EUROsimA 2025

Council of the EU

Study Guide

Establishing an EU Customs Data Hub and an EU Customs Authority
Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence

Council of the European Union Study Guide

European Union Simulation in Ankara (EUROsimA) 2025

Organized by
Foreign Policy and International Relations Society
Middle East Technical University
Üniversiteler Mah. Dumlupınar Bulvarı No: 1
İktisadi ve İdari Bilimler Fakültesi B Binası Zemin Kat

06800, Çankaya, Ankara, Türkiye

EUROsimA 2025
Ankara - Türkiye 2025

TABLE OF CONTENTS

LETTER FROM THE SECRETARY GENERAL

Dear Participants,

My name is Burak Eren Ceyhan, I am a second-year International Relations major studying in the Middle East Technical University and it is my utmost pleasure and honor to be serving as the Secretary General of EUROsimA'25.

Considering that I am 21 years old and EUROsimA'25 will be the 21st edition of out conference, the history and excellence of EUROsimA needs no further deliberation. As someone who has participated in Model UN, Model EU and Moot Court simulations with a general experience in such simulation conferences in its seventh year; this experience holds a special place in my heart. Myself, my partner the honorable Director General Selin Örsak and our academic and organization teams have worked night and day to present you with the best experience possible. In that regard, I expect you all from the most experienced to the first timer participant alike to give it your all and ensure that EUROsimA'25 reaches its full potential.

One sentiment that stuck with me from my previous EUROsimA experiences was a sentence all former and current Secretary Generals stated in their closing speeches; "EUROsimA is, and always will be, a family business.". I get the meaning more than ever as I am preparing this letter. I would like to thank my family that has given me their all despite my demanding deadlines and feedback, it would not have been the same without you.

I am very excited to see you all soon; please prepare to the conference with your best efforts and make the most of your experience of fun and learning. Good luck.

Burak Eren Ceyhan Secretary-General

LETTERS FROM UNDER SECRETARY GENERALS AND ACADEMIC ASSISTANTS

Most esteemed participants, I am Derin Engür, a first-year Business Administration student from METU. I have been involved in MUN conferences since the beginning of high school, and EUROsimA is and always will be a special experience for me. I had the great fortune of being a member of this organization as both an Under-Secretary general and an academic assistant of the European Parliament. EUROsimA taught me a lot about friendship, hard work and of course solidarity. These lessons were ones that I will carry with me throughout my life. Enough being said, I want to welcome you all to this conference which is very special to me.

This year, I am the Under-Secretary General of the European Parliament, which is in my opinion, is the cornerstone of EUROsimA. Working together with the Council of the European Union, this committee will definitely be a remarkable experience for all of you. This year our first topic will be about "customs union," a subject that has been a significant matter of debate in the EU since it's very foundation and will always be a crucial topic to the existence of the Union. I and my academic assistants Rüzgar Bakır and Alperen Arifoğlu have tried to explain the topic best we can. Our second topic will be about "AI Liability Directive"; this agenda will be delivered to you by Ata Yağız Topaloğlu, I want to thank him as well for all he has done and all he will do as the head of OLP during the conference. While I will not be able to be with you during the conference due to unforeseen circumstances I leave you to the capable hands. Have fun in EUROsimA 25'!

Kindest regards,

Derin Engür

Under Secretary General of the European Parliament

Hello everyone,

I am Ata Yağız Topaloğlu. I am a second-year Political Science and Public Administration student, as well as a first year International Relations minor student. In high school, I had the opportunity to take part in MUNs and thanks to DPUIT, I have been involved in making EUROsimA's in the last two years. Last year, as an Academic Assistant and this year as an Under-Secretary General, I had the opportunity to organize this prestigious conference and learn its environment of team-work and friendship.

As I stated before, I am the Under-Secretary General of the Council of the European Union. Working together with the European Parliament, under the OLP procedure - we will have a remarkable experience together. We will be covering two topics together related to the "customs union" and the "AI liability directive". Working together with the EP, I want to thank the EP's Under-Secretary General Derin Engür for his hard work and successful collective team work. As well as I would like thank our academic assistants, Dila Demircan, Rüzgar Bakır and Alp Arifoğlu.

Kindest regards,

Ata Yağız Topaloğlu

Most esteemed and distinguished participants,

I am Rüzgar Bakır and I am studying Physics Engineering at Hacettepe University. I have been taking a part in MUNs for 3 years and EUROsimA takes a special place in my heart, where I experienced my first committee board member experience, in the Council of the European Union. From that moment, the OLP procedure and the committees regarded to it are holds a remarkable place for me.

In the 2025 edition of EUROsimA, I'll be serving you as the Academic Assistant of European Parliament, which is the most unique committee one can ever experience. Cooperation and coordination with the Council of the European Union, working on proposals and amending them continuously and while experiencing the heated debate atmosphere in the Parliament will be an unforgettable memory for you.

With all being said, I want to thank Derin Engür and Burak Eren Ceyhan for giving me this chance to be a part of the EUROsimA, helping and supporting me all the time. I also want to thank to Alperen Arifoğlu for his support in this process.

I wish you all a great conference filled with fruitful debates and of course, fun!

Don't hesitate to get in contact with me through ruzgar.bakir@outlook.de.

Sincerely,

Rüzgar Bakır

Academic Assistant of the European Parliament

Dear Delegates,

Welcome to the Council of the European Union at EUROsimA 2025! These upcoming few days promise to be stimulating for me with all the creative ideas and solutions you will be proposing.

There are two subject matters that you will be confronting this year: Establishing EU Customs Data Hub and Establishing EU Customs Authority; and Proposal for a Directive Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence. These matters shall provoke your thinking about the future of the EU from creating international trade within EU more efficient and secure, to ensuring that legal systems keep pace with fast moving AI technologies.

In preparation, I advise you to try to stay as open-minded and collaborative as possible. The best solutions come from listening to one another and debating well. And remember: this is also a chance for all of us to learn from each other and probably have a little fun in solving some world issues.

In case of a question, you can always reach me via email. I wish you all a wonderful conference and look forward to meeting you soon.

Best of luck,

Dila Demircan - Academic Assistant of Council of the European Union

dila.dmrcan@gmail.com

Honourable Participants,

It is my utmost pleasure to welcome you to this year's edition of EUROsimA as the Academic Assistant both the European Parliament and the Council of the European Union. My name is Alp Arifoğlu, a freshman student at Ankara University, the department of Political Science and Public Administration.

This year EUROsimA's European Parliament and the Council of the European Union will consider debating two crucial topics. As the Academic Assistant of both committees, I can make you sure that these topics will be fun and educative at the same time.

To keep it brief, I would lastly like to mention several individuals who have played significant roles in the process of preparing the committees. First, Burak Eren Ceyhan, the Secretary-General, for his great leadership and efforts throughout the process. Next Derin Engür and Ata Yağız Topaloğlu, who are the Under Secretaries-General for the committees that I serve as the Academic Assistant, thank you for your presence.

If you have any further inquiries, do not hesitate to contact me via: alparifoglu@icloud.com

Sincerely,

Alp Arifoğlu

Academic Assistant to the European Parliament and the Council of the European Union.

INTRODUCTION TO THE COMMITTEES

The Council of the European Union, also referred to as the Council or Council of Ministers, is one of the key institutions of the European Union (EU). Along with the European Parliament (EP), the Council is responsible for the enactment of EU legislation via binding legal measures such as directives and regulations, as well as drafting resolutions and non-binding guidance. These stages can be completed in alliance with the Parliament, in accordance with the ordinary legislative procedure (OLP), or solely (European Parliament 2024a).

With the Treaty of Lisbon, the co-decision procedure was introduced under the label of Ordinary Legislative Procedure (OLP) and was recognized as the main legislative procedure within the EU, requiring the joint approval of the European Parliament and the Council so that both of them would be granted equal legislation powers. The procedure starts with a proposal from the Commission and may entail up to three readings. During the very first reading, Parliament considers the proposal and, with simple majority, amends the proposal, approves it, or rejects it. Afterwards, the Council can either accept the Parliament's position or amend it, triggering a second reading. During the second reading, Parliament must approve or amend the Council's position by absolute majority within a time limit; if disagreements linger after the second reading, the conciliation phase will start and create a joint text from representatives of both institutions. The final agreement must then be ratified by both Parliament and Council to become law (European Parliament 2024a).

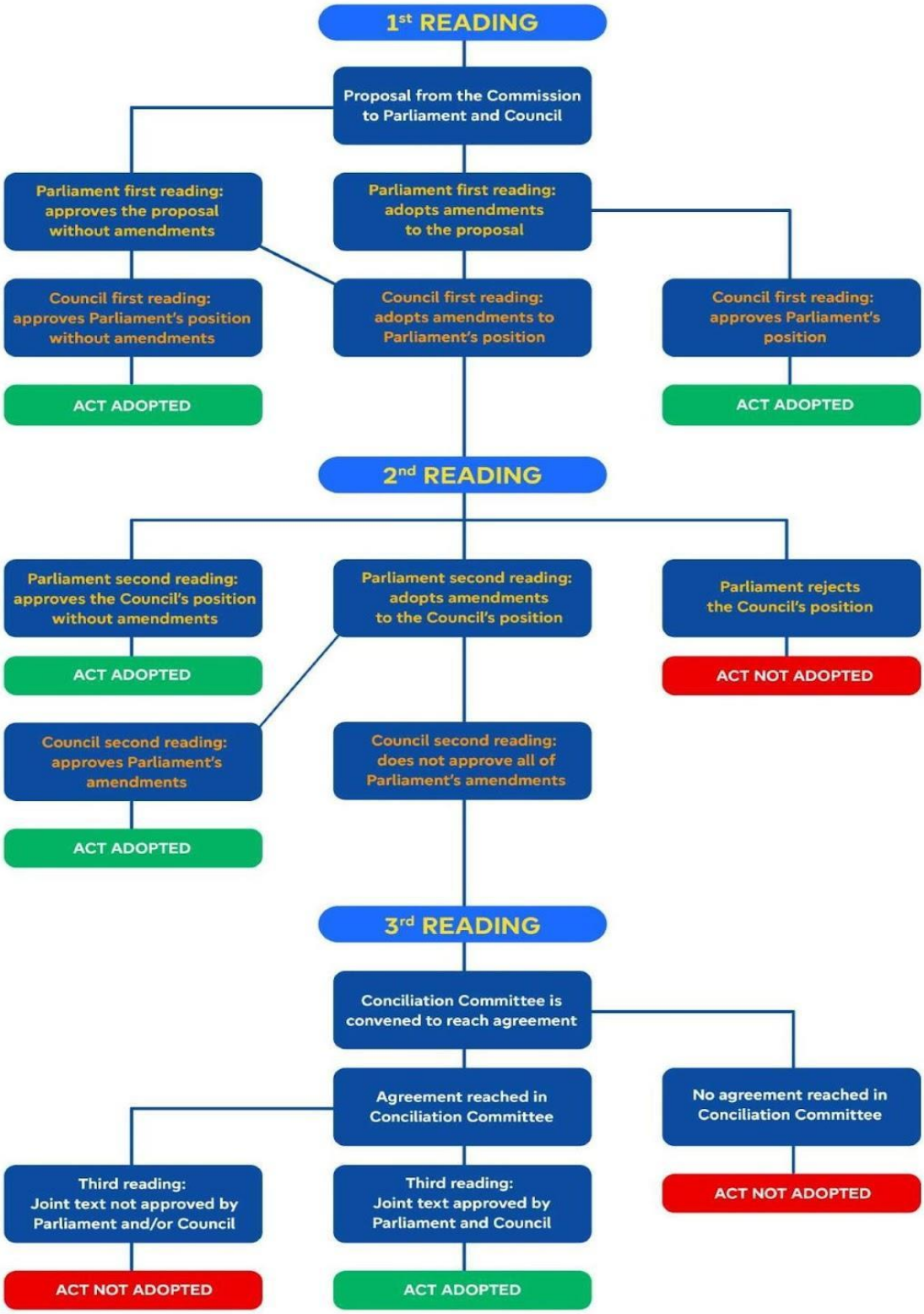


Figure 1. Sketch of the ordinary legislative procedure. (European Parliament 2024a)

The decisions that are adopted by the Council require a simple majority, a qualified majority, or full consensus while the Parliament requires simple majority except a few specific policy areas. A simple majority is attained when the number of for votes are higher than the number of against votes. Since each member state has one vote, when reached 14 in favour votes, simple majority is reached. A qualified majority has two steps: 55% of the Council's member states need to vote in favour, and those 55% must be representing the 65% of the total EU population. Full consensus is only needed for voting upon two topics: social policy and taxation (European Parliament 2024b).

The Treaties of the European Union, particularly Articles 16 TEU and 237–243 TFEU, form the very basis for the Council's and Parliament's powers and operations, distributing legislative, budgetary, and policy responsibilities to the latter. The legislative determination of the Council arises mostly under the ordinary legislative procedure, whereby the Council acts powerfully with the European Parliament and alongside the Commission in maintaining democratic legitimacy and balance of power within the EU. Beyond legislating, the Council is positioned to encompass essential tasks such as adoption of the budget, consideration and conclusion of international agreements, and coordination of economic policy. Decision-making procedures within the Council range from simple majority to qualified majority and unanimity, which means the different interests of member states being seen through either the lens of unity or that of flexibility within the institutional framework of the EU (European Parliament 2024b).

