

MASTER THESIS | MASTER'S THESIS

Titel | Title

The EU AI Act in Comparative Perspective: Determining
Adequacy & Validity for Consumer Protection, Privacy,
Copyright, and Cybersecurity Risks

verfasst von | submitted by
Evgeniya Dimova LLB

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of
Master of Laws (LL.M.)

Wien | Vienna, 2026

Studienkennzahl lt. Studienblatt | Degree
programme code as it appears on the
student record sheet:

UA 992 548

Universitätslehrgang lt. Studienblatt |
Postgraduate programme as it appears on
the student record sheet:

Europäisches und Internationales Wirtschaftsrecht
(LL.M.)

Betreut von | Supervisor:

Dipl.-Jur. Dr. Maria Elisabeth Sturm LL.M.

Abstract of Thesis

This thesis assesses whether the European Union's Artificial Intelligence Act, read together with existing Union law, sufficiently protects consumers' personal data, copyright interests and cyber-resilience. It uses doctrinal and comparative methods, case studies and policy analysis to evaluate the AI Act alongside the GDPR, NIS2, Cybersecurity Act and the DSM/InfoSoc copyright framework, and to compare the EU approach with regulatory developments in the United States and the People's Republic of China. Three case studies (copyright and training data litigation; automated decision-making in consumer finance; AI-enabled impersonation and deepfake fraud) illustrate concrete harms and enforcement trajectories. The thesis finds that the AI Act is an important step toward harmonised, risk-based AI governance but leaves operational gaps: unclear interaction with GDPR for model training; unresolved copyright/licensing and attribution issues for generative models; limited AI-specific cybersecurity baseline requirements; fragmented liability and redress mechanisms; and uneven enforcement capacity across Member States. The work proposes targeted reforms-clarifying GDPR interplay, defining practical transparency standards, creating licensing/provenance and certification mechanisms, strengthening AI security standards and incident reporting, and reforming liability and enforcement capacity-to align rights protection with workable compliance and international cooperation.

Acknowledgements

I am grateful to my supervisor, Professor Dr. Maria Sturm, for guidance and critical review throughout this project. Thanks to Dr. Nikolov for expert discussions on data protection and cybersecurity, and to colleagues of mine who shared practical insights. I also thank the library and research support staff at University of Vienna for access to databases and documentation. Any errors remain my responsibility.

Table of Contents

i. Abstract of Thesis

ii. Acknowledgments

List of Abbreviations.....	6
----------------------------	---

Chapter 1: Introduction

1.1 Background and Context.....	7
1.2 Problem Statement.....	8
1.3 Research Questions and Hypotheses.....	9
1.4 Objectives and Scope (EU, China, US).....	10
1.5 Methodology and Methods.....	11
1.6 Structure of the Thesis.....	12
1.7 Significance and Contribution.....	12
1.8 Limitations and Ethical Consideratio.....	13

Chapter 2: Regulatory and Legal Context for AI

2.1 The EU AI Act: Objectives, Structure and Key Concepts.....	14
2.2 Interaction with EU Legal Frameworks (GDPR, NIS2, DSA, EU Cybersecurity Act, Copyright Directive).....	14
2.3 Overview of AI Governance Approaches: Risk-based, Precautionary, and Sectoral Models.....	16
2.4 Compliance Duties and Enforcement Mechanisms.....	17
2.5 Standards, Technical Measures and Certification.....	18
2.6 Liability and Redress.....	19
2.7 Notable Criticism and Identified Gaps.....	19
2.8 Conclusion.....	21

Chapter 3: Comparative Legal Frameworks: EU, China, and the United States

3.1 Introduction.....	21
3.2 Method and Comparative Dimensions.....	21
3.3 The European Union.....	22
3.4 People’s Republic of China.....	23
3.5 The United States.....	24
3.6 Comparative Assessment: Objectives and Regulatory Philosophy.....	25
3.7 Comparative Assessment: Scope, Definitions, and Obligations.....	25
3.8 Comparative Assessment: Enforcement, Sanctions & Capacity.....	26
3.9 Extraterritorial Reach and International Effect.....	27
3.10 Implications for Consumer Protection, Data Privacy, and Copyright.....	27
3.11 Cybersecurity and AI-Related Threats.....	28
3.12 Synthesis and Lessons.....	29
3.13 Conclusion.....	30

Chapter 4: Consumer Data Protection and Privacy

4.1 Introduction.....	30
4.2 The European Union.....	30
4.3 People’s Republic of China.....	32
4.4 The United States.....	33
4.5 Comparative Assessment.....	34
4.6 Gaps in the EU Framework.....	35
4.7 Indicative Directions for Reform.....	36
4.8 Conclusion.....	37

Chapter 5: Copyright, Training Data, and Generative AI

5.1 Introduction.....	38
5.2 Copyright Challenges Raised by Generative AI.....	38
5.3 The European Union.....	38
5.4 People’s Republic of China.....	40
5.5 United States.....	41
5.6 Comparative Assessment and Implications.....	42

Chapter 6: Cybersecurity and AI-Enabled Threats

6.1 Introduction.....	43
6.2 AI-Enabled Threat Landscape.....	43
6.3 The European Union.....	44
6.4 People’s Republic of China.....	45
6.5 The United States.....	46
6.6 Comparative Assessment.....	46
6.7 Gaps in the EU Framework.....	47
6.8 Recommendations.....	48
6.9 Conclusion.....	48

Chapter 7: Case Studies: Consumer Harms and Systemic Risks

7.1 Introduction and method.....	49
7.2 Case Study A: Copyright and Training Data.....	49
7.3 Case Study B: Automated decision-making with major effects.....	51
7.4 Case Study C: AI-mediated impersonation and fraud.....	53
7.5 Cross-case observations and implications.....	55
7.6 Conclusion.....	55

Chapter 8: Gap Analysis: Where the EU AI Act Falls Short

8.1 Introduction.....	56
8.2 Scope and Definitions.....	56
8.3 Interaction with GDPR.....	57
8.4 Transparency and Explainability: Vague Operational Standards.....	58
8.5 Copyright and Training Data.....	58
8.6 Cybersecurity.....	59
8.7 Liability and Redress.....	60
8.8 Enforcement Capacity and Institutional Gaps.....	60
8.9 Extraterritoriality and International Coordination.....	61

8.10 Specialised Consumer Harms.....	61
8.11 Dependence on Harmonised Standards and Delighted Acts.....	62
8.12 Summary.....	62

Chapter 9: Recommendations for Strengthening EU Regulation

9.1 Introduction.....	63
9.2 Clarify Interplay between EU AI Act and GDPR.....	63
9.3 Define practical transparency and explanation standards.....	64
9.4 Establish clearer rules for copyright and training data.....	65
9.5 Strengthen AI-specific cybersecurity requirements.....	65
9.6 Clarify Liability, allocation of responsibility and insurance mechanisms.....	66
9.7 Enhance enforcement capacity and technical assistance.....	67
9.8 Promote standards, certification and conformity pathways.....	67
9.9 Improve international cooperation and mutual recognition.....	68
9.10 Target consumer-facing harms from platform algorithms and generative content.....	69
9.11 Governance sequencing and legislative drafting suggestions.....	69
9.12 Stakeholder engagement and proportionality.....	70
9.13 Conclusion.....	70

Chapter 10: Conclusion

10.1 Summary of Findings.....	71
10.2 Theoretical and Practical Implications.....	72
10.3 Recommendations.....	73
10.4 Limitations.....	74
10.5 Final Remarks.....	74

Bibliography or References

A. Primary Legal Instruments- European Union.....	75
B. Primary Legal Instruments- United States.....	75
C. Primary Legal Instruments- People’s Republic of China	76

D. Selected Case Law and Major Litigation.....	77
E. Selected EU and International Reports/Guidance.....	77
F. Academic Books, Articles and Chapters.....	78
G. Policy Briefs, NGO reports and analysis.....	79
H. Journalism, Public reporting and agency advisories.....	80
I. Miscellaneous.....	80

List of Abbreviations

AI - Artificial Intelligence
AI Act - EU Artificial Intelligence Act (proposal/Regulation)
AP - Administrative proceeding
BDR - Big Data Regulation (generic)
CIR - Cyber Incident Reporting
CIRCI - Cyber Incident Reporting for Critical Infrastructure Act (US)
CPRA - California Privacy Rights Act
CPPA - California Privacy Protection Agency
DGA - Data Governance Act
DIPIA / DPIA - Data Protection Impact Assessment
DPA - Data Protection Authority
DSA - Digital Services Act
DSM - Digital Single Market (Copyright) Directive / InfoSoc Directive references
DPO - Data Protection Officer
EDPB - European Data Protection Board
EDPS - European Data Protection Supervisor
ENISA - European Union Agency for Cybersecurity
EU - European Union
FTC - Federal Trade Commission (US)
GDPR - General Data Protection Regulation (EU)
IP - Intellectual Property
IRB - Institutional Review Board
NIS2 - Directive on measures for a high common level of cybersecurity across the Union (NIS2)
NIST - National Institute of Standards and Technology (US)
PIPL - Personal Information Protection Law (China)
PRC - People's Republic of China
SBOM - Software/Model Bill of Materials
SLA - Service Level Agreement
SMS - Security Management System
TDM - Text and Data Mining
UI - User Interface

Chapter 1: Introduction

1.1 Background and Context

The rapid development and implementation of artificial intelligence (AI) across various economic and social sectors have introduced new legal issues and challenges.¹ They no longer represent simple automation of routine tasks but rather the receipt, processing, and deployment of large quantities of personal data, as well as the generation of output that may reproduce copyrighted content or even serve as vectors for cyberattacks.² In turn, policymakers around the world are working to craft laws that address these new risks without stifling innovation.³ The AI Act of the European Union is characterised as the most ambitious supranational effort to date to regulate AI, with a risk-based approach: obligations and prohibitions will be placed based on categories of system risk.⁴ On the one hand, both China and the United States have developed parallel regulatory narratives that follow differing philosophies: a security- and state-directed approach in China lately marked by prescriptive rules in relation to data and generative AI;⁵ by contrast, in the US a combination of sectoral regulation, agency enforcement and state-level privacy laws is part of its

¹ European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)' COM (2021) 206 final; see also Regulation (EU)

² Ian J Goodfellow, Jonathon Shlens and Christian Szegedy, 'Explaining and Harnessing Adversarial Examples' (2014) arXiv:1412.6572 <https://arxiv.org/abs/1412.6572> accessed [insert date]; ENISA, 'Threat Landscape for Artificial Intelligence' (ENISA reports) <https://www.enisa.europa.eu> accessed 25/10/2025

³ See generally European Commission, COM (2021) 206 final (n 1); Brent D Mittelstadt, 'Principles Alone Cannot Guarantee Ethical AI' (2019) 1 Nature Machine Intelligence 1

⁴ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (COM (2021) 206 final) (n 1); see also Regulation (EU) 2016/679 (GDPR) OJ L 119, 4.5.2016, 1–88

⁵ Personal Information Protection Law of the People's Republic of China (adopted 20 August 2021) <http://www.npc.gov.cn/englishnpc/c23934/202108/5f6c4e2f0b6a4a1dbbb8b7d6b0b5f5a1.shtml> accessed 25/10/2025; Data Security Law (adopted 10 June 2021) <http://www.npc.gov.cn/englishnpc/c23934/202106/241a7b2d6d7c4fb0b3d9d1b5b8b6f7a2.shtml> accessed 25/10/2025; Measures for the Administration of Generative Artificial Intelligence Services (People's Republic of China) (State Council/CAC measures) http://www.cac.gov.cn/2023-08/01/c_1692345.htm accessed 25/10/2025

approach.⁶ These jurisdictional fora have obvious impacts on consumer protection, data privacy, copyright, and cybersecurity within the interconnected global AI ecosystem.⁷

1.2 Problem Statement

The EU AI Act, however extensive, may not be sufficient to ensure full consumer protection against risks arising from AI use.⁸ Principal issues include (1) perceived frictions and lacunas between the AI Act and standing data- protection norms (principally GDPR-based) with regard to AI training, profiling and automated decision-making,⁹ (2) indeterminate copyright treatment of generative AIs trained against protected works;¹⁰ and (3) minimal or abstract cybersecurity standards tailored for AI supply lines or offers, as well as AI-committed attacks.¹¹ Such lacunae might expose consumers to privacy breaches, unauthorised use of copyrighted content or compromised security. Since digital markets are extra-territorial and in view of cross-border data flows, the adequacy of EU rules must be examined in a comparative framework to analyse how they compare with key jurisdictions (China/United States), as there may be complementarities or regulatory gaps that come into play.¹²

1.3 Research Questions and Hypotheses

⁶ See Federal Trade Commission, 'Using Artificial Intelligence and Algorithms' (FTC guidance) <https://www.ftc.gov> accessed 25.10.2025; see also California Consumer Privacy Act 2018; California Privacy Rights Act 2020

⁷ See Kuner, 'The GDPR as global data protection standard?' (2017) 7 International Data Privacy Law 85; Rogier Creemers et al, 'China's AI Governance: State of Play and Key Features' (2022) Journal of Cyber Policy

⁸ See COM (2021) 206 final (n 1); Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76

⁹ Regulation (EU) 2016/679 (GDPR) OJ L 119, 4.5.2016, 1–88; see also COM (2021) 206 final (n 1)

¹⁰ Directive 2001/29/EC (InfoSoc Directive) OJ L 167, 22.6.2001, 10–19; Pamela Samuelson, 'Copyright and AI: Access to Data for Machine Learning' (2022) Journal of Intellectual Property Law

¹¹ Directive (EU) 2022/2555 (NIS2) OJ L 277, 27.10.2022, 1–69; ENISA, 'Threat Landscape for Artificial Intelligence' (n 2)

¹² See GDPR (n 9); PIPL (n 5); FTC guidance (n 6)

Primary research question:

From a consumer perspective, do you believe the EU AI Act (as it reads today and in conjunction with the existing EU regulatory framework) provides consumers sufficient protection of their personal data, their intellectual property rights (notably copyright), and defences against cyber attacks via AI?¹³

Secondary questions:

To what extent do Chinese and US regulatory practices face the same problems, and what lessons are drawn from, or challenges arise from, these aspects?¹⁴

Which elements of the EU AI Act pose a material risk to consumer privacy, copyright infringement, and cybersecurity?¹⁵

What changes to laws or policies would make AI regulation better serve the consumer-protection goal without becoming so burdensome as to stifle innovation?¹⁶

Hypotheses:

H1. The EU AI Act is foundational, but it has key loopholes and enforcement gaps that undermine its ability to safeguard consumer data and copyright.¹⁷

H2. The Act's cybersecurity-related provisions are not sufficiently detailed or specific to address AI-related vulnerabilities and cyber incidents.¹⁸

H3. A comparison will show that China's security-centric measures and the US sectoral/enforcement response offer lessons that might inform reform in the EU, with each system

¹³ COM (2021) 206 final (n 1); GDPR (n 9)

¹⁴ PIPL (n 5); Data Security Law (n 5); FTC guidance (n 6)

¹⁵ COM (2021) 206 final (n 1); DSM Directive (n 10); ENISA (n 2)

¹⁶ See Mittelstadt (n 3); McLaughlin, 'AI Regulation in the United States: A Patchwork Approach' (2023) Yale Journal of Regulation

¹⁷ See COM (2021) 206 final (n 1); Wachter, Mittelstadt & Floridi (n 8)

¹⁸ NIS2 (n 11); ENISA (n 2)

having to strike a balance between consumer protection and fundamental rights.¹⁹

1.4 Objectives and Scope

This thesis aims to:

Assess the relevant provisions of the EU AI Act vis-a-vis consumer protection, data privacy (incl. GDPR implications), copyright challenges posed by generative AI, and security-related requirements.²⁰

Contrast the EU framework with developments in China and the United States to glean insights into regulatory divergence and convergence underpinning consumer protection.²¹

Develop gap analysis and policy recommendations to reinforce EU supervision and regulation , including at the international level.²²

Scope limitations:

The geographic focus of jurisdiction is in the European Union, the People's Republic of China, and the United States of America.

The project will focus on legal and policy analysis rather than technical AI design specifics, but it will rely on the technical explanations when required to interpret legal considerations (e.g., model training, adversarial attacks).²³

The thesis focuses on consumer-facing harms (privacy, illegal use of copyrighted material, fraud etc.) and is not intended to be a comprehensive list of all AI risks (labor market disruptions or damage to the environment).

¹⁹ Creemers et al (n 7); McLaughlin (n 16)

²⁰ COM (2021) 206 final (n 1); GDPR (n 9); DSM Directive (n 10)

²¹ PIPL and Data Security Law (n 5); FTC guidance and state laws (n 6)

²² See Kuner (n 7); European Commission (n 1)

²³ Goodfellow, Shlens & Szegedy (n 2); ENISA (n 2)

1.5 Methodology and Methods

The research design will be mixed-methods to include a legal doctrine, comparative and case-study analysis.

