Compliance in Trade and Information Technology

CEJ
COMPLIANCE ELLIANCE JOURNAL

ISSN 2365-3353
Volume 10 • Number 2
Fall 2024

Compliance Elliance Journal (CEJ)
Volume 10, Number 2, 2024
ISSN: 2365-3353
This version appears in print and online. CEJ is published twice per year, in spring and fall.

Title: Compliance Compliance in Trade and Information Technology

Website: www.cej-online.com

E-Mail: info@hendrikschneider.eu

Address:
Taunusstrasse 7
65183 Wiesbaden, Germany

Telephone: +49 611 95008110

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

Compliance Compliance in Trade and Information Technology

TABLE OF CONTENTS

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

EDITORIAL

Compliance in Trade and Information Technology

This edition elucidates the disparate complexes wherein compliance is applicable and demonstrates the evolving landscape of regulatory frameworks across a multitude of sectors. It examines the way compliance standards evolve in response to emerging technologies, ethical challenges, and international regulations.

Jan-Phillip Graf provides insights into the diverse regulatory mechanisms of compliance that impact artificial intelligence. Graf's analysis reveals that the EU AI Act strives for a proactive and comprehensive framework to balance risk and innovation, whereas the U.S. employs a piecemeal and decentralized approach, responding to each case individually.

Dr. Yannick Neuhaus, Philipp Karger and Demian Frank emphasise the necessity for the creation of a unified regulatory framework for the handling of archaeological artefacts. In this context, they explore the potential for self-protection within the art market through the establishment of a compliance network, outlining the fundamental principles that could inform the establishment of such a compliance system.

Alexander Sellmayer and Anselm Fischer investigate the interrelationships between the German Supply Chain Act (LkSG), the Money Laundering Act (GwG), and the German Criminal Code (StGB) about potential human rights risks.

Claudia Chiauzzi offers an in-depth examination of the disparate policies pertaining to AI in the United States, China, and the European Union, shedding light in the potential hazards associated with AI and compliance. Additionally, she delineates the function of AI ethics and compliance officers.

Luminita Diaconu provides a comprehensive overview of the protection regime for human-made products, which is central to modern environmental and public health policy. She emphasises the necessity for a robust

regulatory framework to identify and control harmful substances, with the aim of protecting human health and the environment.

Finally Nedret Madak explains compliance and risks of criminal liability for food labelling.

With our best regards,

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

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

TWO MODELS OF REGULATION: ARTIFICIAL-INTELLIGENCE COMPLIANCE IN THE UNITED STATES AND THE EUROPEAN UNION

Jan-Phillip Graf

AUTHOR

Jan-Phillip Graf is a J.D. Candidate at Yale Law School and a Ph.D. candidate at the German Institute for International Law of Peace and Armed Conflict at Ruhr University Bochum. He also serves as an Executive Articles Editor for the Yale Journal of International Law and an Editor for the Yale Law Journal. He has previously worked for the U.S. District Court for the Southern District of New York and the International Law Commission of the United Nations.

TABLE OF CONTENTS

I. INTRODUCTION

At least for the last few years, talk about artificial intelligence (AI) has been all over the corporate world. From boardrooms[1] to annual reports and shareholder proposals[2] to high-stakes litigation,[3] AI has become a mainstay of business news. Unsurprisingly, regulators on both sides of the Atlantic have already devoted considerable attention to issues surrounding AI's legal governance.[4] On the American side, President Biden issued a detailed executive order on the "safe, secure, and trustworthy development and use of artificial intelligence" in October 2023, instructing "the Federal Government to ensure the effective formulation, development, communication, industry engagement . . . and timely implementation of AI-related policies."[5] The President's order came after a flurry of regulatory activity on the state level that is just getting started.[6] On the European side, the EU passed the so-called AI Act, which will come into effect in progressive stages beginning on August 2, 2024, and aims to be the world's first comprehensive regulation of AI.[7]

Like any emerging technology, AI poses specific regulatory challenges.[8] First and foremost, any regulation needs to define its „subject"—artificial intelligence in this case. Problematically, however, a unified definition of AI has not yet emerged and might not even be feasible, considering the evolving nature of the underlying technology.[9] The second issue is what one researcher termed the "velocity problem," which describes the staggering pace at which AI applications develop, making regulations of today outdated in real-time.[10] The third challenge relates to the "black-box" nature of AI. This means neither developers nor policymakers can fully know what harm AI might cause and how to best protect

[1] *See, e.g.*, *AI Readiness for C-Suite Leaders*, MIT TECH. REV. 4 (2024), https://www.technologyreview.com/2024/05/29/1092235/ai-readiness-for-c-suite-leaders [https://perma.cc/M6H8-BRCR]; Reid Blackman & Ingrid Vasilu-Feltes, *The EU's AI Act and How Companies Can Achieve Compliance*, HARV. BUS. REV. (Feb. 22, 2024), https://hbr.org/2024/02/the-eus-ai-act-and-how-companies-can-achieve-compliance [https://perma.cc/VS8Y-98PJ].

[2] William Savitt et al., *AI in the 2024 Proxy Season: Managing Investor and Regulatory Scrutiny*, PROGRAM ON CORP. COMPLIANCE & ENF'T (Mar. 19, 2024), https://wp.nyu.edu/compliance_enforcement/2024/03/19/ai-in-the-2024-proxy-season-managing-investor-and-regulatory-scrutiny [https://perma.cc/MCH6-54WE].

[3] Bruce Barcott, *AI Lawsuits Worth Watching: A Curated Guide*, TECH POLICY.PRESS (July 1, 2024), https://www.techpolicy.press/ai-lawsuits-worth-watching-a-curated-guide [https://perma.cc/4983-PUQX]; Hannah Albarazi, *These Are the High-Stakes AI Legal Battles to Watch in 2024*, LAW360 (Jan. 1, 2024, 8:02 AM ET), https://www.law360.com/articles/1774888/these-are-the-high-stakes-ai-legal-battles-to-watch-in-2024 [https://perma.cc/M8VX-8UW9].

[4] Yoshija Walter, *Managing the Race to the Moon: Global Policy and Governance in Artificial Intelligence Regulation—A Contemporary Overview and an Analysis of Socioeconomic Consequences*, 4 DISCOVER A.I., no.14, 2024 at 4-11; Nathalie A. Smuha, *From a 'Race to AI' to a 'Race to AI Regulation': Regulatory Competition for Artificial Intelligence*, 13 L. INNOVATION & TECH. 57, 69-83 (2021).

[5] Exec. Order No. 14110, 3 C.F.R. 657, 697 (2024).

[6] Louis W. Tompros et al., *State Governments Move to Regulate AI in 2024*, PROGRAM ON CORP. COMPLIANCE & ENF'T (Mar. 11, 2024), https://wp.nyu.edu/compliance_enforcement/2024/03/11/state-governments-move-to-regulate-ai-in-2024 [https://perma.cc/3CNG-C4RK].

[7] Regulation 2024/1689 of the European Parliament and of the Council of June 13, 2024, Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689) [hereinafter AI Act].

[8] *See generally*, Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, and Strategies*, 29 HARV. J. L. & TECH. 353 (2016); Tom Wheeler, *The Three Challenges of AI Regulation*, BROOKINGS (June 15, 2023), https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation [https://perma.cc/6UZK-CT3N].

[9] *See, e.g.*, Matt O'Shaughnessy, *One of the Biggest Problems in Regulating AI Is Agreeing on a Definition*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Oct. 6, 2022), https://carnegieendowment.org/posts/2022/10/one-of-the-biggest-problems-in-regulating-ai-is-agreeing-on-a-definition [https://perma.cc/6EPR-K5GA]; Bryan Casey & Mark A. Lamley, *You Might Be a Robot*, 105 CORNELL L. REV. 287, 287 (2020) ("No one has been able to offer a decent definition of robots and AI—not even experts.").

[10] Wheeler, *supra* note 8.

against it.[11] Predictions range from limited concerns about automated fraud all the way to near-apocalyptic scenarios.[12] The fourth major issue concerns uncertainty about the nature of potential enforcement mechanisms and the gravity of sanctions for noncompliance.[13] As a result, the overarching challenge for regulators is to design an AI-governance structure that strikes a cogent balance between protecting against abstract risks while enabling, or even encouraging, innovation in a critical, emerging industry.

Naturally, these issues translate into compliance challenges that corporate actors—developers, distributors, and users of AI—face after a plethora of regulatory activity on both sides of the Atlantic. On the most fundamental level, it still remains unclear which technologies will be covered by any given definition of AI. Will regulators opt for general, inclusive definitions or adopt risk-based categorizations of different AI technologies? Likewise, the substantive scope of AI compliance also remains speculative. Will certain technologies be prohibited? What sort of internal and external compliance measures will be required? Additionally, as a consequence of the relative novelty of most AI-related rules, practice guidelines and enforcement mechanisms are still in the development phase, creating substantial uncertainty about the practical implementation of any compliance regime. Thus, the constantly evolving nature of AI and the relative novelty of its regulatory regimes raise unique compliance challenges which this Article will focus on.

To that end, the Article will compare the most recent developments in AI regulation in the EU and the United States, investigating to what extent both economies follow different or convergent regulatory models and what compliance issues each approach raises. Accordingly, Part II introduces the EU's AI Act, focusing on its definitions, scope, and enforcement. Part III shifts to the more decentralized U.S. system, analyzing Executive Order 14110 and federal enforcement initiatives before providing an overview of state-level initiatives. Part IV compares both regulatory approaches on a more abstract level, arguing that the more decentralized, issue-specific American model leaves the AI sector room for experimentation and innovation while the comprehensive European model provides more legal certainty and predictability. Even though AI regulation is in constant flux and the infant compliance movement is at a moment of considerable uncertainty, this Article will conclude by recommending several initial compliance strategies.

[11] Margot E. Kaminski, *Regulating the Risks of AI*, 103 B.U. L. REV. 1347, 1356-65 (2023); Bartosz Brozek et al., *The Black Box Problem Revisited: Real and Imaginary Challenges for Automated Legal Decision Making*, 32 A.I. & L. 427, 427-28 (2024).

[12] Tamlyn Hunt, *Here's Why AI May Be Extremely Dangerous—Whether It's Conscious or Not*, SCI. AM. (May 25, 2023), https://www.scientificamerican.com/article/heres-why-ai-may-be-extremely-dangerous-whether-its-conscious-or-not [https://perma.cc/24MM-WJW3]; Cade Metz, *What Exactly Are the Dangers Posed by A.I.?*, N.Y. TIMES (May 7, 2023), https://www.nytimes.com/2023/05/01/technology/ai-problems-danger-chatgpt.html [https://perma.cc/CA2N-7MWQ].

[13] *See* Wheeler, *supra* note 8.

II. THE EU'S APPROACH: COMPREHENSIVE REGULATION UNDER THE AI ACT

AI had been on the EU's radar for a number of years[14] when the European Commission published a "White Paper on Artificial Intelligence" in February 2020,[15] commencing a consultation process that led the Commission to formally propose an AI Act in April 2021.[16] After extensive negotiations between the European Council and the European Parliament, an agreement was reached in December 2023,[17] which the Parliament approved in March 2024 and the Council approved in May of the same year.[18] The result of this process is a 144-page document with 180 recitals, 113 operative articles, and thirteen annexes, purporting to be the world's first comprehensive regulation of AI. While the Act's general provisions take effect on August 2, 2024 (twenty days after its publication in the Official Journal of the EU), other parts will only enter into force over the next three years until the entire Act becomes binding on August 2, 2027.[19] This Section will briefly outline the Act's scope and enforcement mechanisms, keeping in mind that this is only an initial analysis as the EU has just started the implementation process which will further develop the Act's legal requirements through delegated acts.

A. Definitions and General Scope

Since one of the main purposes of the AI Act is protection "against the harmful effect of *AI systems*,"[20] the definition of what qualifies as an *AI system* is fundamental. While the definition changed considerably throughout the legislative process,[21] it developed in tandem with recommendations from the OECD's Council on Artificial Intelligence,[22] and generally covers:

---

[14] *See, e.g.*, *Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe*, at 5, 13-16, COM (2018) 237 final (Apr. 25, 2018) (calling for an "EU Initiative on AI" while also "[e]nsuring an appropriate ethical and legal framework"); Ursula von der Leyen, *A Union that Strives for More: My Agenda for Europe*, https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf [https://perma.cc/7NKC-J43F] (setting out the agenda on AI of then-candidate for President of the European Commission: "In my first 100 days in office, I will put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence.").

[15] *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, COM (2020) 65 final (Feb. 19, 2020).

[16] *Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021).

[17] *Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI*, EUR. PARLIAMENT (Dec. 9, 2023), https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai [https://perma.cc/C3UF-8M3L].

[18] *Artificial Intelligence (AI) Act: Council Gives Final Green Light to the First Worldwide Rules on AI*, EUR. COUNCIL (May 21, 2024), https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai [https://perma.cc/9A4Z-8FAU].

[19] AI Act art. 113. *See also* Martin Braun, Anne Vallery & Itsiq Benizri, *European Union AI Act Published in Official Journal—Critical Milestones on the Road to Full Applicability*, WILMERHALE (July 16, 2024), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240716-european-union-ai-act-published-in-the-official-journal-critical-milestones-on-the-road-to-full-applicability [https://perma.cc/7RGR-FSJT].

[20] AI Act art. 1(1) (emphasis added).

[21] *See* David Fernandez-Llorca et al., *An Interdisciplinary Account of the Terminological Choices by EU Policymakers Ahead of the Final Agreement on the AI Act: AI System, General Purpose AI System, Foundation Model, and Generative AI*, A.I. & L., Aug. 2024, at 4.

[22] Working Party on AI Governance, *Explanatory Memorandum on the Updated OECD Definition of an AI System*, OECD (Mar. 2024), https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_3c815e51/623da898-en.pdf [https://perma.cc/J4ML-FYGE].

> [M]achine-based system[s] that [are] designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infer[], from the input [they] receive[], how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[23]

According to Stipulation 12 of the Act, the main purpose of this definition is to "distinguish [AI] from simpler traditional software systems or programming approaches" highlighting that "[a] key characteristic of AI systems is their capability to infer . . . [to] enable[] learning, reasoning or modeling" and its "self-learning capabilities, allowing the system to change while in use." As early commentators pointed out, however, such a definition is "incredibly broad, as it encompasses virtually all algorithms" making it hard for "computer scientists . . . to determine whether this Regulation applies to them."[24] Others observed that the Act "covers almost every computer program" which "may lead to legal uncertainty for developers, operators, and users of AI systems."[25] Overall, it seems like the EU's attempt to distinguish conventional "software" from "AI systems" without limiting the definition to pure machine learning and keeping it open-textured enough to anticipate future developments, resulted in an exceedingly broad definition.[26]

Nevertheless, despite the definition's (presumably deliberate) breadth, it points to four prongs that will characterize regulated products: (1) they are machine-based; (2) exhibit a certain degree of autonomy and adaptability; (3) have the capacity to make inferences; and (4) can generate outputs that have a real-world influence. What this language means in practice and how far-reaching EU regulators will cast their regulatory net will only become visible in future agency practice and implementation guidelines. Conceptually, however, the Act supplies future regulators with a definition that has the potential to capture almost any use of AI. This provides an immense degree of regulatory flexibility, which, at the moment, translates into uncertainty for AI developers and users on whether their products will fall under the Act's scope.

However, Article 2 of the AI Act which defines the Regulation's personal and territorial scope, sets first limits to its reach. Accordingly, the Act only covers *providers*[27] and *deployers*[28] of AI systems, "irrespec-

[23] AI Act art. 3(1).

[24] Natalie Smuha et al., *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, 14 (Aug. 5, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991 [https://perma.cc/Q5GM-HCGJ] (commenting on an earlier version which had shortfalls similar to the final definition copied here).

[25] Martin Ebers et al., *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robots and AI Law Society (RAILS)*, 4 MULTIDISCIPLINARY SCI. J. 589, 590 (2021) (commenting on an earlier version which had shortfalls similar to the final definition copied here).

[26] Fernandez-Llorca et al., *supra* note 21, at 3-5.

[27] AI Act art. 3(3) ("'[P]rovider' means a natural or legal person, public authority, agency or other body that develops an AI system . . . and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.").

[28] *Id.* art. 3(4) ("'[D]eployer' means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.").

tive of whether [they] are established or located within the Union or a third country," as well as *importers*[29] and *distributors*[30] based in the EU. This means, that the AI Act might have wide-reaching extraterritorial effects, extending its regulatory obligations to providers and deployers based outside the EU that "place[] on the market"[31] or "put[] into service"[32] their AI systems in the Union. However, purely personal, non-professional uses of AI are exempted from the regulation.[33] The Act also does not extend to AI systems *exclusively* used for "military, defence or national security purposes" or models "specifically developed . . . for the sole purpose of scientific research and development."[34] Interestingly, Article 2(8) also supplies the temporal limitation that the "Regulation does not apply to any research, testing or development activity regarding AI systems . . . prior to their being placed in the market." Thus, even though the exact scope of the Act's definitions and exemptions is still reasonably vague, a clear legislative intent is already discernible: broad application to corporate/professional actors inside and outside of the EU with exemptions for state and private uses of AI.

B. Substantive Scope

In terms of its substantive scope, the AI Act works like a risk-based product classification[35] that divides AI systems into five risk categories: (1) prohibited AI practices; (2) high-risk AI systems; (3) certain AI systems that pose "specific transparency risks;" (4) general-purpose AI models; and (5) all other AI systems.[36] Depending on what category a system falls into, different compliance obligations apply.

1. Prohibited AI Practices

Chapter II, which corresponds to Article 5 of the Act, prohibits certain "AI practices" that pose an "unacceptable risk." While the specific definitions of prohibited AI practices are rather detailed, they can be grouped into three rough categories. The first category includes purposefully fraudulent uses of AI like "subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques."[37] The second category encompasses social scoring or (racial) profiling systems as well as "the untargeted scraping of facial images from the internet" or the "use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions."[38] The third area concerns the "use of biometric categorization systems," especially when they relate to a protected

[29] *Id.* art. 3(6) ("'[I]mporter' means a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.").

[30] *Id.* art. 3(7) ("'[D]istributor' means a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.").

[31] *Id.* art. 3(9) ("'[P]lacing on the market' means the first making available of an AI system or a general-purpose AI model on the Union market.").

[32] *Id.* art. 3(11) ("'[P]utting into service' means the supply of an AI system for first use directly to the deployer or for own use in the Union for its intended purpose.").

[33] *See id.* art. 2(10).

[34] *See id.* arts. 2(3) & 2(6).

[35] *See* Fernandez-Llorca, *supra* note 21, at 3.

[36] Mehdi Ansari et al., *EU to Adopt Sweeping Regulation of Artificial Intelligence*, PROGRAM ON CORP. COMPLIANCE & ENF'T (Feb. 20, 2024), https://wp.nyu.edu/compliance_enforcement/2024/02/20/eu-to-adopt-sweeping-regulation-of-artificial-intelligence [https://perma.cc/YVL4-J87P].

[37] *See, e.g.*, AI Act art. 5(1)(a-b).

[38] *See*, *id.* art. 5(1)(c-f).

personal status (like race or religion).[39] However, Sections 2 and 3 of Article 5 carve out narrow exceptions that allow the judicially sanctioned use of biometric surveillance for certain law-enforcement activities.

2. High-Risk AI Systems

Chapter III, spanning Articles 6-50, covers the classification and regulation of "high-risk AI systems," which "pose a significant risk of harm to the health, safety or fundamental rights of natural persons."[40] Generally, there are two ways for an AI system to fall into the high-risk category. First, under Article 6(1), AI systems that are a safety component of potentially dangerous products listed in Annex I count as high-risk.[41] Second, according to Article 6(2), AI systems listed in Annex III automatically fall into the high-risk bucket. Annex III, lists eight high-risk areas for AI systems: (1) biometrics; (2) critical infrastructure; (3) education and vocational training; (4) employment and workers' management; (5) access to essential public and private services and benefits; (6) otherwise permitted law enforcement; (7) migration and border control; and (8) justice administration and democratic processes. Any AI system that falls into one of these buckets is presumptively high-risk unless "it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making."[42] This determination shall be made and documented by the provider in accordance with future Commission guidelines.[43] Additionally, Article 7, in conjunction with Article 97, allows the Commission to amend Annex III to keep it current.