AGENDA ITEM I: ESTABLISHING AN EU CUSTOMS DATA HUB AND EU CUSTOMS AUTHORITY

Table of Contents

I. Background of EU Customs Authority and Data Hub

A. Definition and Scope of Customs Authority and Data Hub

The European Union (EU) customs framework is a cornerstone of the Union's internal market and external trade relations. As global commerce continues to digitize and supply chains become more complex, the need to modernize customs operations has become increasingly urgent. Central to this modernization is the proposal to establish a unified EU customs authority and a centralized customs data hub. Together, these mechanisms aim to improve coherence, data transparency, risk management, and enforcement across all Member States**.**

A **customs authority** is defined as a public body entrusted with the administration, enforcement, and supervision of customs legislation and procedures. At present, each EU Member State has its own national customs administration operating under a common legal framework, primarily the Union Customs Code (UCC), yet with variations in execution and enforcement. This fragmented model often leads to inefficiencies and inconsistencies in the application of rules (European Commission 2023a).

The proposed EU customs authority would serve as a supranational institution with overarching powers to coordinate national customs services, conduct centralized risk assessments, and ensure harmonized implementation of EU customs law. While national authorities would retain operational roles, a central EU authority would provide strategic oversight, data analysis, and enforcement coordination. This centralized body would also serve as the primary interlocutor for international customs cooperation and trade facilitation initiatives (European Commission 2023b).

As for the **customs data hub**, it refers to a centralized digital infrastructure designed to collect, store, and analyze customs-related information in real time. This system would consolidate data

from all Member States and economic operators into a single access point. Unlike today's fragmented digital systems, where each country operates its own database with limited interoperability, a unified data hub would ensure seamless access to trade and customs information across borders (European Commission 2023c).

This hub would be essential to implementing the **Data-Driven Customs Model**, as outlined in the European Commission's reform proposals. It would facilitate early risk detection, fraud prevention, and rapid response by enabling comprehensive data analytics. The data hub would include interfaces with TARIC, short for the Integrated Tariff of the European Union, import/export declarations, economic operator registration systems, and customs decision records (European Commission 2023d).

B. Historical Background of EU customs and Data Collection

The historical evolution of the European Union's customs framework reflects the broader trajectory of European integration. From the establishment of a customs union in the 1950s to the development of sophisticated digital systems in the 21st century, the EU has progressively harmonized its customs policies and mechanisms. Understanding this development is essential for appreciating the rationale behind current reform efforts, including proposals for a centralized customs authority and a unified customs data hub.

a) The Treaty of Rome and the Creation of the Customs Union

The foundation of the EU's customs system lies in the Treaty of Rome (1957), which established the European Economic Community (EEC). A core objective of the Treaty was the creation of a customs union, which entailed the elimination of customs duties and quantitative restrictions between Member States, alongside the adoption of a common external tariff for goods entering the Community from third countries (European Commission 2023a).

The customs union became fully operational in 1968, marking the first major step toward a single internal market. By removing internal border checks and standardizing external trade policies, the EU was able to create a more seamless commercial environment. This integration was not only economic but also legal and institutional, requiring Member States to implement common rules and procedures in a coordinated manner (European Commission 2023a).

b) The Community Customs Code

As the EU expanded and internal market integration deepened, there was a growing need for a unified legal framework to govern customs operations across all Member States. This led to the adoption of the Community Customs Code (CCC) in 1992. The CCC provided a comprehensive and coherent set of rules for the application of customs procedures throughout the European Communities, the initial creation body of EU (European Commission 2023b).

The CCC was significant because it codified and consolidated previously scattered customs regulations, introducing clarity and legal certainty for businesses and national authorities alike. It also laid the groundwork for further automation and modernization by promoting uniformity in documentation, declarations, and valuation methods.

c) TARIC: Digital Integration of Tariff Information

An essential milestone in the EU's digital customs evolution was the development of TARIC, the Integrated Tariff of the European Union. TARIC is a digital tool that compiles all EU measures relating to customs tariffs, commercial policy, and agricultural legislation into a single online database (European Commission 2023c).

Introduced to support the uniform application of customs rules across Member States, TARIC provides real-time information on duty rates, tariff suspensions, quotas, prohibitions, and trade restriction measures. It is continuously updated by the European Commission and serves as a critical reference point for customs officials, traders, and other stakeholders.

TARIC also serves as a precursor to broader digital customs initiatives, demonstrating the value of centralized, accessible, and harmonized information in improving the accuracy and efficiency of customs processes.

d) The Union Customs Code (UCC): A Digital Transformation

The most ambitious reform of the EU customs framework came with the Union Customs Code (UCC), which entered into force on May 1, 2016. Replacing the CCC, the UCC introduced a comprehensive overhaul of customs legislation, with a clear emphasis on digitalization, simplification, and uniform application across the EU (European Commission 2023d).

One of the key objectives of the UCC was to create a fully electronic customs environment. It mandated the replacement of paper-based procedures with digital systems, the harmonization of customs declarations, and the introduction of centralized clearance mechanisms. The UCC also expanded the role of authorized economic operators, (AEOs) and promoted the use of risk management and data analysis to streamline controls and target illegal trade more effectively.

The UCC represents a shift toward data-driven customs governance, in which digital systems are not merely supportive tools but integral to the functioning of the customs union. It has paved the way for the development of initiatives such as the proposed EU Customs Data Hub, which would further centralize and integrate customs-related information across the Union.

C. Recent Trends and Developments

The rapid evolution of global trade and technology in the 21st century has placed increasing pressure on the European Union's (EU) customs framework to modernize and adapt. With the rise of digital business models, complex supply chains, and growing trade volumes, the traditional customs infrastructure—built around physical borders and paper-based procedures—faces limitations. Recent EU initiatives emphasize the need for a more agile, technology-driven customs system, focused on risk management, simplification, and fraud prevention. This transformation is essential to ensure that EU customs can remain effective, competitive, and secure in a globalized and digitized economy thus several trends have emerged in the EU's political landscape.

a) Aligning customs with new business models and technologies

The growth of digital commerce and complex global supply chains has exposed the limitations of the EU's traditional customs infrastructure. In response, the EU is promoting a **data-driven customs model**, which relies on pre-arrived digital information to enhance real-time risk assessment and reduce physical checks (European Commission 2023a).

Emerging technologies like artificial intelligence and blockchain are also being integrated to automate controls and improve targeting of high-risk consignments. These innovations are central

to the proposed **EU Customs Data Hub**, which would consolidate and process customs data across the Union (European Commission 2023b).

b) Reducing Administrative Burden

Businesses currently face fragmented national procedures across the EU, leading to unnecessary costs and delays. To simplify this, the Commission proposes a Single EU Customs Interface and streamlined data submission through a central platform (European Commission 2023c). These changes build on the Union Customs Code (UCC), which mandated the digitalization of customs processes. However, reforms now seek to ensure full implementation and uniform procedures across all Member States (European Commission 2023d).

c) Preventing Fraud

Customs fraud undermines revenue collection and fair competition. Common tactics include undervaluation and misclassification of goods. Fragmented enforcement and data silos make detection of such issues more difficult (European Commission 2023e). A proposed EU Customs Authority would centralize risk management and improve coordination across Member States. It would also oversee platform obligations, requiring marketplaces to share customs data to combat VAT fraud and non-compliant imports (European Commission 2023b).

II. ISSUES RELATED TO CUSTOMS DATA HUB AND AUTHORITY

A. Complexity of importing goods into the EU

The European Union (EU), as one of the world's largest trading blocs, has an extensive customs framework designed to protect its internal market and regulate external trade. However, this framework has become increasingly complex for importers, particularly small and medium-sized enterprises (SMEs). Major challenges include multiple reporting requirements, fragmented digital systems, inconsistent governance, complex tariff calculations, and a lack of centralized data coordination. These issues hamper trade efficiency, increase compliance costs, and weaken enforcement against illicit activities

a) Repetitive Customs Reporting and Burden on Traders

Importing goods into the EU often entails multiple layers of reporting. A single transaction can require importers to submit data to customs authorities up to five times, including pre-arrival declarations, entry summary declarations, customs declarations, excise filings, and post-clearance documentation. Each submission often goes through a different system or authority, leading to redundancy and delays (European Commission 2023a). According to the EU Customs Reform Impact Assessment, this repetition not only strains the administrative capacity of businesses but also undermines the efficiency of customs authorities (European Commission 2023b). The World Bank's Doing Business Report has similarly noted that while the EU performs well overall, the time to comply with import documentation remains disproportionately high compared to some global peers and that hinders the process of quality assurance of the common processes as well as wasting valuable money and time of both traders and member states (World Bank 2020).

The fragmented submission process is particularly burdensome for SMEs, which lack the internal infrastructure or personnel to manage complex compliance. In contrast, large multinationals often maintain entire customs departments or contract specialized intermediaries. This asymmetry

creates an uneven playing field, distorting competition and discouraging participation in international trade.

Efforts like the Single Window initiative and the proposed EU Customs Data Hub aim to consolidate reporting into a single platform. If implemented effectively, such measures could dramatically reduce administrative repetition and allow customs authorities to better leverage shared data for risk management (European Commission 2023c).

b) Fragmented Digitalization and the Rise of E-Commerce

Another critical challenge in EU imports is the fragmented approach to digitalization, which varies widely among Member States. Despite a common legal framework under the Union Customs Code (UCC), Member States have developed national IT systems independently, leading to inconsistent interfaces and compliance requirements (European Court of Auditors 2022). This fragmentation is particularly problematic given the explosion of e-commerce. Online platforms now facilitate millions of small parcels entering the EU every day, often bypassing traditional customs channels. The OECD has warned that this growth increases the risk of undervalued or misdeclared goods, especially when Member States fail to coordinate data or inspection priorities (OECD 2021).

In practice, this means a parcel entering through Belgium may be subject to different checks and data entry protocols than one entering via Poland, even under the same legal regime. Importers must adapt to 27 national systems, each with distinct procedures and digital capacities, increasing the complexity and cost of doing business.

c) Fragmented Governance and Uneven Enforcement

Governance in EU customs remains largely nationalized, despite efforts to harmonize policy. Each Member State operates its own customs authority, interprets regulations within national contexts, and sets its own enforcement priorities. This creates disparities in implementation, allowing illicit actors to exploit the weakest entry points. Member States apply customs rules inconsistently, especially in high-risk sectors like textiles, electronics, and alcohol. This inconsistency distorts competition within the Single Market and creates opportunities for fraud and tax evasion (European Court of Auditors, 2021).

Moreover, customs cooperation among Member States remains insufficient. While the Customs Risk Management Framework promotes coordination, it lacks enforcement mechanisms and is often undermined by national interests (European Commission, 2023e). This is evident in the underreporting of violations, limited data-sharing, and divergent use of risk profiling.

d) Complex Tariff Calculation and Procedural Barriers

The European Union (EU) maintains one of the most structured and comprehensive customs regimes globally. The Common Customs Tariff (CCT), the Combined Nomenclature (CN), and harmonized procedural systems collectively aim to streamline the entry of goods while protecting internal markets. However, the same systems that seek to unify EU trade policies also create substantial complexities for businesses, especially those based outside the Union. Complex tariff calculations, burdensome documentation, and non-uniform application of customs procedures continue to function as significant trade barriers.

i.The Framework of the Common Customs Tariff

The EU uses a common external tariff, the Common Customs Tariff (CCT), which applies uniformly across all member states for goods entering from non-EU countries. This ensures that the customs duty applied to an imported good is the same regardless of the point of entry into the Union. While harmonization promotes market integrity, the calculation process involves multiple layers of assessment that are often difficult to navigate, particularly for small and medium-sized enterprises (European Commission 2024).

ii. Classification of Goods

A central feature of EU tariff calculation is product classification. Goods are classified under the Combined Nomenclature (CN), which aligns with the international Harmonized System (HS) of the World Customs Organization (WCO). The CN uses an eight-digit code to identify products and apply corresponding duties. These classifications are updated annually and are detailed in the EU's TARIC database, which adds legal and statistical subdivisions that influence not only tariffs but also licensing, quotas, and anti-dumping duties (European Commission 2024).

Incorrect classification can lead to severe administrative and financial penalties. For instance, misclassifying a textile as a synthetic fabric rather than natural fiber could trigger higher tariffs or additional safety inspections. Traders are responsible for correct classification and are liable for retroactive assessments, even in cases where they relied on third-party customs agents.

iii. Determining Origin

In addition to classification, tariff application is heavily influenced by rules of origin. Goods that meet specific origin criteria may qualify for preferential tariff rates under EU trade agreements. The EU distinguishes between preferential origin—used to apply benefits under Free Trade

Agreements (FTAs)—and non-preferential origin, which pertains to general trade policy, including anti-dumping and safeguard measures (European Commission 2024). Determining origin often involves complex "value-added" calculations and compliance with product-specific rules, such as proof of "sufficient processing," which varies by sector.

iv. Customs Valuation

The valuation of goods is another pivotal element in determining the total customs duty. The EU adopts the method outlined in the World Trade Organization's Customs Valuation Agreement, using the transaction value as the primary basis. This value must reflect the price actually paid for the goods, adjusted for additional costs such as freight, insurance, and royalties. However, difficulties arise when transactions involve related parties, bundled goods, or when goods are imported under consignment or leasing arrangements (European Commission 2024). Customs authorities frequently challenge declared values, resulting in reassessments, delays, and even legal disputes.

v. Documentation and Compliance Burdens

Even when tariff liabilities are understood, administrative complexity remains a core barrier to trade. Traders must provide a wide array of documentation: customs declarations, commercial invoices, certificates of origin, import licenses, and—in some sectors—sanitary or phytosanitary certificates, meaning document that certifies plants', plant products'... sanitary import requirements. The Union Customs Code (UCC) aims to simplify and digitalize these procedures, but implementation across member states has been inconsistent (European Court of Auditors 2021).

For instance, while one member state may accept digital documentation and process declarations within hours, another may require hard copies and take several days. These differences create uncertainty and inefficiency, especially for traders managing supply chains across multiple EU ports.

vi. Risk Management and Controls

Customs authorities use risk-based controls to select consignments for inspection. These controls are informed by a mix of EU-wide and national risk criteria. However, inconsistent application of these criteria across member states leads to unequal treatment of traders. According to a European Court of Auditors report, certain high-risk goods are subject to more frequent checks in some countries than others, undermining the uniformity of the single market (European Court of Auditors 2021).