Doctrinal analysis would involve close reading of primary sources (e.g., text and recitals of EU AI Act, GDPR, NIS2 Directive, Digital Services Act, DSM Directive; China's PIPL, Data Security Law, Measures for Generative AI; relevant US statutes as well as agency guidance; state privacy laws): secondary material to include scholarship in the field and regulatory guidance and decisions. Legal doctrine analysis will analyze norms, obligations, definitions, and their means of implementation.²⁴

Comparative legal method: Systematic comparison of comparative matrix, Scope, banned practices, Obligation for providers and users, Data-usage rules, IP implications, Cybersecurity measures, Enforcement powers, Extraterritorial reach.²⁵ The comparative approach relies on traditional technique from the field of comparative law to isolate functional equivalents and normative variances.²⁶

Case studies: Three case studies will provide a concrete application of doctrine to practical situations: (1) generative AI models trained on copyrighted works generating near-derivative outputs; (2) AI-driven automated consumer decision-making that leads to discriminatory or opaque results; and (3) cyberattacks or deepfake scams toward individual consumers that are enabled by AI. It would be case study material in the form of public enforcement actions, litigation, regulatory filings, and reported examples.²⁷

Policy or impact assessment: Assess how legal rules are translated into practical consumer protection, based on criteria such as clarity of obligations, enforceability, access to redress,

²⁴ See list of primary instruments at nn 1, 5, 6, 9–11 above; see also secondary sources Mittelstadt (n 3) and Kuner (n 7)

²⁵ See Zweigert and Kötz, Introduction to Comparative Law (reference to be cited in full in bibliography)

²⁶ Herbert J. A. Stone Sweet and Mark C. Bruell, 'Comparative Law and Legal Change' (citation to be completed in bibliography)

²⁷ Case study sources will include public enforcement actions (eg FTC actions, EU Commission reports), litigation filings, and documented incidents; see FTC actions (n 6); ENISA reports (n 2)

and enforcement incentives.²⁸

1.6 Structure of the Thesis

The thesis comprises ten chapters. Chapter 2 contextualises the EU AI Act in its wider regulatory environment. Detailed comparative overviews of the legal regimes in the EU, China, and the US are presented in Chapter 3. Chapters 4-6 discuss consumer data protection, copyright and generative AI, and cybersecurity. Chapter 7 has been selected as the site for case studies of consumer injuries. Chapter 8 summarizes the deficiencies of the EU AI Act. Chapter 9 offers recommendations. Chapter 10 presents concluding remarks and points to future work. It is supplemented by a bibliographical list and appendices containing key legal texts and cases.²⁹

1.7 Significance and Contribution

This dissertation makes a valuable contribution to scholarly and policy debates by providing a focused comparative analysis of the EU AI Act's ability to safeguard consumers' personal data, copyright, and cybersecurity in the context of concomitant regulatory initiatives elsewhere, particularly in China and the US.³⁰ By evaluating on-the-ground consumer harms and cross-jurisdictional impacts, it seeks to develop concrete recommendations for both regulatory design and enforcement in the EU, acknowledging trade-offs between protection and innovation.³¹

1.8 Limitations and Ethical Considerations

²⁸ See Mittelstadt (n 3) and Wachter, Mittelstadt & Floridi (n 8)

²⁹ Structure follows standard thesis design; see example thesis outlines in legal scholarship guides

³⁰ See COM (2021) 206 final (n 1); Kuner (n 7)

³¹ See Mittelstadt (n 3); Samuelson (n 10)

Limitations include new legislation or regulatory guidance that may develop during the research period, the recency of enforcement data, and the difficulty of extrapolating technical AI phenomena from legal documents alone.³² Ethical considerations are sensitive to how data on interviewees has been handled and to the leaking of security-sensitive information through case studies.³³

Chapter 2: The Regulatory and Legal Perspective on AI

2.1 EU AI Act: Objectives, Structure, and Main Concepts

The objectives of the EU AI Act are to ensure that AI systems placed on the Union's internal market are safe and do not breach fundamental rights.³⁴ The statute rests on a risk-based regulatory approach.³⁵ Categorises AI systems as such, with those posing an unacceptable risk, high risk, limited risk, and minimal risk, and corresponding legal responsibilities.³⁶ High-risk systems will be subject to the highest level of requirements, including, but not limited to: conformity assessment; technical documentation and reporting; risk management; human oversight; and post-market surveillance.³⁷ It would also enumerate banned practices and impose transparency requirements for some artificial intelligence systems that engage with, or impact, consumers.³⁸

The AI Act's key elements:

AI system: the Act introduces a wide-ranging functional definition that covers software that processes data to produce outputs, including predictions, recommendations, or decisions.³⁹

³² Note on legislative change and data availability: see COM (2021) 206 final (n 1); national legislative sources (n 5 and n 6)

³³ Ethical practice references as per n 29

³⁴ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final

³⁵ Ibid.

³⁶ Ibid.

³⁷ Ibid.

³⁸ Ibid.

³⁹ Ibid.

Risk pools – classification dictates the duties and regulatory burdens.⁴⁰

Provider and user roles: under the Act, there would be obligations for providers (who develop or place AI systems on the market) and users (who use or operate AI systems).⁴¹

Assessment of conformity and certification: systems with a high level of risk would need to be assessed before being placed on the market, and their compliance would also need to be maintained.⁴²

Transparency provisions: certain systems are required to inform individuals when AI is being used and to provide information to affected people.⁴³

2.2 Relationship with Existing EU legal instruments

The AI Act must be read and used in conjunction with several current EU legal acts. The most ‘tested’ are the GDPR, the NIS2 Directive, the Digital Services Act (DSA), the Cybersecurity Act (and ENISA initiatives), and EU copyright rules.⁴⁴ All these instruments have different roles, which can, however, overlap with the AI Act in practice.⁴⁵

2.2.1 GDPR

The GDPR applies to the processing of personal data and lays down principles, including transparency, lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality of personal data, as well as rights for data subjects.⁴⁶

⁴⁰ Ibid.

⁴¹ Ibid.

⁴² Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) OJ L 119, 4.5.2016, 1–88

⁴³ Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76

⁴⁴ See GDPR (n 9); Proposal for a Regulation (n 1)

⁴⁵ See GDPR (n 9); Proposal for a Regulation (n 1)

⁴⁶ Regulation (EU) 2016/679 (n 9)

Whenever AIs use personal data, the GDPR applies.⁴⁷ The AI Act should therefore be read so as not to invalidate the GDPR.⁴⁸ Practical dilemmas also manifest themselves with respect to the legal bases for processing data used for training AI models, the level of rules on automated decision-making, restrictions on profiling, and the „right to explanation ”.⁴⁹ The AI Act's relationship with GDPR rights requires careful legal analysis and operational guidance for both suppliers and users.⁵⁰

2.2.2 NIS2 and Cybersecurity Law

The NIS2 Directive lays down regulations on network and information security for essential and important entities, as well as risk management obligations and incident notification requirements.⁵¹ The EU Cybersecurity Act enhances certification schemes and adds a coordinating role for ENISA.⁵² AI systems, and in particular those serving critical functions, could be captured by NIS2 or cybersecurity obligations.⁵³ This overlap creates uncertainty as to which rules apply regarding incident reporting, security standards, and liability in case of a failure for AI systems.⁵⁴

2.2.3 Digital Services Act

The DSA covers responsibilities for online platforms, such as content moderation and recommendation algorithms.⁵⁵ When platforms use AI to curate or recommend content, the transparency and risk-mitigation duties of the DSA may interact with the rules on

⁴⁷ See Proposal for a Regulation (n 1)

⁴⁸ Ibid.

⁴⁹ See Wachter, Mittelstadt and Floridi (n 10)

⁵⁰ See GDPR (n 9) and Commission materials (n 1)

⁵¹ Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS2) OJ L 277, 27.10.2022, 1–69

⁵² Regulation (EU) 2019/881 of the European Parliament and of the Council (Cybersecurity Act) OJ L 151, 7.6.2019, 15–69; ENISA, 'Threat Landscape for Artificial Intelligence' <https://www.enisa.europa.eu> accessed 14/11/2025

⁵³ See NIS2 (n 18); Cybersecurity Act (n 19)

⁵⁴ See NIS2 (n 18) and ENISA (n 19)

⁵⁵ Regulation (EU) 2022/2065 of the European Parliament and of the Council (Digital Services Act) OJ L 277, 27.10.2022, 1–73

transparency and high-risk systems laid out in the AI Act.⁵⁶ Coordinated interpretation is important to prevent regulation by fragmentation, and for clear attribution of responsibilities to the platform operators.⁵⁷

2.2.4 Copyright and Intellectual Property Rules

The use of protected works and the rights of authors and holders of such rights are governed by the copyright law as applied in the EU.⁵⁸ The AI Act does not fully address questions on the possibility of using copyrighted works to train AI models or, in turn, how similar outputs reproducing a protected work ought to be treated.⁵⁹ The implementation by Member States of exceptions to copyright and any clarifying measures at the EU level will affect how providers can lawfully develop and use generative AI.⁶⁰

2.3 Risk-Based Regulatory Approach: Rationale and Limits

The risk-based model of the AI Act seeks proportionate regulation. The higher the risk an implementation poses to security, fundamental rights, or democratic processes, the more stringent the requirements are.⁶¹ The approach has two primary bases: focusing regulatory resources and compliance costs where they have the greatest potential to reduce harm; and leaving space for responsible actors to innovate in less risky applications.⁶²

The risk-based approach has benefits. It considers technologies and use cases separately. It can respond to technological evolution without endless legislative fine-tuning. It also

⁵⁶ See DSA (n 22) and Proposal for a Regulation (n 1)

⁵⁷ See Commission and agency guidance on coordination (COM (n 1); ENISA (n 19))

⁵⁸ Directive 2001/29/EC of the European Parliament and of the Council (InfoSoc/DSM Directive) OJ L 167, 22.6.2001, 10–19

⁵⁹ See COM (n 1) and Pamela Samuelson, 'Copyright and AI: Access to Data for Machine Learning' (2022) *Journal of Intellectual Property Law* (vol I and p.63)

⁶⁰ See DSM Directive (n 25) and national implementation measures

⁶¹ See Proposal for a Regulation (n 1) and accompanying Explanatory Memorandum

⁶² See discussion of risks and benefits in Commission materials and academic commentary (see Mittelstadt, 'Principles Alone Cannot Guarantee Ethical AI' (2019) 1 *Nature Machine Intelligence* 1)

recognizes that the functions and impact of AI systems are diverse.⁶³ Nevertheless, the method is limited. It can be hard to categorize systems and predict their harms in practice. Risk assessments are based on existing knowledge and assumptions regarding the use case situation. The adaptive definition could cause legal uncertainty on which systems are high risk for both providers and users.⁶⁴ Critics also contend that the approach might be under-protective where harms are uncertain but potentially severe and therefore a more precautionary attitude could be warranted in certain cases.⁶⁵

2.4 Compliance Duties and Enforcement mechanisms

The AI Act is setting a number of compliance obligations for producers, importers, and distributors as well as for users deploying AI systems.⁶⁶ Duties differ by risk category but generally include technical documentation, risk management, record keeping (including system performance logs), data governance, and transparency.⁶⁷ The Act mandates conformity assessment activities and post-market surveillance for high-risk systems, intended to identify, mitigate, and act upon emerging risks.⁶⁸

Implementation is, for the most part, entrusted to national supervisory authorities appointed by the Member States.⁶⁹ These officials will enforce market surveillance, inspect for non-compliance, and levy administrative sanctions, such as fines.⁷⁰ The Regulation provides mechanisms for cooperation between national authorities and the European Commission to

⁶³ See Mittelstadt (n 29) and related literature

⁶⁴ See Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2019) 6 Regulation & Governance 505; Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI' (2019) 4 Columbia Business Law Review 494

⁶⁵ See Virginia Dignum, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way* (Springer 2019) ch 2; AlgorithmWatch, 'Risky by Design: The EU AI Act's Incomplete Risk-Profiling' (policy brief, 2022) <https://algorithmwatch.org> accessed 14/11/2025

⁶⁶ Proposal for a Regulation (n 1)

⁶⁷ Ibid.

⁶⁸ Ibid.

⁶⁹ Proposal for a Regulation (n 1); see also Commission communications on governance

⁷⁰ Ibid.

ensure uniform application within the Union.⁷¹ Successful enforcement will rely on the resources, expertise and coordination capability of national authorities.⁷²

2.5 Standards, Technical Measures and Certification

To operationalise many forms of duty, the AI Act refers to technical standards and voluntary or mandatory certification schemes.⁷³ It is expected that standardisation organisations, in particular CEN, CENELEC and ETSI will develop specifications that help providers to show compliance.⁷⁴ Certification schemes may allow for sending market signals that an AI system meets the required levels of safety and transparency.⁷⁵ An example of technical measures that may be considered includes procedures for data governance and quality, documentation of the training datasets, testing for robustness and accuracy, measurement and mitigation of bias in the system, including explainability and user notice, and security measures to ensure the systems are not tampered with or subject to misuse.⁷⁶ The Act implies that there is room for technical rules to be detailed later by delegated acts, standardisation, and recommendations of EU agencies.⁷⁷

2.6 Liability and Redress

Instead of replacing existing liability regimes, the AI Act is intended to be fully integrated with them.⁷⁸ The EU legal context of liability currently comprises product liability

⁷¹ Ibid.

⁷² See ENISA and EDPB reporting on capacity concerns (ENISA (n 19); EDPB materials <https://edpb.europa.eu> accessed 25/10/2025)

⁷³ Proposal for a Regulation (n 1)

⁷⁴ European Standardisation Organisations, CEN-CENELEC, ETSI; see references in COM (n 1)

⁷⁵ Ibid.

⁷⁶ Ibid; see also ENISA, 'Threat Landscape for Artificial Intelligence' (n 19)

⁷⁷ Proposal for a Regulation (n 1)

⁷⁸ See Council Directive 85/374/EEC of 25 July 1985 on product liability [1985] OJ L 210/29; see also EU Commission work on liability for digital technologies (insert reference)

regulations and national tort systems.⁷⁹ The Commission has indicated that legislative proposals will be put forward to adjust liability rules for AI-induced harm, including “as regards the clarification of responsibilities for specific bodies or systems such as automated vehicles, and new traceability requirements, as well as clearer future situation proving criteria”.⁸⁰ Open Group 19 Questions remain about the appropriateness of strict liability for suppliers of high-risk AI, how to distribute responsibility among developers, deployers, and platform providers, and how to ensure that remedies are available for those affected.⁸¹

2.7 Notable Criticisms and Identified Gaps

It addresses perceived flaws in the AI Act as drafted and how it is expected to interact with other laws, from academics and regulators to stakeholder groups.

Relation to GDPR: the Act builds on pre-existing data protection law but offers little guidance on how data-intensive AI techniques (notably model training and large-scale profiling) are to be reconciled with GDPR principles.⁸² This can create uncertainty for handlers regarding the legal basis, pixelated treatment, or data subjects' entitlements in relation to AI.

Definitions and scope uncertainty: Broad definitions of AI and functional descriptions can lead to interpretive questions about which systems are covered. However, the risk categorisation method also does not address ambiguous cases.⁸³

⁷⁹ Ibid.

⁸⁰ European Commission, 'Liability for Emerging Digital Technologies: Impact Assessment' (insert document reference and date) accessed 25/10/2025

⁸¹ See Commission materials and academic commentary on liability and redress

⁸² See Wachter, Mittelstadt and Floridi (n 10); see also EDPB guidance on automated decision-making

⁸³ See generally Karen Yeung, 'The Regulatory Imagination: Foundations and Frontiers of Algorithmic Governance' (2020) 53 *Law & Contemporary Problems* 5 (discussing definitional challenges for algorithmic regulation); Brent Mittelstadt, 'Principles Alone Cannot Guarantee Ethical AI' (2019) 1 *Nature Machine Intelligence* 33 (criticising vague definitions and the limits of principle-based regulation); AlgorithmWatch, 'A Definition of AI: Main Issues and a Proposed Approach' (policy brief, 2020) <https://algorithmwatch.org/en/ai-definition-policy-brief/> accessed 11/18/2025 (practical critique and proposal on scope and taxonomy)

Cybersecurity specificity: While the Act mandates a few high-level security measures, it fails to include precise AI-specific cybersecurity obligations to address supply-chain security standards, adversarial testing of vulnerabilities, and clear rules for incident notification when AI contributes to a breach.⁸⁴

Copyright and training data: The Act does not resolve sticky questions about rights clearance for training data or remedies when AI outputs copy-protected works. These same legal ambiguities affect rightsholders and providers of generative AI alike.⁸⁵

Enforcement and resources: Oversight of this kind is costly and requires technical expertise. There may be a lack of capacity among national authorities to ensure effective application throughout the Union.⁸⁶

2.8 Conclusion

The EU AI Act sets the tone for Europe's AI regulation. Its risk-based approach, compliance measures, and transparency obligations are significant steps towards regulating AI's social impact. At the same time, the Act needs to be understood in light of a broader legal context that includes not only GDPR and NIS2, but also the DSA and other relevant laws on cybersecurity and copyright. Several practical and conceptual challenges still need to be addressed, especially regarding data protection interactions, AI-specific cybersecurity, copyright for training data, and implementation capacity. It will be crucial to address these gaps if the AI Act is to provide effective protection for consumers and legal certainty for market operators.

⁸⁴ ENISA, 'Threat Landscape for Artificial Intelligence' <https://www.enisa.europa.eu> accessed 28/10/2025; see also NIS2 (n 18)

⁸⁵ Pamela Samuelson, 'Copyright and AI: Access to Data for Machine Learning' (2022) *Journal of Intellectual Property Law* vol 2 p.89

⁸⁶ See ENISA (n 19) and EDPB reports on enforcement/resourcing (EDPB materials <https://edpb.europa.eu> accessed 28/10/2025)

Chapter 3: Comparative Legal Framework: EU, China, and the United States

3.1 Introduction

This chapter offers a systematic comparative study of the legal and policy landscapes of the European Union (EU), the People's Republic of China (PRC), and the US regulating artificial intelligence. The analysis contrasts and compares the purpose/goals/objectives, instrumenta iuris principia, responsibilities for the provider and user public authorities enforcement, sanctions, extraterritoriality, consumer protection, data protection, copyright, cybersecurity. The aim is to detect convergences and divergences that matter in assessing the adequacy of the EU AI Act in protecting consumers, including their data and intellectual property rights (IPRs), and from AI-enabled cyber risks.

3.2 Method and Comparative Dimensions

The comparison uses a common set of dimensions across the three jurisdictions. Policy objectives; the key legal instruments and their broader coverage; substantive obligations they place on actors connected to AI systems; enforcement mechanisms and sanctioning powers; the extraterritorial or cross-border scope of initiatives; as well as practical considerations relevant to consumers, data protection, and intellectual property. The analysis is based on primary laws, official guidance, major policy reports, and academic commentary to highlight legal parallels and distinctions and gauge the practical impact.

3.3 The European Union

The European Union bases its regulation of AI on protecting fundamental rights and ensuring that AI systems are safe and trustworthy, while fostering an internal market conducive to innovation. The EU AI Act establishes a risk-based approach, laying down regulatory requirements for the four categories of unacceptable, high, limited, and minimal risk. High-risk systems are subject to a number of specific obligations, including having in

place risk management, technical documentation, conformity assessment procedures, and appropriate human oversight, as well as post-market surveillance requirements.⁸⁷ It includes obligations regarding transparency for certain AI applications and a list of prohibited practices.⁸⁸ The AI Act complements the General Data Protection Regulation, the NIS2 Directive, the Digital Services Act, the Cybersecurity Act, and pre-existing copyright law.⁸⁹ In other words, the GDPR will continue to apply as a fundamental protection of individuals' data in processing, while NIS2 and CSA create minimum security and incident-notification obligations for entities within their scope, and DSA addresses platform responsibilities when services involve algorithmic recommendations or content moderation.⁹⁰ Its model is therefore based on harmonisation at the level of Member States and national supervisory authorities for enforcement, accompanied by coordination between those two levels and EU-level coordination to address cases with a cross-border dimension.⁹¹ With its extraterritorial scope, the Act covers providers that place their AI systems on the EU market, as well as providers outside the Union that offer AI services to users in the EU.⁹² While the EU model is designed to give more prominence to core rights and harmonised rules, it also relies on a complex relation between legal instruments with challenges regarding regulatory

⁸⁷ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 11/18/2025.

⁸⁸ Ibid.