Generally, Article 8 requires high-risk AI systems to comply with seven obligations enshrined in Articles 9-15. First, providers need to establish, implement, document, and maintain a *risk management system* "requiring regular systematic review and updating."[44] Establishment of such a system includes the "identification and analysis [and] estimation and evaluation of the risks" in order to adopt "appropriate and targeted risk management measures."[45] Second, any high-risk systems that require training on data sets are subject to data quality criteria and governance standards set out in Article 10. Third, before placement on the EU market, developers are required to compile technical documentation that "demonstrate[s] that the high-risk AI system complies with the requirements [of the Act]" as specified in Annex IV and provide such documentation to the designated national authorities.[46] Additionally, such systems need to "technically allow for automatic recording of events [logging] . . . [i]n order to ensure a level of traceability."[47] Likewise, developers need to ensure that the systems are "sufficiently transparent to enable deployers to interpret [their] output" and provide them with "instructions for use . . . that include concise, complete, correct and clear information."[48] Sixth, they should be designed

[39] *Id.* art. 5(1)(g-h).
[40] *Id.* art. 6(3).
[41] Annex I lists EU harmonization legislation concerning certain products like toys, machinery, lifts, explosive devices, or aviation equipment where the use of AI systems as safety components would pose a particularly high risk.
[42] AI Act art. 6(3).
[43] *Id.* art. 6(4-5).
[44] *Id.* art. 9(2).
[45] *Id.* art. 9(2)(a-d).
[46] *Id.* art. 11(1).
[47] *Id.* art. 12(1-2).
[48] *Id.* art. 13(1-2).

to allow for effective human oversight during their operation.[49] Finally, the Act requires that high-risk systems are built to "achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle."[50] All these seven obligations will be further fleshed out by the Commission until 2026.[51]

While these seven standards apply to high-risk AI systems as such, they only become effective if properly implemented by the systems' providers, employers, importers, and distributors. The AI Act places the heaviest burden on AI system *providers*. Under Article 16, they must "ensure that [they] are compliant with the [seven] requirements" set out in the previous paragraph. To that end, providers have a number of additional obligations that include: putting in place a quality management system "proportionate to the size of the provider's organization" (Article 17); keeping certain records for ten years after the market entry of the AI system (Article 18); cooperating with competent national and EU authorities (Article 21); and appointing an authorized representative within the EU for providers based outside the Union (Article 22). Finally, Article 20 requires providers to "immediately take the necessary corrective actions" when they realize that their system does not comply with any of the Act's regulations or "to withdraw it, to disable it, or to recall it, as appropriate."

In accordance with Articles 23 and 24, *importers* and *distributors* have a number of subsidiary duties to ensure that the *providers* of high-risk AI systems have complied with all their obligations and that the system they market has undergone the required EU certification under Article 43. They also have obligations to abstain from marketing systems they believe to be non-compliant. *Deployers* of high-risk AI systems, in turn, have a duty to "ensure they use such systems in accordance with the instructions," assign oversight to trained personnel, and "cooperate with the relevant authorities."[52] Of course, all actors along the "AI value chain" have an obligation under Article 79(1) to inform the provider and market surveillance authority should an AI system "present risks to the health or safety, or fundamental rights, of persons." The market surveillance authority will then investigate the system and recommend corrective action or require its withdrawal.[53] Interestingly, "deployers that are bodies governed by public law, or are private entities providing public services" have to perform a "fundamental rights impact assessment" outlining the "specific risks of harm likely to have an impact" and "the measures to be taken in the case of the materialization of those risks."[54] A key oversight function is also accorded to so-called notifying bodies that conduct the conformity assessments specified in Article 43 to ensure and certify that high-risk AI systems comply with the standards explained above.[55] Such notifying bodies, whether they are public or private entities, will be certified and monitored by a national "notifying authority."[56]

[49] *Id.* art. 14.

[50] *Id.* art. 15(1).

[51] On how these practice guidelines will be developed, see *infra* Section II.C.

[52] AI Act art. 26.

[53] *Id.* art. 79(2).

[54] *See id.* art. 27(1).

[55] *See id.* art. 28.

[56] *Id.* art. 28(1).

3. Certain AI Systems with Heightened Transparency Obligations

Article 59, which corresponds to Chapter IV of the Act, requires that certain AI systems coming into close or direct contact with the larger public inform their users that they are interacting with an AI "in a clear and distinguishable manner at the latest at the time of the first interaction or exposure."[57] Such systems include those "generating synthetic audio, image, video or text content," "emotion recognition . . . [or] biometric categorization system[s]," or those "that generate[] or manipulate[] image, audio or video content constituting a deep fake."[58] Article 50(7) additionally instructs the Commission to develop "codes of practice" that further clarify what labeling and information obligations attach to such content-generating AI systems. Noticeably, Article 50 includes broad exceptions for "AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences."

4. General Purpose AI Models

The AI Act differentiates between general-purpose AI systems (GPAIS) and general-purpose AI models with systemic risk. Overall, GPAIS are defined as:

> [M]odel[s] . . . trained with a large amount of data using self-supervision at scale, that display[] significant generality and [are] capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.[59]

Additionally, a GPAIS qualifies as presenting *systemic risk* if it either "has high impact capabilities," which the Act defines as "capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models,"[60] or if the Commission determines a system to fall into that category.[61] Presumptively, all AI systems whose "cumulative amount of computation used for its training" exceeds 10^{25} floating points (FLOPS) will be classified as having *systemic risk* because of their sheer computing power.[62] As a point of reference, at the time of writing only GPT-4 (OpenAI's newest model) and Google's Gemini are said to have transcended this threshold.[63] However, considering the rapid pace at which these models' computation power has increased, the Commission is encouraged to review this threshold regularly.[64]

[57] *Id.* art. 50(5).
[58] *Id.* art. 50(2-4).
[59] *Id.* art. 3(63).
[60] *Id.* art. 3(64).
[61] *Id.* art. 51(1)(a-b).
[62] *Id.* art. 51(2).
[63] Robi Rahman, David Owen & Josh You, *Tracking Large-Scale AI Models*, EPOCH AI (Apr. 5, 2024), https://epochai.org/blog/tracking-large-scale-ai-models [https://perma.cc/R675-ZNQ3].
[64] AI Act art. 51(3).

Overall, providers of GPAIS have obligations targeted at making these models more explainable, including the provision of technical documentation to deployers and the public along the criteria specified in Annex XI.[65] Providers of GPAIS with systemic risks have additional obligations to "perform model evaluations," "assess and mitigate possible systemic risks," "keep track of, document, and report . . . serious incidents and possible corrective measures," and "ensure an adequate level of cybersecurity protection."[66]

C. Enforcement

The AI Act envisions a three-level enforcement structure with the AI Office and the European Artificial Intelligence Board at the top, national competent authorities on the member-state level, and notifying bodies on the lowest level. At the EU level, the so-called AI Office has been established within the Commission's Directorate-General for Communication Networks. It will function as the "central coordinating and monitoring mechanism" regarding the Act's implementation.[67] The AI Board, which includes one representative from each member state, is supposed to function as a moderator between the Commission and the member states by coordinating the activity among member states, exchanging technical expertise, sharing best practices, and harmonizing administrative standards.[68] Importantly, the Commission can also request "recommendations and written opinions" from the Board on any of the codes of conduct, practice guidelines, and further regulations the Act authorizes to promulgate.[69] Additionally, the so-called "advisory forum" "shall represent . . . stakeholders" and "provide technical expertise and advise [to] the Board and the Commission."[70] Likewise, a "scientific panel of independent experts" will advise the AI Office, especially regarding the systemic risk of GPAIS and the surveillance of the global AI market.[71]

On the national level, each member state must establish a "notifying authority" and a "market surveillance authority" which are collectively referred to as "national competent authorities."[72] The national notifying authorities will "carry[] out the . . . assessment, designation and notification of conformity assessment bodies"[73]—the public or private entities that "perform[] [the] third-party conformity assessment activities"[74] specified for high-risk AI systems and GPAIS. The market surveillance authorities, established under the general market-surveillance and product-regulation framework,[75] are in-

[65] *Id.* art. 53(1).

[66] *Id.* art. 55(1). Article 56 of the Act further encourages the Commission to draw up "codes of practice" that further elaborate the technical standards for providers of GPAIS.

[67] *The AI Office: What Is It, and How Does It Work?*, EU A.I. ACT (Mar. 21, 2024), https://artificialintelligenceact.eu/the-ai-office-summary [https://perma.cc/3S7M-WUTH].

[68] AI Act art. 66(a-d).

[69] *Id.* art. 66(e).

[70] *Id.* art. 67.

[71] *Id.* art. 68.

[72] *Id.* art. 70.

[73] *Id.* art. 3(19).

[74] *Id.* art. 3(21).

[75] *See generally* Regulation (EU) 2019/1020, of the European Parliament and the Council of 20 June 2019 on Market Surveillance and Compliance of Products and Amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, 2019 O.J. (L 169/1).

tended to monitor AI products on the market for their compliance with the AI Act and other EU harmonization legislation.[76] These authorities can be independent government agencies but will most likely be established as new departments of already existing agencies. In Germany, for example, the *Deutsche Akkreditierungsstelle* will serve as the notifying authority and the *Bundesnetzagentur* as the market surveillance authority.[77]

In terms of remedies, the Act restricts natural and legal persons' standing to lodging complaints with the responsible market surveillance authority, which will "take[] into account" such complaints "for the purpose of conducting market surveillance activities."[78] In general, however, most enforcement powers are shared between the Commission, the AI Office, and member states.[79] Likewise, member states are responsible for "lay[ing] down the rules on penalties and other enforcement measures,"[80] which can be quite hefty. For violations of Article 5 on prohibited AI practices, for instance, the higher of up to EUR 35 million or 7% of the offender's "total worldwide annual turnover" may be imposed as a fine.[81] Lower, but still substantial fines may be imposed for other violations of the Act.[82]

Lastly, it should be noted that although the AI Act formally entered into force on August 2, 2024, most of its provisions will only become effective after a specified period.[83] Thus, by February 2, 2025, Chapter I (general provisions and definitions) and Chapter II (prohibited AI practices) will take effect.[84] By August 2, 2025, Chapter III, Section 4 (domestic authorities), Chapter VII (EU authorities), and Chapter XII (penalties) will apply.[85] All other provisions will take effect on August 2, 2026, except for those related to high-risk AI systems, which will only enter into force on August 2, 2027.[86] It is likewise important to be alert to the fact that the Commission must publish its implementing acts and guidelines for practical implementation by May 2, 2025, for GPAIS, and by February 2, 2026, for all other systems.[87]

[76] *See* AI Act arts. 74-77.

[77] *The AI Act: Responsibilities of the EU Member States*, EU A.I. ACT (Aug. 22, 2024), https://artificialintelligenceact.eu/responsibilities-of-member-states [https://perma.cc/8CKY-XBN2].

[78] AI Act art. 85.

[79] *Id.* arts. 88-94.

[80] *Id.* art. 99(1).

[81] *Id.* art. 99(3).

[82] *Id.* arts. 99(4), 100, 101. *See also* Tim Hickman et al., *Long Awaited EU AI Act Becomes Law After Publication in the EU's Official Journal*, WHITE & CASE (July 16, 2024), https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal [https://perma.cc/72UA-LUDJ].

[83] For a concise overview of the Act's timetable, see generally Braun, Vallery & Benizri, *supra* note 19; *Implementation Timeline*, EU A.I. ACT (Aug. 1, 2024), https://artificialintelligenceact.eu/implementation-timeline [https://perma.cc/LKX6-BAWW].

[84] AI Act art. 113(a).

[85] *Id.* art. 113(b).

[86] *Id.* art. 113(c).

[87] *Id.* arts. 56(9); 72; 6(5).

III. THE AMERICAN APPROACH: ISSUE-SPECIFIC REGULATION AND SELECTIVE ENFORCEMENT

The regulation of AI technologies in the United States is significantly less coordinated, centralized, and comprehensive.[88] Although congressional leaders expressed growing concern about AI's capabilities and unpredictability, federal legislative proposals have not succeeded so far.[89] Initially, the federal government followed a seemingly "laissez-faire approach," more focused on keeping a competitive edge rather than regulating AI meaningfully.[90] Beginning in the late Trump administration,[91] however, a process started that finally culminated in President Biden issuing Executive Order 14110 in October 2023, which has been described as the "most sweeping guidelines" on the federal level.[92] Still, apart from this initial step, the overall regulatory framework remains scattered across various federal agencies while many states have started to draft their own AI bills.[93] Therefore, this Section provides a brief snapshot of existing AI regulations and enforcement activities on the federal level before identifying broad regulatory trends in the states.

A. Executive Order 14110 and Other Federal Initiatives

Building on previous government reports,[94] Executive Order 14110 on the "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" calls for a "government-wide effort to guide responsible AI development and deployment through federal agency leadership, regulation of industry, and engagement with international partners."[95] Generally, Executive Orders are an instrument that allows presidents to direct federal policies, but only to the extent of the president's inherent constitutional and statutory powers.[96] The Biden administration used this power in Executive Order 14110 to stipulate eight "guiding principles and priorities" and to "direct[] over 50 federal entities to engage in more than

[88] Benjamin Cedric Larsen & Sabrina Küspert, *Regulating General-Purpose AI: Areas of Convergence and Divergence Across the EU and the US*, BROOKINGS (May 21, 2024), https://www.brookings.edu/articles/regulating-general-purpose-ai-areas-of-convergence-and-divergence-across-the-eu-and-the-us [https://perma.cc/L6SF-JKW4].

[89] Vera Bergengruen, *AI Regulation Takes Baby Steps on Capitol Hill*, TIME (Sept. 14, 2023), https://time.com/6313892/ai-congress-regulation-hearings [https://perma.cc/G56R-57XU].

[90] Benjamin Cedric Larsen, *The Geopolitics of AI and the Rise of Digital Sovereignty*, BROOKINGS (Dec. 8, 2022), https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty [https://perma.cc/H7M5-A59F].

[91] *See* Exec. Order No. 13859, 84 Fed. Reg. 3967 (Feb. 11, 2019) (on "Maintaining American Leadership in Artificial Intelligence"); Exec. Order No. 13960, 85 Fed. Reg. 78939 (Dec. 3, 2020) (on "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government?).

[92] Tate Ryan-Mosley & Melissa Heikkilä, *Three Things to Know About the White House's Executive Order on AI*, MIT TECH. REV. (Oct. 30, 2023), https://www.technologyreview.com/2023/10/30/1082678/three-things-to-know-about-the-white-houses-executive-order-on-ai [https://perma.cc/ZBB6-6KXU].

[93] *See* David Plotinsky & Giovanna M. Cinelli, *Existing and Proposed Federal AI Regulation in the United States*, MORGAN LEWIS (Apr. 9, 2024), https://www.morganlewis.com/pubs/2024/04/existing-and-proposed-federal-ai-regulation-in-the-united-states [https://perma.cc/2NKN-N2C4] (providing an overview of current and anticipated federal regulation of AI); Goli Mahdavi, Amy de La Lama & Christian M. Auty, *US State-By-State AI Legislation Snapshot*, BCLP (June 7, 2024), https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html [https://perma.cc/S27J-365F] (providing an overview of enacted, proposed, and failed AI laws in every U.S. state).

[94] Off. of Sci. & Tech., *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*, WHITE HOUSE (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [https://perma.cc/TVL2-SE2X]; Nat'l Inst. of Standards & Tech., *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, U.S. DEP'T COM. (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf [https://perma.cc/RX34-HV8Y].

[95] LAURIE HARRIS & CHRIS JAIKARAN, CONG. RSCH. SERV., R47843, HIGHLIGHTS OF THE 2023 EXECUTIVE ORDER ON ARTIFICIAL INTELLIGENCE 1 (2024).

[96] *See generally*, ABIGAIL A. GRABER, CONG. RSCH. SERV., R46738, EXECUTIVE ORDERS: AN INTRODUCTION 1-2 (2021).

100 specific actions."[97] These policy areas include (1) safety and security, (2) innovation and competition, (3) worker support, (4) consideration of AI bias and civil rights, (5) consumer protection, (6) privacy, (7) federal uses of AI, and (8) international leadership.[98] Evidently, this Article cannot summarize the—often highly specific—policy recommendations the Executive Order makes. However, the following paragraphs will identify particularly relevant areas for corporate compliance.

The Order's first policy priority is the safety and security of AI.[99] Under this category, it follows the two-pronged goal of addressing the "most pressing . . . biotechnology, cybersecurity, critical infrastructure, and . . . national security [risks]" while also ensuring "effective labeling and content provenance" so that consumers realize when they are interacting with AI.[100] In practice, the Order asks thirty federal entities to develop guidelines, best practices, reporting procedures, regulations, risk assessments, and other measures aimed at this objective.[101] The second policy priority of "innovation and competition" is mainly aimed at facilitating visa and immigration procedures for "AI talent," financing AI research and education programs, and addressing copyright concerns.[102] Likewise, the Order asks for reporting and guidelines on AI's potential impact on the labor market.[103]

Another policy priority that has received heightened attention in the United States is the consideration of biased AI and its adverse impacts on civil rights. Thus, the Executive Order calls for a number of reports, assessments, and guidance "to ensure AI complies with all Federal laws and to promote robust technical evaluations, careful oversight, engagement with affected communities, and rigorous regulation."[104] Important for compliance, the Order's fifth policy area prioritizes the application of federal consumer protection laws to AI, with a particular focus on "critical fields like healthcare, financial services, education, housing, law, and transportation."[105] Importantly, Section 8(a) encourages independent regulatory agencies (like the Federal Trade Commission (FTC) or the Securities and Exchange Commission (SEC)) to use their administrative rulemaking powers to "protect American consumers from fraud, discrimination, and threats to privacy." Interestingly, this has become one of the fastest-evolving areas of AI enforcement, as will be discussed below.

On the institutional side, Executive Order 14110 established the White House Artificial Intelligence Council under the chairmanship of the Assistant to the President and Deputy Chief of Staff for Policy and with the participation of 29 secretaries and heads of other federal departments. The AI Council's task is to "coordinate the activities of agencies across the Federal Government to ensure . . . [the] implementation of AI-related policies."[106]

[97] HARRIS & JAIKARAN, *supra* note 95, at 1-2.
[98] *Id.*
[99] *See* Exec. Order No. 14110, 3 C.F.R. §§ 2(a), 4 (2024).
[100] *Id.* § 2(a).
[101] HARRIS & JAIKARAN, *supra* note 95, at 3-6.
[102] *Id.* at 6-8.
[103] *Id.* at 9-10.
[104] Exec. Order No. 14110 §2 (d). *See also* Exec. Order No. 14074, 87 Fed. Reg. 32945 (2022) ("Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety").
[105] Exec. Order No. 14110 § 2(e).
[106] *Id.* § 12(a).

Overall, it has become clear at this point that Executive Order 14110 significantly differs from the EU's AI Act in at least three ways. First, while the AI Act aims to regulate AI systems comprehensively across all policy areas, the Executive Order focuses on more than 100 different projects scattered over eight policy-priority areas. Second, the Order is exclusively targeted at executive-branch agencies, while the AI Act regulates developers, deployers, the EU, and member states altogether. Third, although the Executive Order contemplates concrete deliverables like studies, reports, or draft regulations, this does not compare to the binding legal obligations and fines that the AI Act entails. On the other hand, both documents try to balance security with room for innovation and provide for staggered implementation over the next years.

B. Federal Enforcement Activities

The decentralized, issue-focused approach to AI governance is also reflected in the way federal agencies and courts have responded. In contrast to the EU's "all at once" approach, U.S. agencies seem to hold out for a specific problem or case to issue rules and guidance just on that issue. In doing so, they often rely on existing statutes or legal doctrines which they transpose to the "new case" of AI. The following paragraphs will provide three examples of agency responses that—although not comprehensive—are typical of the United States' current approach to AI compliance.