Moreover, unpredictable delays resulting from additional inspections—especially on sensitive goods such as electronics or perishables—can derail time-sensitive deliveries and increase operational costs.

vii. Technical Barriers and Standards

Outside traditional customs duties, technical barriers to trade (TBT) also complicate market access. These include conformity assessments, labeling rules, and product-specific regulations. Although the EU works to harmonize standards internally and align them with international norms, exporters from third countries must often undergo redundant testing and certification procedures (European Commission 2024e). This problem is exacerbated in sectors such as pharmaceuticals, chemicals, and electronics, where non-compliance can result in outright bans.

The EU's customs and tariff regime is an advanced, harmonized system designed to protect the integrity of the internal market and ensure fair trade. Nevertheless, the complexity embedded in tariff classification, origin determination, and valuation—combined with the procedural inconsistencies across member states—continues to act as a substantial barrier for external traders. While reforms such as the Union Customs Code and TARIC aim to bring greater transparency and digitalization, their effectiveness depends heavily on uniform implementation across the Union. Continued policy coordination and investment in digital customs platforms will be crucial to removing these hidden barriers and enhancing the EU's position as a global trade partner.

B. Funding and Customs Duties

Through strict rules and tight controls on how funds are used, and by ensuring transparent and accountable spending, the EU provides funding for a range of projects and programmes. EU funding comes in several forms, including:

- **Grants**: Funds awarded to individuals or organisations that apply with project proposals following a call for proposals,

- **Horizon Europe**: Prizes given to winners of Horizon Europe competitions,

- **Loans**: Provided to EU member states and non-EU partner countries,

- **Subsidies**: Managed by national or regional authorities,

- **Financial instruments**: Support EU policies and programmes through loans, guarantees, and equity (European Commission 2024).

These EU funds are managed in three different ways: direct management, shared management, and indirect management. In the direct management method, EU funding is handled directly by the European Commission. In shared management, the European Commission and national authorities jointly oversee the funds. Finally, in indirect management, funding is administered by partner organisations or other external authorities, either within or outside the EU (European Commission 2024; European Union 2024).

a) Direct Management

The European Commission makes payments, assesses the results, launches the calls for proposals, evaluates submitted proposals, signs grant agreements and monitors project implementation. As mentioned before, the European Commission is solely responsible for all steps in the implementation of programmes. Application of this type of funding can be made by answering calls for proposals and calls for proposals under direct management can be found on the "funding and tenders portal (SEDIA)" (European Commission 2024).

b) Shared Management

Responsibility for running a programme is shared jointly between the European Commission and national authorities in European Union countries. Vast majority (70%) of EU programmes are run this way. In EU countries; regional, local, and national authorities choose which projects to be financed and they are responsible for their day-to-day management. EU countries and the

Commission work together to ensure the projects are successfully completed and money is well spent (European Commission 2024). Shared management is often used in the areas of agriculture and “cohesion policy” through the following funds:

- Cohesion Fund
- European Regional Development Fund
- European Social Fund Plus
- Just Transition Fund
- European Agricultural Fund for Rural Development
- European Maritime and Fisheries Fund (European Commission 2024)

c) Indirect Management

In the indirect management method, the funding programmes are partly or fully implemented by third parties, such as national authorities or international organisations. These fundings are evaluated as the forms of subsidies, thus, application for these funds can be made at the national level.

Most of the EU budget for international development and humanitarian aid is implemented under the indirect management method and indirect management programmes account for approximately 10% of the overall European Union budget (European Commission 2024).

Since the abolition of the sugar levies in 2017, customs duties on imports from outside the EU became the only traditional own resources of the European Union budget. After the “Council

Decision 70/243 of 21 April 1970", which is about the replacement of financial contributions from Member States, the Commission started to collect its own resources to finance the EU budget, instead of relying on Member States' financial contributions entirely (European Communities 1970).

Customs duties have always existed as a direct source of revenue to the European Union budget; hence, they are referred to as "Traditional Own Resource (TOR)". On the contrary, national contributions and taxes which are made available to the European Union budget by the Member States are not direct sources for the EU budget (European Commission 2024).

d)Collections, Payments and Control of Customs Duties

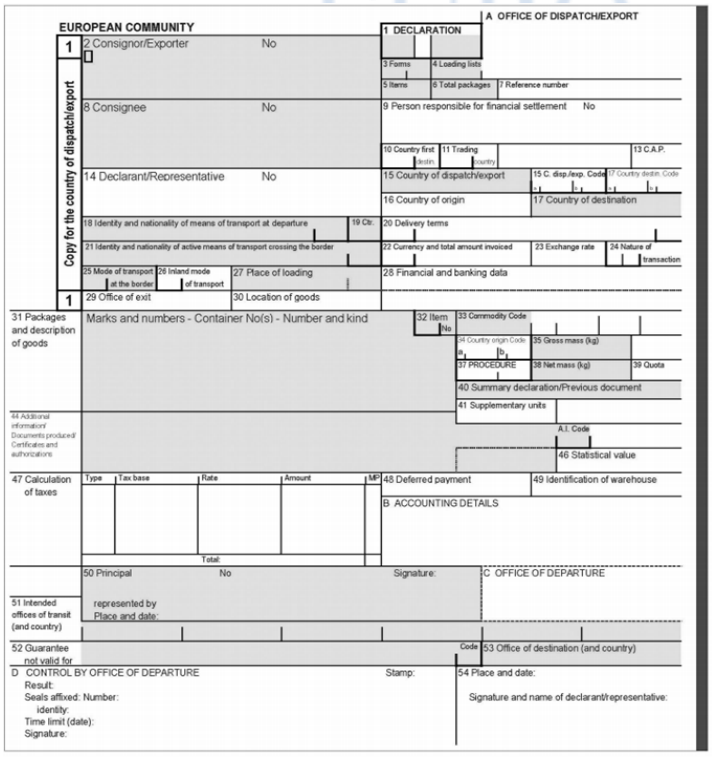
Member States are responsible for the collection of customs duties, and they must have adequate control infrastructure to ensure that their administrations carry out their duties in an appropriate manner. In between 2021-2027, 25% of the collected customs duties will be retained by the Member States, which also be an incentive to ensure a diligent collection of the amounts due to them. Member States inform the Commission of the amount of TOR to be credited to the account through a detailed statement of entitlements. The collection of TOR is carried out in accordance with EU customs legislation and the rules which laid down in the "Own Resources Decision (Council Decision No 2020/2053)" and in the "Council Regulation on implementing measures for own resources". Furthermore, the responsibility of any losses of TOR is on the Member States (European Commission 2025).

e) Single Standard Application and Documents

i. The Single Administrative Document (SAD)

The single administrative document (SAD) is a form which is used for customs declarations in the European Union, Türkiye, Iceland, Norway, Switzerland, the Republic of North Macedonia and Serbia. Being composed of a set of eight copies each with a different function, it reduces the administrative burden and increases the standardization and harmonization of data collected during the trade (European Commission 2024).

The main usage of SAD is regulating the trades with non-EU countries and for the movement of non-EU goods within the EU. It remains applicable in certain extremely limited cases of EU goods inside of the European Union (European Commission 2024).



(Custran 2020)

ii. EU Single Window Environment for Customs

The aim of the European Union Single Window Environment for Customs is streamlining and digitizing customs procedures by allowing traders to submit all necessary information and data throughout a single portal. This system enhances and intensifies cooperation between customs and regulatory authorities and as a consequence, this portal is reducing administrative burdens and improving efficiency (European Commission 2024).

Detailed regulations governing the Single Window Environment, including the establishment of national single window systems and the EU Customs Single Window Certificates Exchange System (EU CSW-CERTEX), are documented in "Regulation 2022/2399" of European Union (European Commission 2024).

f) Stopping Criminal Activities

In the fight against organised crime, terrorism and fraud the front line belongs to the customs authorities who cooperates effectively with administrations and agencies for the relevant policies regarding borders and internal security.

According to European Union data, about 83.000 officials work all day at airports, seaports, border crossings, customs laboratories and inland customs offices in order to prevent illegal and dangerous goods from entering the European Union. Not only officials but sniffer dogs that specialized in detection of illegal drugs, explosives, tobacco products, suspicious food and large amounts of cash (European Commission 2024).

C. UNIFICATION OF CUSTOMS AUTHORITY

a) Sovereignty Issues of National Customs and Security Concerns

The European Union (EU) Customs Union represents a cornerstone of the EU's internal market, facilitating the free movement of goods by eliminating customs duties among member states and establishing a common external tariff. However, the interplay between national customs sovereignty and the overarching goals of a unified customs system has presented ongoing challenges, particularly concerning security and enforcement (World Customs Organization, n.d.).

i. The Legislations and EU Framework

While the EU holds exclusive competence over customs legislation, the implementation and enforcement of the established laws remain the responsibility of individual member states. This dual structure has led to significant discrepancies in the application of customs controls, undermining the uniformity of the Customs Union. The European Court of Auditors has highlighted that such inconsistencies allow non-compliant operators to exploit weaker entry points, thereby compromising the EU's financial interests and security (European Court of Auditors 2021).

Moreover, the existence of 111 disparate IT systems across member states, lacking interconnectivity, exacerbates administrative burdens and hampers efficient customs operations. This fragmentation not only increases operational costs but also impedes the EU's ability to respond cohesively to emerging threats and challenges (Global Counsel 2023).

ii. Security Implications of a Unified Customs System

The push towards a more integrated customs system aims to bolster the EU's capacity to address security concerns effectively. The European Commission's proposed EU Customs Data Hub seeks to centralize customs declarations, enabling real-time data analysis and improved risk management (European Commission 2023). By leveraging artificial intelligence and machine learning, the system aspires to provide a comprehensive overview of supply chains, facilitating the identification and interception of illicit goods (Global Counsel 2023).

However, the transition to such a unified system raises concerns about national sovereignty and the potential dilution of individual member states' control over their borders. The balance between enhancing collective security and preserving national autonomy remains a delicate issue, necessitating careful consideration and collaboration among member states.

iii. Challenges

The harmonization of customs procedures and systems across the EU is a complex endeavor, fraught with technical, political, and operational challenges. The European Commission's Customs Action Plan outlines a series of measures aimed at modernizing customs operations, including the adoption of advanced data analytics and the establishment of a new governance framework. These initiatives underscore the need for a coordinated approach that respects national sovereignty while enhancing the EU's collective security posture (European Commission 2020).

Furthermore, the recent geopolitical landscape, marked by increased global trade tensions and security threats, underscores the urgency of reforming the EU's customs infrastructure. A unified

and efficient customs system is pivotal in safeguarding the EU's internal market and ensuring the safety and well-being of its citizens.

The interplay between national customs sovereignty and the objectives of a unified EU customs system presents a multifaceted challenge. While the integration of customs operations promises enhanced security and efficiency, it must be pursued in a manner that respects the autonomy of member states. For this objective the two important innovations have been proposed which will be investigated in the following subtopics.

b) Trust and Check Traders

In response to the evolving landscape of global trade and the increasing complexity of supply chains, the European Union has initiated comprehensive reforms to modernize its customs framework. A central component of this reform is the introduction of the "Trust and Check" (T&C) trader status, designed to enhance compliance, streamline customs procedures, and foster a more efficient trading environment within the EU (European Commission 2024).

The T&C program aims to build upon the existing Authorized Economic Operator (AEO) framework by introducing a more dynamic and technologically integrated approach to customs compliance. By leveraging real-time data and advanced risk management tools, the program seeks to enhance supply chain security by granting customs authorities access to traders' electronic systems, the program facilitates real-time monitoring of goods movement, thereby improving the detection and prevention of illicit activities. Then, it aspires to streamline customs procedures as Trusted traders benefit from reduced administrative burdens, including the ability

to release goods without active customs intervention, provided that necessary information is available in advance. Lastly it is designated to promote compliance and efficiency. The program encourages traders to maintain high standards of compliance, offering incentives such as periodic payment of customs duties and fewer physical inspections (European Commission 2024).

i. Eligibility Criteria for T&C Status

To qualify for T&C status, traders must meet stringent criteria that demonstrate their reliability and commitment to compliance. According to the European Commission's proposal:

- Compliance Record: Applicants must have no serious or repeated infringements of customs legislation and taxation rules.

- Operational Control: Traders should exhibit a high level of control over their operations and goods flows, supported by robust internal procedures and record-keeping systems.

- Financial Solvency: Applicants must demonstrate good financial standing, ensuring their ability to meet customs obligations (European Commission 2024).

ii. Benefits of the T&C Program

The T&C status offers several advantages to authorized traders such as simplified customs clearance procedures, centralized customs interaction, deferred duty payments and reduced physical inspections that will significantly reduce the complexity and burden of the customs process as a whole. The listed benefits are explained in detail below:

- Simplified Customs Clearance: Authorized traders can release goods into circulation without active customs intervention, expediting the import process.

- Centralized Customs Interaction: T&C traders can manage all EU customs dealings through a single customs authority in their Member State, regardless of where goods enter the EU.

- Deferred Duty Payments: Traders are permitted to determine and defer the payment of customs duties periodically, improving cash flow management.