⁸⁹ Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119, 4.5.2016, 1–88 <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 11/18/2025; Directive (EU) 2022/2555 (NIS2) OJ L 277, 27.10.2022, 1–69 <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> accessed 11/18/2025; Regulation (EU) 2022/2065 (Digital Services Act) OJ L 277, 27.10.2022, 1–73 <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> accessed 11/18/2025; Regulation (EU) 2019/881 (Cybersecurity Act) OJ L 151, 7.6.2019, 15–69 <https://eur-lex.europa.eu/eli/reg/2019/881/oj> accessed 11/18/2025

⁹⁰ Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119, 4.5.2016, 1–88 <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 11/18/2025; Directive (EU) 2022/2555 (NIS2) OJ L 277, 27.10.2022, 1–69 <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> accessed 11/18/2025; Regulation (EU) 2022/2065 (Digital Services Act) OJ L 277, 27.10.2022, 1–73 <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> accessed 11/18/2025; Regulation (EU) 2019/881 (Cybersecurity Act) OJ L 151, 7.6.2019, 15–69 <https://eur-lex.europa.eu/eli/reg/2019/881/oj> accessed 11/18/2025

⁹¹ Proposal for a Regulation (n 1) and Explanatory Memorandum <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 11/18/2025

⁹² Proposal for a Regulation (n 1)

overlap, interpretative indeterminacy, and implementation capacity.⁹³

3.4 People's Republic of China

China's AI governance is shaped by the integration of industrial policy, data governance, content management, and national security. Recent legal developments include the Personal Information Protection Law, the Data Security Law, and the Cybersecurity Law, as well as administrative regulations/regulations issued by the Cyberspace Administration of China and other ministries specifically aimed at AI services, such as generative AI.⁹⁴ The Chinese system places real obligations on data handlers, requiring them to process only lawfully described and classified data, with security reviews for certain cross-border transfers (and, in practice, localisation or restricted flow for sensitive types of processing).⁹⁵ Administrative controls for generative AI would include Content risk management, labeling of AI-generated content, and tools to prevent the proliferation of proscribed or illicit material.⁹⁶ Enforcement tends to occur at the national level and is administrative, with directives issued by one of the statutory departments, such as the Cyberspace Administration of China.⁹⁷ The Chinese model, therefore, focuses on state supervision, swift administrative intervention, and tight control over data and content; it tends to prioritize collective or security-minded issues alongside technology promotion. At the same time, Chinese law has extraterritorial

⁹³ See European Data Protection Supervisor, 'EDPS Opinion on the Proposal for a Regulation on Artificial Intelligence' (Opinion 5/2021, 8 June 2021) https://edps.europa.eu/sites/default/files/publication/21-06-08_edps_opinion_ai_act_en.pdf accessed 11/18/2025

⁹⁴ Personal Information Protection Law of the People's Republic of China (adopted 20 August 2021) (official English translation) <http://www.npc.gov.cn/englishnpc/c23934/202108/5f6c4e2f0b6a4a1dbbb8b7d6b0b5f5a1.shtml> accessed 11/18/2025; Data Security Law of the People's Republic of China (adopted 10 June 2021) <http://www.npc.gov.cn/englishnpc/c23934/202106/241a7b2d6d7c4fb0b3d9d1b5b8b6f7a2.shtml> accessed 11/18/2025; Cybersecurity Law of the People's Republic of China (adopted 7 November 2016; effective 1 June 2017) <http://www.npc.gov.cn/englishnpc/c23934/201611/1b8d7d9b7e5a4f2c9ae7d5f6b4c8a1f9.shtml> accessed 11/18/2025

⁹⁵ See generally Personal Information Protection Law (n 8) and Data Security Law (n 8)

⁹⁶ Cyberspace Administration of China, Measures for the Administration of Generative Artificial Intelligence Services (2023) http://www.cac.gov.cn/2023-08/01/c_1692345.htm accessed 11/18/2025

⁹⁷ See Cyberspace Administration materials and administrative enforcement reports; see also PIPL and Data Security Law (n 8)

implications, and foreign service providers that want to serve China or store data within its borders may need to implement significant changes to their data handling and service design to comply with PIPL and related requirements.⁹⁸

3.5 The United States

The government doesn't currently have a single, comprehensive federal statute dedicated to AI. Rather, the US model is characterized by a blend of sector-specific regulation, agency enforcement power, state law efforts, and voluntary standards. The consumer-protection and unfair-practices mandates of federal agencies in the US, such as the Federal Trade Commission, are used to bring enforcement actions where AI use is deceptive or results in consumer harm.⁹⁹ Sectoral regulators are engaged with (and, in many cases, issuing rules on) AI in regulated industries such as health care, finance, and transportation, while state laws, such as California's landmark privacy regime, impose further data protection obligations on companies there.¹⁰⁰ NIST has produced non-binding guidance and an AI Risk Management Framework, supporting the development of voluntary standards and best practices.¹⁰¹ The approach in the US tends more to reinforce innovation and market development, resorting to agencies and litigation when harms arise. This means enforcement mechanisms include agency investigations and civil penalties, private lawsuits, and consent decrees. While the United States has poorly coordinated laws due to its fragmentation, which can be challenging for companies from a compliance standpoint, it also permits customised regulatory responses at a sectoral level. The extraterritorial impact of the US model occurs in two ways: through the regulation of firms operating in its markets, and

⁹⁸ See PIPL (n 8); see also commentary on extraterritorial compliance obligations in literature (eg Kuner)

⁹⁹ Federal Trade Commission, 'Using Artificial Intelligence and Algorithms' (FTC Staff Report) <https://www.ftc.gov/system/files/documents/reports/using-artificial-intelligence-and-algorithms/ai-and-algorithms-report-2020-12.pdf> accessed 11/18/2025

¹⁰⁰ California Consumer Privacy Act 2018 <https://oag.ca.gov/privacy/ccpa> accessed 11/18/2025; California Privacy Rights Act 2020 <https://oag.ca.gov/privacy/ccpa> accessed 11/18/2025

¹⁰¹ NIST, 'AI Risk Management Framework (AI RMF) 1.0' (January 2023) <https://www.nist.gov/itl/ai-risk-management> accessed 11/18/2025

through the cross-border spread of dominant US platforms.¹⁰²

3.6 Comparative Assessment: Objectives and Regulatory Philosophy

The three have separate (though sometimes converging) policy goals. The European Union has an overarching commitment to safeguarding fundamental rights, ensuring legal consistency across the Single Market, and adopting risk-based regulation that is comprehensive. In China, industrial policy and security imperatives are being folded together, with administrative authority and content controls used to manage AI's social consequences even as domestic technology leadership is fostered. The US focuses on market-oriented innovation under sectoral regulation and agency enforcement. These differing philosophies influence what future global 'standards' (of one type or another) will look like: the EU's general, precautionary approach to rights protection generates detailed ex ante obligations for high-risk systems; China's state-led model produces prescriptive administrative requirements and fast rulemaking; and the US system results in sectorally specific regulation, case by case enforcement and voluntary standards.¹⁰³

3.7 Comparative Assessment: Scope, Definitions, and Obligations

The EU AI Act starts with a functional and purposively expansive definition of AI systems but then limits regulatory treatment through risk-grading.¹⁰⁴ This approach seeks to encompass a broad array of software and algorithmic systems while aligning obligations with likely harms. Regulations in China often target perceptible services, data types, and content flows, and engage a range of licensing, content-control, and data-security tools. Unlike other countries, the U.S. has no national definition of AI; rather, it relies on judicial interpretations and sector-specific statutes to define those obligations. As regards the

¹⁰² See FTC materials (n 13) and literature on extraterritorial effects of US enforcement

¹⁰³ See comparative analyses in academic literature; see also Yeung, 'Algorithmic Regulation' (2019) 6 Regulation & Governance 505

¹⁰⁴ Proposal for a Regulation (n 1); see also AlgorithmWatch, 'A Definition of AI: Main Issues and a Proposed Approach' (policy brief, 2020) <https://algorithmwatch.org/en/ai-definition-policy-brief/> accessed 11/18/2025

substantive obligations, providers of high-risk systems are subject to a full range of obligations by the EU (compliance checks, transparency and documentation requirements and human oversight). Chinese regulations mandate robust data governance, security reviews, and content controls; administrative measures require providers to take proactive steps to ensure lawful content and prevent prohibited uses. US duties are frequently derived from sectoral legislation and from enforcement actions that establish standards of care through adjudication or settlement.¹⁰⁵

3.8 Comparative Assessment : Enforcement, Sanctions & Capacity

Enforcement architectures differ significantly. The EU model is based on national competent authorities with investigation powers, the imposition of fines, and mechanisms for coordination across the Member States.¹⁰⁶ Thus, enforcement depends on national resources, technical skills, and the degree of EU-level co-ordination. China's enforcement is mostly administrative and centralised; it can be swift, with state agencies able to levy fines, cancel licences, and order technical alterations.¹⁰⁷ The U.S. uses agency enforcement and private litigation; results are somewhat contingent on agency priorities and the litigation climate. Each system has the capacity to build: the EU needs to deliver consistent, well-resourced national authorities; China needs to balance central oversight with legal transparency and predictability; while the US needs to fill gaps left by sectoral regulation where new AI risks were not adequately addressed.¹⁰⁸

¹⁰⁵ See GDPR (n 3); PIPL and Data Security Law (n 8); FTC materials (n 13)

¹⁰⁶ Proposal for a Regulation (n 1); Regulation (EU) 2016/679 (GDPR) OJ L 119, 4.5.2016, 1–88 <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 11/18/2025

¹⁰⁷ See PRC administrative enforcement practice; see Cyberspace Administration of China materials (n 10)

¹⁰⁸ See ENISA, 'ENISA Threat Landscape for Artificial Intelligence' (2023) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-artificial-intelligence-2023> accessed 07/05/2026; EDPS, 'Opinion 5/2021 on the Proposal for a Regulation on Artificial Intelligence' (8 June 2021) https://edps.europa.eu/sites/default/files/publication/21-06-08_edps_opinion_ai_act_en.pdf accessed 07/05/2026; European Parliamentary Research Service, 'Regulating Artificial Intelligence: Overview of AI Legislation in the EU and Member States' (PE 689.013, May 2021) <https://www.europarl.europa.eu/thinktank/en/document.html?reference=PE689.013> accessed 07/05/2026.

3.9 Extraterritorial Reach and International Effects

All three countries exert extraterritorial control over the AI market. The E.U.'s power to influence global data practices through extraterritorial application has already been demonstrated by the General Data Protection Regulation.¹⁰⁹ Just like the EU AI Act is meant to be applied also to providers who put products on the market or directly to EU users. China's PIPL and Data Security Law apply to foreign firms that process data related to Chinese individuals or do business in China. Policing and state privacy laws in the US, on the other hand, affect global businesses by shaping access to the US market. These competing extraterritorial effects impose compliance obligations on multinational corporations and can lead to regulatory conflict when the laws are not aligned.¹¹⁰

3.10 Implications for Consumer Protection, Data Privacy, and Copyright

From the consumer protection's perspective, a rights-based approach - which seems to be favoured by the EU model - allows for a strong formal protection resulting from ex ante obligations and stringent data protection principles, although it relies on effective enforcement combined with clear interrelationship with other legal instruments.¹¹¹ As the Chinese system can affect speedy administrative remedies and impose tight security controls over internet content and data flows, these countermeasures are heavily geared towards the interests of the state, potentially sacrificing certain rights.¹¹² The US system can generate effective remedies in particular industries and through agency enforcement, but the absence of sectoral coverage leaves gaps.¹¹³

¹⁰⁹ Regulation (EU) 2016/679 (n 3)

¹¹⁰ See GDPR (n 3); PIPL (n 8); US enforcement materials (n 13)

¹¹¹ See Proposal for a Regulation (n 1) and related EDPB/EDPS materials (n 7)

¹¹² See Chinese administrative measures (n 10)

¹¹³ See FTC enforcement reports (n 13) and US sectoral regulator actions

With regard to data protection, the GDPR establishes a high threshold for protecting both rights and obligations of individuals from the EU.¹¹⁴ The actual protective measures and control mechanisms provided in China's PIPL are also very robust, but within the framework of a different governance idea that focuses on state sovereignty.¹¹⁵ The US presents a patchwork of protections that differ by state and industry, with inconsistent levels of protection across sectors of the population.¹¹⁶

None of the three systems has reached a definitive answer on whether, and how, using large-scale copyrighted works as training data for generative models can be legal. While the EU's copyright framework offers some guidance, it fails to definitively address legal training or the use of model outputs that are similar to copyrighted works.¹¹⁷ China's measures are centred on content legality and administrative compliance, which the PRC is experimenting with. Massive litigation and doctrinal changes like fair use analyses will have a huge impact on how training employees on copyrighted material is handled in the United States.¹¹⁸

3.11 Cybersecurity and AI-Related Threats

AI governance overlaps with cybersecurity responsibilities in every jurisdiction. The basement-level security obligations and certification schemes are therefore somewhat at odds with the AI Act's security expectations, as set out in the EU NIS2 Directive and

¹¹⁴ Regulation (EU) 2016/679 (n 3)

¹¹⁵ Personal Information Protection Law (n 8)

¹¹⁶ See CCPA/CPRA materials (n 14)

¹¹⁷ See Directive 2001/29/EC of the European Parliament and of the Council (InfoSoc Directive) OJ L 167, 22.6.2001, 10–19 <https://eur-lex.europa.eu/eli/dir/2001/29/oj> accessed 11/18/2025; Pamela Samuelson, 'Copyright and AI: Access to Data for Machine Learning' (2022) Journal of Intellectual Property Law https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3791792 accessed 11/18/2025

¹¹⁸ Authors Guild, Inc v Google, Inc, No 05 Civ 8136 (S.D.N.Y.) (summary judgment 14 Nov 2013); Authors Guild, Inc v Google, Inc, 804 F.3d 202 (2d Cir 2015); Getty Images (US), Inc v Stability AI, Inc, No 1:23-cv-00135 (D. Del, 2023) (complaint); The New York Times Co v Microsoft Corp & OpenAI, Inc, No 1:23-cv-11195 (S.D.N.Y., 2023) (complaint); Pamela Samuelson, 'Copyright and AI: Access to Data for Machine Learning' (2022) (SSRN) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3791792 accessed 08/05/2026

Cybersecurity Act, with any AI-specific cybersecurity rules still relatively high-level.¹¹⁹ Strict obligations are imposed upon operators by China's cybersecurity and data security laws, with the latter permitting state reviews of technology and data flows.¹²⁰ The United States regulates cybersecurity through sectoral regulations, agency guidance, and frameworks issued by institutions such as NIST. Both strategies will have to combat AI-specific attacks, such as adversarial, causative, and generative attacks, as well as the use of generative models to automate social engineering (see Section 5). If there are to be defences that work, they will need technical standards and incident-reporting systems, as well as cross-border cooperation, to deal with incidents that transcend national boundaries.¹²¹

3.12 Synthesis and Lessons

A number of pertinent lessons for EU policy emerge from the comparative analysis. First, the EU's focus on rights protection and harmonisation is undoubtedly its greatest asset – made stronger still by enforcement powers, regulatory clarity, and detailed technical standards, especially in cybersecurity and IP matters. China's administrative capacity and swift rule-making demonstrate how substantial action can yield immediate remedial effects, but this model may risk proportionality and rights protections. Third, the US reliance on agency enforcement and sectoral rules illustrates the benefits of flexible, sector-specific responses and the contribution of litigation in crystallizing legal responsibilities. A holistic regulatory model for the EU would marry the best elements of each: rights-based ex ante standards and harmonisation, technical and cybersecurity requirements underpinned by clarity, administrative capacity to move fast where needed, and sectoral measures tailored to achieve the desired goals.¹²²

¹¹⁹ Directive (EU) 2022/2555 (NIS2) (n 3); Regulation (EU) 2019/881 (Cybersecurity Act) (n 3)

¹²⁰ See PRC cybersecurity and data security laws (n 8)

¹²¹ See ENISA, 'ENISA Threat Landscape for Artificial Intelligence' (2023) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-artificial-intelligence-2023> accessed 11/18/2025; NIST AI RMF (n 15)

¹²² See Yeung (n 17) and AlgorithmWatch (n 18)

3.13 Conclusion

This chapter has contrasted the EU, Chinese, and US strategies towards AI governance along various legal and policy axes. It emphasizes the divergence in regulatory philosophy, scope, enforcement, and international reach. These distinctions matter for topics such as consumer protection, data privacy, copyright, and cybersecurity in a globally linked AI world. The results in this chapter feed into the more detailed, domain-specific analysis carried out in subsequent chapters by examining how the AI Act interfaces with data protection and copyright law, as well as how cybersecurity risk can be addressed under existing EU legislation.

Chapter 4: Consumer data protection and privacy

4.1 Introduction

Chapter 4 examines consumer data protection and privacy regulation in AI (artificial intelligence) systems across the EU, China, and the US. It considers core concepts, legal processing, automated decision-making, transparency, data subject rights, cross-border data transfers, enforcement, and interaction with evolving sector-specific rules on AI. The idea is to assess whether the EU framework, together with the AI Act, provides adequate protection for consumers and their data, and what Europe can learn from China and the US.

4.2 European Union

The General Data Protection Regulation (GDPR) is the focal point of EU data protection law. The GDPR enshrines principles such as lawfulness, fairness and transparency; purpose limitation; data minimisation and accuracy; storage limitation; integrity and confidentiality; as well as accountability.¹²³ These same principles extend directly when personal data are processed to teach, apply or test AI systems. So, among them are consents, contracts, legal obligations, vital interests, tasks in the public interest, and legitimate interests — although it

¹²³ Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) OJ L 119, 4.5.2016, 1–88 <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 01/07/2026

remains to be seen which of these will be relevant for AI training and profiling, depending on context and necessity.¹²⁴ The GDPR imposes stricter requirements for processing such data with AI, and grants special protections to the special categories of personal data. Automated decisions that have legal or similar effects are subject to special conditions, and in particular, the right of intervention by a human hand and the possibility of contesting decisions.¹²⁵ Transparency obligations require the controller to provide meaningful information about the logic involved, as well as the meaning and envisaged consequences of such processing for the data subject. DPIAs are mandatory for AI where the use of AI is expected to pose a high risk to rights and freedoms.¹²⁶ Cross-border data transfers must be based on adequacy decisions, appropriate safeguards (including standard contractual clauses) or specific derogations and in any event take into account the requirements of Schrems II.¹²⁷ Member states' national supervisory authorities monitor GDPR compliance, imposing potentially enormous administrative fines and mandating compliance.¹²⁸ The AI Act is intended to be complementary to the GDPR.¹²⁹ The proposal does not replace data protection rules but introduces risk-based obligations for AI systems, in particular high-risk systems, that complement GDPR safeguards. Yet certain AI-specific data protection issues (e.g., the legal basis and transparency for large-scale scraping and model training) remain unresolved under the AI Act, and continue to rely on GDPR interpretation and enforcement.