1. Securities and Exchange Commission

At the end of 2023 and encouraged by the Biden Administration's Executive Order, the SEC, the independent agency regulating and overseeing the U.S. securities market, became increasingly concerned with so-called "AI washing," which means the public misrepresentation of SEC-regulated companies' AI capabilities.[107] So far, the SEC's main focus has been consumer-facing fraud by investment advisors who promise unrealistically high returns as a result of their "proprietary AI trading system[s]."[108] For example, in March of this year, the SEC announced the settlement in two cases against the investment advisory firms Delphia USA Inc. and Global Predictions Inc.[109] Both had disclosed in their SEC filings or communications to clients that they used "a predictive algorithmic model" or "machine learning to analyze the collective data" even though they did not.[110] Observers predict that these cases only mark the beginning of the SEC's enforcement related to fraudulent AI disclosures within its mandate. It is therefore recommended that SEC-regulated public companies, investment advisers, and broker-dealers "be clear and accurate" surrounding AI-related disclosures or statements.[111]

---

[107] Joel M. Cohen et al., *Navigating New Frontiers in Regulatory Enforcement: The SEC Increases Scrutiny of Artificial Intelligence*, WHITE & CASE (Dec. 20, 2023), https://www.whitecase.com/insight-our-thinking/navigating-new-frontiers-regulatory-enforcement-sec-increases-scrutiny [https://perma.cc/JZJ2-63MC].

[108] *Artificial Intelligence (AI) and Investment Fraud: Investor Alert*, SEC (Jan. 25, 2024), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/artificial-intelligence-fraud [https://perma.cc/JSZ9-NK89].

[109] *SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence*, SEC (Mar. 18, 2024), https://www.sec.gov/newsroom/press-releases/2024-36 [https://perma.cc/4U4X-F9XJ].

[110] Andrew J. Ceresney, *AI Enforcement Starts with Washing: The SEC Charges Its First AI Fraud Cases*, PROGRAM ON CORP. COMPLIANCE & ENF'T (Apr. 2, 2024), https://wp.nyu.edu/compliance_enforcement/2024/04/02/ai-enforcement-starts-with-washing-the-sec-charges-its-first-ai-fraud-cases [https://perma.cc/U73E-72XM].

[111] *Id.*; *see also* John F. Savarese, Wayne M. Carlin & David B. Anders, *Summer Takeaways in SEC Enforcement*, PROGRAM ON CORP. COMPLIANCE & ENF'T (Sept. 16, 2024), https://wp.nyu.edu/compliance_enforcement/2024/09/16/wachtell-memo-summer-takeaways-in-sec-enforcement [https://perma.cc/HG2A-VH2M].

2. Federal Trade Commission

Another agency that has recently geared up its AI regulatory activities is the FTC, the independent agency overseeing antitrust and consumer protection laws. Due to the FTC's broad mandate, its AI-related activities have a wide range. One enforcement priority has been the application of existing consumer protection laws to AI products, especially when they have biased or discriminatory effects.[112] In particular, the FTC has announced its intent to bring more actions against companies using AI-based facial-recognition software in a discriminatory manner,[113] individuals and entities engaging in fraudulent AI deception (e.g., by using chatbots, deep fakes, or voice clones),[114] commercial actors making exaggerated and unsubstantiated claims about AI in their marketing materials,[115] or companies that rely on human-like generative AI (like chatbots) to deceive an individual into making harmful choices.[116] Additionally, at the beginning of 2024, the FTC issued inquiry orders under Section 6(b) of the FTC Act to Alphabet, Amazon, Anthropic, Microsoft, and OpenAI to further "scrutinize corporate partnerships and investments with AI providers to build a better understanding of these relationships and their impact on the competitive landscape."[117] The initial prediction that this investigation was the leadup to further antitrust enforcement against the biggest developers of generative AI was confirmed when the FTC began a formal investigation into Microsoft for allegedly structuring a deal with the AI startup Inflection to avoid antitrust review.[118]

3. Federal Litigation

Even though AI technologies have only been in mainstream use for a little over a year, they have already given rise to a growing number of lawsuits in federal courts as plaintiff-side law firms hope to seize the moment.[119] Similar to the issue-specific approach of other federal enforcers, AI cases have

[112] Marian A. Waldmann, Elisabeth Hutchinson & Laura Linda Miller, *FTC Gears Up for AI Enforcement: No Brakes in Sight*, MORRISON FOERSTER (Feb. 6, 2024), https://www.mofo.com/resources/insights/240206-ftc-gears-up-for-ai-enforcement-no-brakes-in-sight [https://perma.cc/5T8T-AL75].

[113] *See, e.g.*, Complaint, Fed. Trade Comm'n v. Rite Aid Corp., 2023 WL 8869509 (E.D. Pa. 2023) (No. 2:23-cv-5023) (arguing that the use of an AI-based facial recognition system for identifying patrons that had previously engaged in criminal behavior without security measures protecting against biases would violate Section 5 of the FTC Act); *see also* Cambridge Analytica, LLC, Docket No. 9383, 2019 WL 3935311 (F.T.C. Aug. 16, 2019) (ordering the deletion of data and any resulting work product that Cambridge Analytica's GSRApp had collected deceptively from Facebook).

[114] Michael Atleson, *Chatbots, Deepfakes, and Voice Clones: AI Deception for Sale*, FED. TRADE COMM'N (Mar. 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale [https://perma.cc/9WWV-JGLG].

[115] Michael Atleson, *Keep Your AI Claims in Check*, FED. TRADE COMM'N (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check [https://perma.cc/3VPD-9DXC].

[116] Michael Atleson, *The Luring Test: AI and the Engineering of Consumer Trust*, PROGRAM ON CORP. COMPLIANCE & ENF'T (Apr. 17, 2024), https://wp.nyu.edu/compliance_enforcement/2024/04/17/the-luring-test-ai-and-the-engineering-of-consumer-rust [https://perma.cc/XE3E-4R87].

[117] Victoria Graham, *FTC Launches Inquiry into Generative AI Investments and Partnerships*, FED. TRADE COMM'N (Jan. 25, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-launches-inquiry-generative-ai-investments-partnerships [https://perma.cc/8NCE-9T99].

[118] Dave Michaels & Tom Dotan, *FTC Opens Antitrust Probe of Microsoft AI Deal*, WALL ST. J. (June 6, 2024), https://www.wsj.com/tech/ai/ftc-opens-antitrust-probe-of-microsoft-ai-deal-29b5169a [https://perma.cc/YS83-2GPM].

[119] Michael A. Mora, *This Lawyer Is Becoming a Thorn in the Side of AI Companies*, NAT'L L. J. (Mar. 15, 2024), https://www.law.com/2024/03/15/this-lawyer-is-becoming-a-thorn-in-the-side-of-ai-companies [https://perma.cc/6YHR-3HCN].

so far focused on "five main legal theories . . . privacy, copyright, trademark, right of publicity (and facial recognition), and tort cases."[120] Interestingly, the majority of such cases have been filed in the Northern District of California, and all cases involve one of the major AI corporations as the defendant.[121] Several class-action complaints, for instance, allege that OpenAI and Google violated consumers' economic and privacy rights by scraping their information from the internet without consent.[122] In the second category of cases, authors, photographers, coders, and other creators have argued that their rights under the Digital Millennium Copyright Act were violated when AI models were trained on texts, codes, and other materials they created without their consent or obtaining a proper license.[123] Other lines of cases have attacked the storing of biometric data without consent or potential torts by AI systems.[124] Overall, many of these cases face strong motions to dismiss and the AI bar is still waiting to see what kind of claims will be successful.

C. State-Level Activities

With congressional AI regulation largely out of reach, especially during an election year, the real center of gravity lies in the states. At the time of writing, forty-five states have introduced AI legislation, and thirty-one have either enacted or passed bills or resolutions concerning aspects of AI.[125] Since states like California or New York have dozens of AI bills under consideration at the moment, this Section can only identify general trends emerging all throughout the country. One outstanding example is the so-called Colorado AI Law, set to enter into force in February 2026, which is one of the first comprehensive AI laws in the United States and "imposes sweeping obligations on both AI system deployers and developers doing business in Colorado, including a duty of reasonable care to protect Colorado residents from any know or reasonably foreseeable risks."[126] Areas of particular legislative attention have been the protection of data privacy, discriminatory AI practices (especially in hiring and credit

[120] Luke Rushing & Samuel Lowry, *Generative AI Litigation: A One-Year Check-In*, AM. BAR ASSOC. (May 9, 2024), https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2024/spring/generative-ai-litigation-one-year-check-in [https://perma.cc/7SEV-S8YQ]; *see also* Bruce Barcott, *AI Lawsuits Worth Watching: A Curated Guide*, TECH POL'Y (July , 2024), https://www.techpolicy.press/ai-lawsuits-worth-watching-a-curated-guide [https://perma.cc/9FTV-BVQK].

[121] *Id.*

[122] *See, e.g.*, Class Action Complaint, P.M. v. OpenAI LP, Dkt. No. 3:23-CV-03199 (N.D. Cal. June 28, 2023); Class Action Complaint, J.L. v. Google, Dkt. No. 3:23-cv-03440 (N.D. Cal. July 11, 2023).

[123] *See, e.g.*, N.Y. Times Co. v. Microsoft Corp., Dkt. No. 1:23-cv-11195 (S.D.N.Y. Dec. 27, 2023); Amended Complaint, Authors Guild v. OpenAI Inc., Dkt. No. 1:23-cv-08292 (S.D.N.Y. Dec. 5, 2023); Complaint, Andersen v. Stability AI Ltd., Dkt. No. 3:23-cv-00201 (N.D. Cal. Jan. 13, 2023); Class Action Complaint, DOE 1 v. GitHub, Inc., Dkt. No. 4:22-cv-06823 (N.D. Cal. Nov. 3, 2022); Class Action Complaint, Tremblay v. OpenAI, Inc., Dkt. No. 3:23-cv-03223 (N.D. Cal. June 28, 2023); Complaint, Silverman v. OpenAI, Inc., Dkt. No. 3:23-cv-03416 (N.D. Cal. July 7, 2023); Amended Complaint, Getty Images (US), Inc. v. Stability AI, Inc., Dkt. No. 1:23-cv-00135 (D. Del. Mar. 29, 2023).

[124] *See* Complaint for Damages, Jack Flora v. Prisma Labs Inc., Dkt. No. 3:23-cv-00680 (N.D. Cal. Feb. 15, 2023); Amended Complaint, Walters v. OpenAI, L.L.C., Dkt. No. 1:23-CV-03122 (N.D. Ga. Sept. 8, 2023) (alleging libelous actions by ChatGPT which produced text, eventually used by a journalist for reporting on a legal case, that the plaintiff was accused of embezzlement when he was not).

[125] For an overview, see Mahdavi, La Lama & Auty, *supra* note 93; *see also Artificial Intelligence 2024 Legislation*, NAT'L CONF. STATE LEGISLATURES (Sept. 9, 2024), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation [https://perma.cc/L53B-MUBY].

[126] Avi Gesser et al., *Recently Enacted AI Law in Colorado: Yet Another Reason to Implement an AI Governance Program*, PROGRAM ON CORP. COMPLIANCE & ENF'T (June 20, 2024), https://wp.nyu.edu/compliance_enforcement/2024/06/20/recently-enacted-ai-law-in-colorado-yet-another-reason-to-implement-an-ai-governance-program [https://perma.cc/X2JJ-GRTR].

reporting), and election integrity.[127] Measures adopted by states range from the mere appropriation of funds, the creation of AI task forces, and the regulation of government uses, to the enactment of new AI crimes like the "fraudulent use of deepfakes."[128] Altogether, this provides a considerable challenge to corporations doing business on a national level as they need to monitor dozens of emerging legislative initiatives across more than 50 jurisdictions to avoid potential liability as plaintiffs' lawyers are on the lookout for the most favorable state laws to begin litigation.[129]

IV. CONCLUSION, OUTLOOK, AND RECOMMENDATIONS

This Article has provided a brief overview of contrasting approaches the two most important global jurisdictions for AI regulation have adopted. On the European side, the EU AI Act attempts to provide a proactive and comprehensive regulatory framework that mitigates potential risks while still leaving sufficient room for technological innovation. On the American side, a much more piecemeal and decentralized approach has emerged where federal agencies, courts, and state legislatures react to the emerging challenges of AI on a case-by-case basis. What both approaches have in common is that they are trying to regulate a technology that is still emerging. Their reactions, however, follow markedly different approaches—one that is forward-looking and all-encompassing in the EU and one that is narrowly tailored and cautious in the United States.

Is it possible to pass judgment on which approach is more promising from a corporate compliance perspective? As so often in the early stages of a new compliance movement, a clear answer has not emerged. While the EU AI Act provides one unified framework with extensive and detailed obligations and a set timeframe, allowing corporate actors to implement new compliance measures, many of the Act's definitions and requirements are sufficiently ambiguous to have a hampering effect on an AI industry that is already lagging behind. Also, the burdensome documentation, information, and reporting requirements for high-risk AI systems will only add to what corporations perceive as an overburdening bureaucracy, especially to the detriment of smaller entities and startups lacking the manpower for effective compliance. The American approach, on the other side, comes with its own challenges. While the case-by-case, decentralized approach appears to leave corporate actors considerable room for innovation, they currently operate in a legal sphere of uncertainty, with dozens of federal agencies and states promulgating new rules on a regular basis. This, in turn, leads to high monitoring costs and potential exposure to litigation or agency enforcement for practices that one thought were legal. Overall, transnational corporations operating on both sides of the Atlantic have to contend with the "worst of two worlds" as they face the extensive compliance requirements of the EU AI Act and are also exposed to the uncertainty of the current U.S. approach. More international cooperation would be desirable.

[127] Lawrence Norden, *States Take the Lead on Regulating Artificial Intelligence: Trends in State Legislation Could Guide Congress's Approach to Regulating this New Technology*, BRENNAN CTR. (Nov. 6, 2023), https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-artificial-intelligence [https://perma.cc/34DV-FEXL].

[128] *Artificial Intelligence 2024 Legislation*, *supra* note 125.

[129] Hope Anderson, Earl Comstock & Erin Hanson, *AI Watch: Global Regulatory Tracker—United States*, WHITE & CASE (May 13, 2024), https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states [https://perma.cc/XJ2X-M55B].

However, corporations can adopt several concrete steps that will allow them to confront the current uncertainty and integrate AI risks into their overall compliance programs.[130] On the most basic level, corporate actors should begin by compiling a central inventory of all AI systems they use and rank the systems' respective compliance risks. A particular focus should be devoted to high-risk systems (especially the systems prohibited in the EU), as all regulators see them as an enforcement priority.[131] Relatedly, compliance officers should begin monitoring their respective jurisdictions for new developments by signing up for legislative newsletters, industry publications, and their law firm's client alerts. On the institutional level, clear monitoring responsibilities for identifying and assessing AI risks should be assigned to one or multiple persons.[132] Depending on a business's degree of complexity or exposure to high-risk AI models, a cross-institutional AI-compliance committee should be considered. Additionally, clear AI policies "outlin[ing] expectations and any prohibitions or limitations on employees' use of AI" should be adopted in tandem with an overall AI-compliance strategy that should, at a minimum, include employee training and documentation to be prepared for future audits.[133] Without a doubt, the age of artificial-intelligence compliance has arrived, and despite divergent regulatory approaches and the uncertainty they bring, compliance departments should not sit idle but act proactively.

[130] The recommendations in this paragraph are loosely adopted from Melissa MacGregor et al., *Achieving Sensible AI Regulation*, DEBEVOISE & PLIMPTON (July 18, 2023), https://www.debevoise.com/-/media/files/insights/publications/2023/07/18--achieving-sensible-ai-regulation.pdf [].

[131] Anderson, Comstock & Hanson, *supra* note 129.

[132] MacGregor, *supra* note 130.

[133] Avi Gesser et al., *Giving AI Governance a Risk-Based Approach*, DEBEVOISE & PLIMPTON (Nov. 2023), https://www.debevoise.com/insights/publications/2023/11/giving-ai-governance-a-risk-based-approach [https://perma.cc/68SZ-JA6J].

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

COMPLIANCE STANDARDS IN THE ACQUISITION PRACTICE OF ARCHAEOLOGICAL COLLECTIONS AND MUSEUMS

The trade in archaeological cultural goods against the background of their protection from destruction and illegal transfer

Yannick Neuhaus, Philipp Karger, Demian Frank

AUTHORS

Dr. Yannick Neuhaus is a lawyer in the field of commercial and medical criminal law. He studied law, art history and archaeology at the Westphalian Wilhelms University in Münster. In addition to medical and commercial criminal law, his professional interests include criminal law relating to the arts.

Philipp Karger is currently majoring in the history of law at the Ludwig-Maximilians-Universität in Munich. His professional interests include art law, particularly in the context of restitutions and archaeological debates.

Demian Frank is a sociologist working in research since 2017. He studied sociology and political science at the Johannes Gutenberg University Mainz and the Goethe University Frankfurt. In the field of law, he works in the investigation of criminal behavior within organizations.

The authors are employees of the law firm Kanzlei für Wirtschafts- & Medizinstrafrecht of Professor Dr. Hendrik Schneider in Wiesbaden, Germany.

TABLE OF CONTENTS

I. THE NEED TO ESTABLISH COMPLIANCE STANDARDS FOR MUSEUMS AND COLLECTIONS

The export and import of archaeological objects, as it is the case with other rare or endangered objects, is subject to a differentiated legal regime.[1] For Germany, the legal framework is constituted by International law, European law and national regulations.

It is of the utmost importance to consider the applicable law in the context of every acquisition transaction. The applicable legislation is not always straightforward to ascertain, as it varies depending on the nature and origin of the goods in question, as well as the countries of export and import. The legal framework conditions must therefore be determined for each acquisition or sale, as they are fundamental for the derivation of specific legal obligations as well as the associated compliance standards. Adhering to these frameworks forms the foundation of a compliance culture.[2]

Compliance with acquisition standards is a prerequisite for further legal use of property, for example by exhibiting or reselling it. In addition to financial losses, criminal or civil claims, non-compliance can above all lead to damaging a good reputation. which is important for every player in the arts and culture, including auction houses and private collectors.

II. REASONS FOR THE DENSITY OF REGULATION: THREATS TO AND PROTECTION OF ARCHAEOLOGICAL CULTURAL PROPERTY

A. Contemporary witnesses and the heritage of mankind

Archaeological cultural goods[3] and archaeological objects as a whole are of fundamental importance to humanity. They are evidence of and symbols for past epochs which, in addition to the scientific interest that archaeologists have in them, are increasingly being used for historical communication and are appreciated with growing interest by society at large.[4]

In fact it is the archaeologist who fulfills an important educational function through the appropriate presentation of finds and findings. Sites such as Pompeii or Machu Pichu have long since become tourist strongholds that are visited by countless visitors every year. The resulting (ab)use has led to efforts being made to channel or stem the flow of visitors.[5]

[1] Neuhaus, Der Schutz archäologischer Objekte vor illegalem Import, 2024, p. 178 et seq.; Fechner, Rechtlicher Schutz archäologischen Kulturguts, 1991, p. 114-122; Fechner., in: von der Decken/Fechner/Weller (Eds.), Kulturgutschutzgesetz, Nomos Kommentar, 2021, sec. 28 Rn. 5.

[2] Moosmeyer/Lösler, Corporate Compliance, 4. Ed. 2024, p. 397 et seq.

[3] Definition: Archaeological cultural goods represent a sub-area of cultural goods, whereby a strict distinction must be made between the common usage and the legal term "cultural goods".

[4] Neuhaus, Der Schutz archäologischer Objekte vor illegalem Import, 2024, p. 1.

[5] Fechner, Rechtlicher Schutz archäologischen Kulturguts, 1991, p. 114; Gornig, Der internationale Kulturgüterschutz, in: Gornig/Horn/Murswiek (Eds.), Kulturgüterschutz – internationale und nationale Aspekte, 2007, p. 17-63, 38; Goring, Schutz der Kulturgüter vor Umwelteinflüssen und natürlichen Gefahren im nationalen und internationalen Recht, in: Wittinger/Wendt/Ress (Eds.), FS Fiedler, 2011, p. 389-413, 391 et seq.

Scientists are often engaged in providing technical knowledge and creating an understanding and appreciation of the material legacies of past cultures.

A crucial element of this process is to promote the notion that archaeological cultural assets are inherently deserving of protection, as they possess a unique and irreplaceable qualityFor example, every ancient coin, every Mesopotamian scroll seal tells a story and – once put into context – provides information about political, military and social circumstances.[6]

Archaeological objects acquire a special significance primarily through their contextualization, their relationship to other objects, to their respective sites and places of discovery.[7] This allows us to build hypotheses and draw far-reaching conclusions about the use of the object in its cultural context and thus about ancient practices and ideas to further our knowledge of ancient cultures. Removing an object from the context in which it was found makes such an attribution almost impossible and at least more difficult.[8]

B. About the two threat scenarios

Archaeological objects are exposed to two threats: The destruction of the substance and local transportation, which – if this happens undocumented – diminishes the scientific knowledge gained. [9]

There are plenty of examples of both threat scenarios turning into reality. In the crisis regions of the Near and Middle East in particular, there has been and still is looting of ancient sites, plundering of museums and sometimes possibly religiously motivated willful destruction of objects.[10] Take, for example, the demolition of the Buddha statues in Bamiyan. But also in the course of economic development, cultural assets that are part of the cultural heritage of mankind as a whole are repeatedly damaged or destroyed.