- Reduced Physical Inspections: With enhanced transparency and compliance, T&C traders are subject to fewer physical and document-based controls (European Commission 2023).

iii. Challenges and Considerations of T&C

While the T&C program offers significant benefits, it also presents challenges such as implementing the required electronic systems for real-time data sharing necessitating substantial investment in IT infrastructure, granting customs authorities access to internal systems raising concerns about data security and the protection of sensitive commercial information or the exclusion of certain operators since the T&C status is primarily available to importers and exporters, potentially excluding other economic operators like carriers and warehouse keepers from its benefits is possible. (PWC 2024)

In order to conclude, the "Trust and Check" trader program represents a significant advancement in the EU's efforts to modernize its customs framework. By fostering a partnership between

customs authorities and compliant traders, the program aims to enhance supply chain security, streamline procedures, and promote efficient trade practices. However, successful implementation will require careful consideration of technological, legal, and operational challenges to ensure that the program achieves its intended objectives without imposing undue burdens on traders. Another crucial innovation of the proposition is the ‘deemed importer role’ (VAT 2024).

c) Deemed Importer Role

Any individual authorized to use the Import One-Stop Shop (IOSS) and engaging in distance sales of goods imported from third territories or countries is referred to as a "deemed importer" (VAT 2024).

With the proposal, e-commerce intermediaries are required to assume the role of the deemed importer rather than the individual using the platform. Given the rising popularity of digital trade and shopping, this is a crucial step to unify customs procedures and ensure accurate tax collection (European Commission 2025a).

i. Benefits of the ‘Deemed Importer’

First of all, designating e-commerce sites as deemed importers grants authorities more direct enforcement power. All products listed on these platforms must adhere to EU safety and product requirements, including regulations on chemical content, safety certifications, and environmental standards. This heightened accountability prevents inferior or hazardous goods from reaching consumers, thereby enhancing public safety and confidence in online transactions (European Commission 2025).

Then, the measure aims to level the playing field for EU-based sellers and their counterparts in third countries. By subjecting online platforms to the same stringent regulations and requiring them to share product data, the risk of unfair competition is reduced. Non-EU sellers might otherwise circumvent stringent safety and quality controls. Ultimately, this fosters fair competition within the Single Market (Ecommerce Europe 2025).

Another benefit is that when e-commerce platforms are regarded as importers, tools like the EU Customs Data Hub can more easily incorporate product information. This digital oversight expedites customs clearance procedures and simplifies the tracking of non-compliant goods. Utilizing real-time data, authorities can conduct enhanced market surveillance, improving overall regulatory enforcement and reducing delays (Ecommerce Europe 2025).

Lastly, as platforms begin to offer more comprehensive financial and non-financial data, customers receive more precise information about the safety and origin of the goods they purchase. This transparency boosts consumer confidence, which is vital for sustaining and expanding e-commerce in the EU (European Parliament 2024). Nevertheless, there still remain several possible disadvantages and concerns of the proposed role.

ii. Possible Complications

Administrative challenges arise when import duties are transferred to e-commerce intermediaries. Collecting, validating, and transmitting comprehensive product information can be costly and complex, especially for smaller platforms. These compliance expenses might ultimately be passed on to buyers and sellers, potentially hindering market entry and innovation (European Parliament 2024).

Furthermore, the shift to a deemed importer model necessitates robust data management systems and advanced IT infrastructure. Establishing these systems across a diverse range of actors, particularly when handling millions of low-value shipments, is highly challenging. Irregularities or delays in digital data flow can cause bottlenecks in customs operations, leading to potential shipping delays and trade disruptions (European Parliament 2024).

Finally, third-country manufacturers and sellers may perceive the strengthening of e-commerce intermediaries' responsibilities as an additional barrier to market entry. Exporting nations might argue that these actions constitute non-tariff trade barriers, potentially intensifying trade tensions. Balancing consumer protection with free market principles will remain a challenging task for EU policymakers (Ecommerce Europe 2025). The import one-stop shop system is a crucial effort and framework on the issue that can be looked upon as an existing framework on the issue.

iii. Import One-Stop Shop (IOSS)

In response to the digital revolution and the rapid expansion of cross-border e-commerce, the European Union implemented the Import One-Stop Shop (IOSS) system. This simplified VAT (value-added tax) declaration and payment platform aims to streamline cross-border sales and enhance customs procedures (European Commission 2025).

The IOSS is a digital portal that enables businesses to efficiently manage VAT procedures for remote sales of imported goods up to €150. By registering in a single jurisdiction and filing a consolidated quarterly declaration, sellers can avoid navigating the complex VAT regulations of multiple EU Member States. This system ensures that tax is paid at the point of sale, eliminating the need for additional tax collection during customs clearance (European Commission 2025).

The rationale behind the IOSS system encompasses four key areas:

1. **Simplification of Tax Compilations:** Previously, companies involved in international e-commerce faced a maze of intricate VAT laws across various jurisdictions. The IOSS system addresses this fragmentation by offering a single point of contact for VAT registration, declaration, and remittance, benefiting especially smaller businesses (European Commission 2025).

2. **Enhancement of Fair Competition:** Prior to IOSS, local sellers and international e-commerce retailers often operated under different VAT procedures, placing local businesses at a competitive disadvantage. By standardizing the VAT payment process, IOSS helps level the playing field, ensuring all market participants contribute equitably to public revenues (European Commission 2025).

3. **Boosting Transparency and Revenue Collection:** Under IOSS, VAT is collected at the point of sale, ensuring steady revenue for EU member states and reducing the risk of VAT evasion. This proactive approach promotes transparency in the online marketplace and supports the financial stability of the customs system (European Commission 2025).

4. **Adapting the Digital Economy to Traditional Frameworks:** As global trade becomes increasingly digital, a modern solution aligning with the dynamics of e-commerce is essential. The IOSS system modernizes traditional taxation methods, incorporating digital technology to meet the demands of the evolving online marketplace (European Commission 2025).

D. CUSTOMS DATA HUB

Each EU Member State operates its own customs IT infrastructure, which contributes to interoperability problems and inconsistent enforcement. The Customs Data Hub, proposed as part of the 2023 EU Customs Reform Package, aims to centralize customs data processing for the entire Union (European Commission, 2023a). It would act as a single access point for traders, who would no longer need to interact with 27 separate national systems.

By consolidating declarations, tracking, and risk assessments, the Hub would facilitate uniform customs procedures, improve accuracy, and reduce administrative costs. It also supports the long-term goal of a joint EU customs authority, capable of overseeing high-risk flows across borders (European Commission, 2023b). The data hub is a complex mechanism that can be investigated under several of its functions.

a) The Customs Control Tower

The European Union (EU) operates one of the most intricate and expansive customs systems globally, necessitated by its vast internal market and extensive external trade relations. To manage the complexities of cross-border trade, ensure security, and facilitate legitimate commerce, the EU has developed the concept of a "Customs Control Tower." This centralized framework aims to provide comprehensive oversight, streamline customs procedures, and enhance coordination among Member States.

The term "Customs Control Tower" refers to a centralized system that offers real-time visibility and control over customs operations across the EU. It integrates various digital platforms, risk

management tools, and collaborative mechanisms to monitor and manage the flow of goods entering and exiting the EU. By consolidating data and processes, the Control Tower enhances decision-making, ensures compliance, and facilitates efficient trade operations (European Commission 2024). The key components of the control tower are:

1. **Import Control System 2** (ICS2): Launched in phases starting from March 2021, ICS2 is an advanced cargo information system that collects data on goods entering the EU before their arrival. It enables customs authorities to perform risk assessments and security checks, ensuring the safety of the internal market (European Commission 2020).
2. **EU Single Window Environment for Customs:** This initiative allows for seamless data exchange between customs and other regulatory authorities. By providing a single entry point for traders to submit information, it reduces administrative burdens and expedites clearance processes (European Commission 2024).

3. **Customs Control Equipment Instrument (CCEI):** With a budget of €1.006 billion for 2021–2027, the CCEI supports Member States in acquiring modern customs control equipment, such as scanners and detection systems, enhancing the EU's ability to conduct effective inspections (European Commission 2024)

   The proposed customs control tower offers several benefits and functions that can be investigated comprehensively.

i. Enhanced Risk Management

The Control Tower enables proactive risk assessment by analyzing data from various sources. This capability allows customs authorities to identify high-risk consignments and allocate resources

efficiently, thereby preventing illegal activities and ensuring compliance with EU regulations (European Commission 2024).

ii. Improved Trade Facilitation

By streamlining customs procedures and reducing redundancies, the Control Tower facilitates smoother trade flows. Traders benefit from faster clearance times and reduced costs, enhancing the competitiveness of EU businesses in the global market.

iii. Strengthened Collaboration

The centralized system fosters better coordination among Member States' customs authorities. Through shared data and joint operations, such as those coordinated by the European Anti-Fraud Office (OLAF), the EU can effectively combat fraud and smuggling (European Commission 2024).

However, there still remain several issues and challenges to the control tower. The integration of various data sources raises concerns about data security and privacy. The EU addresses these issues by implementing strict data protection measures, ensuring that personal data is processed in compliance with existing legislation (European Commission 2024). Then, the successful operation of the Control Tower depends on the seamless integration of diverse IT systems across Member States. Continuous investment in technology and infrastructure is essential to maintain interoperability and system resilience. Last of all, to maximize the benefits of the Control Tower, customs personnel require ongoing training to adapt to new technologies and procedures. Capacity-building initiatives are crucial to ensure that staff can effectively utilize the system's capabilities (European Commission 2024).

The EU Customs Control Tower represents a significant advancement in the modernization of customs operations. By centralizing oversight, enhancing risk management, and facilitating trade, it strengthens the EU's ability to manage its borders effectively. While challenges remain, particularly in areas of data protection and technological integration, the continued development and refinement of the Control Tower will be instrumental in securing the EU's trade infrastructure and promoting economic growth.

b) Data Storage, AI and Machine Learning Algorithms

To support real-time risk analysis, the Customs Data Hub will rely on secure data storage systems integrated with artificial intelligence (AI) and machine learning (ML). These technologies allow for automated risk profiling, anomaly detection, and predictive analytics (World Customs Organization 2021). For example, ML algorithms can flag repeated undervaluation patterns or identify new fraud tactics across multiple jurisdictions.

Such tools are essential for managing the millions of low-value parcels entering the EU daily via e-commerce. Without automation, customs authorities lack the capacity to inspect or verify a meaningful share of these flows. However, ensuring the data quality and integrity would most possibly remain a key challenge to usage of such tools.

i) Advanced Data Storage Infrastructure

Customs administrations today face the challenge of handling massive volumes of structured and unstructured data originating from a wide variety of sources, including customs declarations, electronic manifest data, cargo scans, trade invoices, and third-party intelligence such as law enforcement databases. This data must be securely stored, efficiently processed, and made available for both real-time operational use and longer-term strategic analysis (European Commission 2023).

The proposed EU Customs Data Hub aims to centralize data storage at the Union level, replacing fragmented national silos with a unified, interoperable data ecosystem (European Commission 2023). Such centralization supports standardized data formats and ensures consistent data quality and accessibility. Additionally, advanced storage solutions incorporate cloud-based platforms and distributed ledger technologies (blockchain) to enhance scalability, data integrity, and traceability (European Commission 2023).

Crucially, data storage systems must comply with stringent security standards and privacy regulations, notably the General Data Protection Regulation (GDPR), to protect personal and commercially sensitive information. This requires implementing strong encryption, role-based access controls, and comprehensive audit trails (European Commission 2023).

ii) Artificial Intelligence and Machine Learning Applications

Building on robust data storage, AI and ML algorithms play a critical role in transforming raw customs data into actionable intelligence. These technologies enable customs authorities to

conduct automated risk profiling, anomaly detection, and predictive analytics with far greater speed and accuracy than manual methods (European Commission 2023).

For instance, ML models can be trained on historical customs data to identify patterns associated with undervaluation, misclassification, or concealment of prohibited goods. By continuously learning from new data inputs, these models improve over time, adapting to evolving fraud techniques and emerging trade trends. AI-driven natural language processing (NLP) tools also assist in analyzing textual documents, such as invoices or certificates of origin, to detect inconsistencies or forged information (European Commission 2023).

Moreover, AI facilitates the prioritization of customs inspections by scoring consignments according to their risk levels. This risk-based approach optimizes resource allocation, ensuring that limited customs personnel focus on high-risk shipments while facilitating faster clearance for low-risk goods, thereby reducing delays and costs for compliant traders (European Commission 2023).

iii)Enhancing Operational Efficiency and Compliance

The integration of AI and ML into customs processing enhances operational efficiency by automating repetitive tasks such as data entry validation, duplicate detection, and document verification. This not only reduces human error but also accelerates processing times, enabling customs authorities to handle increasing trade volumes without proportional increases in staffing (European Commission 2023).

Furthermore, AI-enabled analytics contribute to real-time monitoring of trade flows, alerting customs authorities to unusual shipment routes, sudden changes in trading patterns, or emerging

threats. These capabilities strengthen the EU's capacity to respond swiftly to risks while supporting broader supply chain transparency and security initiatives (European Commission 2023)

Yet, despite the clear benefits, deploying AI and ML in customs processing poses significant challenges. Data quality issues—such as incomplete records, inconsistent formats, or inaccurate inputs—can degrade model performance and lead to false positives or negatives, undermining trust in automated systems (European Commission 2023).

Moreover, customs authorities must address ethical and legal concerns related to algorithmic transparency, accountability, and bias. It is essential that AI-driven decisions, particularly those affecting traders' rights (e.g., detention of goods or imposition of penalties), are explainable and contestable. The EU's emphasis on "explainable AI" seeks to ensure that customs officials and traders alike understand the rationale behind automated risk assessments, preserving fairness and legal certainty (European Commission 2023).

c) Transparency and Provisions of Customs Information

Transparency is one of the core principles underpinning modern customs policy and governance. In the context of the European Union, ensuring that traders, customs brokers, and other stakeholders have access to reliable, timely, and user-friendly information is not merely an administrative objective—it is a legal and economic necessity. As customs procedures grow increasingly complex due to digitalization, security concerns, and trade policy shifts, the provision of clear and accessible customs information becomes essential for legal certainty, business predictability, and compliance.