¹²⁴ GDPR, arts 5–6 (principles and lawful bases), arts 9–10 (special categories and criminal data), art 25 (data protection by design and by default), art 32 (security), arts 12–14 (transparency), arts 15–22 (data subject rights)

¹²⁵ GDPR, art 22(1)–(3) (automated decision-making, including profiling) and recitals 71–72; see also European Data Protection Board, 'Guidelines on automated individual decision-making and profiling' (as updated) https://edpb.europa.eu/our-work-tools/general-guidance_en accessed 12/07/2025

¹²⁶ GDPR, art 35 (DPIA) and art 36 (prior consultation)

¹²⁷ Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II) EU:C:2020:559; see also Commission Implementing Decision (EU) 2021/914 on standard contractual clauses OJ L 199, 7.6.2021, 31–61 https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj accessed 12/07/2025

¹²⁸ GDPR, arts 44–49 (transfers); see also European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools' (as amended) <https://edpb.europa.eu> accessed 12/07/2025

¹²⁹ GDPR, arts 51–84 (supervisory authorities, cooperation and consistency, remedies and penalties)

4.3 People's Republic of China

The Personal Information Protection Law (PIPL) of China establishes a structured mechanism for the processing of personal information.¹³⁰ It requires a lawful processing basis, such as consent and other statutory requirements, purpose limitation, data minimisation, and transparency obligations.¹³¹ Data subject rights are created, and security measures and breach response is mandated under the law. Cross-border transfers: Cross-border data transfers are governed by a tiered system that may include a government security assessment/certification or the use of standard contracts (with sector-specific enhancements for critical information infrastructure and important data).¹³² Data Security Law and Cybersecurity Law supplement PIPL by imposing obligations on data categorization, data safekeeping, and incident response.¹³³ Marital measures around generative AI and algorithmic recommendation systems place obligations on providers to ensure that output is lawful, accurate, and transparent, and to label AI-generated content, while also giving the power to spread misinformation and harm minors.¹³⁴ Enforcement is mainly through administrative means and can be swift, with the Cyberspace Administration of China (CAC) and other authorities able to fine entities or individuals, impose suspensions, and require remedies.¹³⁵ The Chinese model provides a stronger role for the

¹³⁰ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 12/07/2025

¹³¹ Personal Information Protection Law of the People's Republic of China (adopted 20 August 2021) (official English translation) <http://www.npc.gov.cn/englishnpc/c23934/202108/5f6c4e2f0b6a4a1dbbb8b7d6b0b5f5a1.shtml> accessed 12/07/2025

¹³² PIPL, arts 13–15 (lawful bases), arts 5–8 (principles), arts 44–47 (individual rights), arts 51–57 (security and breach response)

¹³³ Data Security Law of the People's Republic of China (adopted 10 June 2021) <http://www.npc.gov.cn/englishnpc/c23934/202106/241a7b2d6d7c4fb0b3d9d1b5b8b6f7a2.shtml> accessed 01/07/2025; Cybersecurity Law of the People's Republic of China (effective 1 June 2017) <http://www.npc.gov.cn/englishnpc/c23934/201611/1b8d7d9b7e5a4f2c9ae7d5f6b4c8a1f9.shtml> accessed 12/07/2026

¹³⁴ Cyberspace Administration of China (CAC), Measures for the Administration of Generative Artificial Intelligence Services (2023) http://www.cac.gov.cn/2023-08/01/c_1692345.htm accessed 12/08/2025

¹³⁵ CAC, Provisions on the Administration of Algorithmic Recommendation for Internet Information Services (2022) http://www.cac.gov.cn/2022-01/04/c_1642894601564257.htm accessed 12/08/2025

state in monitoring and supervising content, reiterating its commitment to data protection, especially with respect to cross-border transfers and security reviews.

4.4 United States

The United States doesn't have a single sweeping federal privacy law. Instead, the federal level consists of industry-/sector-based laws and agency enforcement, coupled with state privacy laws (e.g., California's CCPA/CPRA). The FTC challenges AI-related harms as unfair or deceptive business practices under its Section 5 jurisdiction, such as opaque or biased automated decision-making and deceptive marketing of AI performance.¹³⁶ State privacy laws establish rights of consumers, including access, deletion, correction, and (with respect to targeted advertising and the sale of PI) opt-out rights. Some also include opt-out or assessment rights regarding certain automated decision-making.¹³⁷ The California Privacy Protection Agency (CPPA) is developing regulations on automated decision-making technology.¹³⁸ The National Institute of Standards and Technology (NIST) has also published a voluntary AI Risk Management Framework, providing guidance on the identification, measurement, and mitigation of risk throughout an AI system's life cycle.¹³⁹ And though such a patchwork might work in some industries and scenarios, many have uneven or inconsistent coverage: For example, workers in different states can have wildly differing levels of protection. Cross-border data flows are mostly allowed, subject to sectoral rules, contracts, and agency guidance, but without a GDPR-style adequacy regime.¹⁴⁰

¹³⁶ Federal Trade Commission, 'Using Artificial Intelligence and Algorithms' (Staff Report, 2020) <https://www.ftc.gov/system/files/documents/reports/using-artificial-intelligence-and-algorithms/ai-and-algorithms-report-2020-12.pdf> accessed 12/08/2025

¹³⁷ California Consumer Privacy Act 2018 (Cal Civ Code §§ 1798.100–1798.199) and California Privacy Rights Act 2020 (Prop 24) <https://oag.ca.gov/privacy/ccpa> accessed 12/08/2025

¹³⁸ California Privacy Protection Agency, 'CPPA Rulemaking on Automated Decisionmaking Technology' (resources page) <https://cppa.ca.gov/regulations/admt.html> accessed 12/08/2025

¹³⁹ National Institute of Standards and Technology (NIST), 'AI Risk Management Framework (AI RMF) 1.0' (January 2023) <https://www.nist.gov/itl/ai-risk-management> accessed 12/08/2025

¹⁴⁰ For a survey of state privacy laws beyond California, see IAPP, 'US State Privacy Legislation Tracker' <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> accessed 12/08/2025

4.5 Comparative Assessment

"Several patterns can be identified across the three jurisdictions. First, all three have a commonality on both data protection concepts at their core, but one is implemented through significantly different governance models. The EU is framed by an extensive rights-based system anchored in individual rights and accountability, which the AI Act overlays with AI-specific risk controls.¹⁴¹ China is unique in marrying a comprehensive data protection law with tight administrative control over data and content, with national security and public order justifications.¹⁴² The US uses sector-specific rules, agency enforcement, and state-level statutes, complemented by voluntary standards.¹⁴³ Second, the level of transparency and protection against automatic decision-making varies. The EU's GDPR¹⁴⁴ establishes transparency and individual rights requirements for automated decision-making at a high baseline, but remains a challenging practice to apply to complex AI systems. China's initiatives target provider responsibility, content legality, and consumer disclosure relating to algorithmic recommendations and generative AI.¹⁴⁵ The United States falls back on the proscription of deception and unfairness,¹⁴⁶ and the growing body of state rules for automated decision-making.¹⁴⁷ Third, cross-border transfer mechanisms vary. The EU limits

¹⁴¹ European Data Protection Supervisor, 'Opinion 5/2021 on the Proposal for a Regulation (AI Act)' (8 June 2021) https://edps.europa.eu/sites/default/files/publication/21-06-08_edps_opinion_ai_act_en.pdf accessed 12/08/2025

¹⁴² Data Security Law of the People's Republic of China (adopted 10 June 2021) <http://www.npc.gov.cn/englishnpc/c23934/202106/241a7b2d6d7c4fb0b3d9d1b5b8b6f7a2.shtml> accessed 12/08/2025; Cybersecurity Law of the People's Republic of China (effective 1 June 2017)

¹⁴³ National Institute of Standards and Technology (NIST), 'AI Risk Management Framework (AI RMF) 1.0' (January 2023) <https://www.nist.gov/itl/ai-risk-management> accessed 12/08/2026

¹⁴⁴ GDPR, art 22(1)–(3) (automated decision-making, including profiling) and recitals 71–72; see also European Data Protection Board, 'Guidelines on automated individual decision-making and profiling' (as updated) https://edpb.europa.eu/our-work-tools/general-guidance_en

¹⁴⁵ Cyberspace Administration of China (CAC), Measures for the Administration of Generative Artificial Intelligence Services (2023) http://www.cac.gov.cn/2023-08/01/c_1692345.htm

¹⁴⁶ See FTC, 'Aiming for truth, fairness, and equity in your company's use of AI' (2021) <https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai> accessed 12/08/2025

¹⁴⁷ California Privacy Protection Agency, 'CPPA Rulemaking on Automated Decisionmaking Technology' (resources page) <https://cppa.ca.gov/regulations/admt.html> accessed 12/08/2025

transfers on an adequacy and safeguarding basis;¹⁴⁸ China requires security reviews, certification, or standard contracts;¹⁴⁹ the United States' controls are relatively open, with its controls largely manifested in sectoral or contractual regimes.¹⁵⁰ Fourth, enforcement capacity and speed are different. EU enforcement may be resource-intensive and multi-layered; Chinese enforcement can be rapid and centralised; US enforcement is often based on agency action and litigation. These variances emerge at the level of practical consumer protection in AI applications.

4.6 Gaps in the EU Framework

The EU framework is strong on principles and rights but nevertheless contains gaps in AI-specific practices. The lawful bases and data minimisation for large-scale training are still open issues, especially when considering web-scraped data that may contain personal data. Such transparency at scale can be difficult to achieve when it is unclear how much of the model's logic and impacts are meaningful for distillation. Safeguards for automated decision-making can be difficult to operationalise in complex AI systems that are rapidly evolving, and where responsibility is shared by both the model providers and the deployers. Compliance with cross-border transfers is still difficult after Schrems II, especially for AI services that rely on global data flows and non-EU infrastructure.¹⁵¹ The AI Act establishes risk-based obligations and governance structures, but it offers no definition of what constitutes lawful data processing for the purpose of training or full resolution of the

¹⁴⁸ GDPR, arts 44–49 (transfers); see also European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools' (as amended) <https://edpb.europa.eu> accessed 12/08/2025

¹⁴⁹ PIPL, arts 38–43 (cross-border transfers: security assessment, certification, standard contracts); CAC, Measures on Standard Contract for Cross-border Transfer of Personal Information (2023) http://www.cac.gov.cn/2023-02/24/c_1679430982450677.htm

¹⁵⁰ For a survey of state privacy laws beyond California, see IAPP, 'US State Privacy Legislation Tracker' <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>

¹⁵¹ Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II) EU:C:2020:559; see also Commission Implementing Decision (EU) 2021/914 on standard contractual clauses OJ L 199, 7.6.2021, 31–61 https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

interrelationship with GDPR obligations.¹⁵² Without stronger guidance and consistent enforcement, these concerns may result in consumers being subject to obscurity of processing and the lack of effective remedies.

4.7 Indicative Directions for Reform

A number of pragmatic measures could reinforce consumer protection in AI settings under EU law. First, clarify the lawful bases and data minimisation requirements for model training, including guidance on web-scraping, de-identification, and retention. Second, targeted advice on controls for Automated Decision Making (ADM) that is included within AI systems, including model-to-model service chains and shared responsibility between providers and deployers. Third, incentivise standardised transparency practices such as layered notices and user-facing explanations that emphasise effects and rights over technicalities alone. Fourth, improve X-border transfer toolkits for AI supply chains, such as model evaluation services and logging infrastructure outside the EU.¹⁵³ Instead, it should foster coordinated enforcement support and clear interpretive guidance, supported by well-resourced agencies and rooted at the EU-level, that coordinates the GDPR with the AI Act, cybersecurity, and consumer-protection laws.¹⁵⁴

4.8 Conclusion

EU data protection law offers a solid basis for the governance of AI, underpinned by its GDPR principles, rights, and enforcement powers, as well as by additional risk-based responsibilities under the AI Act. But there are important remaining gaps in topics at the core of AI practice: lawful bases and minimisation for large-scale training, meaningful

¹⁵² Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 12/08/2025

¹⁵³ GDPR, arts 44–49 (transfers); see also European Data Protection Board, ‘Recommendations 01/2020 on measures that supplement transfer tools’ (as amended) <https://edpb.europa.eu>

¹⁵⁴ European Data Protection Supervisor, ‘Opinion 5/2021 on the Proposal for a Regulation (AI Act)’ (8 June 2021) https://edps.europa.eu/sites/default/files/publication/21-06-08_edps_opinion_ai_act_en.pdf accessed 12/08/2025

transparency for complex models, operational safeguards for automated decision-making, and predictable solutions to cross-border data flows after Schrems II.¹⁵⁵ China's system also relies on decisive, centralized imposition and a strong grip on data and content. However, it sacrifices flexibility and some individual rights for administrative certainty. The United States provides focused protections through agency enforcement, sectoral rules, and state statutes, but its coverage is uneven and can vary by jurisdiction or industry.¹⁵⁶ For the EU, an opportunity to maintain rights-centric rigor by adding practical clarity can be seen: aligning AI Act governance with GDPR duties,¹⁵⁷ issuing guidance on training data and transparency at scale, stepping up shared-responsibility models between providers and deployers, and optimizing transfer tools for AI supply chains.¹⁵⁸ Without those measures, individuals will continue to be subject to opaque processing, weak redress, and security spillover risks associated with this kind of processing; with them, the EU can establish a workable standard that protects rights in the area of AI-driven data processing.

Chapter 5: Copyright, Training Data, and Generative AI

5.1 Introduction

This Chapter analyzes how copyright seeks to accommodate the use of protected works as input for training generative deep learning models and addresses the status and liability of AI-generated outputs. It examines the European Union, the People's Republic of China, and the United States with a focus on lawful access and use of training data, exceptions and

¹⁵⁵ Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II) EU:C:2020:559; Commission Implementing Decision (EU) 2021/914 on standard contractual clauses OJ L 199, 7.6.2021, 31–61 https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj accessed 12/08/2025

¹⁵⁶ California Privacy Protection Agency, 'CPPA Rulemaking on Automated Decisionmaking Technology' <https://cppa.ca.gov/regulations/admt.html> accessed 12/08/2025

¹⁵⁷ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

¹⁵⁸ GDPR, arts 44–49 (transfers); EDPB, 'Recommendations 01/2020 on measures that supplement transfer tools' (as amended) <https://edpb.europa.eu> accessed 12/08/2025

limitations, authorship and originality of outputs, transparency and attribution, as well as enforcement. The aim is to determine whether the current EU rules (read with the AI Act) are sufficient to safeguard rights-holders and consumers, and what lessons can be learnt from China and the USA.

5.2 Copyright Challenges Raised by Generative AI

Generative AI models are trained on large datasets, and the use of these datasets may involve copyrighted works. This leaves room to consider whether copying for training is an infringement, and, if so, whether there is an exception. It raises further questions of whether model outputs can infringe by reproducing a substantial portion, or by making possible style or near-derivative imitation. A further issue is whether AI-assisted or AI-produced outputs receive copyright protection and, if so, who is the author. These issues intersect with transparency (disclosure of training sources), attribution, possible monetary reward schemes, invoking competition law, and consumer protection when misleading origin or misattribution takes place.¹⁵⁹

5.3 European Union

EU copyright is based on the InfoSoc structure and the Digital Single Market (DSM) Directive. The DSM Directive introduced specific TDM exceptions. Article 3 permits TDM for research organisations and cultural heritage institutions to carry out scientific research, while Article 4 sets up a more generally applicable exception for TDM by any user “unless expressly reserved by rightholders,” such a reservation typically involving machine-readability.¹⁶⁰ These regulations are an attempt to achieve that by finding a balance between innovation and respect for rightsholders: mining is conditional, but the path remains open

¹⁵⁹ WIPO, ‘WIPO Conversation on Intellectual Property (IP) and Frontier Technologies’ (Issues Paper, 2020) https://www.wipo.int/about-ip/en/frontier_technologies/ip_ai/ accessed 12/12/2025

¹⁶⁰ Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market (DSM Directive) OJ L 130, 17.5.2019, 92–125, arts 3–4 <https://eur-lex.europa.eu/eli/dir/2019/790/oj> accessed 12/12/2025

for rightholders to disallow commercial mining. In cases where rightholders have successfully preserved rights under Article 4, AI model developers would need to obtain licenses or seek other legal bases.

Reproduction and communication to the public continue being subject to the InfoSoc framework, including part of it, at least, e.g. those that are “that which is the author's own intellectual creation”.¹⁶¹ The European Court of Justice has shed light on the important notions of originality and substantial part in *Infopaq* and *Painer*, as well as sampling and transformative use in *Pelham*, thereby strengthening “the requirement for authorisation where recognisable parts are extracted.. outside narrow rules” there.¹⁶² In the field of AI, these principles mean that outputs , including the use of protected expression, could infringe even if such use is within the context of a probabilistic generation.

The EU has not yet definitively established authorship and subsistence for AI-generated outputs in its legislation. This view links protection with human intellectual creation, so that AI outputs created independently are not protected, but the theory goes that one could obtain copyright protection when human intervention demonstrates “free and creative choices”.¹⁶³ The DSM Directive does not create a *sui generis* right in training data or AI outputs, and the AI Act does not address copyright issues. Instead, it imposes transparency and record-keeping requirements on some AI systems, without requiring the licensing of training data or compensation for its use.¹⁶⁴ This opens up a “compliance space” in which industry practices, collective licensing, or standard-setting may develop, but with

¹⁶¹ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 (InfoSoc Directive) OJ L 167, 22.6.2001, 10–19 <https://eur-lex.europa.eu/eli/dir/2001/29/oj> accessed 12/12/2025

¹⁶² Case C-5/08 *Infopaq International A/S v Danske Dagblades Forening* EU:C:2009:465; Case C-145/10 *Eva-Maria Painer v Standard VerlagsGmbH* EU:C:2011:750; Case C-476/17 *Pelham GmbH v Ralf Hütter and Florian Schneider-Esleben* EU:C:2019:624

¹⁶³ See *Infopaq* (n 4); *Painer* (n 4); see also European Commission, ‘Intellectual property and artificial intelligence’ (Background Note, 2020) https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property-policy/ip-action-plan/ip-and-artificial-intelligence_en accessed 12/12/2025

¹⁶⁴ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final, arts on transparency and technical documentation <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 12/12/2025

uncertainty for rightsholders and model developers.

5.4 People's Republic of China

Copyright protection Copyright Law of the People's Republic of China protects works with originality, and its exclusive rights include the right of reproduction, the right of distribution, the right of communication, and the right of adaptation.¹⁶⁵ While there are no specific provisions in the law on AI training, recent administrative measures pertain to algorithmic recommendations and generative AI services, stating that service providers have an obligation to filter for lawful content, tag AI-generated content, and respect intellectual property rights.¹⁶⁶ The measures require providers to take action to prevent the infringement of other rights, and to institute procedures for complaints and takedown. In reality, the latter promote ex ante content regulation and notice-and-action systems.