The repercussions of ongoing construction work on dams in Egypt, Syria, Turkey or Iraq are examples. And also Western countries - above all Germany - are under constant threat from illegal excavations.

Therefore, the threat to archaeological objects posed by illegal removal has recently come under greater and more continuous public scrutiny. Precarious economic situations and political instability in many countries are risks to the protection of cultural property. But also improved technical possibilities and the general pursuit of profit have led to an increase in illicit excavations and illegal trade in the

[6] von Schorlemer, Kulturgutzerstörung, 2017, p. 44.

[7] Fechner, Rechtlicher Schutz archäologischen Kulturguts, 1991, p. 14 et seq.; Gornig, Der internationale Kulturgüterschutz, in: Gornig/Horn/Murswiek (Eds.), Kulturgüterschutz – internationale und nationale Aspekte, 2007, p. 17-63, 30.

[8] Fechner, Rechtlicher Schutz archäologischen Kulturguts, 1991, p.14 et seq.; Gornig, Der internationale Kulturgüterschutz, in: Gornig/ Horn/Murswiek (Eds.), Kulturgüterschutz – internationale und nationale Aspekte, 2007, p. 17-63, 30.

[9] Fechner, Rechtlicher Schutz archäologischen Kulturguts, 1991, p.14 et seq.; Gornig, Der internationale Kulturgüterschutz, in: Gornig/Horn/Murswiek (Eds.), Kulturgüterschutz – internationale und nationale Aspekte, 2007, p. 17-63, 30.

[10] Bogdanos/Patrick, Thieves of Baghdad: One Marine's Passion for Ancient Civilizations and the Journey to Recover the World's Greatest Stolen Treasures, 2005; echner, Rechtlicher Schutz archäologischen Kulturguts, 1991, p. 12. To the destruction of cultural property, motivated by jihadism: von Schorlemer, Kulturgutzerstoerung, 2017, p. 54-57, 133 et seq.

last two decades.[11] UNESCO estimates the global illegal trade in archaeological objects at a total volume of 6 billion dollars.[12] This is said to be the third largest illegal market after the arms and drugs trade.

Against this background, comprehensive protection of cultural property must pursue two objectives: Firstly, it is about substance protection, in which cultural assets are to be protected from destruction. Secondly, it is about preserving the local connection of an object to the context in which it was found.[13]

C. Control function of the legal framework

The legal framework serves these protection purposes. As a rule, however, this does not mean that every export, import or acquisition is outlawed. The decisive factor is compliance with the framework conditions for precisely these actions.

III. Legal framework for the import of archaeological cultural property

A. International legal framework

In recent years, legal regulations have emerged under international and European law that serve both protection objectives.

The Hague Convention of 1954[14] and the so-called Valetta Convention, for example, pursue the protection of cultural property. However, the Hague Convention also serves to protect property.[15]

A general prohibition of removal can be found in Art. 4 para. 3 sentence 1 of the Hague Convention. Accordingly, any kind of theft, looting or other unlawful seizure of cultural property as well as any unreasonable destruction of such property must be prohibited, prevented and, if necessary, stopped.

The prohibition of removal serves to protect territorial allocation, as the prohibition relates solely to the immediate location of an object, which may not be changed even in the event of armed conflict.[16]

[11] Emberling/Hanson (Eds.), Catastrophe, The Looting and Destruction of Iraq's Past, 2008; Wessel, Das schmutzige Geschäft mit der Antike, 2015, p. 37 et seq.; Bogdanos/Patrick, Thieves of Baghdad: One Marine's Passion for Ancient Civilizations and the Journey to Recover the World's Greatest Stolen Treasures, 2005.

[12] UNESCO, CLT/2011/CONF. 207/6, p. 2.

[13] Fechner, Prinzipien des Kulturgüterschutzes, in: Fechner/Oppermann/Prott (Eds.), Prinzipien des Kulturgüterschutzes, 1996, p. 27; Odendahl, Kulturgüterschutz, 2005, p. 407 et seq.

[14] Convention for the Protection of Cultural Property in the Event of Armed Conflict with Regulations for its Execution. The Hague, 14 May 1954. Protocol to the Convention for the Protection of Cultural Property in the Event of Armed Conflict, and resolutions of the Conference. The Hague, 14 May 1954.

[15] Neuhaus, Der Schutz archäologischer Objekte vor illegalem Import, 2024, p. 39 et seq., 50.

[16] Odendahl, Kulturgüterschutz, 2005, p. 120; Radloff, Kulturgüterrecht, 2013, p. 235 et seq.

The protection of archaeological cultural property from illegal removal is pursued by the UNESCO Convention of 1970. This Convention[17] as part of international treaty law is intended to extend the protection of cultural property to illegal imports with regard to the Hague Convention, which focused on the export of cultural property.[18] For the first time, the standard for assessing legality within the meaning of the UNESCO Convention focusses on the law of the country of origin. This intends to strengthen national export restrictions and make them internationally effective.[19]

The import-related provision in Art. 7 b i) obliges the States/Parties to prohibit the import of cultural property that has been stolen from a museum or a religious or secular public monument or a similar institution in another State Party after the entry into force of this Convention for the States concerned. It follows, that legal ownership of an object must be proven and that the object is part of the inventory of a states' institution. The object must therefore be inventoried.[20]

It follows from this that illegally exported cultural property cannot be legally imported.[21] The importing state must therefore comply with the legal provisions of the state of origin.[22]

B. European legal framework

In addition, the EU has issued three regulations that prohibit the illegal transfer of archaeological cultural objects. These include the Iraq Regulation[23] and the Syria Regulation[24], which both relate to the armed conflicts in these states and prohibit the illegal export of objects from these states.

Article 3 (1) prohibits the import, export or the introduction into the territory of the EU of Iraqi cultural property and other items of archaeological, historical, cultural, rare scientific and religious importance including those items listed in Annex II, if they have been illegally removed from locations in Iraq.[25]

Similarly, Art. 11c of the Syria Regulation prohibits the import, export, transfer or provision of related brokering services of cultural property belonging to the cultural property of Syria and other objects of archaeological, historical, cultural, special scientific or religious interest, including those listed in Annex XI, where there is reason to believe that the items have been removed from Syria without the consent of their rightful owners or in violation of Syrian or international law. In particular, if the items are part of

[17] Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property. Paris, 14 November 1970.Transformed in the Federal Republic of Germany: Gesetz zu dem Übereinkommen vom 14.11.1970 über Maßnahmen zum Verbot und zur Verhütung der rechtswidrigen Einfuhr, Ausfuhr und Übereignung von Kulturgut vom 20.04. 2007 (BGBl. 2007 II, p. 626, 627).

[18] Radloff, Kulturgüterrecht, 2013, p. 238.

[19] Odendahl, Kulturgüterschutz, 2005, p. 134 et seq.; Radloff, Kulturgüterrecht, 2013, p. 240; Prott, Strengths and Weaknesses of the 1970 Convention: An Evaluation 40 years after its adoption, 2012.

[20] Similar: Thorn, Internationaler Kulturgüterschutz nach der UNIDROIT-Konvention, 2005, p. 64 sowie Hipp, Schutz von Kulturgütern in Deutschland, 2000, p. 140.

[21] Hipp, Schutz von Kulturgütern in Deutschland, 2000, p. 140; Odendahl, Kulturgüterschutz, 2005, p. 134.

[22] Odendahl, Kulturgüterschutz, 2005, p. 134; *Radloff*, Kulturgüterrecht, 2013, p. 241.

[23] Regulation (EC) No 1210/2003.

[24] Regulation (EU) No 36/2012.

[25] Consider the differentiation „the import of or the introduction into the territory of the Community". See also: *von Schorlemer*, Kulturgutzerstörung, 2016, p. 311 et seq.

public collections listed in the inventories of Syrian museums, archives or libraries worthy of preservation or in the inventories of Syrian religious institutions.

The regulations to prevent illegal imports from the states of Iraq and Syria are supplemented by the Import-Regulation, which broadens the scope of protection and extends illegal imports not to crisis states but to third countries and is therefore intended to prevent illegal imports more comprehensively and generally.

The final version of the Import-Regulation came into force on 28.06.2019. The aim of this regulation is to establish common rules for trade with third countries in order to ensure effective protection against the illicit trafficking of cultural goods, their loss or destruction, the preservation of the cultural heritage of humanity and the prevention of terrorist financing and money laundering through the sale of looted cultural goods to buyers in the Union.[26]

The Import Regulation defines cultural goods in Art. 2 No. 1 and provides for a three-tier system for the introduction[27] and import of cultural goods[28], consisting of a ban, an import licence or an importer statement[29]. The regulation differentiates between the objects listed in Annexes A, B and C.

The movement ban does not stipulate an age or value limit. The import licence, on the other hand, is based on an age limit of 250 years for archaeological objects (Annex Part B.) but does not stipulate a value limit.

C. Regulations in national law using the example of the Federal Republic of Germany

In addition to supranational regulations, many countries have laws that regulate the import and export of cultural objects and make these processes subject to licenses and certificates.[30] In many countries, these regulations date back to the 19th century, such as in Egypt (1858) or the Ottoman Empire (1884), where corresponding antiquities laws were developed based on the European model.

In Germany, the Cultural Property Protection Act regulates the import and export of archaeological cultural property. The KGSG[31] came into force on 06.08.2016.[32] The aim of the new import-regulation was to make the illegal trade in cultural property from other countries, especially third countries, more

[26] Recital (1) of the Import-Regulation; Hemeier/Hilgert, ILLICID, 2020, p. 31 et seq.

[27] Art. 2 no. 2 Import-Regulation.

[28] Art. 2 no. 3 Import-Regulation.

[29] Fechner, in: von der Decken/Fechner/Weller (Eds.), Kulturgutschutzgesetz, Nomos Kommentar, 2021, sec. 28 Mn. 19; Fechner, in: Martin/Krautzberger (Eds.), Handbuch Denkmalschutz und Denkmalpflege, 5. Ed.2022, Part B IV. Kulturgüterschutz, Rn. 143.

[30] Neuhaus, Der Schutz archäologischer Objekte vor illegalem Import, 2024, p. 133 et seq. with examples.

[31] "Kulturgutschutzgesetz vom 31. Juli 2 016 (BGBl. I S. 1914), das zuletzt durch Artikel 40 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist"

[32] Zum Hintergrund der Novellierung mit einem kursorischen Überblick über die Genese des KGSG: Fechner, in: Martin/Krautzberger (Eds.), Handbuch Denkmalschutz und Denkmalpflege,5. Ed., 2022, Part B IV. Kulturgüterschutz, Mn. 153 et seq.

difficult or at best prevent it.[33] The import regulations therefore pursue a preventive protection approach. "Import" within the meaning of the KGSG means the introduction of cultural property into the federal territory.[34] The import ban in Section 28 KGSG is the adapted new version of the former Section 14 KultGütRückG and serves to implement the principles of International and European law already discussed.[35] A case group is provided for each of these case group in Number 1 to 3 of Sec. 28 KGSG.[36]

IV. INTERESTS AND CHALLENGES FOR MARKET PLAYERS

This increasing legalization can be considered a positive development, as international agreements and Europe-wide regulations have led to a consolidation of the legal protection of archaeological cultural property. Nevertheless, for those involved in the legal trade, which includes not only art and antiquities dealers but also state collections, museums and research institutes, compliance with regulations also poses a challenge, given their diversity.[37] In addition to the common interest in preventing destruction and illegal trade, there is still a legitimate interest in legal trade and the possibility of acquiring archaeological cultural objects for collection purposes.[38]

It is sometimes a complex matter as to whether a particular object may be acquired. The challenges here are both legal and factual. First of all, the applicable law must be identified. For example, the UNESCO Convention of 1970 and the Import Regulation refer to the national legislation of the countries of origin. Potential buyers are faced with the actual question of where an archaeological object comes from. Accompanying certificates are sometimes forged or use false information to disguise the provenance, which thereby cannot always be undoubtfully verified.

However, in such a case it cannot necessarily be concluded that the object is from a looted excavation or that it was stolen from a museum and then exported illegally. Particularly in the case of objects from old collections, such evidence often is no longer available, has been lost or can no longer be provided.

The trade in art and antiquities, which also offers archaeological objects, is itself committed to the protection of cultural property.[39] For dealers, the need for legal clarity is paramount.[40] The multitude of regulations and definitions presents dealers with legal challenges, primarily in the form of restitution obligations and the associated financial risks, including loss of reputation and criminal prosecution.[41]

---

[33] Bundesbeauftragte für Kultur und Medien (BKM), Das neue Kulturgutschutzgesetz, Handreichung für die Praxis, 2017, p. 25; BT-Drs. 18/7456, p.91 anknüpfend: Garbers-von Boehm, in: Elmenhorst/Wiese (Eds.), Kulturgutschutzgesetz, Kommentar, 2018, sec. 28 Mn. 2.

[34] Sec. 2 Abs.1 Nr. 5 KGSG.

[35] BT-Drs. 18/7456, p. 90.

[36] Garbers-von Boehm, in: Elmenhorst/Wiese (Eds.), Kulturgutschutzgesetz, Kommentar, 2018, sec. 28 Mn. 7; Fechner, in: Martin/Krautzberger (Eds.), Handbuch Denkmalschutz und Denkmalpflege, 5. Ed. 2022, Part B IV. Kulturgüterschutz, Mn. 196.

[37] Neuhaus, Der Schutz archäologischer Objekte vor illegalem Import, 2024, p. 26.

[38] Neuhaus, Der Schutz archäologischer Objekte vor illegalem Import, 2024, p. 24 et seq.

[39] Sturm, KUR 2016, P.73-79, 73. Vgl. auch: Cahn, Der seriöse Kunsthandel ist sich seiner Verantwortung bewusst, in: Flashar (Eds.), Bewahren als Problem, 2000, p.47-57, 48.

[40] Kreutzer, Kunst und Auktionen 04/2018, p. 12-13, 13.

[41] Anton, Neuer Schutz archäologischer Kulturgüter, in: Wittinger/Wendt/Ress (Eds.), FS Fiedler, 2011, p. 319-351, 321 et seq.; Sturm, KUR 2016, p. 73-79; 77 et seq.; Kohlhaas, Kunst und Auktionen 03/2018, p. 12-13.

For some time now, actors in the art trade have made plans to develop their own rules of conduct and to use these as a guide.[42] Answering the question of legal certainty appears to be the most urgent issue for market participants.[43] In addition, there is the demand for free tradability, which also includes the possibility of importing. This can be justified, for example, by the fact that free trade can also serve the exchange and appreciation of cultural property.[44] However, this poses a risk to cultural ties, with the result that the passage of time makes attribution difficult or impossible.[45]

The aim remains to create a legal framework that provides sufficient security for owners and dealers without losing sight of the objectives of cultural property protection. This includes, in particular, the areas of legal acquisition, documentation and verifiability - and therefore unassailability - which must be taken into account.

V. SELF-PROTECTION THROUGH COMPLIANCE

Against this backdrop, market players began to establish their own standards for acquisition practice - for example through ICOM.[46]

And also museums, state collections and research institutions are now tending to draw up codes of conduct for their acquisition practices on their own initiative. In addition to the necessary compliance with applicable law, this also serves the goal of being able to take individual sector- and institution-specific characteristics into account.

The measures of these initiatives are based on five fundamental principles which will be examined individually below:

- Principle of legality,
- Principle of transparency,
- Principle of documentation,
- Standardisation principle,
- Criteria principle.

A. Principle of Legality: compliance with applicable law

Compliance with applicable law is essential. Every importer and buyer must be aware of the relevant standards and regulations. This applies to both the importing country and the exporting country due

[42] Cahn, Der seriöse Kunsthandel ist sich seiner Verantwortung bewusst, in: Flashar (Eds.), Bewahren als Problem, 2000, p. 47-57, 48 et seq.; Strobl, Kulturgüterrelevante Verhaltenskodizes, 2018, p. 125 et seq.

[43] Anton, Neuer Schutz archäologischer Kulturgüter, in: Wittinger/Wendt/Ress (Eds.), FS Fiedler, 2011, p. 319-351, 322; e.g.: Kohlhaas, Kunst und Auktionen 03/2019, p. 12-13, 12; Kohlhaas, Kunst und Auktionen 03/2019, p. 14-15, 14.

[44] Radloff, Kulturgüterrecht, 2013, p. 142.

[45] Radloff, Kulturgüterrecht, 2013, p. 143.

[46] International Council of Museums; https://www.museumsbund.de/wp-content/uploads/2023/07/dmb-checkliste-standards-fuer-museen-sammeln.pdf

to the reference to the UNESCO Convention of 1970 and member state implementation in national law.

A prerequisite for the acquisition is knowledge of the legal framework. This includes not only prohibitions and restrictions considering the trade of certain objects, but also licensing requirements for export licenses. On an operative level, it is advisable to carry out a structured examination based on a matrix created individually for each object and thus for each acquisition process, which takes into account the interdependencies of international, european and national regulations. This is necessary because different regulations may apply to objects from the same country of origin due to age and value limits, for example. In order to demonstrate compliance with applicable law, measures taken to adhere to identified relevant regulations should be documented and archived.

Ideally, relevant legal documents (of importing and exporting countries) are available to all parties involved in the trade in a language of their understanding.

B. Transparency Principle

Transparency is a fundamental requirement for ensuring accountability and fostering trust between institutions as well as between institutions and the public. Trust is at the core of any economic relationship and traders benefit from a trustworthy reputation. Furthermore, institutions should participate in public discourse and consultations pertaining to acquisitions, particularly for items with a contested historical or cultural significance.

Acquisition processes of state collections and museums should be kept transparent. After acquisition, objects should be made available for further research not only for in-house research but also in cooperation with other institutions. This could further knowledge about an object and support its transparent handling in future acquisitions and sales.

The country of origin and the circumstances of acquisition should be disclosed. These could be disclosed on the homepage, at least in outline. The price and seller do not necessarily have to be explicitly stated.

C. Documentation Principle

For internal documentation, it is important to have a written record of the entire acquisition process that is comprehensible in retrospect. This also includes the initiation of the acquisition, any notes from discussions, background information on the circumstances of the find. Furthermore, it is pivotal to document the rationale behind each decision made during the process, including any ethical considerations and the criteria used to evaluate the item's significance.

D. Standardisation Principle: Standardisation of contracts and internal documents

Further safeguarding is possible through standardized documents and contracts that have each undergone a legal review. This should be repeated at regular intervals of around 2 years to take account of legal changes.

Corresponding legal contracts include loan agreements, gift agreements and purchase agreements. The use of standardised contracts facilitates the reduction of ambiguity and ensures consistency across all transactions. By employing uniform language and provisions, institutions can minimise the risk of misunderstandings and disputes. Furthermore, standardisation enhances efficiency, allowing for the quicker processing and execution of agreements.

E. Criteria Principle: definition of acquisition criteria

Finally, it is advisable to create a standard operating procedure that applies to every acquisition process, and which is based on specific principles. These principles should be determined in a transparent process. They could include for example that so-called unaccompanied objects, i.e. those without proof of origin and export licenses, or cultural objects from war and crisis regions are not acquired. In any trade, each contracting party could state their acknowledgement of these principles.

This list of criteria could be published in order to comply with the principle of transparency.

IV. CONLCUSION

In view of the variety of regulations at different, overlapping levels, a compliance management system tailored to individual needs is essential. Especially when it comes to purchase or resale decision making. After implementation, however, it should not be forgotten that the compliance management system must be regularly reviewed to ensure that it is up to date – especially with regard to the legal framework both in Germany and abroad.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

PROTECTION OF HUMAN RIGHTS IN THE BUSINESS SECTOR

COMPLIANCE INTERFACE IN THE SUPPLY CHAIN ACT AND MONEY LAUNDERING ACT

Alexander Sellmayer, Anselm Fischer

AUTHORS

Alexander Sellmayer is an associate at the law firm rixe.law in Düsseldorf. Rixe.law advises in all areas of commercial and tax criminal law, as well as select areas of general criminal law. In addition to traditional criminal defense, rixe.law advises companies and persons acting on their behalf on various issues relating to compliance.