The European Commission has repeatedly emphasized that transparent customs procedures reduce the risk of arbitrary or discriminatory treatment of traders, foster trust between public authorities and businesses, and enhance the overall competitiveness of the EU as a trading bloc (European Commission, 2023). In its 2023 reform package, the Commission proposes a radical modernization of the way customs information is communicated to the public, rooted in three key strategies: expanding legal accessibility, digitizing trader-facing tools, and improving the real-time visibility of customs decisions (European Commission, 2023).

i) Legal Accessibility and Open Regulatory Architecture

One of the major barriers faced by economic operators—particularly small and medium-sized enterprises (SMEs)—is the difficulty in navigating the legal architecture that governs customs. EU customs legislation includes not only the Union Customs Code (UCC), it also includes additional delegated and implementing acts, but also national implementing provisions, binding tariff and origin rulings, procedural guidance, and case law. For businesses operating across borders, staying abreast of regulatory changes in 27 Member States can be prohibitively complex and costly.

To mitigate this, the Commission aims to consolidate legal information through the Customs Data Hub and its associated interfaces. The reform stipulates that all legal provisions, customs decisions, and procedural documents must be made available in user-friendly, searchable formats across all official EU languages (European Commission 2023). This would build upon existing tools like EUR-Lex and the EU Customs Trader Portal, but with greater integration and contextualization. In particular, the new system would link legal rules directly to transaction-specific queries, such as HS code (a standardized system used to classify traded products) classifications or origin determinations.

Furthermore, the Commission plans to expand access to binding rulings, such as Binding Tariff Information (BTI) and Binding Origin Information (BOI) decisions, which are currently fragmented across national systems which would take the binding responsibility from separate member states and gather them under the single authority of EU. A centralized EU database would allow traders to reference previous rulings, assess the legal precedent for their own goods, and reduce the likelihood of disputes at the point of entry (European Commission 2023).

ii) Digital Tools for Trader Support

Digital transparency also encompasses the availability and usability of online trader interfaces. Currently, tools such as Access2Markets, the EU Customs Decision System (CDS), and national customs portals offer various services, including customs duty calculation, tariff quota information, and online applications for authorizations. However, the user experience remains inconsistent, and traders often need to consult multiple systems to complete a single import transaction.

The proposed Customs Data Hub would integrate these services into a single digital platform, where traders could submit declarations, consult legislative databases, track shipment status, and interact with customs authorities in real time (European Commission 2023). Importantly, the Hub will also provide customized information tools based on the trader's profile, risk rating, and transaction history. This represents a move from passive information dissemination to proactive digital assistance.

Moreover, the EU intends to leverage the Data Hub to implement pre-lodgement validation, meaning that errors in customs declarations—such as incorrect classifications or missing documents—can be flagged automatically before submission. This significantly reduces the risk

of administrative penalties, shipment delays, or goods being held at the border, especially for inexperienced traders.

iii) Real-Time Visibility and Decision Transparency

Transparency must also extend to the way customs decisions are made and communicated. Historically, customs procedures have been opaque, with decisions—such as the assignment of risk profiles or the rejection of declarations—rarely explained in detail. This lack of clarity erodes trader confidence and inhibits the development of robust compliance strategies.

To address this, the Customs Data Hub and its Customs Control Tower component will include tools for real-time monitoring of customs flows and decisions. Traders will be able to track the progress of their declarations, receive electronic notifications of inspection outcomes, and obtain digitally certified explanations for customs decisions, such as why a particular shipment was flagged for further control (European Commission 2023). These developments are not only beneficial for operational efficiency but are also essential for due process and the protection of traders' rights under EU law.

In parallel, the Commission is considering mechanisms to publish anonymized customs enforcement data, including risk indicators and the number of inspections per sector or origin country. Such transparency fosters public accountability and allows businesses to benchmark their own performance against industry standards.

Despite its ambitions, the transparency agenda faces several hurdles. First, data protection laws, particularly the General Data Protection Regulation (GDPR), impose strict limits on how personal or commercially sensitive information can be shared, even for the sake of public transparency.

Second, there remains significant variation in digital readiness among Member States, with some customs administrations still reliant on manual or partially digitized systems. Finally, the shift to full digital transparency will require substantial training and cultural change within customs authorities, who must adapt from a gatekeeping role to a more collaborative and service-oriented approach.

III. Existing EU Legislations, Institutions and Frameworks

A. EU Value-Added Tax in the Digital Age Reform (2022)

The EU's VAT system, established decades ago, has struggled to keep pace with the rapid digitalization of the economy. Issues such as VAT fraud, administrative burdens, and inconsistencies across member states have highlighted the need for comprehensive reform. In 2020, EU countries lost an estimated €99 billion in VAT revenues, with a significant portion attributed to fraud and non-compliance (European Commission 2025).

The Value-Added Tax in the Digital Age (ViDA) introduces real-time digital reporting for cross-border trade, based on e-invoicing. It will give Member States the valuable information they need to step up the fight against VAT fraud, especially carousel fraud (European Commission 2025).

The move to e-invoicing will help reduce VAT fraud by up to €11 billion a year and bring down administrative and compliance costs for EU traders by over €4.1 billion per year over the next ten years. It ensures that, in time, existing national systems converge across the EU and paves the way for EU countries that wish to introduce national digital reporting systems for domestic trade

(European Commission 2025). The main pillars of the initiative as a whole are investigated in the following section.

a) Real Time Digital Reporting and E-Invoicing

A cornerstone of the ViDA reform is the implementation of real-time digital reporting and mandatory e-invoicing for cross-border transactions. By 2030, businesses will be required to issue e-invoices within 10 days of a transaction, enabling tax authorities to access transaction data promptly. This shift aims to reduce VAT fraud by up to €11 billion annually and decrease compliance costs for EU traders by over €4.1 billion per year over the next decade (European Commission 2025).

b) Updated VAT Obligations for Digital Platforms

The reform addresses the VAT treatment of the platform economy, particularly in sectors like short-term accommodation and passenger transport. From 1st of July 2028 onwards, digital platforms facilitating such services will be deemed suppliers as mentioned before, responsible for collecting and remitting VAT when their users do not. This measure seeks to level the playing field between traditional businesses and digital platforms, ensuring fair competition and improved tax compliance (European Commission 2025).

c) Single VAT Registration

Building on the existing one stop-shop (OSS) model as explained priorly, the ViDA reform extends its scope to include more types of transactions, such as the movement of goods across EU borders and all B2C (Business to Consumer) supplies made abroad. This expansion allows businesses to

fulfill their VAT obligations through a single online portal, reducing the need for multiple VAT registrations across member states (European Commission 2025).

By implementing these pillars, the new VAT reform and ViDA are expected to significantly reduce and penalize illegal activities and VAT fraud, simplify compliance with reducing the already complex administrative burdens and lastly enhance the revenue collection from this tax with the expected increase in revenue being around 18 billion euros annually contributing to the EU and the people (European Commission 2025).

B. EU CUSTOMS UNION

The EU Customs Union, established in 1968, makes it easier for EU companies to trade, harmonises customs duties on goods from outside the EU and helps to protect Europe's citizens, animals and the environment. In practice, the Customs Union means that the customs authorities of all EU countries work together as if they were one. They apply the same tariffs to goods imported into their territory from the rest of the world, and apply no tariffs internally. In the case of the EU, this means that there are no customs duties to be paid when goods are transported from one EU country to another. The customs duty from goods imported into the EU makes up around 14% of the total EU budget as part of its 'traditional own resources' (European Union 2020).

With the main principles of uniform tariff application across member states, trade facilitation, revenue collection and security/compliance with the customs union was formed with the ideal of a uniform Europe with uniform customs practices. Nevertheless some applications were outdated

overtime with the mentioned challenges appearing such as fragmented authority, tax and customs fraud, adaptation of new businesses and the privacy and security concerns (European Union 2020).

The modernization of the EU Customs Union is poised to enhance the EU's position in global trade by improving efficiency, ensuring compliance, and safeguarding the internal market. By embracing digital transformation and fostering closer cooperation among member states, the Customs Union can better respond to emerging challenges and opportunities. Continued investment in technology, capacity building, and stakeholder engagement will be essential to realizing the full potential of the reformed Customs Union (European Commission 2025).

C.WISE PERSONS GROUP (2022)

Despite the achievements and implementation of customs union and several legislations since its establishment, the EU recognized the need to conduct a comprehensive research process and analysis on the practices and the challenges that it faced. In order to stimulate “thinking outside the box” in the EU debate on the future of the Customs Union, the Commission called on external expertise and established a “Wise Persons Group on Challenges Facing the Customs Union” (WPG). The primary role of the Group was to reflect on the development of innovative ideas and concepts and deliver a report that contributes to a general inter-institutional debate on the future of the Customs Union (European Commission 2022).

The Wise Persons Group was tasked to reflect on the following 4 topics: e-commerce, risk management, effective management of customs/increasing range of non-financial tasks and future

governance structure as well as identifying any other challenges that the Union might face in the future (European Commission 2022).

On the 31st of March 2022, the Wise Persons Group published their landmark report on how to bring the EU Customs to the next level. Their conclusion was that EU Customs needed an urgent structural change; which, building on the reforms of the last decade, take European customs to the next level and prepare them to address modern challenges, such as new trade models and growing trade volumes, technological developments, the green transition, the new geopolitical context and security risks (European Commission 2022).

The Group recognised important changes to customs legislation and IT in recent years and commends the reform plans set out in the Customs Action Plan adopted by the College (the college of commissioners is composed of Commissioners from 27 EU countries who are appointed as the Commission's leadership) in September 2020. However, it advocates for more fundamental and wide-ranging reforms, expressed in 10 recommendations to be implemented by 2030. These include revised and simpler customs legislations, a new framework of responsibility and trust, streamlined procedures and reduced administrative burden, a new approach to data, a more effective governance. Particular emphasis was put on the need for a paradigm shift, to ensure that EU Customs contributes to Europe's security and defence and act as a Union-wide system, rather than the sum of Member States' individual efforts. Customs are essential in managing crises at the European borders and protecting citizens, businesses and revenues. The report especially focused on 5 main aspects which are one external border, promoting the EU way of life, ensuring proper collection of customs duties and taxes at the border, greening of customs and a new approach to responsibility and trust (European Commission 2022).

The WPG signalled the tendency to improve and change the EU Customs Union for the better in the future and take the new concerns into consideration while analyzing the existing problems that the Union faces, becoming a crucial formation for the issue of EU customs.

D. CARBON BORDER ADJUSTMENT MECHANISM (CBAM)

The EU's Carbon Border Adjustment Mechanism (CBAM) is the EU's tool to put a fair price on the carbon emitted during the production of carbon intensive goods that are entering the EU, and to encourage cleaner industrial production in non-EU countries. By confirming that a price has been paid for the embedded carbon emissions generated in the production of certain goods imported into the EU, the CBAM will ensure the carbon price of imports is equivalent to the carbon price of domestic production, and that the EU's climate objectives are not undermined. The CBAM is designed to be compatible with WTO-rules. It will be composed of two phases; the transitional and definitive phase (European Commission 2025).

a) CBAM Transitional Phase (2023-2025)

The CBAM will initially apply to imports of certain goods and selected precursors of which the production is carbon intensive and at most significant risk of carbon leakage: cement, iron/steel, aluminium, fertilisers, electricity and hydrogen. With this enlarged scope, CBAM will eventually –when fully phased in– capture more than 50% of the emissions in ETS (The European Union Emissions Trading System) covered sectors. The objective of the transitional period is to serve as a pilot and learning period for all stakeholders; importers, producers and authorities alike, and to

collect useful information on embedded emissions to refine the methodology for the definitive period.

During this period, importers of goods in the scope of the new rules will only have to report greenhouse gas emissions (GHG) embedded in their imports, both direct and indirect, without the need to buy and surrender certificates.

As of the 1st of January 2025, a new portal section of the CBAM Registry allows installation operators outside the EU to upload and share their installations and emissions data with reporting declarants in a streamlined manner, instead of submitting it to each declarant separately. It is possible to find more guidance material below in the section "CBAM Registry access for non-EU installation operators.

From early 2025, CBAM declarants will be able to apply for the 'authorised CBAM declarant' status via the CBAM Registry. Their application will be processed by the National Competent Authority of the EU Member State where they are established. This status will become mandatory as of the 1st of January 2026 for the import of CBAM goods in the EU customs territory (European Commission 2025).

b) CBAM Definitive Phase (from 2026 onwards)

CBAM will apply in its definitive regime from 2026 onwards, while the current transitional phase lasts between 2023 and 2025. This gradual introduction of the CBAM is aligned with the phase-out of the allocation of free allowances under the EU Emissions Trading System (ETS) to support the decarbonization of the EU industry. The definitive regime will impose a number of applications (European Commission 2025).

First of all, EU importers of goods covered by CBAM will register with national authorities where they can also buy CBAM certificates. The price of the certificates will be calculated depending on the weekly average auction price of EU/ETS allowances expressed in Euro per tonne of CO_2 emitted. Then, EU importers will declare the emissions embedded in their imports and surrender the corresponding number of certificates each year. Finally, if the importers can prove that a carbon price has already been paid during the production of imported goods, the corresponding amount can be deduced (European Commission 2025).

CBAM means a greener and cleaner Europe with the initiative aiming to encourage and implement the usage of greener production processes and also the cutting of "red tape" while dealing with the deductible applications in customs. A green customs union is a must for the future of the EU and CBAM is definitely significant in that ideal.

E. AUTHORIZED ECONOMIC OPERATOR (AEO) PROGRAMME

The AEO concept is based on the Customs-to-Business partnership introduced by the World Customs Organisation (WCO). Traders who voluntarily meet a wide range of criteria work in close cooperation with customs authorities to assure the common objective of supply chain security. The concept is strongly based on the partnership of customs with the specific economic operator (trader etc) . This implies that the relationship between customs and AEO should be always based on the principles of mutual transparency, correctness, fairness and responsibility. Customs expects the AEO to act in line with customs legislation and to inform customs about any difficulties to comply with the legislation. Customs officers and procedures are expected provide support to achieve such goals (European Commission 2016).

