION.

Today it has become known that the most effective instrument of environmental protection is prevention, given that, by their nature, environmental components, once they have been destroyed, cannot be restored to their original state before degradation. The same idea also underlies the approaches to legal and financial instruments for environmental protection applicable to economic operators in the

[14] Suhanov, E.A. (2010). Drept civil. Volumul IV. Moscova: Wolters Kluwer.

[15] Ardelean, G. (2018). Repararea prejudiciului ecologic. Ed. Globe Edit.

[16] Ţarcă, Ş., & Velișcu, V. (2013). Prejudiciul ecologic provocat de impactul globalizării. Pro Patria Lex, 11(1), 39-46.

production, processing and marketing of products and the provision of services of any kind with a potentially negative impact on the environment. As stated in the specialized local doctrine, according to the principles underlying the legal mechanism of environmental protection, the perpetrator of an imminent threat of environmental damage is to be held liable, even if the damage has not occurred or cannot be ascertained precisely, and this form of liability finds its reason, argument and fairness only in the form of financial liability [17] In the opinion of the same author, expressed in the content of other works, the principle of realization of environmental protection measures by enterprises on the basis of their own resources or credits is the basis of the regulation of the obligation of economic agents to bear the costs of damage prevention. So, we are here taking up the idea that we are also promoting, i.e. the idea of anticipatory liability of economic operators in pecuniary form on the principle of preventive action of environmental liability.[18]

The author bases his position on point 2 of EU Directive 2004/35/EC, which introduces the idea of a fundamental principle of environmental damage prevention, according to which the operator whose activity has caused environmental damage or an imminent threat of such damage should be held financially liable, in order to encourage operators to adopt measures and develop practices aimed at mitigating the risks of environmental damage, so as to reduce exposure to the associated financial risks.

Thus, taking into account the new approaches of the European Union's legal framework in the field of prevention of environmental damage by anticipating its effects and, consequently, financial measures for environmental protection, we believe that the economic-financial instruments in the category of those applied in advance to make the economic operator liable should be based on the principle of preventive action of environmental liability. Moreover, this measure will provide financial guarantees in situations where the economic operator is unable to cover the costs of remediation or cannot be precisely identified due to widespread and diffuse pollution.

VII. CONCLUSIONS

In conclusion, we would like to reiterate the need to establish the principle of preventive liability in environmental law, so as to avoid the difficulties that often arise in identifying environmental damage and its perpetrators, and to anticipate the negative effects on the environment through a set of measures of responsibility, among which are the following.

1. Legal Enshrinement of Preventive Action Principle:

The current legislative framework in Moldova lacks explicit provisions supporting preventive action in environmental liability. The authors argue for comprehensive legislative reform to enshrine this principle within existing laws, thereby providing a robust legal basis for enforcing preventive measures against potential environmental harm. Such reforms would empower regulatory authorities and facilitate more effective environmental protection strategies. The absence of explicit codification of the preventive action principle in Moldova's legal framework undermines the effectiveness of environmental liability mechanisms. Integrating this principle into national legislation would provide a robust

[17] Vrabie, G., & Popescu, S. (1993). Teoria generală a dreptului. Iași: Ștefan Procopiu.

[18] Țeruș, I. (2023). Principiile și funcțiile de bază ale instrumentelor juridico-financiare de protecție a mediului. Anale științifice ale Academiei „Ștefan cel Mare" a MAI al Republicii Moldova, 17, 273.

foundation for proactive environmental protection and liability, ensuring legal clarity and reinforcing accountability for potential harm.

2. Paradigm Shift in Environmental Liability:

Traditional reactive liability mechanisms fall short in addressing the irreversible nature of environmental damage. Embracing preventive liability marks a transformative shift, focusing on preemptive measures, such as pollution taxes and guarantee funds, to avert damage before it occurs. This approach aligns liability with modern sustainability imperatives and ensures accountability even in cases of uncertain harm.[19]

3. Anticipatory Economic-Financial Mechanisms:

The principle of preventive action can effectively underpin anticipatory financial instruments, such as environmental liability insurance or compensatory funds. These mechanisms incentivize polluters to adopt eco-friendly practices, reduce exposure to financial risks, and provide a safety net for damage mitigation. The incorporation of anticipatory liability mechanisms, such as pollution taxes, environmental liability insurance, and compulsory guarantee funds, aligns environmental responsibility with sustainability goals. These mechanisms not only deter potential harm but also ensure financial resources are available for remediation in cases where polluters cannot be identified. Anticipatory Instruments for Economic Operators.

4. Integration with Established Principles:

The preventive action principle complements other core environmental principles, including prevention, precaution, and conservation. Together, they create a cohesive framework for sustainable environmental governance by encouraging anticipatory actions and mitigating the impact of activities with potential environmental risks. There is a compelling need to integrate the preventive action principle with established concepts such as the *"polluter pays' principle"* and "*the precautionary principle"*. By doing so, Moldova can create a cohesive legal framework that not only addresses current environmental challenges but also anticipates future risks. This integration will enhance accountability and provide clearer guidelines for both individuals and corporations regarding their environmental responsibilities.

5. Extension of Liability Scope:

Recognizing categories such as salvage damage, development damage, and loss of opportunity broadens the scope of environmental liability. By addressing indirect and future damages, this approach ensures a more comprehensive response to ecological risks, fostering equity and justice for affected parties.

6. Empowerment of Judicial and Administrative Mechanisms:

The judiciary plays a crucial role in implementing the preventive action principle through civil liability frameworks. Courts should be empowered to mandate cessation of harmful activities even in the absence of proven damage, reinforcing the preventive function of environmental law. This judicial approach can significantly enhance compliance and deter potential violators. The preventive action principle strengthens the role of civil and administrative courts in environmental protection. By allowing

[19] Legea privind protecția mediului înconjurător nr. 1515 din 16 iunie 1993 [Law on Environmental Protection]. În: Monitorul Parlamentului Republicii Moldova, 10/1993.

courts to mandate preventive measures and address administrative failures, this principle ensures a multi-layered enforcement structure that bridges regulatory gaps.

7.New Categories of Environmental Damage:

The concept of new categories of damage, such as preventive costs incurred by individuals or entities to avert potential harm, should be recognized legally. This acknowledgment would allow for compensation mechanisms that incentivize proactive environmental stewardship, thus fostering a culture of prevention rather than reaction.

8. Alignment with EU Directives:

Moldova's alignment with EU Directive 2004/35/EC emphasizes the need for proactive liability frameworks. Incorporating preventive action within national law would harmonize Moldova's environmental liability system with EU standards, enhancing regional cooperation and compliance with international norms.

9. Future Research Directions/ Sustainability Actions:

Further research is needed to explore the practical implications of implementing the preventive action principle in Moldova's legal system. This includes examining case studies from other jurisdictions that have successfully integrated similar principles into their environmental laws, providing valuable lessons for Moldova's legislative evolution and sustainability.

These conclusions emphasize the transformative potential of integrating the preventive action principle into Moldova's environmental liability framework, aligning legal, financial, and administrative systems to address emerging environmental challenges. By emphasizing these conclusions, the paper aims to contribute significantly to the discourse on environmental law reform in Moldova, advocating for a shift towards a more anticipatory and preventive approach to environmental liability that can serve as a model for other nations facing similar challenges.