Anselm Fischer is a legal clerk at rixe.law. Before his clerkship he studied law at the University of Münster and Chuo University in Tokyo.

ABSTRACT

This article analyses compliance interfaces between the German Supply Chain Act (short: LkSG), Money Laundering Act (short: GwG) and German Criminal Code (short: StGB) in connection with human rights risks. The authors conclude that remedies taken only in accordance with the LkSG after a human rights risk has been identified may still constitute a compliance violation within the meaning of the GwG or even a criminal liability under Section 261 StGB.

TABLE OF CONTENTS

I. INTRODUCTION

Global enterprises benefit from the ongoing globalization of production processes. At the same time, there is a social consensus in Europe and Germany that there must be no pursuit of profit at any price - especially not at the cost of human rights. Based on this consensus, enterprises design their corporate culture using buzzwords such as "sustainability", "responsibility" and "integrity". This reflects not only the company's commitment to comply with the law, but even beyond the law to more stringent self-imposed ethical principles.

Despite these corporate assurances, the German legislator felt compelled to pass the LkSG in 2021.

First, this article describes the extent to which the LkSG, Section 261 of the German Criminal Code and the GwG protect human rights.

Second, we describe which enterprises are covered by the LkSG and the GwG, what compliance requirements the respective laws impose and what consequences enterprises and employees face in the event of compliance violations.

Third, we present the individual steps that companies can and should take in cases of verified or suspected human rights violations.

This article discusses the current legal situation. Please note that the European Union published its' three-part legislative package to strengthen anti-money laundering rules in the Official Journal of the European Union on June 19th , 2024: (i) The Anti-Money Laundering Regulation, which will replace the German GwG, will come into effect on July 10th, 2027;[1] (ii) the new European Anti-Money Laundering Authority is scheduled to begin operations on July 1st, 2025;[2] (iii) Member States must implement the requirements of the 6th Anti-Money Laundering Directive into national law by July 10th, 2027.[3]

II. SCOPE OF THE LEGAL PROTECTION OF HUMAN RIGHTS

A. The Supply Chain Act

The Supply Chain Act has been in force since January 1st, 2023.[4] According to the law's reasoning, this law

[1] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Article 90.
[2] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, Article 108.
[3] Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849, Article 78.
[4] BGBl. 2021 I 2959, Article 5 Subsection 1.

> "serves to improve the international human rights situation by laying down requirements for the responsible management of supply chains for certain companies."[5]

The Supply Chain Act was passed to protect human rights. According to Section 2 Subsection 1 and its annex, the Act's scope of protection includes several important international conventions for the protection of human rights.[6]

B. Section 261 of the German Criminal Code

Section 261 Subsection 1 1st Sentence and Subsection 2 describe criminal acts as follows:

> "Whoever, in respect of an object derived from an unlawful act,
> 1. hides it
> 2. exchanges, transfers or takes it with the intent of preventing it being found, confiscated or its origin being investigated,
> 3. procures it for themselves or a third party or
> 4. keeps or uses it for themselves or a third party if they were aware of its origin at the time of obtaining possession of it incurs a penalty of imprisonment for a term not exceeding five years or a fine."

Subsection 2:

> "Whoever hides or conceals facts which may be of relevance to an object as referred to in subsection (1) being found, confiscated or its origin being investigated incurs the same penalty."[7]

"Object" of Section 261 StGB are all legal objects that have an asset value;[8] including intangible objects such as claims and rights.[9] This object must derive from an unlawful act of any kind (so-called "All-Crimes-Approach").[10]

It is particularly important for companies to recognize that an economic perspective is decisive here: objects are to be regarded as tainted if (i) they can be traced back to the predicate offense by means of a causal connection[11] and (ii) are not essentially based on the conduct of a third party.[12] Further, once

[5] BT-Drs. 19/28649, p 2, free translation.

[6] e. g.: Convention No. 29 of the International Labour Organization "Forced Labour Convention", 1930 and its 2014 Protocol; Convention No. 182 of the International Labour Organization "Worst Forms of Child Labour Convention", 1999. The environmental protection pursued by the LkSG is not considered in this article.

[7] Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 22 November 2021 (Federal Law Gazette I, p. 4906); Translation provided by Prof. Dr. Michael Bohlander. Translation completely revised and regularly updated by Ute Reusch (Aug. 14, 2024, 03:07 PM), https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2435.

[8] BT-Drs. 12/989, p 27; Ruhmannseder, BeckOK StGB, Section 261, mn 9 (v. Heintschel-Heinegg et al eds., 62nd ed. 2024).

[9] El-Ghazi, Geldwäschegesetz, Section 261, mn 48 (Herzog, 5th ed. 2023).

[10] BT-Drs. 19/24180, p 42; Ruhmannseder, BeckOK StGB, Section 261, mn10 (v. Heintschel-Heinegg et al eds., 62nd ed. 2024).

[11] German Federal Court of Justice, Resolution of Feb. 18th, 2009 – 1 StR 4/09 and Resolution of Nov. 26th 2009 – 5 StR 91/09; BT-Drs. 19/24180, p 29.

[12] BT-Drs. 12/3533, p 12; German Federal Court of Justice, Judgement of Aug. 15th, 2018 – 5 StR 100/18.

tainted, an asset cannot be rectified by simply mixing it with other legal financial resources.[13] According to the German Federal Court of Justice, exceptions may apply if the share of the predicate offenses is completely insignificant from an economic point of view.[14] Thus, also an indirect chain of conduct is covered by Section 261 StGB.[15]

Section 261 Subsection 9 StGB recognizes the geographical scope of companies' activities, typically spanning across multiple jurisdictions: acts committed abroad can also be suitable predicate offenses for money laundering.[16] Subsection 9 equates objects that originate from an offense committed abroad with an object within the meaning of Section 261 Subsection 1 StGB, if the offense – had it been committed within the German jurisdiction – would also be an illegal act under German criminal law.[17] In addition, the offense must be punishable at the place where it was committed (Subsection 9 No. 1.) or - so an examination of the respective national criminal law is unnecessary - it must be punishable under one of the European Union provisions mentioned in Subsection 9 No. 2.[18]

The German legislator has at least indirectly[19] taken the protection of human rights into account by referring to European regulations and conventions in Section 261 Subsection 9 No. 2 StGB. In some cases, these European standards were expressly adopted to protect human rights. This applies to the frameworks mentioned in Section 261 Subsection 9 No. 2 lit. b) (protection of the right to asylum)[20], lit. f) (combating human trafficking and forced labor)[21], lit. g) (combating the sexual exploitation of children)22 and lit. h) (combating terrorism).[23]

Furthermore, when assessing the suspect's intent, Subsection 6 1st Sentence must be considered:

> "Whoever, in the cases under subsections (1) or (2), is recklessly unaware of the fact that the object is one as referred to in subsection (1) incurs a penalty of imprisonment for a term not exceeding two years or a fine."[24]

[13] BT-Drs. 19/24180, p 20.

[14] German Federal Court of Justice, Resolution of May 20th, 2015– 1 StR 33/15; BT-Drs. 19/24180, p 29.

[15] Ruhmannseder, BeckOK StGB, Section 261, mn 15 (v. Heintschel-Heinegg et al eds., 62nd ed. 2024).

[16] BT-Drs. 13/8651, p 12; El-Ghazi, Geldwäschegesetz, Section 261, mn 61 (Herzog, 5th ed. 2023).

[17] Altenhain, Strafgesetzbuch, Section 261, mn 21 (Kindhäuser et al eds., 6th ed. 2023).

[18] Altenhain, Strafgesetzbuch, Section 261, mn 23 (Kindhäuser et al eds., 6th ed. 2023).

[19] However, the protection of human rights was not the legislator's motive for amending Section 261 StGB, but rather Directive 2018/1673/EU gave rise to the amendment; see Altenhain, Strafgesetzbuch, Section 261, mn 4 (Kindhäuser et al eds., 6th ed. 2023).

[20] 2002/946/JHA: Council framework Decision of 28 November 2002 on the strengthening of the penal framework to prevent the facilitation of unauthorised entry, transit and residence, see Article 6.

[21] Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA, see Reasons 7 and 14.

[22] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, see Reason 1 and 50.

[23] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017on combating terrorism and replacing Council Framework Decision 2002/475/JHA and mending Council Decision 2005/671/JHA, see Reason 1, 2 and 35.

[24] Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 22 November 2021 (Federal Law Gazette I, p. 4906); Translation provided by Prof. Dr. Michael Bohlander. Translation completely revised and regularly updated by Ute Reusch (Aug. 14, 2024, 04:36 PM), https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2435.

> "The offender acts recklessly if he disregards the obvious possibility that the object originates from an unlawful act due to particular indifference or gross carelessness."[25]

Section 261 Subsection 7 states:

> "Whoever is liable on account of participation in a prior offence incurs a penalty under subsections (1) to (6) only if they put the object into circulation and thereby hide its unlawful origin."[26]

Circulation covers all acts that result in the offender releasing the incriminated object from his actual power of disposal and a third party acquiring actual power of disposal; this includes depositing illegally obtained cash into a bank account or selling valuables.[27]

Hiding its unlawful origin covers all acts,

> "which aim to give an object the appearance of a different (legal) origin or at least to conceal its true origin."[28]

Participation in a prior offence must be assessed, if the company produces objects under circumstances that violate human rights. If, for example, the company sells these objects with a "fair trade" claim, it may no longer be a non-punishable self-money laundering and the persons acting on behalf of the company must expect to be accused of money laundering.

C. The Money Laundering Act

The protection of human rights did not play a distinct role in the first introduction of the GwG[29] in 1993. The main aim of the law was to combat organized crime.[30] The law obliged

> "in particular banks and other traders to identify their customers and to record and store the identification details."[31]

A link to human rights can now be established via the aforementioned amendment to Section 261 StGB. By defining money laundering as a criminal offense pursuant to Section 261 StGB (Section 1 Subsection 1 GwG), the provisions of European law on the protection of human rights are indirectly applied in the Money Laundering Act (Section 261 Subsection 9 StGB).

---

[25] Altenhain, *Strafgesetzbuch*, Section 261, mn 93 (Kindhäuser et al eds., 6th ed. 2023).

[26] *Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 22 November 2021 (Federal Law Gazette I, p. 4906)*; Translation provided by Prof. Dr. Michael Bohlander. Translation completely revised and regularly updated by Ute Reusch (Aug. 14, 2024, 05:36 PM), https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2435.

[27] BT-Drs. 18/6389, p 14.

[28] BT-Drs. 18/6389, p 14, free translation; German Federal Court of Justice, Judgment of July 17th, 2016 – 2 StR 451/15.

[29] Introduced as "Profit Tracing Act" in 1993, since August 2008 known as "Money Laundering Act", see BGBl. 2008 I 1690.

[30] BT-Drs. 12/2704, p 1.

[31] BT-Drs. 12/2704, p 1, free translation.

III. COMPLIANCE DUTIES IN CONNECTION WITH HUMAN RIGHTS ISSUES

A. The Supply Chain Act

1. Scope of Application

Since January 1st, 2024, the LkSG[32] has been applicable to enterprises, regardless of their legal form, which employ at least 1,000 employees in Germany and have either their central administration, their principal place of business, their administrative headquarters, their statutory seat or a domestic branch office in Germany (Section 1 Subsection 1). Section 1 Subsection 2 regulates the calculation of the threshold value when using temporary workers; Subsection 3 is applicable for affiliated enterprises.[33] However, the LkSG can affect any company regardless of the threshold value if certain requirements are met.[34] As soon as a smaller company provides services or products to another company that is subject to the obligations of the LkSG, it is considered a "direct supplier". As such, the smaller company is included in the risk analysis and, if necessary, in preventive measures and remedial action.[35]

2. Due Diligence Obligations

Section 3 Subsection 1 lists the due diligence obligations of enterprises subject to Section 1.[36] These include, among others:

- Conducting appropriate risk analyses (Section 5),
- Issuing a policy on its human rights strategy (Section 6 Subsection 2),
- Taking appropriate preventive measures in its own area of business (Section 6 Subsection 1 and 3) and vis-à-vis their direct suppliers (Section 6 Subsection 4),
- Taking appropriate remedial action (Section 7 Subsection 1 to 3),
- Ensuring an appropriate internal complaints procedure (Section 8),
- Documentation and reporting (Section 10).

According to Section 4 Subsection 1 1st Sentence enterprises must establish an appropriate and effective risk management system to comply with these due diligence obligations. The enterprise must ensure somebody within the enterprise is responsible for monitoring the risk management, for example by appointing a human rights officer (Section 4 Subsection 3).

[32] The German Federal Ministry of Labour and Social Affairs published an English version of the LkSG available at https://www.csr-in-deutschland.de/EN/Business-Human-Rights/Supply-Chain-Act/supply-chain-act.html (Aug. 28th, 2024, 10:10 AM).

[33] With the adoption of the EU Corporate Sustainability Due Diligence Directive (CSDDD) in June 2024, further changes are expected in this area of supply chains. Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859.

[34] Prof. Dr. Michael Nietsch et al eds., Adressatenkreis und sachlicher Anwendungsbereich des neuen Lieferkettensorgfaltspflichtengesetz, Neue Juristische Wochenschrift, 1, 3 (2022).

[35] Federal Office for Economic Affairs and Export Control, Häufige Fragen zum Thema Lieferkettensorgfaltspflichtengesetz, https://www.bafa.de/DE/Lieferketten/FAQ/_functions/faq_table_lieferketten.html?nn=1469838 (Aug. 28th, 2024, 11:45 AM).

[36] Companies not subject to Section 1 LkSG do not have to fulfill these obligations, see Federal Office for Economic Affairs and Export Control, Häufige Fragen zum Thema Lieferkettensorgfaltspflichtengesetz, https://www.bafa.de/DE/Lieferketten/FAQ/_functions/faq_table_lieferketten.html?nn=1469838 (Aug. 28th, 2024, 11:50 AM).

Next, the actual human rights risks are determined in the risk analysis (Section 5).[37] Such a risk analysis is carried out annually. Furthermore, a risk analysis must be carried out ad hoc

> "if the enterprise must expect a significantly changed or significantly expanded risk situation in the supply chain, for example due to the introduction of new products, projects or a new business field."[38]

According to the LkSG, the risk analysis can come to three conclusions a) there is no human rights risk, b) there is a human rights risk or c) a violation of human rights has occurred or is imminent.

If an enterprise identifies a risk, it must take appropriate preventive measures without undue delay (Section 6 Subsection 1). These include issuing a policy statement on its human rights strategy (Section 6 Subsection 2) and laying down appropriate preventive measures in its own area of business and vis-à-vis their direct suppliers (Section 6 Subsection 1 and 3).

If the enterprise discovers that a violation of a human right has already occurred or is imminent, it must, without undue delay, take appropriate action to prevent, end or minimize the extent of this violation, Section 7 Subsection 1.

The termination of a business relationship is only required ("ultima ratio"),[39] if

> "1. the violation of a protected legal position […] is assessed as very serious,
> 2. the implementation of the measures developed in the concept does not remedy the situation after the time specified in the concept has elapsed,
> 3. the enterprise has no other less severe means at its disposal and increasing the ability to exert influence has no prospect of success."[40]

3. Non-Compliance[41]

The Federal Office of Economics and Export Control acts as the competent authority (Section 19 LkSG) either ex officio (Section 14 Sebsection 1 No. 1 LkSG) or upon request (Section 14 Subsection 1 No. 2 LkSG). The authority has extensive rights of action – they are authorized to: (i) summon people (Section 15 No. 1 LkSG), (ii) enter and inspect the enterprise's premises (Section 16 No. 1 LkSG) and (iii) inspect and examine the enterprises' documents and records (Section 16 No. 2 LkSG). Enterprises and persons summoned are obliged to provide the competent authority with the information and documents requested by the authority (Sections 17 and 18).

[37] The German Federal Office for Economic Affairs and Export Control published a Guidance on conducting a risk analysis as required by the LkSG on their website https://www.bafa.de/SharedDocs/Downloads/EN/Supply_Chain_Act/guidance_risk_analysis.html (Aug. 28th., 2024, 12:05 PM).

[38] see English version of the LkSG provided by the German Federal Ministry of Labour and Social Affairs.

[39] BT.Drs. 19/28649, p 49.

[40] see English version of the LkSG provided by the German Federal Ministry of Labour and Social Affairs.

[41] A more detailed overview provides Dr. Burchardi, LL.M., Lieferkettensorgfaltspflichten: Risiken für die Unternehmensleitung, Neue Zeitschrift für Gesellschaftsrecht, 1467-1473 (2022).

If a breach of the due diligence obligations has been identified, fines between EUR 100,000 and EUR 800,000 may be imposed at company level (Section 24 Subsection 2). If a company has an average annual turnover of more than EUR 400 million, certain breaches of duty can be punished with a fine of up to 2 percent of the average annual turnover (Section 24 Subsection 3).

The LkSG does not provide for individual criminal law consequences such as imprisonment.

B. The Money Laundering Act

1. Scope of Application

Unlike the LkSG, the GwG's[42] scope of application is not linked to enterprises above a certain employee-threshold but is aimed at financial service providers in the broadest sense, as well as at individuals such as lawyers, retailers and art brokers (Section 2 Subsection 1). Particularly, the addressees of both laws are banks and enterprises active in the manufacturing industry.

2. Due Diligence Obligations

The GwG is structured similarly to the LkSG, whereby the stipulated due diligence obligations apply to combating money laundering and terrorist financing (Section 5 Sebsection 1 GwG).

The GwG also provides for the establishment of an appropriate risk management system (Section 4 GwG) and risk analyses (Section 5 GwG). Based on these analyses, further internal security measures must be enacted (Section 6 GwG). Due diligence obligations must also be complied with in relation to contractual partners – so-called "customers" in the GwG and "direct suppliers" in the LkSG (Section 10 - 17 GwG).
As the GwG defines money laundering as everything that fulfills the requirements of Section 261 StGB ("All-Crimes-Approach"; protection of human rights with a foreign connection),[43] the human rights risks and findings identified by the analyses of the LkSG are also relevant in the GwG. In this context, particular attention must be paid to the existing reporting obligation under Section 43.[44]

In the case of human rights risks, the reporting obligation pursuant to Section 43 Subsection 1 No. 1 GwG must be considered,

> "if facts indicate that that an asset associated with a business relationship, brokerage or transaction originates from a criminal offense that could constitute a predicate offense to money laundering" so

[42] The German Federal Financial Supervisory Authority published an (not up-to date) English Version of the GwG available at https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_gwg_en.html (Sep. 29th, 2020).
[43] see II. B. and C. of this article.
[44] Dr. Tobias Eggers et al eds., Lieferkettencompliance und Geldwäsche, Deutscher AnwaltSpiegel, https://www.deutscheranwalt-spiegel.de/compliancebusiness/compliance/lieferkettencompliance-und-geldwaesche-33370/ (Dec. 12th, 2023).

> "the obliged entity is to report this matter, irrespective of the value of the asset in question or the amount of the transaction involved, to the German Financial Intelligence Unit without delay."[45]

Section 43 GwG does not specify the degree of suspicion required for the reporting obligation.[46] However, the German Federal Financial Supervisory Authority states the following in its interpretation and application notes on the Money Laundering Act:[47]

> "The obliged entity and the employees acting on its behalf do not have to be certain that a corresponding asset originates from a predicate offense under Section 261 StGB or relates to terrorist financing. […] In case of doubt, a report must therefore be submitted in accordance with Section 43 Subsection 1 GwG."[48]
> [Emphasis by authors]

The obliged entity does not have to fully clarify the facts, nor is a legal assessment necessary. Rather, the facts must be assessed based on general experience.49 However, a report without sufficient evidence remains inadmissible.[50]

The reduced degree of suspicion required by law and the obligation to report "without undue delay" make it difficult to distinguish between a valid report and an inadmissible report.[51] The consultation version of the interpretation and application notes presented by the German Federal Financial Supervisory Authority in July 2024 does not remedy this situation.[52] The assessment of the facts may be subsequently reviewed by the responsible supervisory authority.[53] Therefore, a clear documentation of the decision-making process and its outcome is advisable for the obligated party.[54]

In case of human rights issues within supply chains, i.e., if a *human rights risk* is already identified as part of an annual or ad hoc risk analysis pursuant to the LkSG, a review of the reporting obligation under Section 43 GwG must always be carried out, whereby a report *may* be made in "*in case of doubt*".