The EU established its AEO concept based on the internationally recognised standards, creating a legal basis for it in 2008 through the 'security amendments' to the "Community Customs Code" (CCC) and its implementing provisions. The programme, which aims to enhance international supply chain security and to facilitate legitimate trade, is open to all supply chain actors. It covers economic operators authorised for customs simplification, security and safety or a combination of the two (European Commission 2016).

Mutual recognition and cooperation with other government authorities are the two main aspects of the AEO concept. Mutual Recognition of AEOs is a key element of the WCO (World Customs Organization) SAFE Framework of Standards to strengthen end-to-end security of supply chains and to multiply benefits for traders and Cooperation with other competent authorities and alignment of programmes have been identified and recognised as a key element for the further development of a robust AEO programme. Lastly, the national AEO contact points ensure that the economic operators established in the EU who wish to apply for the AEO status can submit the application to their AEO competent customs authority of an EU Member State with ease and pace (European Commission 2016).

The Authorised Economic Operator Programme is one of the main pillars of EU customs Union, preserving the harmony and cooperation within the union's customs and implementing the EU single market principle. It strengthens the connection between traders and customs authorities, establishing the much-needed environment of trust and security within the borders of the Union.

IV. COUNTRY AND PARTY STANCES

A. COUNTRY STANCES

Austria: Austria has fully supported and participated under the Union Customs code throughout its recent policies and is open to the formation and innovation of the legislation on the topic. Furthermore they support the formation of a more innovative customs data hub with centralized IT systems with their federal computing centre already integrating customs IT (Sustainable Governance Indicators 2025).

Belgium: Belgium is already a great benefactor of the single eternal border and common tariff regime system under the EU with their economy thriving under such practices. They have indicated to be supporting the Commission's proposal to streamline customs via a centralized data hub and a further centralized system overall (PWC 2024).

Bulgaria: They are fully integrated and operate under the rules of UCC. They have not made any public objections to the new proposal and they comply to UCC and support EU-wide digital customs modernization however they have recently been involved in a tendency to prioritize national customs duties over collective ones (European Commission 2024).

Croatia: They are fully integrated under the UCC as well and have not raised any objections to the EU-wide IT centralization or the continuance and enhancement of the customs union. They also support the legislative actions regarding e-commerce specifically (European Commission 2024).

Republic of Cyprus: Another fully integrated country under the UCC who have not objected to the proposal. They have also benefited from the customs union and trade market throughout recent years so it would be expected of them to also support IT improvement and centralization under the circumstance of sufficient financial support (European Commission 2024).

Czechia: Czechia is fully integrated under UCC and they seem to be supportive of the new IT centralization and the formation of a new customs data hub yet they are in need of technical and financial assistance if such a system was to be implemented (European Commission 2024).

Denmark: Denmark is also fully integrated under the UCC and as one of the most innovative and environment friendly countries in the EU they are supportive of the new customs proposal. They have the technical and financial capacity to improve their IT system if need be (SGI 2025).

Estonia: Estonia is another country integrated fully to the UCC. They have the lowest debt to GDP ratio in the EU with financial stability and innovation is high. They have not made any objections to the proposal (SGI 2025).

Finland: Finland is fully integrated under the UCC and carries the technical and financial expertise to further centralize their IT systems under a common data hub. They are also backing modernization under the Customs Authority proposal (European Commission 2024).

France: France is one of the most influential countries regarding the improvement of the customs code and the creation of a new customs data hub with seamless internal customs. They fully support the investigation and creation of new legislation regarding hub goals, fraud detection, e-commerce control and eventually unified trader interface (European Commission 2024).

Germany: Germany is a long standing guardian of the customs union since 1968 and stresses resilience and unity following Brexit. They are one of the 2 main supporters of the new proposal along with France and advocate removing the low-value import reliefs and boosting centralized data handling for stronger enforcement and regulation (European Commission 2024).

Greece: Greece fully participates under the UCC and is implicitly supportive of the new customs code without any recorder opposition however the issues of technological infrastructure and funding of the newly formed data hub remains issues on their part (SGI 2025).

Hungary: Hungary is also fully integrated under the UCC and endorses modernization and a central IT framework throughout the Union under the new proposal and several reforms (European Commission 2024).

Ireland: They are fully engaged with the UCC and have not had any public friction regarding the issue and have a history of full compliance with the UCC regulations. They also support EU-wide e-commerce and border modernization (European Commission 2024).

Italy: They are fully integrated and a part of UCC without any public objection to the issue and a support for broad modernization and regulations on e-commerce. However their recent shift to national centric policies may also hinder and shift their perspective on the issue of a centralized data hub. Infrastructure for such technology also remains an issue for them (SGI 2025).

Latvia: Latvia participates fully to the UCC and has expressed support for the centralized system, aligning themselves with the EU digital policy and data hub procedures (SGI 2025).

Lithuania: Lithuania is engaged fully under UCC and has implicitly backed the proposal with the assurance of sufficient financial backing and improvement of infrastructure (SGI 2025).

Luxembourg: They are fully integrated under the UCC and support a unified customs IT hub as well as the enhancement of the customs Union (European Commission 2024).

Malta: Malta fully participates in the UCC and has expressed implicit support for the new proposal on several occasions. Their technological capacity would need to be enhanced for the formation of the customs data hub (European Commission 2024).

Netherlands: They are and have been a core member of the customs union and for the proposal, they aim to be one of the key contributors supporting the customs IT reform and the development of a newly centralized customs data hub (SGI 2025).

Poland: Poland fully participates in the UCC and complies with its rules and regulations. They support the reforms and align themselves with the development of digital compliance along member states (European Commission 2024).

Portugal: Portugal is fully integrated under the UCC and has not objected to the proposal of a new customs system. They have also expressed their support for modernization throughout the union as of lately (SGI 2025).

Romania: They are fully integrated under UCC and have shown implicit support as part of the ongoing attempts of digitalization (SGI 2025).

Slovakia: Another full participant of the UCC and has been engaged in the issue from the first issuance of the proposal. They support the central system rollout (SGI 2025).

Slovenia: Fully engaged with the UCC and has been supportive of the proposal without any resistance (European Commission 2024).

Spain: They are also very much supportive of the new regulations and developments under the reforms of streamlined e-commerce handling and the modernization of customs IT as well as the formation of a centralized data hub. Spain is also fully integrated with the UCC (SGI 2025).

Sweden: Sweden is a full participant of the UCC and specifically supports the digital customs modernization with one of the most stable economies in the Union. They also encourage the formation of a joint customs data hub (European Commission 2024).

B. PARTY STANCES

A.European Conservatives and Reformists (ECR)

The European Conservatives and Reformists Group (ECR) is a coalition of center-right to right-wing parties that support conservative policies and Euro-skepticism in the European Parliament. It hosts many political parties, some of which are the Conservative Party of UK or others that support national sovereignty and free-market principles. They advocate for “an EU that gets back to basics to deliver common sense solutions and that at the heart of every decision the EU makes, there should be the consideration of the taxpayers across the union” As a result of their political perspective and skepticism they are against the enhancement of the EU customs authority and the formation of a new data hub stressing the breach of national sovereignty and the concerns of bureaucratic/administrative burdens that the proposal may bring (ECR Group 2025).

B. Europe of Sovereign Nations

The Europe of Sovereign Nations is a political formation of far-right ideology with policies against Islamic ideals, globalist and woke agendas. They are rooted in Greco-Roman as well as biblical traditions and the achievements of science and are dedicated to protect and preserve European culture. It is also important to note that while they do advocate for the single market system they are strongly against a unitary European state and EU centralization, advocating for national sovereignty. This also indicates that they are fully opposed to the formation of a centralized data hub and see both the data hub and the customs union as threats to national sovereignty and independence. They support the idea of retaining customs locally and nationally (Europe of Sovereign Nations, 2025).

C. Group of European People's Party (EPP)

European People's Party also called the Christian Democrats are the majority political party in the European Parliament with the most seats. They are seen as a central right political group. They state that the "promotion of the European model is crucial if we want the European values to have an impact into a rapidly changing world." Thus, they are focused on the preservation and enhancement of the union and its collectivistic practices. The Customs Union being one of the cornerstones of the EU as a whole occupies an important place on their political agenda and they have identified the reforms and improvements of it with the proposal as an absolute must. They are strong advocates of the proposal demanding rapid implementation, emphasizing the importance of a harmonized data across Europe and a pan-European customs authority. EPP believes that "a strong and united union acting together is best suited to face this world's many challenges and threats." (European People's Party, 2024).

D. Group of Greens/European Free Alliance (Greens/EFA)

The European Free Alliance, also known as the Group of the Greens, is a political organization that follows the left-wing ideology in the European Parliament. Great emphasis is made on promoting a future that is more environmentally sustainable as well as LGBTQ+ rights and women's rights by the party. They state that "The potential of the digital transformation is being misused in order to concentrate wealth and power in the hands of the few and is adding to the polarization of the society, strengthening authoritarian forces." The Greens/EFA has shown conditional support to the proposal by acknowledging and promoting the environmental and social reforms that it will bring about by promoıting a culture of cooperation and unity as well as simplifying customs procedures however they also stress the issues and challenges of privacy, transparency and environmental enforcement. These issues lead to a need to further discuss and amend the proposal by identifying the problems it may cause and finding the most efficient solutions in order to ensure that it will indeed be a reform (Greens/EFA 2024).

E. Group of Progressive Alliance of Socialists and Democrats in the European Parliament (S&D)

The Group of the Progressive Alliance of Socialists and Democrats in the European Parliament is a political party in the European Parliament that adheres to central left-wing ideology. The S&D has taken a firm stance on multiple issues from Russia's incursion in Ukraine to housing for everyone and safeguarding social and labour rights of all Europeans. Their motto is "Join us in creating a future that is both fair and sustainable." S&D also offered conditional support to the proposal of the establishment of a new customs data hub and enhancement of customs authority. While they do believe in the need of a centralized and sustainable data hub they also recognize

specific challenges that may occur and demand strong data protection, transparency and SME safeguards. Nevertheless, S&D remains pro-data hub and customs unity as they believe that cooperation and unity through Europe is the way to go (Socialists and Democrats 2025).

E. Patriots for Europe (PfE)

Formerly known as Identity and Democracy, the Patriots of Europe is a right wing political formation that supports the independence and strength of nations alongside cooperation. The group also supports the notion of self-defense as a must for every country even though they are receptive to diplomacy and peace. The PfE believes in supporting European identity, traditions and customs. The group is determined to protect its borders and sovereignty, stop illegal immigration and preserve its cultural identity. As the third largest group in the EP they are the biggest representatives for Euroscepticists and are against EU centralized formations so they oppose the proposal for the enhancement of EU customs authority and especially the creation of a centralized customs data hub. They reject EU-wide systems and support national control (Patriots for Europe 2025).

F. Renew Europe Group

The Renew Europe Group is a politically diverse organisation that holds both left and right wing MEPs and positions. Their opinions shift significantly depending on the issue without restraints on specific political ideologies. They express their stance as “The European Union has the chance to renew itself and be able to deliver on the big issues, deliver on the expectations of our citizens and deliver tangible added-value enabling them to understand how it positively affects their lives. Reuniting Europe through a genuine and deep process of integration of all European countries ,

must remain a key element of our Europe of the future." The Renew group is pro-reform on the customs proposal, aligning with EPP on the matters of modernization and digital advancement. They strongly advocate for the creation of the data hub as they believe it will enhance integration and cooperation in Europe. Renew strongly supports the idea of streamlined customs via unified data systems like the data hub (Renew Europe 2025).

G. The Left

The Left Group in the European Parliament is one of the several left ideologic parties in the European Parliament. They express their vision as "those who want another Europe to have a voice in the European Parliament. The Left stand up for workers, the environment, feminism, peace & human rights. We are committed to bursting the Brussels bubble and bringing the voice of the streets to the European Parliament." The Left are conditional or as one might say cautious supporters of the customs proposals as they are in favor of innovation and sustainable practices in customs yet they expect national oversight, democratic controls and anti-centralization. Their ideals and objective may cause them to be in support or against depending on the course that the proposal takes (The Left 2025).

V. POINTS TO BE ADDRESSED BY THE REGULATION

1. What legal authority will the EU Customs Authority hold over national customs administrations, and how will this authority be exercised without infringing on Member States' sovereignty?

2. What will be the precise institutional structure, composition, and decision-making process of the EU Customs Authority?

3. How will the EU Customs Authority coordinate with Member States to ensure uniform implementation of customs laws and procedures across the Union?

4. What are the core legal and technical standards for the establishment and operation of the EU Customs Data Hub, including its interoperability with national systems?

5. How will the regulation ensure the full compliance of the Customs Data Hub with the General Data Protection Regulation (GDPR) and other EU cybersecurity frameworks?

6. What specific categories of customs data will be collected, stored, and processed by the Data Hub, and what will be the retention and access policies?

7. How will economic operators, including SMEs and e-commerce platforms, interface with the Data Hub for customs declarations and compliance verification?

8. What are the eligibility criteria, obligations, and benefits associated with obtaining "Trust and Check" (T&C) trader status under the new system?

9. What mechanisms will be put in place to ensure the transparency, explainability, and contestability of automated customs decisions derived from AI and machine learning tools?

10. How will the centralized authority oversee and harmonize customs valuation, tariff classification, and origin determination across all Member States?

11. What procedures will be established for appealing or contesting decisions made by the EU Customs Authority, including dispute resolution mechanisms?

12. How will the implementation of the EU Customs Data Hub be phased in across Member States, and what transitional measures will be provided?

13. What financial model will support the establishment, maintenance, and upgrading of the Customs Authority and Data Hub, including Member State contributions or EU budget allocations?