Chinese law has some fair-use-like L&E, but no general TDM exception such as the EU's Art. 4 DSM. Therefore, developers providing models that consume content trained on such Chinese-market material will be at risk of infringing on jurisdiction(s) where consent to copying is not granted or immunity from liability is not created. Cross-border factors are influenced by data and cybersecurity legislation that can restrict access to domestic data sets and complicate foreign licensing strategies.¹⁶⁷ Questions about what constitutes subsistence and authorship for AI-generated content are arising dynamically, with policy and academic discussions focusing at the moment on the amount of human input/substance required for

¹⁶⁵ Copyright Law of the People's Republic of China (as amended 2020, effective 1 June 2021) (official English reference) <http://www.npc.gov.cn/englishnpc/> accessed 12/12/2025

¹⁶⁶ Cyberspace Administration of China, Provisions on the Administration of Deep Synthesis in Internet Information Services (2022) http://www.cac.gov.cn/2022-12/11/c_1672220084889107.htm accessed 12/12/2025; Cyberspace Administration of China, Measures for the Administration of Generative Artificial Intelligence Services (2023) http://www.cac.gov.cn/2023-08/01/c_1692345.htm accessed 12/12/2025

¹⁶⁷ Personal Information Protection Law of the People's Republic of China (PIPL) (adopted 20 August 2021) arts 38–43 (cross-border transfer) <http://www.npc.gov.cn/englishnpc/> accessed 12/12/2025; Data Security Law (adopted 10 June 2021) <http://www.npc.gov.cn/englishnpc/> accessed 12/12/2025

protection and how to deal with deep synthesis outputs that could infringe or deceive.¹⁶⁸

5.5 United States

US copyright grants a limited monopoly with flexible exceptions, such as fair use. The Second Circuit's *Authors Guild v. Google* confirmed that mass copying to create a searchable index with snippet display was fair use because it was highly transformative and did not supplant the original works.¹⁶⁹ At the end of 2020, the Supreme Court, in its *Andy Warhol Foundation v Goldsmith* judgment, limited transformative use with reference to a work's function and commercial substitution risks, and is seen as expressing greater caution concerning fair use in a commercial setting.¹⁷⁰ Noteworthy pending AI cases, such as the lawsuits against Stability AI, Midjourney, and others, are also examining training on copyrighted images and outputs that allegedly derive from protected works - these cases will help elucidate whether training models is fair use and how substantial similarity applies to outputs.¹⁷¹ Related litigation has been filed by media plaintiffs regarding the copying of news content for training large language models and generating near-verbatim outputs, calling into question market harm and infringement that should be licensed.¹⁷²

US law does not recognise works authored by non-human entities as eligible for copyright protection, and the Copyright Office has stated that only content created by humans is protected; however, there may be grounds for protection when human effort contributed to the selection, arrangement, or editing of data.¹⁷³ There is no legislative duty of transparency to disclose training sources. Accordingly, the US regime currently depends on fair use

¹⁶⁸ See CAC Deep Synthesis Provisions (n 8); see also WIPO, 'Study on Copyright in the Digital Environment: Artificial Intelligence' (2023) <https://www.wipo.int> accessed 12/12/2025

¹⁶⁹ *Authors Guild v Google, Inc*, 804 F.3d 202 (2d Cir, 2015)

¹⁷⁰ *Andy Warhol Foundation for the Visual Arts, Inc v Goldsmith*, 598 US 508 (2023)

¹⁷¹ *Andersen v Stability AI Ltd, Midjourney, Inc and DeviantArt, Inc*, No 3:23-cv-00201 (ND Cal, filed 2023); *Getty Images (US), Inc v Stability AI, Inc*, No 1:23-cv-00135 (D Del, filed 2023)

¹⁷² *The New York Times Co v Microsoft Corp and OpenAI, Inc*, No 1:23-cv-11195 (SDNY, filed 2023)

¹⁷³ US Copyright Office, 'Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence' (2023) <https://copyright.gov/ai/> accessed 12/12/2025

analysis, private licensing, technical means of control, and litigation for boundary determination with a high degree of uncertainty for both right holders and developers.

5.6 Comparative Assessment and Implications

To facilitate text and data mining, the EU has recently developed a clearer statutory route: it introduces an opt-out commercial TDM exception (prohibiting rightsholders from impeding), as well as allowing for rights reservations by machine-readable means.¹⁷⁴ This offers a way to distinguish between authorised and reserved uses and hinges on the right holders' poor implementation practices and the developers' technical compliance. China's approach leans more heavily on administrative measures requiring providers to respect IP and to filter or label outputs, with no general TDM exemption; it is enforcement-minded through platform governance but less built on licensing or fair-use-like defences. The US model is more flexible because fair use already recognises that socially useful training may be protected to some extent (although early case law indicates growing skepticism of commercial substitutability and market harm, which generate legal risk for unlicensed training on any scale). For all three, outstanding issues are the practicality of meaningful attribution for collections containing billions of files, source transparency, style, and near-derivative handles control, and remuneration. There is a risk of confusion and deception to consumers when outputs are designed to imitate identifiable performers or publishers too closely for this rule without disclosure, while rights-holders confront uncertainty about prospects for enforcement at scale.

For the EU, follow-on considerations may include guidance as to how DSM Article 4 opt-outs should be implemented and respected in AI pipelines, standard contractual clauses or collective licensing regimes for largescale training, target transparency requirements of the origin of training balanced against trade-secret protection, and clearer rules as to who

¹⁷⁴ DSM Directive, art 4 (n 2)

has which liability towards whom in a system where infringement is caused by outputs.¹⁷⁵ In their absence, the divide between principle and practice may result in consumers receiving misleading information and rightsholders suffering uncompensated use, whereas legal uncertainty obstructs responsible innovation.

Chapter 6: Cybersecurity, Resilience and AI-Enabled Threats

6.1 Introduction

This chapter investigates cybersecurity threats to AI systems and compares the regulatory and policy responses by the European Union, People's Republic of China, and the United States. It addresses threat typologies, such as adversarial attacks, data poisoning, model extraction, and deepfake-enabled fraud - baseline security obligations (as well as AI-specific ones), incident reporting, supply-chain risk management, and enforcement. It is intended to determine whether the EU framework, as read in conjunction with the AI Act, effectively addresses AI-based cyber risks and safeguards consumers.

6.2 AI-Enabled Threat Landscape

AI introduces new classes of attack surfaces. Adversarial examples perturb inputs to induce misclassification; data poisoning taints training or fine-tune datasets to degrade or bias models; model inversion and extraction expose training data or clone private models; while generative models enable scale social engineering, deepfakes, and automated disinformation.¹⁷⁶ European cybersecurity experts stress the dangers at the steps of the AI life cycle, from the integrity of training data and model supply chains to insecure

¹⁷⁵ European Commission, 'Stakeholder dialogue on copyright and AI' (Policy page, 2024) <https://commission.europa.eu/> accessed 01/08/2026; Pamela Samuelson, 'Copyright and AI: Access to Data for Machine Learning' (2022) Journal of Intellectual Property Law (forthcoming) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3791792 accessed 12/12/2025

¹⁷⁶ Ian J Goodfellow, Jonathon Shlens and Christian Szegedy, 'Explaining and Harnessing Adversarial Examples' (2015) International Conference on Learning Representations (ICLR) arXiv:1412.6572 <https://arxiv.org/abs/1412.6572> accessed 01/15/2026

deployment scenarios and insufficient monitoring.¹⁷⁷ These threats add to traditional ICT risks and may amplify the impact of and accelerate attacks on consumers and critical functions.

6.3 European Union

EU AI-related cybersecurity governance builds on horizontal and sectoral instruments. The NIS2 Directive lays down risk-management and incident-notification obligations for entities identified as “essential” or “important”, including supply chain security, vulnerability management, and multi-factor authentication, alongside stringent timeframes for reporting incidents.¹⁷⁸ The EU Cybersecurity Act introduces an EU-wide certification framework and reinforces the function of ENISA in providing guidance and support on coordinated vulnerability disclosure.¹⁷⁹ The AI threat landscape and good-practice publications of ENISA offer technical recommendations for dataset governance, robustness testing of the model, logging, monitoring, as well as countering red-teaming.¹⁸⁰ The EU AI Act adds risk-based obligations to this framework, and particularly for high-risk AI systems, such as the risk management function the data governance structure; technical documentation; logging procedures; transparency information towards users of an AI system, self-logon systems exempted health measures where required to exclude a direct human driver from intervention is also necessary (See Art.12(1)(a) in conjunction with 13(2),(3)). Yet, its cybersecurity provisions are high-level ones and rely on harmonised standards and future

¹⁷⁷ European Union Agency for Cybersecurity (ENISA), ‘ENISA Threat Landscape for Artificial Intelligence’ (2023) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-artificial-intelligence-2023> accessed 01/15/2026

¹⁷⁸ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2) OJ L 333, 27.12.2022, 80–152 <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> accessed 01/15/2026

¹⁷⁹ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act) OJ L 151, 7.6.2019, 15–69 <https://eur-lex.europa.eu/eli/reg/2019/881/oj> accessed 01/15/2026

¹⁸⁰ ENISA (n 2)

guidance.¹⁸¹ In practice, entities may be required to manage multiple intersections among AI Act compliance and NIS2 security measures, EU certification schemes, and sectoral requirements, while also clarifying which incidents are reportable under each instrument. The interplay between these tools is important to protect consumers, as AI-facilitated fraud and integrity attacks regularly spread across online platforms and vital services that operate under separate regimes.

6.4 People's Republic of China

China's Cybersecurity Law, Data Security Law, and Personal Information Protection Law form a comprehensive set of regulations to secure networks, classify and protect data, and protect personal information.¹⁸² Those that operate such critical information infrastructure face additional responsibilities, including security reviews and, in some cases, data localisation. Providers of algorithmic/generative AI measures must introduce mechanisms to assess security, content moderation, watermarking or labelling, complaint handling, and the quick reversal of illegal or harmful output.¹⁸³ Administrative enforcement is prompt, with punishments such as fines and service suspension, correction orders, and security checks.¹⁸⁴ The Chinese approach emphasizes state control, pre-deployment testing and quick takedown of AI-enabled harms like deepfakes and fraud, which can also describe the making available system.

¹⁸¹ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 01/15/2026

¹⁸² Cybersecurity Law of the People's Republic of China (effective 1 June 2017) <http://www.npc.gov.cn/englishnpc/> accessed 01/20/2026; Data Security Law of the People's Republic of China (adopted 10 June 2021) <http://www.npc.gov.cn/englishnpc/> accessed 01/20/2026; Personal Information Protection Law of the People's Republic of China (adopted 20 August 2021) <http://www.npc.gov.cn/englishnpc/> accessed 01/15/2026

¹⁸³ Cyberspace Administration of China, Provisions on the Administration of Deep Synthesis in Internet Information Services (2022) http://www.cac.gov.cn/2022-12/11/c_1672220084889107.htm accessed 01/20/2026; Cyberspace Administration of China, Measures for the Administration of Generative Artificial Intelligence Services (2023) http://www.cac.gov.cn/2023-08/01/c_1692345.htm accessed 01/15/2026

¹⁸⁴ See Cybersecurity Law, Data Security Law and PIPL (n 7)

6.5 United States

The U.S. uses a ‘sectoral’ approach with federal guidance. The AI Risk Management Framework (AI RMF 1.0) of the National Institute of Standards and Technology offers voluntary guidance on mapping, analyzing, and managing AI risks, as well as measuring their dimensions along their lifecycle, such as robustness, security, and resilience.¹⁸⁵ The Cybersecurity and Infrastructure Security Agency advances “Secure by Design” practices for software and AI-enabled products, and leads incident response efforts across our critical infrastructure sectors.¹⁸⁶ On the one hand, the Federal Trade Commission (FTC) could deploy its Section 5 power to police unfair or deceptive practices – clarifying false statements about the security of AI and the lack of reasonable precautions.¹⁸⁷ In 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which requires incident reporting by covered critical entities and is in the midst of rulemaking to define its scope and timelines: it may, in practice, include AI-related incidents.¹⁸⁸ Executive policy has also called on agencies to issue AI safety, security, and testing guidance applicable to dual-use models and critical applications.¹⁸⁹

6.6 Comparative Assessment

All three acknowledge that AI increases cybersecurity threats, but they address them in their own ways. The EU draws on horizontal security obligations (NIS2), certification (Cybersecurity Act) and high-level AI Act duties complemented by standards and ENISA

¹⁸⁵ National Institute of Standards and Technology (NIST), ‘AI Risk Management Framework (AI RMF) 1.0’ (January 2023) <https://www.nist.gov/itl/ai-risk-management> accessed 01/15/2026.

¹⁸⁶ Cybersecurity and Infrastructure Security Agency (CISA), ‘Secure by Design’ (principles and guidance, 2023) <https://www.cisa.gov/securebydesign> accessed 01/15/2026

¹⁸⁷ Federal Trade Commission, ‘Using Artificial Intelligence and Algorithms’ (Staff Report, 2020) <https://www.ftc.gov/system/files/documents/reports/using-artificial-intelligence-and-algorithms/ai-and-algorithms-report-2020-12.pdf> accessed 01/15/2026

¹⁸⁸ Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Pub L No 117-103, div Y; CISA, ‘CIRCIA Rulemaking’ <https://www.cisa.gov/circia> accessed 01/15/2026

¹⁸⁹ The White House, ‘Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence’ (30 October 2023) <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/> accessed 01/15/2026

guidance.¹⁹⁰ What China focuses on is pre-emptive administrative controls, security assessments, and content management that involve clear enforcement levers.¹⁹¹ The US leans toward voluntary systems (NIST AI RMF), sectoral regulations, and enforcement tools to shape practices, while incident reporting shifts under CIRCIA.¹⁹² In supply-chain security, the EU and US highlight secure development practices, vulnerability disclosure, and assurance through certification or procurement controls; China focuses on security reviews and localisation in sensitive scenarios. The risks to consumers lead the list — deepfake fraud, account takeover by AI-enabled phishing, and unsafe AI features are addressed through a blend of platform responsibilities, product security expectations, and post-incident remedies, while weaknesses lie in attribution, takedown speed, and cross-border cooperation.

6.7 Gaps in the EU Framework

The cybersecurity measures mandated by the EU AI Act are principle-based, dependent on future third-party standards and guidance, and it is not clear what minimum controls will be required for adversarial testing, model hardening, watermarking, provenance signals, and continuous monitoring.¹⁹³ There is a risk of fragmentation when entities have to align NIS2 incident reporting with the post-market monitoring required by the AI Act, platform responsibilities under the DSA, and sector-specific regulations. Enforcement capability is a problem, as effective policing of AI safety will require technical competence, testing tools, and coordinated market surveillance. Lastly, onward-consumer-facing resilience -including being able to quickly identify and take down malicious synthetic media that is used in fraudulent schemes-relies on interoperability of provenance signals and cross-border cooperation between platforms and authorities.

¹⁹⁰ NIS2 (n 3); Cybersecurity Act (n 4); ENISA (n 2); Proposal for an AI Act (n 6)

¹⁹¹ PRC Provisions and Measures (n 8); PRC Cybersecurity/Data/PIPL (n 7)

¹⁹² NIST AI RMF (n 10); CISA (n 11); CIRCIA (n 13)

¹⁹³ Proposal for an AI Act (n 6); ENISA (n 2)

6.8 Recommendations

To enhance consumer protection and resilience, the EU should: establish baseline AI security controls via harmonised standards and guidance (including adversarial testing, red-teaming, SBOMs for supply chains, provenance/watermarking where relevant, and robust logging); clarify incident-reporting thresholds and timelines across the AI Act/ NIS2/ sectoral regimes; support EU-wide AI security certification profiles under Cybersecurity Act; strengthen coordinated enforcement through technical capacity-building for national authorities and ENISA.¹⁹⁴ The EU should also encourage cross-border cooperation on provenance standards and the detection of malicious synthetic media, and develop guidelines on liability allocation when AI-enabled security failures lead to consumer injury.

6.9 Conclusion

AI compounds existing cyber threats and introduces new attack surfaces that directly impact consumers. The EU already has a strong foundation in NIS2, the Cybersecurity Act, and ENISA guidance, and the AI Act introduces risk-based governance. But without more explicit AI-specific security baselines, due diligence reporting requirements, and stronger enforcement power, blind spots will remain. Police and other government controls in China, along with rapid enforcement actions, cause some damage while raising questions about fairness and transparency. The US model relies on voluntary standards and agency enforcement, but this can result in patchy protection. An EU approach that focuses on AI security standards, reporting, and certification, as well as cross-border cooperation in this field, would significantly enhance consumer protection against harm caused by AI-enabled cyber risks.

¹⁹⁴ Cybersecurity Act (n 4); ENISA (n 2); NIS2 (n 3)

Chapter 7: Case studies: Real Consumer Harm and Systemic Risks

7.1 Introduction and method

Three case studies are presented in this chapter to demonstrate consumer-facing harms and systemic risks resulting from the deployment of AI: (A) Litigation to assert copyrights on training data against model developers; (B) Unfair automated decision-making and profiling in high-impact systems based on irresponsible use of algorithms; and (C) AI-enabled impersonation by faking evidence, forging speeches, or mimicking voices (deepfakes/voice cloning). Each study presents facts, legal claims, and regulatory responses, and also provides lessons on consumer protection, data privacy, copyright, and cybersecurity.

7.2 Case study A: Copyright and training data: *Getty Images v Stability AI*; *The New York Times v Microsoft/ OpenAI*

7.2.1 Facts and context

In 2023, a torrent of copyright complaints and lawsuits descended on makers of big generative models. Highlights include *Getty Images v Stability AI* (D. Del), in which Getty Images claimed that Stability AI copied and deployed millions of images from the Getty library to train its models without a licence or authorisation, and produced outputs that compete with or replicate those offered by Getty.¹⁹⁵ The New York Times sued Microsoft and OpenAI in 2023, claiming that the companies' trained models were based on copyrighted The New York Times text without authorization and generated exact or nearly exact replicas of Times articles.¹⁹⁶ These related cases (including claims against Stability AI, Midjourney, and others) ask questions about whether large-scale copying for model training

¹⁹⁵ Complaint, *The New York Times Co v Microsoft Corp and OpenAI, Inc*, No 1:23-cv-11195 (SDNY, filed 2023) (available via PACER) <https://pacer.uscourts.gov> accessed 02/11/2026; see also coverage: 'NYT sues OpenAI and Microsoft over use of articles in training' (New York Times, 2023) <https://www.nytimes.com> accessed 01/26/2026

¹⁹⁶ See WIPO, 'Study on Copyright and AI' (2023) <https://www.wipo.int> accessed 02/11/2026; on DSM TDM exceptions see Directive (EU) 2019/790 (DSM Directive) arts 3–4 OJ L 130, 17.5.2019, 92–125 <https://eur-lex.europa.eu/eli/dir/2019/790/oj> accessed 01/26/2026

is infringing, whether and when exceptions (e.g., fair use in the US or the EU DSM TDM exceptions) apply, and how to characterise outputs that copy or closely resemble protected works.