[45] Free translation of Section 43 Subsection 1 No. 1 GwG.

[46] The degree of suspicion was controversial for some time. An overview of the past dispute provides da Rose, Geldwäschegesetz, Section 43, mn 16 (Herzog, 5th ed. 2023).

[47] The German Version is available at https://www.bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl_ae_auas_gw.html (Aug. 29th, 2024, 01:13 pm).

[48] Federal Financial Supervisory Authority, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, Oct. 2021, p 73; free translation.

[49] Federal Financial Supervisory Authority, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, Oct. 2021, p 73.

[50] BT-Drs. 17/6804, p. 35, 36.

[51] da Rose, Geldwäschegesetz, Section 43, mn 20 (Herzog, 5th ed. 2023).

[52] The German Version is available at https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Konsultation/2024/kon_06_24_Konsultation_AuA_AT.html (July 9th, 2024).

[53] Federal Financial Supervisory Authority, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, Oct. 2021, p 75.

[54] da Rose, Geldwäschegesetz, Section 43, mn 21 (Herzog, 5th ed. 2023).

If the risk analysis identifies that the risk has materialized into a *human rights violation*, a report *must* be made in accordance with Section 43 GwG. At the same time, the "All-Crimes-Approach" and Section 261 Subsection 9 StGB as well as the reduced subjective requirements of Section 261 Subsection 6 StGB suggest a realisation of Section 261 StGB.

However, Section 261 Subsection 8 StGB allows leniency following voluntary disclosure. In this case, the perpetrator or participant must inform the competent authority[55] of all known circumstances of the unlawful act committed; this also includes the known circumstances of the predicate offense.[56] If the company's own money laundering officer or head of department reports the offense, the perpetrator or participant may only benefit from the leniency application, if he or she has prompted the money laundering officer or head of department.[57] However, the report must be made at a time when the money laundering has not been fully or partially "discovered" by the authorities.

This poses an increased risk, particularly for employees of companies that work in larger teams, of not being able to benefit from the voluntary disclosure. If, for example, only one employee has disclosed the facts of the case to the money laundering officer and the latter has made a voluntary disclosure immediately afterwards, the offense is now "discovered" within the meaning of Subsection 8 and the other team members involved are cut off from the possibility of impunity. However, impunity can be achieved if, between the first knowledge of the money laundering officer and his report, other parties involved disclose themselves to him, even if this only happens at the request of the officer.[58]

In addition, a suspicious activity report in accordance with Section 43 GwG only results in an obligation to terminate the business relationship in exceptional cases.[59]

3. Non-Compliance[60]

Pursuant to Section 56 Subsection 1 1st Sentence 1 No. 69 GwG, anyone who fails to submit a report or submits it incorrectly, incompletely or untimely according to Section 43 Subsection 1 GwG is in breach of the regulations. The impending amount of the fine depends on the type of offense (level of intent) and the type of the entity (natural or legal person/financial sector). Based on these distinctions, fines between EUR 100,000 and EUR 5,000,000 can be imposed. The fine may amount up to 10 percent of the total turnover achieved by a legal entity in the financial year preceding the administrative decision.

In addition, criminal liability for money laundering under Section 261 StGB, aiding and abetting money laundering or obstruction of prosecution or punishment (Section 258 StGB) may also be considered.[61]

[55] pursuant to Section 158 Subsection 1 of the German Code of Criminal Procedure these authorities are the public prosecution office, the police authorities and police officers and local courts; pursuant to Section 27 Subsection 1 of the Money Laundering Act the German Financial Intelligence Unit can also be informed.

[56] Altenhain, Strafgesetzbuch, Section 261, mn 124 (Kindhäuser et al eds., 6th ed. 2023).

[57] Altenhain, Strafgesetzbuch, Section 261, mn 125 (Kindhäuser et al eds., 6th ed. 2023).

[58] Concerning this group of cases see Altenhain, Strafgesetzbuch, Section 261, mn 125 (Kindhäuser et al eds., 6th ed. 2023).

[59] Federal Financial Supervisory Authority, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, Oct. 2021, p 79, 80.

[60] A more detailed overview provides da Rose, Geldwäschegesetz, Section 56, mn 106a (Herzog, 5th ed. 2023).

[61] da Rose, Geldwäschegesetz, Section 56, mn 18 (Herzog, 5th ed. 2023).

In individual cases, the obliged entity may also be involved in the criminal offense of financing terrorism (Section 89c StGB).[62]

IV. CONCLUSION

The identification of possible human rights violations does not only play a role in the scope of application of the Supply Chain Act. Due to the broad scope of application of Section 261 StGB - which in turn also takes human rights violations into account - the Money Laundering Act, particularly its reporting obligation under Section 43 GwG, also becomes relevant.

Consequently, violations of due diligence obligations of the LkSG can also have consequences under the Money Laundering Act and criminal law. Therefore, it is essential for the *obligated parties of both laws* to establish communication channels between LkSG compliance-departments and GwG compliance-departments. However, if a reliable exchange process is established, it is possible that GwG compliance-departments will not have to identify any human rights violations along the supply chain themselves.

If a *human rights risk* has been identified as part of a risk analysis of the LkSG, a report in accordance with Section 43 GwG must also be examined and submitted in case of doubt. If a *human rights violation* has been identified along the supply chain, in addition to a report in accordance with Section 43 GwG, a voluntary disclosure may also be made in accordance with Section 261 Subsection 8 of the Criminal Code.

However, human rights risks also trigger obligations for companies that are *only obliged under the GwG*. In this case, the obligation to report under Section 43 GwG and the examination of a voluntary disclosure under Section 261 Subsection 8 StGB remains in place.

One welcome development is that some parties will no longer be bound by anti-money laundering obligations when the Anti-Money Laundering Regulation comes into force in 2027. Under current German law, persons trading in goods, are obliged to file a report in accordance with Section 43 of the GwG, irrespective of a cash limit. This obligation will no longer apply.[63] However, this has no effect on the scope of application of Section 261 StGB. Corporate officers may still be liable to prosecution if they intentionally accept funds that originate from a criminal source. In order to counter these risks, internal reporting systems for financial anomalies must be maintained.

[62] Federal Financial Supervisory Authority, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, Oct. 2021, p 72.

[63] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, reason 18.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

THE ENVIRONMENTAL CONTROL PROVISIONS RELATED TO HUMAN ACTIVITIES AND THEIR POTENTIAL IMPACT ON THE ENVIRONMENT

Considerations on The Harmful Substances and Products, Based on The Example of The Republic of Moldova

Liminita Diaconu

AUTHOR

Luminita Diaconu PhD student has been a university-lecturer since 1996 She has 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 Environmental Law/Ecological Control.

ABSTRACT

The protection regime for products of human activity is a critical component of modern environmental and public health policy. This paper provides a broad overview of the general considerations surrounding the regime for pollutants and products, which aim to protect both human and environmental well-being. This paper gives a historical overview of the evolution of environmental policies concerning the management of waste and chemical substances. It discusses the growing recognition of the potential risks posed by various human-made substances and products, enumerating the provisions related to the regime of harmful products and substances This article underlines the need for a robust regulatory framework to address these concerns, outlining the primary objectives of the substances and products regime, including the protection of human health, the preservation of the environment and the promotion of sustainable production and consumption. It examines the key components of the regime, such as the identification and classification of harmful substances, the establishment of safety standards and exposure

limits, and the implementation of control measures and enforcement mechanisms, by exploring the complexities and challenges associated with the effective implementation of the toxic substances and products regime, including scientific uncertainties, stakeholder interests and the need for international cooperation. In conclusions we summarize the key findings and highlight the importance of continued research, policy development and collaborative efforts to further strengthen the protection regime for products of human activity. This article provides a concise yet comprehensive overview of the key aspects covered and sets the stage for a detailed examination of the pollutant and product regime and its impact on the environment and public health.

TABLE OF CONTENTS

I. INTRODUCTION

In the course of human evolution, humans have consistently engaged in activities aimed at ensuring comfort, security, and social status, as these factors are indispensable for sustaining life.

It can be argued that the convenience of life is enhanced only when certain income-producing industrial activities are carried out. This results in the production of waste products, which may, depending on their nature and quantity, interfere with the good life. In the past, the low population density and the almost exclusive use of natural products did not result in the same level of waste production. The lifestyle of the average person has changed significantly over time. While waste production was previously less common, the advent of scientific progress has led to a notable increase in the quantity and diversity of waste products. In recent decades, the degradation of environmental factors on our planet has reached alarming levels, with pollutants reaching concentrations that exceed any previous limits.

As a consequence of scientific and technical progress, humans have also been able to utilize a variety of energies and materials that they would otherwise be unable to process without the use of specialized technologies, machinery and processes. However, the use of these materials and energies often has a detrimental impact on the environment and, consequently, on humans. The assurance of a sustainable existence for living nature, including humankind, in the context of substantial (accidental or deliberate) introduction of toxic chemical substances into the environment, resulting from human activities, is contingent upon the implementation of rigorous control measures pertaining to their production, transportation and utilization. Furthermore, in the current era, the entities tasked with the responsibility of exercising control are in possession of comprehensive data concerning the intended destination, characteristics, biological impact and behavior of these substances within the environment.[1]

Nevertheless, it is currently perceived that the development of legislative and institutional mechanisms, control and regulatory measures, information provision and other components of the system of risk and hazard assessment of potentially toxic chemicals and toxic wastes in the Republic of Moldova is still in its infancy. The current toxicological safety system is primarily focused on the elimination of harmful substances, yet it fails to provide adequate protection for the environment and does not align with international recommendations and standards. The absence of an adequate organizational infrastructure and the lack of coordination between the various stakeholders and institutions in this field represent significant challenges in the Republic of Moldova. Furthermore, the functions of different organizations are often duplicated, and there is also a lack of coordination in actions. A mechanism for the preventive assessment of the risk, danger, and effects of potentially toxic chemical substances and toxic waste is lacking. The courts are responsible for control, but they only record the result of the harmful action on humans and the environment. Consequently, in the Republic of Moldova, the limits of acceptable contamination by potentially toxic chemicals are frequently exceeded. These substances are present in the water, air, soil, and biotic components (wild and cultivated flora and fauna), resulting in the degradation of natural ecosystems, a decline in the quality of drinking water, and the failure of agricultural production to meet sanitary-hygienic standards.

[1] I. Trofimov, G. Ardelean, A. Crețu, Dreptul mediului, ed. Editura Bons Offices, Chișinău, 2015, pag 171

These discrepancies collectively contribute to the absence of a regulatory framework that guarantees the protection of waste through the prevention and appropriate management of all categories of waste. As a result, the shortcomings of environmental legislation, coupled with the absence of economic rationale in addressing harmful substances, further exacerbates the risk to public health and the well-being of the population. The issue of the utilization of industrial toxic waste or its interment represents a matter of significant urgency, necessitating an expeditious resolution. At the time of writing, there is no incineration facility for toxic waste within the country; instead, it is frequently transported alongside other industrial by-products to landfills designated for household waste. In light of the prevailing circumstances, it is imperative that prompt action be taken, and that those responsible for these infringements be subjected to stringent penalties.[2]

II. A HISTORICAL OVERVIEW OF THE EVOLUTION OF ENVIRONMENTAL POLICIES CONCERNING THE MANAGEMENT OF WASTE AND CHEMICAL SUBSTANCES.

Following the collapse of the Soviet Union and the subsequent declaration of independence by the Republic of Moldova, one of the most significant environmental challenges pertained to the unresolved issue of waste and toxic chemical substances, particularly pesticides, that had been stored in agricultural production facilities. The continued presence of these substances in these warehouses, which were originally constructed for the storage of pesticides and other natural fertilizers, posed a considerable risk to the natural environment and the health of the population. The creation of this situation can be attributed to the arbitrary demolition of warehouses for the storage of pesticides and natural fertilizers following the implementation of the agrarian reform, which permitted the privatization of these objects in rural areas. Consequently, a considerable quantity of unidentified and prohibited pesticides were left in open storage. During this period, numerous cases of the burial of unusable and prohibited pesticides were discovered in various unsanctioned locations.

At the same time, in 1998, approximately 68 companies and cooperatives were granted licenses, through which they imported and sold over 10,000 tons of pesticides and mineral fertilizers within the republic. Approximately 30 agents were responsible for the illicit importation of 6.3 tons of pesticides. The storage of toxic waste on the premises of the companies in large quantities represents a significant risk of environmental contamination, particularly in the municipality, where the population is particularly high. In the context of these deviations, other violations have also been identified, including the authorization of the construction of oil filling stations in residential areas.

The chaos and disaster caused by the poor management of waste, chemical substances, products and harmful substances demonstrates the absence of a regulatory legal framework based on well-considered and coherent environmental policies. The initial policy document in the field of the environment was the Concept of Environmental Protection (1995), which delineated the principal directions and mechanisms of environmental protection policy during the transition period towards a market economy.

Subsequently, the National Strategic Action Program in the field of environmental protection was developed and approved by the decree of the President of the Republic of Moldova (No. 6 October 1995). The action plan for the implementation of the program delineated the planned activities until 2005.

This was followed by the National Plan of Actions in the Field of Environmental Protection (1996), which was developed in accordance with the provisions set forth in the Program of Actions in the Field of Environmental Protection in Central and Eastern European countries. The current framework of environmental policies is undergoing development and includes several documents of a rectoral nature. These reflect the objectives and directions of action in a number of fields, including waste and chemical management, pollution prevention, biodiversity conservation, water supply and sewerage, desertification, and forestry. Nevertheless, a significant proportion of these documents comprise concepts that are no longer relevant and require updating. Furthermore, the development of policy documents is essential for certain environmental components and aspects, including the protection of atmospheric air, soil, and useful mineral resources. In summary, the absence of a comprehensive framework strategy has resulted in a dearth of strategic planning within the environmental sector in the Republic of Moldova. This has led to a lack of a unified vision at the governmental level and the fragmentation of the sector. A strategy for the management of waste in Moldova for the period 2023-2028 has recently been approved.[3] The strategy establishes a set of objectives and measures regarding the collection, transportation, treatment, recovery and disposal of waste in Moldova. In 2014, in order to address the shortcomings identified in the preceding environmental strategic planning, the environmental strategy for the period 2014-2024 was adopted. Among its fundamental objectives is the establishment of integrated management systems for waste and chemical substances, which will contribute to a 30% reduction in the volume of stored waste and a 20% increase in recycling rate by 2028.

III. PROVISIONS RELATED TO THE REGIME OF HARMFUL PRODUCTS AND SUBSTANCES

The objective of the legal regime of harmful products and substances is to avoid the harmful effects that may result from the use of different substances, materials and energies. It is evident that the exponential growth of the chemical industry in recent decades, coupled with the multitude of pernicious risks to the environment, has necessitated the regulation of hazardous chemical products, including those that entail chronic effects on health and the quality of the environment following prolonged and repeated exposure. The issue is further compounded by the multitude of products and substances used in a variety of forms, which interact synergistically, necessitating increasingly precise and technically oriented regulations.[4] In consequence, in recent years, particular attention has been devoted to the regulations pertaining to the management, storage and utilization of products with a deleterious effect. In accordance with the legislation pertaining to this field,[5] a deleterious product is defined as material intended for use in the national economy, the presence of which in the environment can disrupt the normal functions of human, plant and animal organisms and ecosystems. A deleterious substance is defined as any substance that, coming into contact with living organisms, can cause them harm.

The legal regime of harmful products and substances constitutes a system of norms and rules that regulate the activities in the field of manufacturing, delivery, transportation, storage, handling, use, import and export of these products and substances, as well as the cultivation of plants for the purpose of obtaining harmful substances.

[3] Government Decision no.301 of 24.04.2014 on the approval of the environmental strategy for 2014-2024, Official Gazette no.104-109 of 06.05.2014

[4] Mircea Dutu, Dreptul Mediului,ed.3,Bucharest,2010,p.458

[5] Law nr.1236 of 03.07.1997 on Harmful products and services regime, Official Gazette,nr.67-68 of 16.10.1997

The legal regime of harmful products and substances includes

- administration and control of the use of harmful products and substances,
- authorization of activities related to the management of harmful products and substances
- the content of the rights and obligations of natural and legal persons
- the manufacture of harmful products and substances
- storage of harmful products and substances
- transporting harmful products and substances
- the use of harmful products and substances
- neutralization of harmful products and substances
- import and export of harmful products and substances
- legal responsibility for violating the legislation regarding harmful products and substances

A. Administration and control of the use of harmful products and substances,

State administration in the field of the use of harmful products and substances represents a type of activity that includes the possibility and obligation of state bodies to direct the manufacturing, storage, use processes, as well as other activities related to the use of harmful products and substances.

The control in the field of the use of products and harmful substances includes a series of activities undertaken by the central and specialized bodies in order to verify the compliance of the activities of use, storage, manufacturing, export, transportation, etc. of harmful substances according to the provisions of the legislation in force.
The administrative competence in this field is distributed among the following bodies:

- Ministry of Health
- Ministry of Agriculture and Food Industry
- Ministry of the Environment
- The Civil Protection and Exceptional Situations Service of the Ministry of the Interior
- Ministry of Economy
- Local public administration authorities

In addition to the aforementioned bodies, the Government also has the following attributions:

a) adopt decisions and other normative acts in matters related to the regime of harmful products and substances

b) approve the national register of potentially toxic chemical substances;

c) approve the measures to prevent accidents and damages at the warehouses of harmful products and substances;

d) establish the perimeter and mode of operation of the specialized platform for the neutralization and burial of unused harmful products and substances and their waste;

e) ensure the training and improvement of personnel for the activities in this field.

In carrying out its control and administration functions, the Ministry of Health is responsible for the following:

a) exercising state control over compliance with legislation regarding the regime of harmful products and substances;

b) establishing, maintaining and updating the National Register of potentially toxic chemical substances;

c) updating the Regulation regarding the use and neutralization of harmful products and substances and their waste;

d) approving the Regulation on the manner of transportation.

Furthermore, the Ministry of Health is responsible for regulating the storage, use, and listing of mineral fertilizers and pesticides, as well as chemical and biological preparations used for plant protection and stimulation. Additionally, the Ministry approves activities involving the use of harmful products and substances. It also establishes maximum permitted concentrations of harmful substances in soil, water, air, and food products. Moreover, the Ministry performs toxicological assessments of potentially toxic chemical substances and approves their registration.

At the same time, The Ministry of Agriculture and Food Industry is responsible for the following:

a) ensuring compliance with legislation regarding the management of pesticides and mineral fertilizers;

b) preparing a list of chemical and biological preparations for the protection and stimulation of plant growth and presenting it to the Interdepartmental Republican Council for approval of chemical and biological products for protection and stimulation.

c) certifies chemical and biological products for the protection and stimulation of plant growth, or provides evidence of the application of pesticides in agriculture;[6]

d) establishes a network of laboratories for the analysis and control of pesticide and mineral fertilizer quality, as well as the control of compliance with established norms for their concentration in soil, feed, food, and animal and vegetable products.

[6] Legea 211/2011 privind regimul deseurilor, republicata 2014

In discharging its duties, the Ministry of the Environment, as the central environmental authority, is responsible for the following:

a) Exercise state control over compliance with laws and other normative acts regarding the protection of the environment, in the process of manufacturing, storage, transportation, use, neutralization and burial of harmful products and substances and their waste;

b) Coordinate the regulation on how to use and neutralize harmful products and substances and their waste. The regulation governing the transportation, storage, and utilization of mineral fertilizers and pesticides. The list of chemical and biological preparations for the protection and stimulation of plant growth is as follows:

c) The coordination of the National Register of potentially toxic chemical substances, the placement of specialized platforms for the neutralization and burial of unusable harmful products and substances and their waste.

When talking about The Civil Protection and Emergency Service of the Ministry of Internal Affairs, in collaboration with the Ministry of the Environment, it fulfils the following functions:

a) the coordination and supervision of the import, export, transportation, use and neutralization of harmful products and substances (chemical, biological, explosive, flammable); Within the country's borders, the following duties are carried out:

b) the registration and approval of lists of dangerous loads;

c) the approval of lists of economic agents that utilize harmful products and substances, as well as the lists of units authorized to transport dangerous loads;

d) the creation and approval of lists by mutual agreement with the Ministry of Transport and Road Infrastructure, the Minister of Internal Affairs, and the Ministry of Health are responsible for accounting for the resources and capabilities required to prevent accidents during the transportation and utilization of harmful products and substances, as well as to address the consequences of any malfunctions.

e) Supervises compliance by natural and legal persons with civil protection requirements for the manufacture and use of harmful products and substances and for the transportation of dangerous loads;

f) The coordination of measures implemented by local public authorities with the objective of preventing and removing the consequences of potential accidents and fires.