14. How will the centralized system contribute to fraud detection, VAT enforcement, and enhanced supply chain security without compromising efficiency?

15. How will the EU Customs Authority engage with third countries and international organizations to ensure compatibility with global customs standards and agreements?

VI. BIBLIOGRAPHY

European Parliament. 2024a. "The Council of the European Union." Accessed June 8, 2025.https://www.europarl.europa.eu/factsheets/en/sheet/24/the-council-of-the-european-union

European Parliament. 2024b. "The Ordinary Legislative Procedure - step by step." Accessed June 8, 2025. https://www.europarl.europa.eu/olp/en/ordinary-legislative-procedure/overview

European Commission. *Union Customs Code (UCC)*. Updated 2023a. https://taxation-customs.ec.europa.eu/customs-4/customs-code/union-customs-code-ucc_en.

European Commission. *Reform of the EU Customs Union*. Updated 2023b. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-reform_en.

European Commission. *EU Customs Data Hub: Background and Objectives*. Updated 2023c. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-data-hub_en.

European Commission. *TARIC – The Integrated Tariff of the European Union*. Updated 2023d. https://taxation-customs.ec.europa.eu/customs-4/customs-tariff/taric_en.

European Commission. *The Customs Union: Historical Overview*. Updated 2023e. https://taxation-customs.ec.europa.eu/customs-4/what-customs-union_en.

European Commission. *Community Customs Code*. Updated 2023f. https://taxation-customs.ec.europa.eu/customs-4/customs-code/community-customs-code-ccc_en.

European Commission. *TARIC – The Integrated Tariff of the European Union*. Updated 2023g. https://taxation-customs.ec.europa.eu/customs-4/customs-tariff/taric_en.

European Commission. *Union Customs Code (UCC)*. Updated 2023h. https://taxation-customs.ec.europa.eu/customs-4/customs-code/union-customs-code-ucc_en.

European Commission. *EU Customs Reform: Why Do We Need a New Approach?*. Updated 2023i. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-reform_en.

European Commission. *Towards a New Customs Union: Reform Package 2023*. Updated 2023j. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-reform_en.

European Commission. *EU Customs Data Hub*. Updated 2023k. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-data-hub_en.

European Commission. *The Union Customs Code (UCC)*. Updated 2023l. https://taxation-customs.ec.europa.eu/customs-4/customs-code/union-customs-code-ucc_en.

European Commission. *Fighting Customs Fraud*. Updated 2023m. https://taxation-customs.ec.europa.eu/customs-4/combating-fraud-and-illicit-trade_en.
European Commission. *Customs Reform: Impact Assessment*. Updated 2023n. https://taxation-customs.ec.europa.eu/system/files/2023-05/customs-reform-impact-assessment.pdf

European Commission. *Towards a New Customs Union: 2023 Reform Package*. Updated 2023o. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-reform_en

European Commission. *Single Window Environment for Customs*. Updated 2023p. https://taxation-customs.ec.europa.eu/single-window_en

European Commission. *EU Customs Data Hub*. Updated 2023r. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-data-hub_en

European Commission. *Customs Risk Management Framework*. Updated 2024a. https://taxation-customs.ec.europa.eu/customs-4/security/customs-risk-management_en

European Commission. *Customs Union: Governance Challenges*. Updated 2024b. https://taxation-customs.ec.europa.eu/customs-4/what-customs-union_en

European Court of Auditors. *Special Report on Customs Enforcement*. 2021. https://www.eca.europa.eu

World Bank. *Doing Business Report: Trading Across Borders*. 2020. https://www.doingbusiness.org

OECD. *Trade and E-Commerce Challenges in Customs*. 2021. https://www.oecd.org

European Parliament. *Customs Classification and Tariff Complexity*. 2020 c. https://www.europarl.europa.eu

Europol. *Illicit Trade and Customs Fraud in the EU*. 2022. https://www.europol.europa.eu

World Customs Organization. *Digital Customs Guidelines*. 2021. https://www.wcoomd.org
European Commission. *EU Customs Reform Package – Customs Data Hub Proposal*. 2023s. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-data-hub_en

European Commission. *Towards a New EU Customs Authority*. 2024c. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-reform_en

European Commission. *Overview of the Customs Control Tower*. 2024d. https://taxation-customs.ec.europa.eu/customs-4/customs-control-tower_en

European Commission. *Cybersecurity and Data Integrity in Customs*. 2024e. https://taxation-customs.ec.europa.eu/customs-4/customs-it-systems_en

European Commission. *Transparency and Legal Access in Customs Procedures*. 2024f. https://taxation-customs.ec.europa.eu/customs-4/traders-access-information_en

World Customs Organization. *Technology and Innovation in Customs*. 2021. https://www.wcoomd.org
European Commission. *EU Customs Data Hub Proposal*. 2024g. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-data-hub_en

European Commission. *Centralized Data Storage and Digital Infrastructure in Customs*. 2024h. https://taxation-customs.ec.europa.eu/customs-it-systems_en

European Commission. *Innovative Technologies in EU Customs: Blockchain and Cloud Solutions*. 2024i. https://ec.europa.eu/digital-strategy/

European Commission. *Data Protection and Security in Customs Processing*. 2024j. https://ec.europa.eu/info/law/law-topic/data-protection_en

European Commission. *Artificial Intelligence for Risk Management in Customs*. 2023t. https://taxation-customs.ec.europa.eu/customs-4/risk-management_en

European Commission. *Natural Language Processing and Document Analysis in Customs*. 2024k. https://taxation-customs.ec.europa.eu/customs-it-systems_en

European Commission. *Risk-Based Customs Controls Using AI*. 2023g. https://taxation-customs.ec.europa.eu/customs-4/risk-management_en

European Commission. *Automation and Efficiency in Customs Processing*. 2023u. https://taxation-customs.ec.europa.eu/customs-4/customs-reform_en

European Commission. *Real-Time Monitoring of Trade Flows*. 2023v. https://taxation-customs.ec.europa.eu/customs-4/customs-control-tower_en

European Commission. *Data Quality and AI Performance in Customs*. 2023w. https://taxation-customs.ec.europa.eu/customs-it-systems_en

European Commission. *Explainable AI and Legal Certainty*. 2023y. https://digital-strategy.ec.europa.eu/en/policies/explainable-ai

European Commission. *Interoperability and Digital Transformation in Customs*. 2023z. https://taxation-customs.ec.europa.eu/customs-it-systems_en

European Commission. 2024l. *Calculation of Customs Duties*. Accessed June 6, 2025. https://taxation-customs.ec.europa.eu/customs-4/calculation-customs-duties_en.

European Commission. 2024m. *EU Customs Tariff (TARIC)*. Accessed June 6, 2025. https://taxation-customs.ec.europa.eu/customs-4/calculation-customs-duties/customs-tariff/eu-customs-tariff-taric_en.

European Commission. 2024n. *Rules of Origin.* Accessed June 6, 2025. https://taxation-customs.ec.europa.eu/customs-4/international-affairs/eu-legislation-implementing-international-customs-provisions_en.

European Commission. 2024o. *Customs Valuation*. Accessed June 6, 2025. https://taxation-customs.ec.europa.eu/customs-4/customs-procedures/customs-value_en.

European Commission. 2024e. *Technical Barriers to Trade*. Accessed June 6, 2025. https://policy.trade.ec.europa.eu/help-exporters-and-importers/accessing-markets/technical-barriers-trade_en.

European Court of Auditors. 2021. *Customs Controls: Poor Harmonisation Hampers EU Financial Interests*. Accessed June 6, 2025. https://op.europa.eu/webpub/eca/special-reports/customs-controls-4-2021/en/.

European Commission. 2024. p"Single Administrative Document (SAD)." *Taxation and Customs Union*. Accessed June 6, 2025. https://taxation-customs.ec.europa.eu/single-administrative-document-sad_en.

Custran. 2020. "What Is a SAD (Single Administrative Document)?" *Custran Blog*, November 13, 2020. Accessed June 6, 2025. https://custran.com/blog/2020/11/13/what-is-a-sad-single-administrative-document/.

European Commission. 2020. "Are You Ready for ICS2?" *Taxation and Customs Union*. Accessed June 6, 2025. https://ec.europa.eu/newsroom/taxud/items/676572/en.

European Commission. 2024r. "The EU Single Window Environment for Customs." *Taxation and Customs Union*. Accessed June 6, 2025. https://taxation-customs.ec.europa.eu/eu-single-window-environment-customs_en.

European Commission. 2025a. "Customs Control Equipment Instrument." *Taxation and Customs Union*. Accessed June 6, 2025. https://taxation-customs.ec.europa.eu/about-us/eu-funding-customs-and-tax/customs-control-equipment-instrument_en.

European Commission. 2025b. "Joint Customs Operations." *European Anti-Fraud Office (OLAF)*. Accessed June 6, 2025. https://anti-fraud.ec.europa.eu/policy/policies-prevent-and-deter-fraud/joint-customs-operations_en.

1stopVAT. 2024. "EU Customs Union 2028 Reforms: New Deemed Importer Role." Accessed June 6, 2025. https://1stopvat.com/eu-customs-union-2028-reforms-new-deemed-importer-role/

Ecommerce Europe. 2025. "Ecommerce Europe's Position on the EU Customs Union and Third Country Imports." Accessed June 6, 2025. https://ecommerce-europe.eu/wp-content/uploads/2025/02/ECOM-Position-on-EU-Customs-and-Imports-04022025.pdf

European Commission. 2025c. "Tackling the Challenges of E-Commerce Imports." Accessed June 6, 2025. https://commission.europa.eu/news/tackling-challenges-e-commerce-imports-2025-02-05_en

European Commission. 2025d. "Import One Stop Shop (IOSS)." Accessed June 6, 2025. https://vat-one-stop-shop.ec.europa.eu/index_en

European Commission. 2025e. "IOSS Advanced Course Takeaways." Accessed June 6, 2025. https://customs-taxation.learning.europa.eu/pluginfile.php/17298/mod_resource/content/0/IOSS%20Advanced_Course%20Takeaways.pdf

European Parliament. 2024.d "Parliamentary Questions: P-10-2024-002943." Accessed June 6, 2025. https://www.europarl.europa.eu/doceo/document/P-10-2024-002943_EN.html
European Commission. 2020. "The Customs Action Plan - Supporting EU Customs to Protect Revenues, Prosperity and Security." Accessed June 6, 2025. https://taxation-customs.ec.europa.eu/customs-action-plan-supporting-eu-customs-protect-revenues-prosperity-and-security_en.

European Commission. 2025f. "EU Customs Reform." Accessed June 6, 2025. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-reform_en.

European Court of Auditors. 2021. "Customs Controls: Insufficient Harmonisation Hampers EU Financial Interests." Accessed June 6, 2025. https://op.europa.eu/webpub/eca/special-reports/customs-controls-4-

2021/en/.

Global Counsel. 2023. "The Future of the EU Customs Union." Accessed June 6, 2025. https://www.global-counsel.com/insights/report/future-eu-customs-union.

European Commission.n.d. "EU Customs Reform." Accessed June 6, 2025. https://taxation-customs.ec.europa.eu/customs-4/eu-customs-reform_en.

EY. "European Commission Proposes Reforms of EU Customs Legislation."n.d. Accessed June 6, 2025. https://www.ey.com/en_gr/technical/tax/tax-alerts/european-commission-proposes-reforms-of-eu-customs-legislation.

Lux, Michael. "Replacement of the AEO by the 'Trust and Check Trader': What Would Be the Practical Changes for AEOs and Non-AEOs under the EU Commission's UCC Reform Proposal?" *Customs Compliance & Risk Management Journal*, Issue 27, June/July 2024. https://www.customsclearance.net/en/articles/replacement-of-the-aeo-by-the-trust-and-check-trader-what-would-be-the-practical-changes-for-aeos-and-non-aeos-under-the-eu-commissions-ucc-reform-proposal.

PwC. "EU Customs Reform." Accessed June 6, 2025. https://www.pwc.com/gx/en/services/tax/international-tax-services/eu-customs-reform.html.

Gateway. "What Are the Benefits of the Trust and Check Traders Scheme?" Accessed June 6, 2025. https://www.gateway.nl/en/blog/what-are-the-benefits-of-the-trust-and-check-traders-scheme/.

European Commission. "VAT in the Digital Age (ViDA)." Accessed June 6, 2025. https://taxation-customs.ec.europa.eu/taxation/vat/vat-digital-age-vida_en.

EY Luxembourg. "ViDA and the Future of VAT: A Digital Revolution in European Tax Compliance." Accessed June 6, 2025. https://www.ey.com/en_lu/insights/tax/vida-and-the-future-of-vat-a-digital-revolution-in-european-tax-compliance.

KPMG Belgium. "EU Reaches Agreement on VAT in the Digital Age Proposal." Accessed June 6, 2025. https://kpmg.com/be/en/home/insights/2024/12/itx-political-agreement-reached-on-the-eu-vat-in-the-digital-age-proposal.html.

Marosa VAT. "European Union VAT in the Digital Age." Accessed June 6, 2025. https://marosavat.com/vat-in-the-digital-age/.

European Commission.n.d. "Commission Welcomes General Approach on VAT in the Digital Age." Accessed June 6, 2025. https://luxembourg.representation.ec.europa.eu/actualites-et-evenements/actualites/commission-welcomes-general-approach-vat-digital-age-2024-11-05_en.

European Union, "Customs," *European Union*, accessed June 6, 2025, https://european-union.europa.eu/priorities-and-actions/actions-topic/customs_en.

European Commission,n.d. "Wise Persons Group on Challenges Facing the Customs Union (WPG)," Taxation and Customs Union, accessed June 6, 2025, https://taxation-customs.ec.europa.eu/customs-4/wise-persons-group-challenges-facing-customs-union-wpg_en.