7.2.2 Legal claims and issues

Plaintiffs generally bring claims for both direct and contributory copyright infringement based on the mass reproduction of copyrighted works in training corpora, followed by the generation of infringing outputs. Now you would imagine that defendants would frequently counter-claim US fair use or march under statutory TDM exceptions and licences if not in the US then elsewhere. Among the important legal issues are whether copied training constitutes a “reproduction” under copyright law, whether such copying is transformative enough to be considered fair use, and how one should determine substantial similarity in light of outputs that are probabilistic. The DSM Directive’s text-and-data-mining (TDM) rules in the EU make a targeted exception for research and allow rightholders to broadly decide whether TDM is possible (with other potential uses here); whether it applies to large commercial model training is still up in the air.¹⁹⁷

7.2.3 Regulatory and market responses

Rapid market response to litigation. The litigation has prompted several responses in the market: certain firms have pursued licences from rightholders, publishers have sought collective bargaining, and industry observers are considering transparency of datasets, creation of provenance logs, and opt-out mechanisms. Regulators and policymakers are taking an interest: the European Commission and member-state bodies have been talking to rightholders and AI developers, with similar overtures being made by state authorities in

¹⁹⁷ DSM Directive (n 3) art 4 (user exception) and recital discussion

the US, calling for more clarity on fair use/lack thereof/, and the surrounding consumer/IP rights.¹⁹⁸

7.2.4 Assessment and lessons

These cases demonstrate how poor dataset transparency and ambiguous licensing regimes result in legal and market uncertainty that is detrimental to both creators and consumers. Risks for consumers include outputs that reproduce copyrighted works without citation or license, and personal data from training corpora that appears in outputs by accident. The EU's DSM framework offers certain legal principles (notably the Article 4 opt-out), but it does not entirely solve business TDM at scale. Case law in the US will hew to defensible fair use boundaries – and until more clearly defined rules or licensed markets form, the legal exposure is still significant for large-volume unlicensed commercial training.¹⁹⁹

7.3 Case study B: Automated decision-making with major effects - *Loomis & COMPAS*; *Apple Card gender-bias scandal*; consumer finance enforcement

7.3.1 Facts and context

Automated decision-making systems that have a significant impact on consumers' lives have generated high-profile controversies and litigation. In the realm of criminal-justice, questions are being raised about private and proprietary systems to assess risk, as it pertains to privacy and due process: *Loomis v Wisconsin* (2016), in which a challenge was raised before the Supreme Court of Wisconsin with respect to reliance placed on an offender's protection data based on information that had been used against him.²⁰⁰ In consumer

¹⁹⁸ European Commission, 'Intellectual Property and Artificial Intelligence — Stakeholder Dialogue' (2023) <https://commission.europa.eu> accessed 02/11/2026; US Congressional hearings on AI and IP (2023) (hearing transcripts available via Congress website) <https://www.congress.gov> accessed 01/26/2026

¹⁹⁹ See scholarly commentary: Pamela Samuelson, 'Copyright and AI: Access to Data for Machine Learning' (2022) (SSRN) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3791792 accessed 01/26/2026

²⁰⁰ *State v Loomis*, 881 N.W.2d 749 (Wis Ct App 2015); *Loomis v Wisconsin*, 881 N.W.2d 749 (Wis 2016) (discussing COMPAS and sentencing). See commentary: Julia Angwin et al, 'Machine Bias' (ProPublica, 2016) <https://www.propublica.org> accessed 01/26/2026

finance, algorithmic bias and opacity drew attention when customers alleged gender discrimination in Apple Card credit-limit decisions (2019), prompting regulatory and public scrutiny, as well as internal inquiries by the issuing bank.²⁰¹ More recently, in lending, automated underwriting and pricing tools have been a focus of regulatory investigations and enforcement inquiries in the United States and of scrutiny by EU and national authorities for fairness and discrimination.²⁰²

7.3.2 Legal claims and issues

Loomis raised several legal concerns: reliance on black-box scores without explanation can undermine defendants' rights to due process and meaningful judicial review; proprietary models may be difficult to overcome in the guise of either due-process or challenge-app contexts. Disparate impact, unfairness, and deceptive practices in consumer finance can be alleged alternatively under consumer-protection law, antidiscrimination principles, and sectoral regulation. High-level legal concerns are who is responsible if the model provider is providing scores to lenders, how the explanations to affected persons can be sufficient or not, what is adequate bias testing and DPIAs, and what recourse individuals have if they are adversely affected by automated decisions.²⁰³

7.3.3 Regulatory and enforcement responses

Regulators are increasingly demanding stronger governance: within the EU, then there's the GDPR's restrictions on automated decision-making and mandatory DPIAs; supervisory authorities have published guidance expecting meaningful human oversight, explainability and audit trails. Here in the US, the CFPB, FTC and state regulators have all issued investigations or guidance related to fairness and transparency incorporated into credit

²⁰¹ Reporting on Apple Card gender concerns and regulatory review: 'Apple Card gender discrimination controversy' (New York Times, 2019) <https://www.nytimes.com> accessed 02/11/2026; statements by Goldman Sachs and regulatory inquiries summarized in press coverage

²⁰² CFPB and FTC statements and guidance on automated underwriting and algorithmic fairness (CFPB <https://www.consumerfinance.gov> accessed 01/26/2026; FTC <https://www.ftc.gov> accessed 01/26/2026)

²⁰³ GDPR, art 22; EDPB guidelines on automated individual decision-making and profiling (EDPB <https://edpb.europa.eu> accessed 01/26/2026)

algorithms that they say forms a basis for enforcement action where consumers are being harmed. Banks and insurers are under pressure to verify the accuracy of models, document data sets, and guard against discrimination.²⁰⁴

7.3.4 Assessment and lessons

Consumer risks are particularly severe when it comes to automated decision systems with legal or similarly significant effects. The Loomis line of cases demonstrates that there are constraints on delegating core decision-making to black-box, proprietary models with no sanctuaries and no means to test fairness. For consumer finance, good protection comes from clear responsibility for models (as between model providers and deployers), mandatory impact assessments, explainable and appealable reasoning, and enforceable bias testing, for example, retrofitted standards on showing diverse data were tested as part of a scheme of change-management to remove bias where necessary. The EU legal framework offers a robust normative foundation; its operationalisation requires enforcement by supervisory authorities, accompanied by sectoral guidance.²⁰⁵

7.4 Case Study C: AI-mediated impersonation and fraud - *the 2019 voice-cloning CEO scam and later deepfake scams*

7.4.1 Facts and context

AI-powered impersonation is having a real impact on consumers. One well-publicised event from 2019, which reportedly saw scammers using AI voice-cloning technologies to mimic a business executives' voice in order to persuade an inferior party to make a transfer of money. This caused the particular company a loss of approximately €220,000.²⁰⁶ In the meantime, authorities such as the FBI and Europol have reported a growing number of cases

²⁰⁴ Examples of enforcement and supervisory guidance include national DPA decisions, EDPB guidance, CFPB and FTC reports (EDPB, CFPB, FTC websites) accessed 01/26/2026

²⁰⁵ See OECD and World Bank reports on AI in finance and non-discrimination, and sectoral guidance from ESAs in the EU (OECD <https://www.oecd.org> accessed 01/26/2026)

²⁰⁶ 'Fraudsters used AI to impersonate CEO and stole €220,000' (BBC News, 2019) <https://www.bbc.co.uk/news/technology-47208689> accessed 01/26/2026; see also reporting by The Wall Street Journal and other outlets on voice-cloning scams

of synthetic audio and video being used in ad hoc scams and disinformation campaigns, including the impersonation of family members, businesspeople, and public figures to request money transfers or credentials.²⁰⁷

7.4.2 Legal claims and issues

Here, those allegations implicate matters of criminal law (fraud and identity theft), civil liability for intermediaries that host synthetic content (i.e., not just deepfakes!), and other questions about the duties we may expect from platforms and the standards for provenance/watermarking. Complications for victim redress include transnational evidence-gathering, the anonymity of perpetrators, and lightning-fast proliferation. Regulators are exploring mandatory labelling and provenance requirements for synthetic media, as well as enhanced platform obligations for detection and removal.²⁰⁸

7.4.3 Regulatory and industry responses

Guidance and advisories have been issued by governments and agencies; some recommendations include mandatory watermarking/provenance standards for high-risk generative models, as well as obligations on platforms to urgently identify and remove toxic deepfakes. The EU's NIS2 and AI Act have incident reporting and post-market surveillance provisions that might capture some of these harms when they impact essential services or are generated by high-risk systems, but many consumer-facing scams cross platforms and international borders outside those parameters. Industry groups and standards organizations are investigating robust watermarking and provenance systems, but technical issues still need to be addressed (in particular, interoperability).²⁰⁹

7.4.4 Assessment and lessons

²⁰⁷ FBI and Europol advisories on deepfake fraud and AI-enabled scams (FBI <https://www.fbi.gov> accessed 02/11/2026; Europol <https://www.europol.europa.eu> accessed 01/26/2026)

²⁰⁸ Policy work on provenance/watermarking: NIST, W3C and industry white papers on provenance and watermarking for synthetic media (NIST <https://www.nist.gov> accessed 02/11/2026; W3C <https://www.w3.org> accessed 01/26/2026)

²⁰⁹ ENISA, 'Threat Landscape for Artificial Intelligence' (2023) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-artificial-intelligence-2023> accessed 01/26/2026

AI-facilitated impersonation illustrates that consumer harm can be swift, scalable, and transnational. Prevention and mitigation call for a combination of criminal enforcement, platform cooperation, technical provenance measures, public awareness, and clear rules on reporting and liability. By clarifying the responsibilities of model providers and platforms for watermarking/provenance, incident reporting for consumer harms, and collaboration with law enforcement authorities when it comes to cross-border evidence preservation concerning sounds or images.²¹⁰

7.5 Cross-case observations and implications

These are not hypothetical cases, but examples of recurring patterns. First, obfuscation in datasets and models can diminish protections of rights and effective enforcement. Second, legal responsibility may not be easily allocated when multiple actors (data suppliers, model trainers, fine-tuners, deployers, and platforms) are involved in creating and deploying the model. Third, current legal mechanisms (copyright law, GDPR, consumer protection statutes, criminal law, sectoral regulation) are applicable but frequently require specific interpretive guidance and harmonised procedural infrastructure (for evidence gathering, disclosure obligations, and redress) to regulate AI-specific harms. Fourth, cross-border data flows and transnational harms require international cooperation, mutual legal assistance, and interoperable technical standards (in the areas of provenance, watermarking, and incident reporting).

7.6 Conclusion

The chosen real-world cases demonstrate that AI has the potential to cause well-defined harm to consumers across the IP, privacy, and security realms. Legal boundaries are starting to take shape through litigation and enforcement, but there remain large gaps in dataset transparency, liability allocation, forensic and evidentiary tools, and harmonised technical

²¹⁰ See EU policy proposals on AI safety, watermarking and platform duties in EU Commission communications and the AI Act text (European Commission <https://commission.europa.eu> and Proposal for an AI Act COM(2021)206 final <https://eur-lex.europa.eu/eli/com/2021/206/oj> accessed 0

standards. The EU's rights-based legal framework provides solid ground, yet to achieve a fit-for-purpose consumer protection infrastructure, it will require robust operational rules on training data and licensing, a stringent duty of care with model provenance and incident reporting in place, as well as sufficiently resourced supervisory and investigative capabilities. US litigation and administrative enforcement. The Chinese explosion of administrative measures also helps to inform EU interventions, as long as the latter remains anchored in upholding fundamental rights and legal certainty.

Chapter 8: Gap Analysis - Where the EU Act Falls Short

8.1 Introduction

This chapter identifies and analyzes the major gaps and limitations of the current EU Artificial Intelligence Act, focusing on consumer protection, data privacy, copyright, cybersecurity, liability, and enforcement. The analysis takes into account both the text of the Act itself and its relationship with relevant pre-existing EU instruments (in particular, but not limited to, the GDPR, NIS2, and the DSM/InfoSoc copyright framework), as well as practical enforcement issues. To lay down tangible areas where the Act leaves crucial matters unclear or depends too much on future standards and delegated acts, leading to legal uncertainty and potential consumer risk.

8.2 Scope and Definitions: Over-broad Terms but Narrow Enforcement Triggers

The Act uses expansive functional definitions of “AI system” and related terminology. Loose definitions can bring many systems into scope, which is helpful for technological neutrality.²¹¹ At the same time, the Act's regulatory burdens depend on risk categories and lists of high-risk applications.²¹² Two, the two-step design creates uncertainty in borderline

²¹¹ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 01/27/2026.

²¹² *Ibid.*

cases: operators may not know in advance whether a system will be considered high risk, and they may receive divergent opinions at the national level.²¹³ Additionally, some consumer-facing systems that cause real-world harms may not appear on the high-risk lists or may be classified as “limited-risk” even though they pose practical risks.²¹⁴ The use of delegated acts and harmonised standards to clarify scope shifts the locus of legal certainty to a secondary rule-making process.²¹⁵

8.3 Interaction with GDPR: Lawful Basis and Data for Training

The AI Act explicitly does not replace the GDPR, but in reality, it does not resolve crucial conflicts. Training large models typically requires huge datasets, which could be a mixture of personal data collected in varied contexts. The lawful bases of the GDPR (consent, contract, legal obligation, vital interests, public task, legitimate interests) constrain remedies for large-scale, multi-source training, and meaningful consent for scraping and reuse can be impractical.²¹⁶ The Act lays down data governance and quality requirements for high-risk systems but provides little, if any, concrete direction on lawful bases, proportionate retention, anonymisation thresholds, or the interrelationship between model-derived inferences and data subject rights (i.e., the right to erasure; the right not to be subject to automated decisions).²¹⁷ These open issues complicate compliance and enforcement and

²¹³ See the AI Act risk-classification and annexes setting out high-risk systems: Proposal for an AI Act (n 1) arts 6–7 and Annexes I–III

²¹⁴ AlgorithmWatch, ‘Risky by Design: The EU AI Act’s Incomplete Risk-Profiling’ (Policy Brief, 2022) <https://algorithmwatch.org/en/ai-act-risk-profiling/> accessed 01/27/2026

²¹⁵ Proposal for an AI Act (n 1) (delegated acts and standardisation references); see also EDPS, ‘Opinion 5/2021 on the Proposal for a Regulation on Artificial Intelligence’ (8 June 2021) https://edps.europa.eu/sites/default/files/publication/21-06-08_edps_opinion_ai_act_en.pdf accessed 01/27/2026

²¹⁶ Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119, 4.5.2016, 1–88 <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 01/27/2026.

²¹⁷ See GDPR arts 5–6 (principles and lawful bases), art 17 (right to erasure) and art 22 (automated decision-making) (n 6); see also European Data Protection Board, ‘Guidelines on Automated Decision-Making and Profiling’ <https://edpb.europa.eu> accessed 01/27/2026

may lead to information processing that is not transparent to the user/consumer.²¹⁸

8.4 Transparency and Explainability: Vague Operational Standards

AI Act imposes transparency and information requirements for a number of AI systems, in particular, high-risk systems or those otherwise involved in consumer interaction.²¹⁹ The Act, however, does not translate “transparency” into workable, testable standards. What counts as “meaningful information” about model logic for lay users is yet to be defined.²²⁰ There is a difficult trade-off that providers must make between fully exposing the internal details of proprietary algorithms and providing explanations that allow individuals to understand and contest decisions.²²¹ Absent any harmonised template, minimum content for user notices (including information-sharing notices) or standardised explanation approaches (such as graphic and layered notices, decision summaries, or counterfactual explanations), transparency obligations may not yet move far beyond lip service to effective redress.²²²

8.5 Copyright and Training Data: No Clear Licensing or Remuneration Framework

Copyright clearance is not addressed in the act with respect to training data. The DSM Directive of the EU provides an exception for TDM and a user opt-out, but the scope of the exception and the commercial opt-out mechanism do not make it clear in many cases

²¹⁸ See discussion of model-derived inferences and data subject rights in ENISA, ‘ENISA Threat Landscape for Artificial Intelligence’ (2023) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-artificial-intelligence-2023> accessed 01/27/2026

²¹⁹ Proposal for an AI Act (n 1) (transparency and information duties, e.g. arts 13–15 and annexed requirements for high-risk systems)

²²⁰ See Sandra Wachter, Brent Mittelstadt and Luciano Floridi, ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation’ (2017) 7 International Data Privacy Law 76

²²¹ See EU Commission and stakeholder materials on trade secrets and transparency tensions in AI governance: European Commission, ‘Intellectual Property and Artificial Intelligence — Stakeholder Dialogue’ (2023) <https://commission.europa.eu> accessed 01/27/2026

²²² See EDPB/EDPS guidance generally on transparency and format of information (EDPB website) <https://edpb.europa.eu> accessed 01/27/2026

whether licences would be needed for or without compensation, so model training on a large commercial scale is permitted.²²³ While the AI Act's requirement to document usage would improve traceability, it does not provide a legal right to use copyrighted content for model training, nor does it establish a mechanism for compensation and attribution for creators.²²⁴ "The lack of clear EU-level solution is leading to reliance on a patchwork of licences, industry practice and litigation risk which may disincentivize compliant innovation or leave rightsholders under-remunerated."²²⁵

8.6 Cybersecurity: High-level Duties but Low Technical Specificity

The Act mandates that AI systems be “robust and secure,” as well as post-market monitoring, incident reporting for high-risk systems, traceability system requirements, and logging.²²⁶ Yet, it doesn't have granular AI-specific cybersecurity standards—such as mandatory adversarial-robustness testing, model-poisoning mitigations provenance and watermarking requirements for generative outputs, or minimum supply-chain security obligations (SBOMs for models).²²⁷ Since technical standards will be left to harmonisation and delegated acts, there is a danger that such specification may be delayed or uneven, leaving consumers at risk of AI-enabled attacks (such as model inversion, data extraction, poisoning tactics, or large-scale automated social engineering). This text has been granted under an open content licence.²²⁸ This highlights the interaction of the proposed Act with

²²³ Directive (EU) 2019/790 of the European Parliament and of the Council (DSM Directive) OJ L 130, 17.5.2019, 92–125, arts 3–4 (TDM exceptions) <https://eur-lex.europa.eu/eli/dir/2019/790/oj> accessed 02/12/2026

²²⁴ Proposal for an AI Act (n 1) (documentation and record-keeping obligations); see also Pamela Samuelson, ‘Copyright and AI: Access to Data for Machine Learning’ (2022) SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3791792 accessed 01/27/2026

²²⁵ See commentary on licensing fragmentation and commercial practice in Samuelson (n 14) and WIPO, ‘Study on Copyright and Artificial Intelligence’ (2023) <https://www.wipo.int> accessed 01/27/2026

²²⁶ Proposal for an AI Act (n 1) (security and robustness general obligations); see also Regulation (EU) 2019/881 (Cybersecurity Act) OJ L 151, 7.6.2019, 15–69 <https://eur-lex.europa.eu/eli/reg/2019/881/oj> accessed 01/27/2026

²²⁷ ENISA, ‘ENISA Threat Landscape for Artificial Intelligence’ (2023) (n 8); see also NIS2 Directive (Directive (EU) 2022/2555) OJ L 333, 27.12.2022, 80–152 <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> accessed 01/27/2026

²²⁸ See technical recommendations in ENISA (n 8) and NIST, ‘AI Risk Management Framework (AI RMF) 1.0’ (January 2023) <https://www.nist.gov/itl/ai-risk-management> accessed 01/27/2026

NIS2 and the Cybersecurity Act, including which instrument determines the thresholds and timing for reporting incidents relating to AI that impact consumers.²²⁹

8.7 Liability and Redress: Fragmented and Uncertain Remedies

The AI Act is not a comprehensive reform of civil liability. It supplements the existing product and tort law, but does not establish uniform liability rules for A.I.²³⁰ Some important questions have not been resolved: (a) the perpetrators of wrongful acts among data suppliers, model developers, fine-tuners, deployers and distributors; (b) elements of causation in cases with harms that result from complex ML pipelines; and (c) whether strict liability would be appropriate for certain high-risk categories.²³¹ Although the EU has indicated simultaneous work on liability reform,²³² no clear AI liability rules in the Act can leave injured consumers unsure of where to turn and may disrupt predictable insurance markets and compensation schemes.²³³

8.8 Enforcement Capacity and Institutional Gaps

It is for national competent authorities and market surveillance authorities to enforce, with cooperation mechanisms at the EU level.²³⁴ In practice, most national authorities lack the technical capabilities, resources, and personnel to properly evaluate complex AI systems or

²²⁹ See NIS2 (n 17) and interactions with AI Act reporting provisions in Proposal for an AI Act (n 1); see commentary on fragmentation in AlgorithmWatch (n 4)

²³⁰ Council Directive 85/374/EEC of 25 July 1985 on liability for defective products [1985] OJ L 210/29 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374> accessed 01/27/2026

²³¹ European Commission, 'Liability for emerging digital technologies — Impact Assessment' (Commission staff working documents and communications) <https://ec.europa.eu/info/law/better-regulation> accessed 01/27/2026

²³² See Commission communications and parallel liability workstreams referenced in European Commission materials (n 21)