The Ministry of Economy is responsible for the state regulation of matters pertaining to the safety of individuals who, in the course of their work, may potentially come into contact with harmful products or substances.

The local public administration authorities, in collaboration with the territorial authorities for health and the environment, are responsible for:

a) establishing the boundaries for the location of warehouses intended for the storage of harmful products and substances;

b) preparing an annual list of economic agents in the administered territory who manufacture, use or trade particularly harmful substances, as well as a list of transport companies authorized to operate in the region. To transport dangerous loads within the specified territory and submit the relevant lists for approval to the Civil Protection and Exceptional Situations Service of the Ministry of Internal Affairs and the Ministry of the Environment.

c) Developing and approving the account of the necessary resources and capabilities to prevent accidents and to address the potential consequences of such incidents within the designated territory.

d) Annually approving, in agreement with the relevant bodies, the measures to protect the population of the administered territory and the environment against the negative effects of harmful products and substances;

e) Ensuring that the means of notifying the population in the administered territory are maintained in a satisfactory technical condition in case of danger caused by natural calamities, the use of harmful products and substances or man-made breakdowns;

f) Immediately, In the event of the discharge of particularly harmful substances into the environment, the relevant authorities must be informed and measures taken to remove the consequences of these discharges.

Furthermore, the relevant authorities must be informed of any non-compliance with regulations regarding the transportation, storage, and use of pesticides and mineral fertilizers.

B. Authorization of activities related to the management of harmful products and substances

Activities in the field of manufacturing and use of harmful products and substances for medicinal, sanitary-veterinary, industrial, agricultural, forestry, educational, scientific, and commercial purposes, as well as in the field of their import and export, are carried out on the basis of authorizations issued and registered by the bodies authority of the Ministry of Health, the Ministry of Agriculture and the Food Industry, the Ministry of the Environment, the Service of Civil Protection and Exceptional Situations, of the Ministry of Internal Affairs. Upon ceasing the activities related to the management of harmful products and substances, the economic agent in question is obliged to return, within 20 days, the authorization of the body that issued it.

It is prohibited to import, export and use pesticides and mineral fertilizers without a license or authorization issued by the competent bodies. If it is found that the authorized economic agent does not comply with the regime of products and harmful substances provided by legislation and normative acts, the license or authorization for the activities related to their management are revoked by the body that released it.

C. The Rights and obligations of natural and legal persons

The following obligations are incumbent upon natural and legal persons:

> a) compliance with the sanitary rules and technical regulations for the manufacture, use, storage, transportation, processing, neutralization, and burial of harmful products and substances, including the implementation of measures to prevent and remove harmful effects on humans and on the environment;
>
> b) maintenance of a special register of the products and harmful substances used, and presentation of this register to the environmental and health authorities upon request.[7]

In the event of non-compliance with the aforementioned requirements, which may result in environmental pollution and jeopardize public health, the manufacture and use of harmful substances shall be prohibited in accordance with the decisions adopted by the central control bodies.

D. The production of detrimental products and substances

Harmful products and substances are manufactured by specialized economic agents, respecting the requirements of the technological processes that are approved by the Ministries under which the respective units are located, and are coordinated with the Ministry of Health and the Ministry of the Environment. Wastewater, gaseous evacuations, waste and residues liquids, solids and pastes, resulting from the manufacture and conditioning of products and harmful substances, are purified, accumulated, stored, preserved, neutralized or liquidated according to the technological requirements and the provisions of ecological legislation. Each product and each harmful substance is manufactured through authorized technologies and biotechnologies and is delivered accompanied by technical regulations for use, as well as quality and compliance certificates.

E. Storage

Harmful products and substances are stored in special rooms, set up in accordance with the regulations approved by the Ministry of Health in agreement with the Ministry of the Environment. In the warehouses, in special registers, strict records are kept of the products and harmful substances, stored and delivered according to the regulations coordinated with Ministry of Health. Harmful products and substances are released only to persons and economic agents authorized to use them.

[7] https://gov.md/sites/default/files/document/attachments/chapter_28_consumer_and_health_protection.pdf

F. Transportation

The transportation of harmful products and substances is conducted in accordance with an order issued by the manager of the transport unit or the duly authorized individual, which specifies the technical regulations applicable to each mode of transport. The transportation is conducted with the presence of an appointed companion, a specialist in the field, who has undergone training in the specifics of the transportation method, the potential harmfulness of the products, and the measures to be taken in case of damage to the packaging, breakdown, and so forth. In the case of the transportation of harmful substances and products, the use of specialized means of transport is imperative. It is prohibited to park vehicles carrying explosive products and substances, or those that may emit harmful gases, in populated areas. Furthermore, it is forbidden to transport products and harmful substances in damaged packaging, and without supervision.

G. Handling and use

The handling and use of products and harmful substances is carried out in accordance with the norms and technical requirements, with the sanitary rules and protection of work and the environment, revised for each product or harmful substance.

Economic agents that carry out activities related to the use of products and harmful substances are obliged to keep records of their movement in special registers, the form of which is approved by the Ministry of Health. The register also keeps records of land cultivated with plants from which harmful substances are extracted, as well as the volume of collective products, stored and processed.[8]

H. Neutralization

Harmful products and substances are neutralized according to the regulation regarding the storage, use, neutralization, and burial of toxic substances and residues.

I. Import and export

The import and export of products and harmful substances are carried out based on the licenses issued by the competent bodies, with the approval of the Ministry of the Environment. The importer's declaration, made on his own responsibility, must be attached to the import license, in which the name and characteristics of the products or harmful substances to be introduced into the country will be specified.

[8] https://cis-legislation.com/document.fwx?rgn=126077

J. Legal responsibility for violating the legislation on harmful products and substances

It is crucial to hold those responsible for the improper handling of harmful substances accountable. This is a vital step in ensuring the efficiency of the supervision and control of such activities. Those who fail to take responsibility for their actions will be held to account. This has a preventive, educational and remedial character that will discourage those who intend to give priority to profit in relation to the quality of environmental factors.

Therefore, for violating the provisions of the legislation regarding the use of harmful products and substances, natural persons will be held to account accordingly.

Moldova has implemented a comprehensive legal framework to ensure compliance with international standards on the regulation of harmful products and substances in alignment with International Conventions and EU Regulations.

At the same time, Moldova has ratified key international conventions such as the UN Convention against Corruption and relevant Council of Europe conventions in this field.[9]

Moldova's legislation has been updated to align with EU directives and regulations, including

- The EU's Biocidal Products Regulation (Regulation (EU) No. 528/2012).[10]
- Domestic Laws and Regulations-The Law on Chemicals (Law No. 277/2018) unequivocally provides the legal basis for the administration and control of hazardous chemical substances in Moldova.
- Another important aspect, is that Moldova has issued regulations, such as Order No. 344 in 2020, to align with the EU's Biocidal Products Regulation and establish requirements for the placement and use of biocidal products.

Other relevant laws include the Law on General Product Safety and the Law on Consumer Protection, and regulations governing the import/export of restricted goods.[11]

IV. CONCLUSIONS

Moldovan authorities, such as the National Agency of Public Health, the National Agency on Regulation of Nuclear, Radiological and Chemical Activities, and the National Agency on Safety of Foodstuffs, are responsible for supervising and enforcing regulations on harmful products and substances. The legal framework sets out clear penalties and enforcement mechanisms, including fines, license revocation, and criminal liability, for violations of the regulations.

[9] https://www.trade.gov/country-commercial-guides/moldova-prohibited-and-restricted-imports
[10] https://cis-legislation.com/document.fwx?rgn=126077
[11] https://gov.md/sites/default/files/document/attachments/chapter_28_consumer_and_health_protection.pdf

In doing so, The Republic of Moldova has established a comprehensive legal framework to regulate the management of harmful products and substances.

The following key provisions are included:

– Administration and Control of Harmful Products and Substances

  The Law on Chemicals (Law No. 277/2018)[12] and related regulations provide the legal basis for the administration and control of harmful chemical substances in Moldova. This includes requirements for registration, authorization, and oversight of activities involving hazardous chemicals.

– Authorization of Activities Related to Harmful Products and Substances

  Moldovan legislation requires authorization and licensing for various activities involving harmful products and substances, such as the production, storage, transportation, and use of chemicals, biocidal products, and other potentially dangerous goods. The relevant laws and regulations set out the specific authorization procedures.

– Rights and Obligations of Individuals and Businesses

  The legal framework clearly defines the rights and obligations of both natural and legal persons with respect to harmful products and substances. This includes requirements for proper handling, reporting, and safe disposal, as well as consumer protection measures.

– Production, Storage, and Transportation of Detrimental Products

  This covers requirements for facilities, equipment, and operational procedures.

– Handling, Use, and Neutralization

  The regulations provide detailed requirements for the proper handling, use, and neutralization of harmful products and substances, including personal protective equipment, waste management, and emergency response procedures[13] .

– Legal Responsibility and Enforcement

  The legal framework sets out clear penalties and enforcement mechanisms for violations of the regulations on harmful products and substances, including fines, license revocation, and criminal liability in serious cases, related to Consumer Protection and Information.

[12] https://www.fao.org/faolex/results/details/en/c/LEX-FAOC205190/

[13] https://www.trade.gov/country-commercial-guides/moldova-prohibited-and-restricted-imports

Evidently, Moldovan law requires businesses to comply with various consumer protection measures, such as displaying prices correctly, providing information on commercial purpose, and responding to consumer complaints. In conclusion, the Republic of Moldova has developed a comprehensive system of laws and regulations to manage the risks associated with harmful products and substances, covering all aspects from authorization to disposal. This regulatory framework is designed to protect public health, worker safety, and the environment while facilitating the responsible use of necessary chemicals and materials.

Moldova has revised its list of standards for general product safety to align with relevant EU standards, and has also implemented EU regulations on the placement and use of biocidal products through domestic legislation.

In summary, Moldova coordinates closely with the EU to harmonize its product safety regulations, market surveillance, and enforcement mechanisms, while also participating in key EU information-sharing and cooperation systems. This alignment with the EU acquis is an important part of Moldova's European integration process.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

AI IN ACTION: ETHICAL AND COMPLIANCE CHALLENGES IN THE AGE OF INTELLIGENT MACHINES

New challenges for the world and the European Union

Claudia Chiauzzi

AUTHOR

Claudia Chiauzzi is a dedicated and accomplished Privacy and Compliance Specialist currently working for one of the largest companies in Italy.

With a background in law, her expertise lies in societal, administrative, compliance, and privacy matters. She graduated in 2021. Claudia enrolled in a Level II Master in Compliance. Claudia is expanding her knowledge base by attending various classes on AI, privacy, compliance, and ethics.

TABLE OF CONTENTS

I. WHAT IS AI?

Artificial Intelligence (AI) continues to strengthen its foothold in the workplace. But what does this mean for the field of Compliance and Ethics? How can enterprises leverage AI, and how can compliance officers safeguard and utilize this technology?

Artificial Intelligence (AI) is a term that lacks a universally accepted definition. It can be described as the simulation of human intelligence processes by machines. This may encompass various systems, processing methods, machine vision, speech recognition, and language processing[1].

A. The Compliance Risks of AI

2023 could be dubbed "The Year of Artificial Intelligence Breakthroughs". In 2024, various companies will begin to implement and use AI-related tools. The reason is straightforward: AI enables faster, more innovative, and more useful information for market analysis and strategic planning in companies' financial departments, thereby saving money and reducing budget expenses.
The importance of AI is a key driver of future growth. However, it also introduces a significant set of risks that society must consider when deciding to integrate it into organizations and their processes[2]. The most notable Compliance risk associated with AI lies in the threat of data breaches due to inadequate security measures, and potential discrimination in decision-making.

B. The Role of AI Ethics and Compliance Officers

The roles of Compliance Officers and Ethics Officers, which in some countries are fulfilled by the same individual, are evolving. The governance of AI is a critical issue with global implications. As nations grapple with the transformative potential of artificial intelligence, they face complex decisions about regulation, ethics, and innovation. This ongoing education enables them to proactively address potential ethical and compliance issues, ensuring that their organizations remain compliant and uphold the highest ethical standards.[3]

[1] See: Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.", "The versatility of AI systems is evident in their application across different domains. See: Nilsson, N. J. (2014). Principles of Artificial Intelligence. Morgan Kaufmann.

[2] See: Smith, J. (2023). The Year of AI Breakthroughs. Tech Innovations Journal.", "The economic benefits of AI are matched by significant compliance risks. See: Brown, A. (2023). AI in Financial Planning: Opportunities and Risks. Financial Times.", "Bias in AI decision-making is a major concern. See: O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing Group."

[3] See: Johnson, K. (2023). Ethics and Compliance in the Age of AI. Harvard Business Review.", "Understanding AI and its risks is fundamental for Compliance Officers. See: Dignum, V. (2019). Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way. Springer.

Specifically, the duties of a Compliance and Ethics Officer encompass various responsibilities, including:

- Ensuring that AI systems align with universally accepted ethical values and providing relevant guidelines.
- Enforcing and monitoring the industry's compliance with both longstanding and recent regulations, laws, and policies.
- Collaborating with legal experts, product managers, and data science specialists to understand how to mitigate risks associated with AI projects.
- Monitoring the performance and impact of AI systems.

The first step towards achieving positive outcomes is to understand AI. This involves not only studying various draft regulations, laws, and recommendations but also understanding the different tools used in AI. This knowledge is crucial for assessing the risks associated with this new technology. While it's impossible to be familiar with every AI tool, it's beneficial to at least know the most common ones or those that might be used within the officer's company.

Officers also have a responsibility to ensure that AI systems are developed, deployed, and used in a lawful and ethical manner. However, the starting point for addressing these issues should be the legislation of the country in which the company operates. Compliance Officers and Ethics Officers should ask themselves the following questions before, during, and after the development of new AI tools:

- Does your data model account for biases?
- How representative is your dataset?
- How accurate are your predictions based on big data?
- Are there any ethical or fairness concerns associated with your reliance on big data?

II. WHAT'S THE LATEST IN THE WORLD OF COMPLIANCE?

For countries, embracing AI is a strategic move to secure a prominent role in the global AI innovation race. By being early adopters in their specific domains, countries a gain a competitive edge and bolster their economies.

The outcome of this debate will shape the future of AI governance, affecting economic competitiveness, technological progress, and societal well-being. AI legislation varies significantly across the globe due to differences in regulatory priorities, cultural perspectives, and technological development levels. Overall, while some countries prioritize innovation and economic growth in their AI strategies, others emphasize ethical considerations, privacy protections, and societal impacts. The diversity in AI legislation reflects differing national priorities and approaches to managing the opportunities and challenges posed by AI technologies.

Canada, for example, emphasises the ethical and responsible use of AI through initiatives such as the Automated Decision-Making Directive, which requires transparency and accountability in AI systems used by federal agencies. Canada also supports AI research and development, addressing privacy concerns and promoting fairness in AI applications[4], while Japan has adopted guidelines and strategies for AI development, focusing on ethics, security and international cooperation. The Japanese approach includes promoting human-centred AI, ensuring security and addressing the social and economic challenges posed by AI technologies and organisations[5].

Finally, within this framework, one should not forget the OECD and UNESCO, which develop international guidelines and standards for AI ethics, privacy and transparency with the aim to harmonize AI regulation across borders and promote global cooperation in addressing the ethical and societal impacts of AI[6].

Currently the United States, the European Union, and China are the three pivotal entities in the establishment and enforcement of AI compliance frameworks and regulations.

Specifically, China's strategy is designed to steer and financially support the advancement of AI. In contrast, the European Union prioritizes individual rights, while the United States embraces what might be termed a "*market-driven approach*". This approach results in regulatory measures that are predominantly implemented reactively, following market failures or to address associated issues. The governance of AI remains a contentious issue, one need only look, for instance, at the disagreement between the US and the EU over binding legislation. The EU considers the US executive order on AI laudable but unenforceable, while US policymakers argue that the European AI law imposes excessive burdens and stifles innovation. The ongoing debate between addressing long-term and short-term risks remains unresolved. While concerns about the potential negative consequences of AI persist, there is growing support for immediate oversight of existing AI systems, especially in the US.

A. United States Policy on Artificial Intelligence

In recent years, United States policymakers have prioritized the development and regulation of Artificial Intelligence (AI) platforms, focusing heavily on ensuring safety, security, and trustworthiness. Their efforts seek to uphold U.S. global leadership while mitigating the risks associated with this transformative technology, both to national security and individual citizens.

In 2023, Senate and House committees introduced more than 30 bills addressing various facets of AI to Congress. A significant milestone occurred on October 30, 2023, when President Joe Biden issued a landmark Executive Order. This order aims to advance civil rights, establish robust standards for AI security and safety, and foster competition and innovation within the AI sector.

[4] See: "Responsible use of artificial intelligence in government, Government of Canada".;Government of Canada. "Directive on Automated Decision-Making." Treasury Board of Canada Secretariat, April 1, 2020

[5] See: "Japan's AI Strategy. "AI for Everyone: Comprehensive AI Strategy." Cabinet Office of Japan, June 2019; Japanese Society for Artificial Intelligence. "Ethical Guidelines." 2017.

[6] See: "OECD Principles on Artificial Intelligence." OECD Legal Instruments, May 2019; UNESCO. "Recommendation on the Ethics of Artificial Intelligence." UNESCO, November 2021.

Key components of the Executive Order include:

- Protecting Consumer Privacy: Ensuring that AI deployments respect and safeguard consumer privacy rights.
- Establishing Safety and Security Standards: Requiring AI companies to disclose their safety testing results to the government, thus ensuring accountability and transparency.
- Creating Best Practices for the Justice System: Developing guidelines for the ethical and effective use of AI in the justice system.
- Promoting Competition and Innovation: Encouraging a competitive environment that spurs innovation while preventing monopolistic practices.
- Impact on the Labor Market Report: Mandating a comprehensive report to assess the potential effects of AI advancements on the labor market.[7]

These initiatives underscore the United States' commitment to harnessing AI's benefits while responsibly managing its societal impacts, reflecting a proactive approach to shaping the future of AI governance[8].

B. Regulation of Artificial Intelligence in China

The Chinese government has been one of the pioneers of AI, in fact the first initiatives were launched in 2015 and grew year after year. Confirming this, AI holds a prominent place in China's 14th Five-Year Plan (2021-2025), where it ranks first among "frontier industries". Furthermore, China boldly aims to become the world leader in AI by 2030[910].

To implement its strategic approach to the development of the AI industry, the Chinese central government has issued a series of policy documents aimed at promoting the growth of AI. Indeed, China's approach to regulating the AI phenomenon is characterised by the use of laws to address specific AI-related issues. As of now, China has enacted the following set of regulations.

The Algorithm Recommendation Regulation came into effect on March 1, 2022. This regulation pertains to the use of algorithmic technologies such as generation and synthesis, customized pushing, sorting and selection, retrieval and filtering, planning and decision-making to provide information to users.

[7] See: White House (2023, October 30): FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence.

[8] See: National Institute of Standards and Technology. (2023). Ethical Guidelines for AI: Enhancing Transparency and Accountability. NIST Special Publication 800-223.

[9] See: "Outline of the Fourteenth Five-Year Plan for the National Economic and Social Development of the People's Republic of China and the Vision 2035" (2021,March,03), Xinhua News Agency.

[10] See: "Ministry of Industry and Information Technology of the People's Republic of China. (2023). Regulations on the Development and Management of AI Technology. Beijing: MIIT".

On January 10, 2023, the Deep Synthesis Regulation was implemented[11]. Its primary objective is to impose obligations on users and providers of AI-based technologies that facilitate the creation of virtual digital humans online, as well as to prevent, guarantee, establish, and maintain an adequate level of security and protection of rights.

The Regulation on Generative AI became effective on August 15, 2023.[12] This law addresses various aspects of AI and introduces new restrictions for companies providing these services to consumers regarding the results produced and the training data used.

The Scientific and Technological Ethics Regulation came into force on December 1, 2023[13]. The scope of this regulation covers technological and scientific activities involving: (i) animals in experimental activities; (ii) humans as research participants; (iii) ethical challenges in areas such as ecology, personal information data, health.

III. THE FUTURE OF THE EUROPEAN UNION: THE EU AI ACT

Since March 2018, the European Union has been actively working on developing a comprehensive set of rules for the placement and development of AI systems within the EU market. This initiative also aims to stimulate innovation and investments in AI across Europe. On February 13, 2024 the EU AI Act was approved by the Committees of the EU Parliament. The final vote in the legislative assembly was scheduled for April.

The most recent update occurred on May 21, 2024, when the EU Council has approved the Artificial Intelligence (AI) Act[14]. After being signed by the Presidents of the European Parliament and the Council, the legislative act will be published in the Official Journal of the EU in the coming days and will enter into force twenty days after its publication. The new Regulation will apply two years after its entry into force, with some exceptions for specific provisions.

The AI Act forms a crucial part of the political guidelines for 2019-2024, during which the Commission plans to introduce legislation for a coordinated European approach on the ethical and human implications of AI. The aim of the AI Act would be to improve the functioning of the internal market and promote the deployment of reliable, human-centred AI, while ensuring a high level of protection of health, safety and fundamental rights, as set out in the Charter of Fundamental Rights of the European Union, including democracy, the rule of law and the protection of the environment, against harmful effects of AI systems in the Union, and promoting innovation.[15]

[11] See: "China Law Translate (2023, December 10) Provisions on the Administration of Deep Synthesis Internet Information Services".

[12] See: China Briefing (2023, July, 27): How to Interpret China's First Effort to regulate GENERATIVE AI MEASURES.

[13] See: Han Kun Han Kun Law Firm Han Kun (2023, April, 08) - Opinions | Brief Comment on "Measures for Ethical Review of Science and Technology (Trial) (Draft for Public Comments).

[14] See: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM/2021/206 final

[15] See: Council of the EU, Press release (2024, May, 21) Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI.

A key aspect of the EU legislation lies in its attempt to strike a balance between 'protection' and 'innovation'. By optimizing operations, prediction, and resource allocation, the use of Artificial Intelligence can support environmentally and socially beneficial outcomes, while also providing key competitive advantages to companies and the European Union.

The specific objectives of the AI framework can be summarized as follows:

- Ensure that AI systems placed in the EU market respect Union Values and existing laws on fundamental rights.
- Enhance governance and effective enforcement of existing laws on fundamental rights and safety requirements applicable to AI systems.
- Prevent the development of market fragmentation and promote a single market for safe, lawful, and trustworthy AI applications.
- Ensure legal certainty to facilitate innovation and investment in AI

To achieve these goals, the EU has adopted the following approach:

- Overhaul of the governance system with some enforcement powers at the EU level.
- Different rules for users and providers depending on the level of risk ("*high risk approach*"). The Regulatory Framework categorizes the risk into four levels: "unacceptable risk; high risk; limited risk and minimal risk".
- Extension of the list of prohibitions, but with the possibility of the use of remote biometric identification by law enforcement authorities in public spaces[16].
- Better protection of rights by requiring that operators of risky AI systems carry out a fundamental rights impact assessment before deploying an AI system.
- Prioritizing transparency, traceability, safety, environmental friendliness, and non-discrimination in AI systems used in the EU.
- Creation of the European AI Office, which will work alongside national market surveillance authorities, to ensure coordination and supervise the enforcement and implementation of new rules of artificial intelligence.

IV. THE BIGGEST CHALLENGE FOR THE EUROPEAN UNION

The European Union faces a formidable challenge in harmonizing its diverse legislative framework for Artificial Intelligence (AI). This framework necessitates strict adherence to existing EU laws, including the EU Charter of Fundamental Rights, EU Regulation 2016/679, Directive (EU) 2016/680, and various national regulations. This requirement introduces substantial complexities and hurdles during the stages of implementation and enforcement.

[16] See: Council of the EU. (2023, December 9). Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world. Consilium. Retrieved February 2, 2024.

The integration of AI legislation into the existing legal landscape poses a significant efficiency concern, potentially diminishing the EU's attractiveness compared to other global counterparts. Analysis reveals a notable disconnect between AI regulations and other legislative areas, highlighting an unresolved issue.

To bolster its appeal, ensure effective integration of AI technologies, and promote the European AI market, the EU must address these challenges comprehensively. It is crucial for the EU to streamline its regulatory approach, fostering cohesion across its legal frameworks while maintaining alignment with fundamental rights and ethical considerations.[17]

[17] See: "Challenges in AI regulation and governance in the EU" European Parliamentary Research Service (2023). Artificial Intelligence: Challenges for Europe.", "For more insights on the impact of AI on society and economy, see: Acemoglu, D., & Restrepo, P. (2019). Artificial Intelligence, Automation and Work. NBER Working Paper No. 24196.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

DECEPTIVE FOOD LABELS À LA "ORGANIC" OR "FAIRTRADE": FRAUD IN GERMAN CRIMINAL LAW?

Nedret Madak

AUTHOR

Nedret Madak is an attorney-at-law at the law firm Witzel Erb Backu & Partners in Munich, Germany, and also holds a Bachelor of Laws degree in business law. In practice, he specializes in business criminal law and tax criminal law. Nedret Madak defends companies as well as individuals.

TABLE OF CONTENTS

I. INTRODUCTION

This article examines the question of whether a manufacturer is liable to prosecution for fraud if he sells food that is labeled, for example, as "organic" or "fairtrade" even though the product does not actually meet these criteria. In the present article, this legal question is examined based on the (objective) offense of fraud under Section 263 (1) of the German Criminal Code ("StGB"), which provides a fine or a prison sentence of up to five years. In particularly cases such as commercial fraud, a prison sentence of up to ten years may be imposed. In order not to overload the article, the relationship between the food producer ("**seller**") and the buyer is considered.[1]

In view of the international nature of this medium, this article merely aims to raise awareness of this criminal law issue. Therefore, the main features of the objective elements of fraud are presented and the legal opinions are summarized concisely. With regard to causality and the subjective elements of fraud, it can be anticipated in this constellation that no specific peculiarities are recognizable, which is why these points will not be discussed. In addition to the Section 263 (1) StGB discussed here, other criminal offenses may also be relevant.

II. THE GERMAN OFFENSE OF FRAUD ACCORDING TO SECTION 263 (1) STGB

In objective terms, the following requirements must be met:

- Deception
- Error of the deceived person
- Disposition of assets
- Financial loss

A. Deception

An act of deception is understood to be the influence on a person's perception in order to cause an error.[2] This can be done by pretending false facts, distorting or suppressing true facts - it is undisputed that deception can also be caused by implied behavior.[3]

Typically, sellers print recognized labels on their food packaging (e.g. "organic"). In any case, such labels are based on facts that can cause deception.4 When it comes to the seller's own labeling (e.g. simply: "organic eggs"), this may be assessed differently. In these cases, the decisive factor is whether the seller provides sufficient information regarding the own label. Only then can the seller mislead the customer. [5]

[1] For differentiation in other circumstances: *Heghmanns*, ZIS 2015, 102 (102).

[2] *Perron*, in: Schönke/Schröder, 30th edition 2019, Section 263 StGB no. 11.

[3] *Perron*, in: Schönke/Schröder, 30th edition 2019, section 263 StGB no. 11.

[4] *Hefendehl*, in: Münchener Kommentar, 4th edition 2022, section 263 StGB no. 101.

[5] *Hefendehl*, in: Münchener Kommentar, 4th edition 2022, section 263 StGB no. 101.

B. Error of the Deceived Person

An error exists if the deception creates or maintains a misconception about facts.[6] The deceptive act must therefore lead to a misconception on the part of the customer. If food packaging is incorrectly labeled and the customer assumes that it is correct, an error is given.

However, this presupposes that the customer is actively thinking about the meaning of the labeling in the first place.[7] Anyone who does not give any thought to this and chooses a product from the shop shelf without thinking about the meaning of a certain label cannot be subject to error. This also poses practical challenges for law enforcement authorities. With products sold by the thousands or millions, it can be difficult to find out what each customer was thinking. This could already be an initial approach for the criminal defense.[8]

The fact that a customer has no exact idea of the material background of the food label does not exclude an error. It is sufficient for the customer to recognize that organic products must meet special requirements compared to conventional products[9]. Particularly in the case of mass-business, it is sufficient if the customer has a so-called "co-awareness" - i.e. simply assumes that the label meets all required standards.[10]

C. Disposition of Assets

Any action, toleration or omission that directly leads to a reduction in the customers assets is a disposition of property.[11] This requirement is regularly met in the cases discussed because the customer buys a certain food product or pays a higher price for this product than for conventional products precisely because of the expectations created by the label. In this respect, the deceptive error leads to the customer paying the specified purchase price.

D. Financial Loss

A financial loss is present if the comparison between the customers assets before and after the erroneous disposition of assets results in a minus.[12] A loss is to be denied if the customer receives compensation that compensates for his loss of assets. The present legal question revolves primarily around this requirement.[13] For example, a customer who buys a product for 1 euro because it is allegedly from "fair production in Europe" and then discovers that the product was actually produced in Vietnam does not necessarily cause a damage to their assets.[14] After all, he may have received a quality and usable product in return for a purchase price that is not out of line with the market.

[6] *Dannecker*, in: Graf/Jäger/Wittig, 3rd edition 2024, section 263 StGB no. 79.
[7] See *Perron*, in: Schönke/Schröder, 30th edition 2019, section 263 StGB no. 39.
[8] However, please note: BGH, judgment of 22.05.2014 - 4 StR 430/13.
[9] *Puschke*, ZLR 2019, 225 (230 f.); *Perron*, in: Schönke/Schröder, 30th edition 2019, section 263 StGB no. 39.
[10] *Magnus*, in: Tsambikakis/Rostalski,1st edition 2023, section 263 StGB no. 100 f.
[11] *Kindhäuser/Hoven*, in: Kindhäuser/Neumann/Paeffgen/Saliger, 6th edition 2023, section 263 StGB no. 197 f.
[12] BGH, judgment of 23.02.1982 - 5 StR 685/81.
[13] BGH, judgment of 04.03.1999 - 5 StR 355-98.
[14] In a prominent case: https://www.lto.de/recht/nachrichten/n/fynn-kliemann-verfahren-eingestellt-stade.

In any case where value-relevant factors on the market are actually negatively affected, compensation is excluded. If, for example, meat is labeled as "organic" although it was produced conventionally and therefore has a lower quality per se and therefore a lower value due to actual circumstances (e.g. inferior food for animals[15]), there is actually no compensation - which means there is a financial loss.[16] Sellers have already been convicted in such cases.[17]

However, what is the case if the product advertised as "organic" is correspondingly more expensive, although it was not actually produced organically, but does not show any significant difference in quality to an "organic product" - is there no compensation for financial loss in this case either?

The requirement "financial loss" can in principle be corrected by the "doctrine of misappropriation": It is recognized that financial loss cannot be assessed solely on an economic basis. This would lead to the customers non-economic financial dispositions caused by the deception being disregarded, even though he made them precisely because of the deception.[18]

1. Basic Case of Doctrine of Misappropriation

This is recognized, for example, in donation cases.[19] Anyone who (deceptively) donates for charitable reasons does not expect any economic compensation. However, they make the disposition of assets because they believe that their donation will achieve a social purpose. If this social purpose is not achieved due to the deception, the customers assets are nevertheless damaged according to the doctrine of misappropriation[20]: This is because there was no compensation in the form of the achievement of the purpose.

2. Exchange-business with an Additional Social Aspect

Some hold a different view in case of economic exchange transactions with an additional feigned social aspect: anyone who buys food on the assumption that part of the purchase price or the (increased) purchase price serves a social purpose (e.g. "organic product") should not suffer financial loss if they receive a compensatory economic consideration in return, even if the social purpose was not achieved at all.[21] The decisive factor therefore remains whether a compensatory consideration was received.

If this is the case, there is no financial loss and therefore no fraud.[22] Usually, this is likely to be the case if a product - despite being deceptively advertised as "organic" - is of comparable quality. There is no financial loss given in this constellation because the increased price is then compensated. However,

[15] See *Heghmanns*, ZIS 2015, 102 (102).

[16] LG Bielefeld, judgment of 07.06.2010 - 1 KLs - 6 Js 9/09 / 1/10; LG Kiel, judgment of 13.02.2009 - 3 Kls 8/08.

[17] LG Bielefeld, judgment of 07.06.2010 - 1 KLs - 6 Js 9/09 / 1/10; LG Kiel, judgment of 13.02.2009 - 3 Kls 8/08.

[18] See BGH, judgment of 10.11.1994 - 4 StR 331/94; *Hefendehl*, in: Münchener Kommentar, 4th edition 2022, section 263 StGB no. 31 f.

[19] *Hefendehl*, in: Münchener Kommentar, 4th edition 2022, section 263 St
#GB no. 31 f.

[20] BGH, judgment of 07.09.2011 - 1 StR 343/11.

[21] *Eisele*, in: Strafrecht BT II, 6th edition 2021 no. 630; see *Schröder*, in: Momsen/Grützner, 2nd edition 2020 section 18 no. 134 f; *Puschke*, ZLR 2019, 225 (232); *Satzger*, JURA 2009, 518 (524).

[22] *Eisele*, in: Strafrecht BT II, 6th edition 2021 no. 630; *Satzger*, JURA 2009, 518 (524); *Puschke*, ZLR 2019, 225 (232); *Heghmanns*, ZIS 2015, 102 (105 f.).

this means that the doctrine of misappropriation, which is recognized in jurisdiction, is not taken into account.[23] It also considers a financial loss to exist if an economic exchange-business for the customer was also linked to a social purpose that was not achieved.[24]

Though, the prerequisite for this is that the achievement of the social purpose was necessary for the customer and a decisive basis for the conclusion of the business - i.e. the customer would not have concluded the transaction without this social condition, despite the exchange of goods.[25] It is argued that a typical customer does not consider the purchase of organic eggs, for example, to be *necessary* because, if there were no organic eggs, they would possibly fall back on conventional eggs.[26] Whether this is actually the case is questionable, especially in view of the growing social awareness of animal welfare, climate-friendly and social-friendly consumption. Presumably, some customers would actually refrain from buying conventional eggs or switch to substitute products if organic eggs were not available. This can be countered by the fact that a customer's subjective expectations would impact the determination of a financial loss.[27]

III. RELEVANCE FOR COMPLIANCE MANAGEMENT SYSTEMS IN COMPANIES

From a preventative perspective, companies must be aware of this legal uncertainty as part of their compliance management system and align their compliance measures accordingly. This is because recent cases show that the prosecution authorities have discontinued proceedings for reasons of expediency and not because a fraud offense was completely ruled out.[28]

Instead, each case must be considered individually.[29] The labels discussed here are not exhaustive; the considerations can be applied to a large number of food labels (e.g. "certified sustainable fisheries", "GMO-free", "animal welfare initiative"). In addition, the considerations can in principle also be applied to other business sectors, such as the textile industry ("Blue Angel" or "Global Organic Textile Standard"). The legal situation is clearer for products of actual inferior quality on the market that are labelled as organic although they come from conventional production: there is a clear risk of criminal liability here, which should not be neglected - especially in a business context this will be considered as commercial fraud, which leads to a higher threat of punishment.

[23] BGH, judgment of 10.11.1994 - 4 StR 331/94.

[24] BGH, judgment of 11.09.2003 - 5 StR 524/02; see *Perron*, in: Schönke/Schröder, 30th edition 2019, section 263 StGB no. 105.

[25] BGH, judgment of 11.09.2003 - 5 StR 524/02; see *Perron*, in: Schönke/Schröder, 30th edition 2019, section 263 StGB no. 105.

[26] See *Heghmanns*, ZIS 2015, 102 (106).

[27] see *Heghmanns*, ZIS 2015, 102 (107 f.).

[28] In this regard: https://www.lto.de/recht/nachrichten/n/fynn-kliemann-verfahren-eingestellt-stade, section 153a (1) StPO; https://rp-online.de/nrw/staedte/geldern/boehmermann-vorwuerfe-ermittlungen-gegen-illbruck-nun-eingestellt_aid-89722591, section 153 (1) StPO.

[29] See *Dannecker*, in: Graf/Jäger/Wittig, 3rd edition 2024, section 263 StGB no. 318.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

BOOK RECOMMENDATION

The Leader Upheaval Handbook: Lead Teams on an Innovation & Collaboration Journey with The 3-4-5 Method, 2023, ISBN 978-1639053476

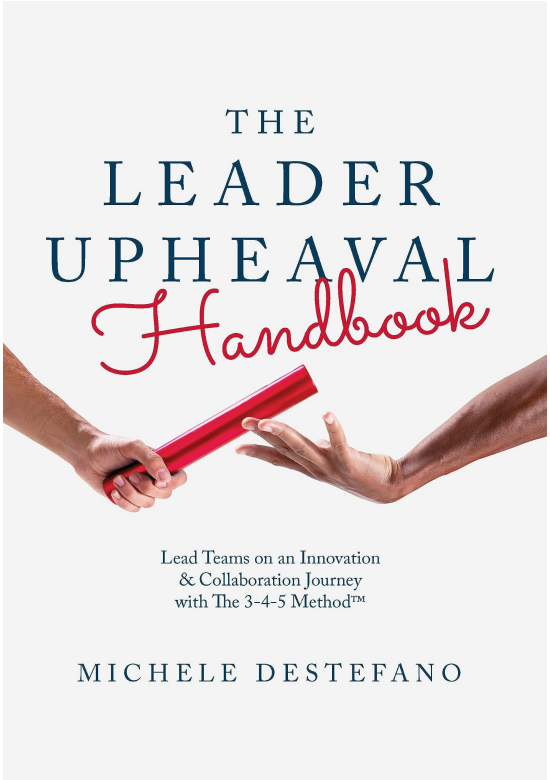
Michele DeStefano - FOUNDER AND CONTENT CURATOR CEJ

AUTHOR

Michele DeStefano is the founder and director of » LawWithoutWalls and a Professor of Law at » Miami Law. She is an expert in entrepreneurship in the law. Her scholarship focuses on the growing intersections between law and business and legal entrepreneurship. Through qualitative interviews of general counsels and other professional service providers, Michele's research investigates the impact changes in the law and business marketplace (including litigation funding, social media, public relations, regulation) will have on the legal profession and its potential for innovation. Her latest project includes over seventy interviews of general counsels and chief compliance officers of large, publicly traded corporations to analyze and assess the changing role of compliance.

In addition to spearheading LawWithoutWalls, Michele presents regularly on Innovation, Teaming, Collaboration, Compliance, Technology and Education, and Litigation Funding. She teaches courses on the changing legal profession, law, technology, and innovation, civil procedure, professional responsibility, and compliance. Recently, she was recognized by the ABA as one of ten » 2013 Legal Rebels.

From 2003 to 2004, Michele clerked for Chief Judge William G. Young of the Federal District Court of Massachusetts. She also worked for a year as a Special Master on a patent law case. Before attending law school, she was a Senior Marketing Manager at Levi Strauss & Company (1995-1998) and an Account Executive at Leo Burnett Advertising Company (1991-1995). Michele earned a J.D., magna cum laude, from Harvard Law School and a B.A., magna cum laude, from Dartmouth College and has been admitted to the Massachusetts, Minnesota, and District of Columbia bars.



SUMMARY

One of the barriers to innovation in professional services is a lack of training in how to apply design thinking principles and lead multidisciplinary teams in collaborative problem solving. With this handbook, which accompanies her other books Leader Upheaval and Legal Upheaval, Professor Michele DeStefano attempts to fill in this training gap.

DeStefano – a former marketing executive and now a professor at the University of Miami School of Law and Affiliated Faculty and Program Chair in Harvard Law School's Executive Education program – has spent over a decade researching client-centricity, collaboration, and innovation. This handbook, and the method it is based on, are the fruit of DeStefano's 13 years of experience leading over more than 230 multidisciplinary, multicultural, and intergenerational teams on a 4-month innovation journey from a problem to a viable solution.

In a conversational and descriptive fashion, DeStefano provides detailed instructions on how to get teams to proactively collaborate and innovate with a process she developed over the years. The 3-4-5 Method™ helps teams move from problem to innovative solution in 3 Phases, over 4 months or less, in 5 Steps. With real examples, this handbook brings to life how to help teams collaborate on solving problems or seizing opportunities of any kind and yield a higher level of collaboration, inclusivity, creative thinking, and actionable results.