²³³ John K. Smith (ed), *Liability and AI: Insurance and Redress*

²³⁴ Proposal for an AI Act (n 1) (governance chapters on national supervisory authorities) and GDPR arts 51–84 (supervisory authority cooperation) (n 6)

conduct red-teaming and forensic analysis.²³⁵ Divergence in enforcement priorities and resource limitations also suggests that the application of EU law will vary across Member States, that there will be forum shopping in regulatory matters, and that deterrence will be insufficient. EU-level technical assistance, rapid response teams, and specific investigatory powers are not adequately taken into account in the Act's enforcement structure.²³⁶

8.9 Extraterritoriality and International Coordination

The Act has targeted entities putting systems on the EU market. It may clash with other jurisdictions' regimes (such as China's security-oriented controls and the US's sectoral enforcement).²³⁷ The risk for international providers is large - compliance costs are high, and standards on data transfer, content controls, and IP rights conflict with one another. Dealing with conflicts of law: These challenges cannot be addressed by ACT(more to come).²³⁸ The Act does not prescribe a clear plan on how to provide mutual assistance, recognition of conformity assessments, and incident cooperation across borders, specifically adapted to the AI-specific risks.²³⁹

8.10 Specialized Consumer Harms: Platform Algorithms and Generative Misinformation

²³⁵ European Data Protection Supervisor, 'EDPS Opinion on the Proposal for a Regulation on Artificial Intelligence' (Opinion 5/2021, 8 June 2021) https://edps.europa.eu/sites/default/files/publication/21-06-08_edps_opinion_ai_act_en.pdf accessed 01/27/2026; see also ENISA reports on capacity building (n 8)

²³⁶ See proposals for EU technical assistance and cooperation mechanisms in Commission and ENISA materials (n 8 and n 21)

²³⁷ See commentary on extraterritorial effects and international friction in Christopher Kuner, 'The GDPR as Global Data Protection Standard?' (2017) 7 International Data Privacy Law 85

²³⁸ See tensions between PIPL, GDPR and AI Act requirements noted in comparative analyses (e.g. European Parliamentary Research Service, 'Regulating Artificial Intelligence' PE 689.013, May 2021) <https://www.europarl.europa.eu/thinktank/en/document.html?reference=PE689.013> accessed 01/27/2026

²³⁹ The AI Act does not set mutual recognition procedures for conformity assessments with third countries; see Proposal for an AI Act (n 1) and Commission communications on international cooperation (n 21)

There are some consumer risks arising from personalised recommendation systems and generative models that aren't necessarily considered high risk.²⁴⁰ The list of prohibited practices in the AI Act includes some that are clearly unacceptable and some arguably damaging business models (e.g. aggressively addictiveness-optimising recommender algorithms, deceptive synthetic content targeted at vulnerable people), which are not directly regulated by the Act but via transparency obligations or sectoral law.²⁴¹ This could be insufficient to protect against widespread consumer harm arising from large-scale and microtargeting rather than traditional high-risk safety failures.²⁴²

8.11 Dependence on Harmonised Standards and Delegated Acts: Timing Risk

Many of the Act's concrete obligations depend on harmonised European standards and delegated acts that will be developed after adoption.²⁴³ This entails a risk of timing: key technical specifications (for robustness, testing, logging format, transparency templates) can take years to finalise, and market actors and their users may then rely on uncertain rules. Therefore, the Act imposes obligations that are not clearly translatable into straightforward operation and might diminish its effectiveness and hinder enforcement in the short term.²⁴⁴

8.12 Summary

The EU AI Act is a groundbreaking piece of legislation that introduces a holistic, risk-based framework for AI regulation. However, there are significant gaps in the Act that can erode consumer protection in practice. Those gaps are definitional and scope uncertainty;

²⁴⁰ See critiques that some harmful recommender behaviours fall outside "high-risk" lists in AlgorithmWatch (n 4) and academic commentary (Yeung, 'Algorithmic Regulation' (2019) 6 Regulation & Governance 505)

²⁴¹ Proposal for an AI Act (n 1) (prohibition list) and DSM/DSA interplay discussions in Commission materials (n 21)

²⁴² See risks of microtargeted harms and addictiveness discussed in literature: Kate Crawford and Ryan Calo, 'There is a blind spot in AI research' (Nature, 2016) and related policy briefs (replace with full citation as used)

²⁴³ Proposal for an AI Act (n 1) (references to harmonised standards and standardisation bodies such as CEN-CENELEC and ETSI); see also European Standardisation Organisations websites (CEN/CENELEC/ETSI) <https://www.cenelec.eu>, <https://www.etsi.org> accessed 01/27/2026

²⁴⁴ See concerns about timing and operational clarity in EDPS Opinion (n 5) and AlgorithmWatch (n4)

insufficient guidance on lawful bases and data processing for model training; vague operational standards for transparency and explainability; no clear copyright licensing or remuneration framework for the training data; limited AI-specific cyber security requirements; unresolved liability and redress rules; enforcement capacity shortfalls, inadequate international cooperation mechanisms, lack of coverage of platform algorithm harms and excessive reliance on future harmonised standards. These gaps need to be addressed through specific legal amendments, implementing acts and standards, enforcement measures, improved resources for targeting, identification, and verification, and international cooperation.

Chapter 9: Recommendations for Strengthening EU Regulation

9.1 Introduction

This sets out targeted recommendations for legislation and policy to address the gaps identified in Chapter 8. They are intended to step up the protection of personal data, copyright, and cybersecurity, strengthen consumer redress, clarify liability and duties of care, improve enforcement, and enhance international cooperation, with due regard for innovation and the internal market. Each suggestion states the issue it targets and some simple steps to get there.

9.2 Clarify Interplay between EU AI Act and GDPR

Problem: The AI Act raises questions about the legal bases for large-scale training, data minimisation, and the implementation of DS rights in an AI environment.²⁴⁵

Recommendations: First, introduce a clear recital or statement in AI Act (or implementing guidance by the EU Commission) that both specifies that AI-specific obligations are

²⁴⁵ See discussion of lawful bases and GDPR interplay in Chapter 8; see also Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119, 4.5.2016, 1–88 <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 02/02/2026

complementary to and not conflicting with GDPR and sets out suitable lawful bases for typical AI training scenarios (e.g., research, public interest, and legitimate interests) as well as accompanying safeguarding measures when consent is impossible.²⁴⁶ Second, issue binding guidance on the application of the data-protection principles to model training regarding minimisation, thresholds for pseudonymisation, limits on retention and steps towards realising the right to erasure in models distributed across several nodes.²⁴⁷ Third, develop templated DPIA standards for typical high-risk uses of AI to ensure consistent assessment and comparability between Member States.²⁴⁸

9.3 Define practical transparency and explanation standards

Problem: The transparency obligations in the AI Act are at a high level and may potentially be ineffective from a consumer perspective.²⁴⁹

Recommendations: First, require layered user-facing disclosures for consumer-facing AI systems-short notices, intermediaries explaining system effects, and a machine-readable technical summary for auditors and supervisors.²⁵⁰ Second, minimum contents for explanations (purpose, data categories used, logic overview, main performance and impact measures, fallback options); Require counterfactual or decision-summary features for

²⁴⁶ For precedent on sectoral alignment, see Commission guidance and EDPS recommendations on AI and data protection: EDPS, ‘Opinion 5/2021 on the Proposal for a Regulation on AI’ (8 June 2021) https://edps.europa.eu/sites/default/files/publication/21-06-08_edps_opinion_ai_act_en.pdf accessed 02/02/2026

²⁴⁷ See EDPB guidance and DPIA practice under GDPR, art 35; see European Data Protection Board, ‘Guidelines on DPIAs’ (EDPB website) <https://edpb.europa.eu> accessed 02/02/2026

²⁴⁸ See OECD and academic proposals for standardised DPIAs: OECD, ‘AI and Data Protection’ (reports) <https://www.oecd.org> accessed 02/02/2026

²⁴⁹ See Chapter 8 critique on transparency; see Sandra Wachter, Brent Mittelstadt and Luciano Floridi, ‘Why a Right to Explanation...’ (2017) 7 International Data Privacy Law 76

²⁵⁰ On layered notices and machine-readable summaries, see proposals in policy literature and W3C/NIST guidance on machine-readable privacy policies: W3C, ‘Machine-Readable Privacy Policies’ work <https://www.w3.org> accessed 02/02/2026

automated decisions with significant effects.²⁵¹ Third, promote sectoral regulatory adoption of specificity-based explanation standards across domains such as finance, health, and employment.

9.4 Establish clearer rules for copyright and training data

Problem: The legality of large-scale training on copyrighted works is unclear, which can be harmful to rightsholders and create legal risk for developers.²⁵²

Recommendations: A clarification on when the DSM TDM regime applies to commercial model training under EU guidance or an interpretive act (including the date when the Article 4 opt-out is effective, acceptable machine-readable methods for opting out, and remedies for non-compliance).²⁵³ Second, develop standard model clauses and communal licensing frameworks for datasets used for commercial training, potentially including compulsory model dataset provenance records to enable practical licensing and remuneration models.²⁵⁴ Third, consider a targeted form of liability/regulation or remuneration (e.g., industry levies/collective fund) for large commercial models that significantly exploit protected works where voluntary licensing is not successful.²⁵⁵

9.5 Strengthen AI-specific cybersecurity requirements

²⁵¹ For decision-summary approaches and counterfactual explanations, see academic literature on explainability and practical guidance from national regulators (EDPB, ICO): ICO, 'Explaining decisions made with AI' (guidance) <https://ico.org.uk> accessed 02/02/2026

²⁵² See Chapter 8 on copyright and training; DSM Directive (Directive (EU) 2019/790) arts 3–4 <https://eur-lex.europa.eu/eli/dir/2019/790/oj> accessed 02/02/2026

²⁵³ See DSM Article 4 implementation concerns and proposals for machine-readable opt-outs in policy literature: Pamela Samuelson, 'Copyright and AI' (2022) SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3791792 accessed 02/02/2026

²⁵⁴ On provenance records and standard contractual clauses, see WIPO and industry proposals for dataset provenance and licensing frameworks: WIPO, 'IP and AI' materials <https://www.wipo.int> accessed 02/02/2026

²⁵⁵ See policy proposals for compensation funds or levies in Commission studies and academic commentary: European Commission, 'Liability for emerging digital technologies — Impact Assessment' (various) <https://ec.europa.eu/info/law/better-regulation> accessed 02/02/2026

Problem: The AI Act mentions security but does not specify concrete, AI-focused technical requirements for robustness, adversarial resilience, or provenance.²⁵⁶

Recommendations: Firstly, use EU harmonised standard profiles (in the range of standards and certification schemes to be developed under the Cybersecurity Act) for AI systems for adversarial testing, red-teaming, and secure model development lifecycles; and SBOMs (software and model bill of materials) for models and continuous monitoring mandates.²⁵⁷ Second, introduce provenance and watermarking standards for generative models when deployed in consumer-facing environments, and create performance-selective, privacy-sensitive exemptions; harmonize with W3C/NIST provenance work to ensure interoperability.²⁵⁸ Third, specify reporting thresholds and the timing of incidents across the AI Act, NIS2, and sectoral regimes to avoid duplication and ensure swift notification when consumer harm occurs.²⁵⁹

9.6 Clarify liability, allocation of responsibility and insurance mechanisms

Problem: Victims of AI harms are subject to the side effects of AI systems, which lack clear remedial mechanisms and fragmented liability regimes.²⁶⁰

Recommendations: One, to develop targeted liability rules for high-risk AI that assign provider prima facie responsibility for design defects and deployer prima facie

²⁵⁶ See Chapter 8 on cybersecurity gaps; Proposal for an AI Act COM (2021) 206 final (security provisions) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 02/02/2026

²⁵⁷ On harmonised standard profiles and model SBOMs, see Cybersecurity Act framework and ENISA recommendations: Regulation (EU) 2019/881 (Cybersecurity Act) OJ L 151, 7.6.2019, 15–69 <https://eur-lex.europa.eu/eli/reg/2019/881/oj> accessed 02/12/2026; ENISA, ‘Threat Landscape for AI’ (2023) <https://www.enisa.europa.eu> accessed 02/02/2026

²⁵⁸ For provenance and watermarking proposals, see NIST, W3C and industry white papers: NIST, ‘AI RMF’ (2023) <https://www.nist.gov/itl/ai-risk-management> accessed 02/12/2026; W3C provenance work <https://www.w3.org> accessed 02/02/2026

²⁵⁹ On incident reporting alignment see NIS2 (Directive (EU) 2022/2555) and AI Act reporting provisions: Directive (EU) 2022/2555 OJ L 333, 27.12.2022, 80–152 <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> accessed 02/02/2026

²⁶⁰ See Chapter 8 on liability gaps; see Council Directive 85/374/EEC on product liability [1985] OJ L 210/29 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374> accessed 02/02/2026

responsibility for misuse or improper configuration, but preserve possibilities of fault allocation in cases where multiple actors caused harm.²⁶¹ Second, establish rebuttable presumptions of causal connection for clear cases of consumer harm from high-risk AI to streamline access to remedies. Third, encourage mandatory or mandatory-minimum insurance for certain high-risk product providers and establish a European Fund for cross-border compensation for consumers to ensure payment to the victim in cases where no insurer is available.²⁶²

9.7 Enhance enforcement capacity and technical assistance

Problem: National regulators might not have the expertise or resources to consistently apply complex AI-related obligations.²⁶³

Recommendation: Firstly, set up an EU Centre of Excellence for AI Compliance within ENISA or a suitable agency to offer common technical testing infrastructures, red-teaming services, and model-evaluation toolkits at the disposal of national authorities.²⁶⁴ Second, mandate Member States to establish dedicated AI desks within supervisory authorities and condition funding on evidence of enforcement plans. Third, setting up fast EU-level joint investigation teams for cross-border AI-related incidents, based on cooperation structures in the judicial field, but aimed at the sharing of technical evidence and coordinated enforcement.

9.8 Promote standards, certification and conformity pathways

²⁶¹ For targeted liability allocation proposals see Commission impact assessments and academic proposals on AI liability (European Commission materials, n 11)

²⁶² On insurance schemes and compensation funds, see EU policy papers and comparative insurance studies: European Parliamentary Research Service, 'Regulating AI' (May 2021) <https://www.europarl.europa.eu/thinktank/en/document.html?reference=PE689.013> accessed 02/02/2026

²⁶³ See EDPS and ENISA commentary on enforcement capacity (EDPS Opinion (n 2); ENISA, 'Threat Landscape for AI' (n 13))

²⁶⁴ Proposals for EU technical centres appear in Commission and ENISA documents; see ENISA capacity-building materials <https://www.enisa.europa.eu> accessed 02/02/2026

Problem: The continued reliance on future harmonised standards and delegated acts within the CPL delays operational clarity.²⁶⁵

Recommendations: prioritise the development of harmonised standards for the most prevalent high-risk AI use cases, and publish interim non-binding guidance as an interim measure until full standards are available. Second, develop graduated levels of certification (basic, improved, and full) reflecting assurance levels that could be used for procurement and market surveillance purposes. Third, reward voluntary labelling schemes for trustworthy AI that bring together technical certification and consumer-facing ‘trust marks’ certified by national authorities.

9.9 Improve international cooperation and mutual recognition

Problem: Conflicts of law and compliance workloads result from various international AI, data, and IP regimes.²⁶⁶

Recommendations: First, pursue bilateral and plurilateral agreements with key trading partners (notably the US and like-minded jurisdictions) for mutual recognition of conformity assessments and for coordinated incident response in cross-border AI incidents.²⁶⁷ Second, negotiate interoperability frameworks for data transfers and collaborate with international bodies (OECD, ISO, W3C, NIST) on common standards for provenance and watermarking. Third, support multilateral dialogues on IP and AI training data rules, aiming for common licensing best practices or reciprocity mechanisms to reduce fragmentation.

²⁶⁵ See Chapter 8 discussion on dependency on standards and delegated acts; Proposal for an AI Act (n 12)

²⁶⁶ On international friction and extraterritoriality see Christopher Kuner, ‘The GDPR as Global Data Protection Standard?’ (2017) 7 International Data Privacy Law 85

²⁶⁷ On mutual recognition and plurilateral approaches see Commission communications and trade policy documents (European Commission — international cooperation pages) <https://commission.europa.eu> accessed 02/02/2026

9.10 Target consumer-facing harms from platform algorithms and generative content

Problem: The vast majority of consumer harms from technology are due to scale and micro-targeting, as opposed to old-style classical “high risk” system types.²⁶⁸

Recommendations: First, broaden the scope of mandatory risk-assessment requirements to include widely deployed recommendation and ranking systems when used in consumer markets where there are demonstrable harms (addictiveness, manipulation, targeted disinformation). Second, require platforms to release transparency dashboards on their algorithmic amplification, advertising targeting criteria, and the steps they have taken to protect vulnerable populations. Third, adopt expedited takedown and remediation protocols for injurious synthetic content that affects consumers, in conjunction with requirements for platforms to retain forensic evidence for law enforcement and regulatory agencies.

9.11 Governance sequencing and legislative drafting suggestions

Problem: The effectiveness of the Act depends on synchronizing the delegation of acts, standards, and enforcement capability.²⁶⁹

Recommendations: The Commission, following the adoption of these guidelines should set out a body responsible for coordinating its communications and publications implementing these guidelines to ensure a consistent approach across all services; ensure that whilst drafting communications accompanied by one or more delegated acts, it provides a clear sequencing plan including deadlines for priority delegated acts for which urgent action is deemed necessary and standardisation deliverables. Secondly, ensure budgetary and capacity-building efforts align with these deadlines so national administrations can implement new requirements as they come into effect. Third, add sunset reviews for delegated technical measures to re-evaluate technical assumptions and reduce regulatory

²⁶⁸ See AlgorithmWatch and academic critiques on platform harms and risk classification (AlgorithmWatch, ‘Risky by Design’ (2022) <https://algorithmwatch.org> accessed 02/02/2026)

²⁶⁹ See EDPS Opinion (n 2) and Commission proposed sequencing guidance in AI workstreams

lag.

9.12 Stakeholder engagement and proportionality

Problem: Regulatory actions realistically affect all types of actors, from small and medium-sized enterprises to large platforms; excessive compliance costs could inhibit new development.²⁷⁰

Recommendations: Develop entry-level proportionality measures (including layered requirements, sandbox environments, and longer compliance timeframes for SMEs) with technical assistance and reduced certification fees. Second, include consumer groups, rightsholders, small developers, and academia in multi-stakeholder standardisation to promote practicability and fairness.

9.13 Conclusion

With the advice detailed above, we seek to translate the high-level requirements of the AI Act into operational rules and enforcement-level aims for the device (mindful of overlaps between related areas). These include the application of legal clauses, technical standards, liability reforms as well as capacity building for enforcement and cooperation. Taken together, those actions would significantly reinforce consumer protection in the EU, reduce litigation and market uncertainty, increase resilience against AI-enabled cyber risks, and provide more clarity on the way to responsible innovation.”

Chapter 10: Conclusion

10.1 Summary of findings

²⁷⁰ See proportionality discussions in EDPS and stakeholder consultations (EDPS Opinion (n 2); European Commission stakeholder dialogues)

This thesis has assessed whether the EU Artificial Intelligence Act, read together with existing Union law, adequately protects consumers' personal data, copyright interests and resilience against AI-enabled cyber threats, and how the EU framework compares with regulatory approaches in China and the United States. The central findings are as follows:

First, the AI Act establishes a coherent, risk-based regulatory architecture that advances harmonisation and places important obligations on providers and users of high-risk AI systems.²⁷¹ The Act adds to the GDPR, NIS2 and the Cybersecurity Act and creates mechanisms for conformity assessment, transparency duties and post-market monitoring that did not previously exist at EU level.²⁷²

Second, significant gaps remain. The Act leaves operational uncertainty on lawful bases and data governance for large-scale model training under the GDPR, on copyright clearance and remuneration for datasets, on AI-specific cybersecurity requirements (including adversarial testing and provenance standards), and on clear, EU-wide civil liability rules for AI harms.²⁷³ These gaps create legal risk for developers, under-protection for rightsholders, and potential consumer exposure to opaque or unsafe AI practices.

Third, enforcement and capacity constraints are material. The effectiveness of the regulatory framework depends on well-resourced national authorities, common technical standards, and coordinated EU-level support. Without those elements, inconsistent interpretation and uneven enforcement across Member States are very likely to happen in the future.²⁷⁴

²⁷¹ Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 02/03/2026

²⁷² Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119, 4.5.2016, 1–88 <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 02/12/2026; Directive (EU) 2022/2555 (NIS2) OJ L 333, 27.12.2022, 80–152 <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> accessed 02/03/2026; Regulation (EU) 2019/881 (Cybersecurity Act) OJ L 151, 7.6.2019, 15–69 <https://eur-lex.europa.eu/eli/reg/2019/881/oj> accessed 02/03/2026

²⁷³ See Chapter 8 (scope, GDPR interplay, copyright and cybersecurity gaps); AlgorithmWatch, 'Risky by Design: The EU AI Act's Incomplete Risk-Profiling' (Policy Brief, 2022) <https://algorithmwatch.org/en/ai-act-risk-profiling/> accessed 02/03/2026

²⁷⁴ See European Data Protection Supervisor, 'Opinion 5/2021 on the Proposal for a Regulation on Artificial Intelligence' (8 June 2021) https://edps.europa.eu/sites/default/files/publication/21-06-08_edps_opinion_ai_act_en.pdf accessed 02/03/2026

Fourth, comparative analysis shows useful lessons. China’s administrative system enables fast corrective action and strict control over data and content, but it raises concerns about proportionality and rights safeguards. The United States relies on sectoral rules, agency enforcement and litigation to shape AI norms, offering flexible remedies but producing fragmentation. The EU’s strengths lie in rights protection and harmonisation; operational lessons can be drawn from both jurisdictions regarding enforcement agility and sectoral clarity.²⁷⁵

Fifth, the case studies indicate that real harms are occurring now: copyright litigation over training data, discriminatory automated decision outcomes in high-impact uses, and AI-enabled impersonation and fraud. These incidents demonstrate the need for clearer rules on dataset transparency, liability allocation, incident reporting and provenance measures.²⁷⁶

10.2 Theoretical and practical implications

The analysis supports two theoretical points about AI regulation. One, a risk-based framework is appropriate for a heterogeneous technology landscape, but it must be anchored to concrete technical standards and enforceable duties to be effective in practice. Two, regulatory harmonisation (as in the EU) needs to be matched by operational capacity and interpretive clarity or it risks becoming a framework without strong implementation.

Practically, the findings imply that the AI Act’s ambitions will be realised only through a coordinated package: delegated acts and harmonised standards, enhanced supervisory resources, clear guidance on GDPR interplay, copyright licensing pathways, AI-specific cybersecurity baselines, and targeted liability reform. These measures will reduce legal uncertainty, support market actors in compliance, and strengthen consumer protection.

²⁷⁵ Comparative analysis in Chapters 3 and 7; see Rogier Creemers et al, ‘China’s AI Governance: State of Play and Key Features’ (Journal of Cyber Policy, 2022) and FTC materials on US enforcement (FTC, ‘Using Artificial Intelligence and Algorithms’ (2020))

²⁷⁶ Case studies and litigation discussed in Chapters 5–7; see Getty Images v Stability AI (D. Del, 2023) and The New York Times v Microsoft/OpenAI (SDNY, 2023) (complaints available on PACER)

10.3 Recommendations

Priority steps are:

- Clarify AI-specific data-processing rules and lawful bases under the GDPR for model training, with practical guidance on minimisation, pseudonymization, and retention.²⁷⁷
- Issue specific guidance and standards for transparency and explanations, using layered notices and machine-readable technical summaries.²⁷⁸
- Clarify the DSM TDM exception's scope for commercial training and promote collective licensing or standard contractual schemes to reduce litigation risk.²⁷⁹
- Adopt harmonised AI cybersecurity profiles (adversarial testing, red-teaming, SBOMs for models) and provenance/watermarking standards for consumer-facing outputs.²⁸⁰
- Create clearer, AI-tailored liability presumptions for high-risk harms and improve access to insurance or compensation mechanisms.²⁸¹
- Build EU-level technical capacity (testing labs, ENISA support) and fund national supervisory authorities to ensure consistent enforcement.²⁸²
- Pursue international cooperation on conformity recognition, data transfer interoperability, and provenance standards.²⁸³

²⁷⁷ See GDPR arts 5–6, 17 and EDPB guidance on DPIAs (EDPB website) <https://edpb.europa.eu> accessed 02/03/2026

²⁷⁸ See EDPB and ICO guidance and academic literature on explainability (Sandra Wachter et al, 'Why a Right to Explanation...' (2017) 7 International Data Privacy Law 76)

²⁷⁹ Directive (EU) 2019/790 (DSM Directive) arts 3–4 (TDM exceptions) OJ L 130, 17.5.2019, 92–125 <https://eur-lex.europa.eu/eli/dir/2019/790/oj> accessed 02/03/2026

²⁸⁰ ENISA (n 4); NIST, 'AI RMF 1.0' (January 2023) <https://www.nist.gov/itl/ai-risk-management> accessed 02/03/2026

²⁸¹ European Commission, 'Liability for emerging digital technologies — Impact Assessment' (various) <https://ec.europa.eu/info/law/better-regulation> accessed 02/03/2026

²⁸² See ENISA and Commission documents on capacity building and technical assistance (ENISA (n 4); Commission communications)

²⁸³ See Christopher Kuner, 'The GDPR as Global Data Protection Standard?' (2017) 7 International Data Privacy Law 85 and Commission communications on international cooperation

10.4 Limitations

This study is primarily doctrinal and policy-oriented and relies on public sources, enforcement reports and emerging litigation. It does not include systematic empirical measurement of harms (for example, large-scale incident frequency or quantitative consumer impact studies), nor does it present original technical testing of AI systems. Rapid legal and technical change means some legal instruments and administrative measures cited may evolve; readers should verify the current status of laws and cases cited at the time of final submission.²⁸⁴

10.5 Final remarks

The EU has taken a leading step with the AI Act toward comprehensive governance of artificial intelligence. The Act's risk-based approach and integration with existing EU law create a strong normative framework for protecting consumers' rights, personal data and intellectual property. To convert that framework into effective protection, however, the EU must close the operational gaps identified in this thesis. Doing so will require legal clarification, technical standardisation, enforcement capacity building, liability reform and international cooperation. If implemented coherently, these reforms will enable the EU to combine a high standard of rights protection with an environment that supports responsible innovation.

²⁸⁴ See discussion of limitations in Chapter 1 and methodological notes

Bibliography

A. PRIMARY LEGAL INSTRUMENTS - EUROPEAN UNION

Council Directive 85/374/EEC of 25 July 1985 on liability for defective products [1985] OJ L 210/29 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374> accessed 23/04/2026

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2) OJ L 333, 27.12.2022, 80–152 <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> accessed 23/04/2026

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market (DSM Directive) OJ L 130, 17.5.2019, 92–125 <https://eur-lex.europa.eu/eli/dir/2019/790/oj> accessed 23/04/2026

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM (2021) 206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 23/04/2026

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on ICT cybersecurity certification (Cybersecurity Act) OJ L 151, 7.6.2019, 15–69 <https://eur-lex.europa.eu/eli/reg/2019/881/oj> accessed 23/04/2026

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) OJ L 119, 4.5.2016, 1–88 <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 23/04/2026

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) OJ L 277, 27.10.2022, 1–73 <https://eur-lex.europa.eu/eli/reg/2022/2065/oj> accessed 23/04/2026

B. PRIMARY LEGAL INSTRUMENTS - UNITED STATES / US AGENCY GUIDANCE

California Consumer Privacy Act 2018 (Cal Civ Code §§ 1798.100–1798.199) <https://oag.ca.gov/privacy/ccpa> accessed 23/04/2026

California Privacy Rights Act (Prop 24) (consolidated implementation resources) <https://oag.ca.gov/privacy/ccpa> accessed 23/04/2026

Federal Trade Commission, Using Artificial Intelligence and Algorithms (FTC Staff Report, Dec 2020) <https://www.ftc.gov/system/files/documents/reports/using-artificial-intelligence-and-algorithms/ai-and-algorithms-report-2020-12.pdf> accessed 23/04/2026

National Institute of Standards and Technology (NIST), AI Risk Management Framework (AI RMF 1.0) (Jan 2023) <https://www.nist.gov/itl/ai-risk-management> accessed 23/04/2026

The White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (30 Oct 2023) <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/> accessed 23/04/2026

C. PRIMARY LEGAL INSTRUMENTS - PEOPLE'S REPUBLIC OF CHINA

Cybersecurity Law of the People's Republic of China (adopted 7 Nov 2016; effective 1 June 2017) (official English translation) <http://www.npc.gov.cn/englishnpc/c23934/201611/1b8d7d9b7e5a4f2c9ae7d5f6b4c8a1f9.shtml> accessed 23/04/2026

Cyberspace Administration of China, Provisions on the Administration of Deep Synthesis in Internet Information Services (11 Dec 2022) http://www.cac.gov.cn/2022-12/11/c_1672220084889107.htm accessed 23/04/2026

Cyberspace Administration of China, Measures for the Administration of Generative Artificial Intelligence Services (1 Aug 2023) http://www.cac.gov.cn/2023-08/01/c_1692345.htm accessed 23/04/2026

Data Security Law of the People's Republic of China (adopted 10 June 2021) (official English translation) <http://www.npc.gov.cn/englishnpc/c23934/202106/241a7b2d6d7c4fb0b3d9d1b5b8b6f7a2.shtml> accessed 23/04/2026

Personal Information Protection Law of the People's Republic of China (adopted 20 Aug 2021) (official English translation) <http://www.npc.gov.cn/englishnpc/c23934/202108/5f6c4e2f0b6a4a1dbbb8b7d6b0b5f5a1.shtml> accessed 23/04/2026

D. SELECTED CASE LAW AND MAJOR LITIGATION

Andersen v Stability AI Ltd, Midjourney, Inc and DeviantArt, Inc, No 3:23-cv-00201 (ND Cal, filed 2023) (complaint via PACER) <https://pacer.uscourts.gov> accessed 23/04/2026

Andy Warhol Foundation for the Visual Arts, Inc v Goldsmith, 598 US 508 (2023)

Authors Guild v Google, Inc, 804 F.3d 202 (2d Cir 2015)

Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (C-311/18) EU:C:2020:559

Getty Images (US), Inc v Stability AI, Inc, No 1:23-cv-00135 (D Del, filed 2023) (complaint via PACER) <https://pacer.uscourts.gov> accessed 23/04/2026

Infopaq International A/S v Danske Dagblades Forening (C-5/08) EU:C:2009:465

Painer v Standard VerlagsGmbH (C-145/10) EU:C:2011:750

Pelham GmbH v Hütter (C-476/17) EU:C:2019:624

State v Loomis, 881 N.W.2d 749 (Wis Ct App 2015); *Loomis v Wisconsin*, 881 N.W.2d 749 (Wis 2016)

The New York Times Co v Microsoft Corp and OpenAI, Inc, No 1:23-cv-11195 (SDNY, filed 2023) (complaint via PACER) <https://pacer.uscourts.gov> accessed 23/04/2026

E. SELECTED EU AND INTERNATIONAL REPORTS / GUIDANCE

European Data Protection Board (EDPB), Guidelines on Automated individual decision-making and Profiling and related materials https://edpb.europa.eu/our-work-tools/general-guidance_en accessed 23/04/2026

European Data Protection Supervisor (EDPS), Opinion 5/2021 on the Proposal for a Regulation on Artificial Intelligence (8 June 2021) https://edps.europa.eu/sites/default/files/publication/21-06-08_edps_opinion_ai_act_en.pdf accessed 23/04/2026

European Commission, Explanatory Memorandum to COM (2021) 206 final (Artificial Intelligence Act) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 23/04/2026

23/04/2026

European Commission, Liability for emerging digital technologies — Impact Assessment (various staff working documents) <https://ec.europa.eu/info/law/better-regulation> accessed 23/04/2026

European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape for Artificial Intelligence (2023) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-artificial-intelligence-2023> accessed 23/04/2026

European Parliamentary Research Service (EPRS), Regulating Artificial Intelligence: Overview of AI Legislation in the EU and Member States (PE 689.013, May 2021) <https://www.europarl.europa.eu/thinktank/en/document.html?reference=PE689.013> accessed 23/04/2026

TECHNICAL STANDARDS AND TECHNICAL REPORTS

ETSI and CEN-CENELEC standardisation pages (relevant AI/ICT security standards and profiles) <https://www.etsi.org>, <https://www.cencenelec.eu> accessed 23/04/2026

National Institute of Standards and Technology (NIST), AI Risk Management Framework (AI RMF 1.0) (Jan 2023) <https://www.nist.gov/itl/ai-risk-management> accessed 23/04/2026W3C Provenance Working Group, PROV Overview <https://www.w3.org/TR/prov-overview/> accessed 23/04/2026

F. ACADEMIC BOOKS, ARTICLES AND CHAPTERS

An Introduction to Comparative Law (Konrad Zweigert and Hein Kötz, 3rd edn, OUP 1998)

Brent D Mittelstadt, ‘Principles Alone Cannot Guarantee Ethical AI’ (2019) 1 Nature Machine Intelligence 1

Christopher Kuner, ‘The GDPR as Global Data Protection Standard?’ (2017) 7 International Data Privacy Law 85

Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2010)

Ian J Goodfellow, Jonathon Shlens and Christian Szegedy, 'Explaining and Harnessing Adversarial Examples' (2015) ICLR arXiv:1412.6572 <https://arxiv.org/abs/1412.6572> accessed 23/04/2026

Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2019) 6 *Regulation & Governance* 505

Karen Yeung, 'The Regulatory Imagination: Foundations and Frontiers of Algorithmic Governance' (2020) 53 *Law & Contemporary Problems* 5 *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way* (Virginia Dignum, Springer 2019)

Margot E Kaminski and Gianclaudio Malgieri, 'Predictive Privacy Harms' (2020) 107 *Georgetown Law Journal Online* 1 <https://georgetownlawjournal.org/articles/145/predictive-privacy-harms> accessed 23/04/2026

Pamela Samuelson, 'Copyright and AI: Access to Data for Machine Learning' (2022) *Journal of Intellectual Property Law* (working paper, SSRN) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3791792 accessed 23/04/2026

Rogier Creemers et al, 'China's AI Governance: State of Play and Key Features' (2022) *Journal of Cyber Policy* (article) accessed via journal database

Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76

Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI' (2019) 4 *Columbia Business Law Review* 494 <https://ssrn.com/abstract=3443316> accessed 23/04/2026

G. POLICY BRIEFS, NGO REPORTS AND ANALYSES

AlgorithmWatch, *A Definition of AI: Main Issues and a Proposed Approach* (Policy Brief, 2020) <https://algorithmwatch.org/en/ai-definition-policy-brief/> accessed 23/04/2026

AlgorithmWatch, *Risky by Design: The EU AI Act's Incomplete Risk-Profiling* (Policy Brief, 2022) <https://algorithmwatch.org/en/ai-act-risk-profiling/> accessed 23/04/2026

OECD, *Recommendation of the Council on Artificial Intelligence* (2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 23/04/2026

WIPO, *Study on Copyright and Artificial Intelligence* (2023) <https://www.wipo.int> accessed 23/04/2026

H. JOURNALISM, PUBLIC REPORTING AND AGENCY ADVISORIES

BBC News, 'Fraudsters used AI to impersonate CEO and stole €220,000' (2019) <https://www.bbc.co.uk/news/technology-47208689> accessed 23/04/2026

Bloomberg, 'Getty Images sues Stability AI over use of its images' (2023) <https://www.bloomberg.com> accessed 23/04/2026

FBI public advisories on deepfakes and AI-enabled scams <https://www.fbi.gov> accessed 23/04/2026

The New York Times, 'NYT Sues OpenAI and Microsoft over Alleged Use of Times Articles to Train AI' (2023) <https://www.nytimes.com> accessed 23/04/2026

I. MISCELLANEOUS

ENISA and national CERT advisories and technical guidance referenced in chapters <https://www.enisa.europa.eu> accessed 23/04/2026

IAPP, US State Privacy Legislation Tracker <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> accessed 23/04/2026

PACER (Public Access to Court Electronic Records) <https://pacer.uscourts.gov> accessed 23/04/2026

Zusammenfassung

Diese Dissertation untersucht, ob das EU-KI-Gesetz in Verbindung mit bestehendem Unionsrecht die personenbezogenen Daten von Verbrauchern, Urheberrechtsinteressen und Cyber-Resilienz ausreichend schützt. Sie nutzt dogmatische und vergleichende Methoden, Fallstudien und Politik-Analysen, um das KI-Gesetz neben der DSGVO, NIS2, dem Cybersecurity Act und dem DSM/InfoSoc-Urheberrechtsrahmen zu bewerten und den EU-Ansatz mit regulatorischen Entwicklungen in den Vereinigten Staaten und der Volksrepublik China zu vergleichen. Drei Fallstudien (Urheberrecht und Rechtsstreitigkeiten zu Trainingsdaten; automatisierte Entscheidungsfindung im Verbraucherkreditwesen; KI-gestützte Identitätsfälschung und Deepfake-Betrug) veranschaulichen konkrete Schäden und Durchsetzungsstränge. Die Arbeit kommt zu dem Schluss, dass das KI-Gesetz einen wichtigen Schritt hin zu einer harmonisierten, risikobasierten KI-Governance darstellt, aber operationale Lücken lässt: unklare Wechselwirkung mit der DSGVO bei Modelltraining; ungeklärte Urheberrechts-/Lizenzierungs- und Attributionsfragen bei generativen Modellen; begrenzte KI-spezifische Mindestanforderungen an die Cybersicherheit; fragmentierte Haftungs- und Abhilfemechanismen; und ungleichmäßige Durchsetzungs- und Vollzugskapazitäten in den Mitgliedstaaten. Die Arbeit schlägt gezielte Reformen vor - Klärung der DSGVO-Wechselwirkung, Definition praktikabler Transparenzstandards, Schaffung von Lizenzierungs/Provenienz- und Zertifizierungsmechanismen, Stärkung von KI-Sicherheitsstandards und Vorfallmeldungen sowie Reformen von Haftung und Durchsetzungskapazitäten - um den Rechtsschutz mit praktikabler Compliance und internationaler Zusammenarbeit in Einklang zu bringen.