European Commission,n.d. "Carbon Border Adjustment Mechanism," Directorate-General for Taxation and Customs Union, accessed June 6, 2025, https://taxation-customs.ec.europa.eu/carbon-border-adjustment-mechanism_en.

European Commission. *Authorised Economic Operators (AEO) Guidelines*. Rev. 6. Brussels: Directorate-General for Taxation and Customs Union, 11 March 2016. https://taxation-customs.ec.europa.eu/document/download/1268be1d-1203-4375-a729-0186974ba49b_en?filename=aeo_guidelines_en.pdf.

The Left in the European Parliament, *The Left*, accessed June 11, 2025, https://left.eu/.

European People's Party, *European People's Party*, accessed June 11, 2025, https://www.epp.eu/.

Greens–European Free Alliance, *Greens–European Free Alliance*, accessed June 11, 2025, https://www.greens-efa.eu/en/.

European Conservatives and Reformists Group. *European Conservatives and Reformists Group*. Accessed June 11, 2025. https://www.ecrgroup.eu/.

Patriots for Europe. *Patriots for Europe*. Accessed June 11, 2025. https://patriots.eu/.

Renew Europe Group. *Renew Europe Group*. Accessed June 11, 2025. https://www.reneweuropegroup.eu/.

Socialists & Democrats. *Socialists & Democrats*. Accessed June 11, 2025. https://www.socialistsanddemocrats.eu/.

Bertelsmann Stiftung, ed. *SGI Network *. Accessed June 11, 2025. https://www.sgi-network.org/.

AGENDA ITEM II: PROPOSED AI LIABILITY DIRECTIVE

TABLE OF CONTENTS

a. **Transparency and Complexity of AI Systems**

b. **Diffusing Responsibility**

iii.Relevant EU Legislation

a. **EU AI Act**

b. **Digital Services Act (DSA)**

c. **Revised Product Liability Directive (PLD)**

VI. Proposed AI Liability Directive (AILD)

A. Presumption of Causality

B. Disclosure of Evidence

VII. CHALLENGES AND FUTURE CONSIDERATIONS

A. Addressing Cross-Border Liability

B. Uncertainties in Causation and Enforcement

C. Regulatory Gaps and Overlaps

Ç. Legal Personhood for AI

D. Emerging Global Trends

E. Balance Between Innovation and Consumer Protection

VIII. PARTY STANCES

IX. COUNTRY STANCES

X. QUESTIONS TO BE ADDRESSED IN THE DIRECTIVE

XI. BIBLIOGRAPHY

I. KEY WORDS

A. Artificial Intelligence

The capability of machines or software to perform tasks that typically require human intelligence, such as reasoning, learning, problem-solving, perception, or language understanding. AI systems operate by analyzing data, recognizing patterns, and making decisions or predictions with varying degrees of autonomy and adaptability (OECD 2024).

B. AI Liability

The legal responsibility for harm or damage caused by AI systems, raising novel questions about how to apply traditional concepts of fault and causation when AI's complex, autonomous behavior makes it difficult to determine who (developer, user, etc.) is liable for an AI-caused injury (Chandler et al. 2025).

C. AI Libel

Defamation arising from false statements generated by an AI system (Addleshaw Goddard 2023). In an AI libel scenario, a model like a generative chatbot produces and publishes an untrue, damaging allegation about someone, harming that person's reputation. Legally, the victim of an AI-generated defamatory statement has the same rights and remedies as if a human or publication made the statement, though it raises complex questions about who should be held liable for the harm.

D.AI Risk Management

The process of systematically identifying, assessing, and mitigating the potential risks associated with AI systems. Effective AI risk management is guided by frameworks and standards to ensure AI technologies are deployed in a safe, trustworthy, and legally compliant manner, addressing issues from safety and bias to security and accountability (Badman 2024).

E.AI Transparency and Accountability

The processes and decisions made by AI systems being clear and understandable; transparent. Organizations and individuals responsible for these actions and the impacts of their AI systems being accountable (Dialzara 2024).

F.AI Winter

A period in the history of artificial intelligence marked by a significant decline in interest, funding, and research progress in AI. During an "AI winter," the overly high expectations of prior AI "hype" cool off into disappointment, leading to reduced investment and a slowdown in AI development until the field regains momentum in a later "AI spring" or revival period (Krdzic n.d.).

G.AI-Generated Misinformation "Hallucinations"

Incorrect or misleading information that AI models generate. These hallucinations can be an issue for AI systems that are designed to make crucial decisions, such as medical diagnoses or financial trading (Google Cloud n.d.b).

H.Algorithm

A process or set of rules a machine, particularly a computer, follows in action, reasoning, computation, or other problem-solving operations (European Commission 2019).

I.Artificial General Intelligence

A hypothetical stage in the development of Machine Learning in which AI systems match or exceed the intellectual capabilities of human beings; such as the capability to comprehend, learn, and perform intellectual tasks. Artificial General Intelligence (AGI) represents the fundamental of AI development: replication of the human mind and behavior to address a wide range of complex problems (IBM 2024d).

J.Autonomy of AI Systems

Extent to which a system can learn or act independently after its autonomy and automation processes are assigned. Human supervision can occur at any stage of the system's lifecycle (OECD 2024).

K.Bias in AI

Systematic and unfair prejudice in an AI system's outputs or decisions, which results in certain groups being treated less favorably than others. Such algorithmic bias often stems from biased training data or flawed design and can lead to discriminatory outcomes that raise ethical and legal concerns (Best 2022).

L.Big Data

Extremely large and complex data sets (including structured and unstructured data) that exceed the processing capabilities of traditional data-management systems. When properly

collected, managed, and analyzed, big data can reveal patterns and insights that inform better decisions and strategies (Badman & Kosinski 2024).

M.Black-box AI

An AI system, often a deep learning model, that produces decisions or outputs without offering an interpretable explanation of how it arrived at its conclusions; essentially a "data in, answer out" model with opaque internal logic (Kelly 2025).

E. Burden of Proof

Legal standard which determines whether a legal claim is valid or not based on the produced evidence. It ensures that legal decisions are made based on reality and not conjecture. The party initiating a lawsuit must support its claims through verification (Investopedia 2025).

N.Civil Liability

The legal responsibility of a person or entity to redress harm or injury caused to another through civil legal mechanisms (as opposed to criminal law). In practice, civil liability usually entails an obligation to compensate the injured party (e.g. through monetary damages) as determined in civil court proceedings (Masterson & Hall 2025).

O.Contentious

Describes an issue or matter that is disputed or open to argument and legal challenge. A contentious matter is one likely to give rise to disagreement or litigation, meaning it can be contested by opposing sides in a court or debate setting (The Law Dictionary n.d.).

P.Computer Vision

A field of artificial intelligence that enables computers to interpret and understand visual inputs such as digital images or videos (IBM 2021a). It allows machines to identify and classify objects in the visual world and make decisions or take actions based on what they "see," effectively simulating aspects of human vision.

Q.Deep Learning

A subset of machine learning that uses multilayered neural networks (called deep neural networks) to simulate complex human-like decision-making processes (Holdsworth 2024).

R.Machine Learning

A computational method that is a specialization of artificial intelligence which enables a computer to learn to conduct tasks by analyzing a large data basis without manual programming (Google Cloud n.d.a).

S.Jurisprudence

The science or philosophy of law. It involves the theoretical and analytical study of legal systems and principles, examining the nature of law, its underlying concepts, and how law should operate in society (Britannica 2025).

T.GPU (in AI Context)

A Graphics Processing Unit – a specialized processor originally designed for fast graphics rendering – now widely used to accelerate AI computations. Its highly parallel architecture allows it to perform many calculations simultaneously, making GPUs essential for training and running complex machine learning models and other data-intensive AI tasks (Google Cloud n.d.c)

U.Expert Systems

AI programs, prominent in the 1970s–1980s, that emulate the decision-making ability of human experts in a specific field (Lutkevich n.d.). An expert system relies on a built-in knowledge base of facts and rules and an inference engine to apply those rules to new facts; by simulating the judgment of a domain expert, it can offer conclusions or advice on specialized problems (Lutkevich n.d.).

V.Fault-based Liability

A liability rule requiring the plaintiff to prove the defendant was at fault, through negligent or intentional wrongdoing, in causing the harm. In fault-based regimes, liability attaches only if the injured party can show the defendant's breach of a duty of care led to the damage (Sachora 2020).

Y.Hard Law

Binding legal rules and obligations that are enforceable through courts or regulatory authorities. This term encompasses formal sources of law like statutes, regulations, and treaties – instruments that carry legal force and must be complied with, as opposed to non-binding "soft law" guidelines (ECHR n.d.).

X.High-Risk AI

AI systems are categorized in accordance with their capability to cause harm, or impact fundamental rights, making them liable to stricter regulatory scrutiny (European Commission n.d.a).

Y.Intermediary Liability

The legal responsibility of internet intermediaries – such as online platforms, hosts, or service providers – for unlawful or harmful content and activities by users of their services. Intermediary liability rules determine to what extent, if at all, these middlemen can be held liable for users' conduct; for example, EU law traditionally provides conditional "safe harbors" to intermediaries so they are not automatically liable for user-posted content unless they fail to act upon known illegality (Media Defence n.d.).

Z.Limited Legal Personhood

A restricted form of legal personality granted to an entity, allowing it to hold certain rights and duties without full human legal status. For example, an AI system might be endowed with the capacity to own property or enter contracts under limited legal personhood, while ultimate responsibility and broader rights remain with human actors or organizations overseeing it (Sud&Sud 2025).

AA.Internet of Things

A network of interconnected physical devices, vehicles, appliances, and other objects embedded with sensors, software, and network connectivity, which enables them to collect and exchange data. These "smart" devices communicate and operate with minimal human intervention, automating tasks and providing data-driven insights across many domains (IBM 2023).

AB.Narrow AI

Also known as "weak AI," it refers to AI systems designed to perform a single task or a limited range of tasks with a high level of competence (Investopedia 2022). Narrow AI lacks

general cognitive abilities; it operates only within its specific domain; for example, an AI that plays chess or filters email spam cannot perform unrelated tasks.

AC.Neural Networks

Machine learning models inspired by the human brain, consisting of interconnected artificial "neurons" that work together to recognize patterns, weigh inputs, and make decisions in a manner similar to that of biological neural processes (IBM 2021c).

AD.Product Liability

A person involved in selling a product can be held responsible if the product is sold in a broken or dangerous condition and ends up hurting someone or damaging their property. (McCarter & English, LLP 2024).

AE.Strict Liability

AA system where someone is held responsible for causing harm, even if they didn't mean to or weren't careless. For example, product liability law in the EU imposes strict liability on producers for defective products that cause personal injury or property damage, without the victim needing to prove the producer was negligent (Chandler et al. 2025).

AF.Soft Law

Non-binding rules or guidelines (such as recommendations, declarations, or codes of practice) that lack the force of formal legislation. In contrast to "hard law," soft law instruments are not legally enforceable but can influence behavior and shape policy by providing normative guidance (BBMI Eric 2021).

AG.Symbolic AI

An approach to AI, especially common in earlier decades, that represents knowledge using explicit human-readable symbols and logical rules, rather than statistical learning from data (Dickson 2019). In symbolic AI, the system's behavior is determined by predefined rules and ontologies encoded by experts, which contrasts with the data-driven learning of modern machine learning.

AH.Tort Law

The branch of law dealing with civil wrongs (torts) – acts or omissions that cause harm or injury to others and for which courts impose liability. Its primary aims are to provide relief to injured parties (typically via damages) and to deter wrongful conduct by holding those at fault legally accountable for the harm caused (Cornell Law School n.d.).

AI.Training Data

The dataset of examples used to teach or "train" a machine learning model, allowing the model to learn patterns and refine its predictive rules or parameters by example from that data (Joby 2021).

II. INTRODUCTION TO ARTIFICIAL INTELLIGENCE

A. Definition and Scope of Artificial Intelligence

Artificial Intelligence refers to the machines or software capable of performing tasks that normally require some type of human intelligence; such as learning, problem-solving, perception, and decision-making. With that being said, AI is more than a collection of algorithms. It is the

culmination of efforts spanning mathematics, engineering, neuroscience and philosophy (Mitchell 2025). Key attributes that define AI systems include autonomy, adaptiveness, the ability to learn from data and a capacity for decision-making. According to the European Commission's AI Act, the pioneering framework for AI for the Union, autonomy means the system can operate with some degree of independence from direct human control, making decisions or actions on its own once activated; in addition to this, adaptiveness refers to the ability of an AI system to modify its behavior after deployment by learning from new data or experiences (Martin 2025). Moreover, AI systems are designated to achieve specific objectives, either explicitly or implicitly stated. The internal objectives are different from the intended purpose, which should be externally defined by its provider and the context of use.

It is important to note that the scope of AI is broad, it encompasses a variety of techniques and system types. The European Union (EU)'s definition intentionally casts a wide net to be future-proof, covering everything from simple rule-based systems to complex machine-learning models. However, it also implies that not every software system is considered "AI." The presence of autonomy and intelligent processing is what brings a system under the AI umbrella. For instance, a hardwired calculator is not an AI system, but a recommendation algorithm that learns user preferences could be.

As AI technology evolves, regulators and scholars continue to refine the boundaries of what constitutes AI, but autonomy, adaptiveness and decision-making capacity remain core criteria in defining AI's scope.

B. Key AI Technologies

Modern AI is implemented through a range of foundational technologies and techniques, each contributing to the capabilities and applications of AI systems. Most of those systems often work in combination to produce the desired outcomes. The EU's regulatory framework classifies AI systems based not on the specific technique but on use-case risk. By the use-case risk, the EU aims to explain it through the level of risk varies depending on the specific manner in which the product is used, as certain use cases may inherently involve greater potential for harm or malfunction. However, understanding these technologies is crucial because it is often the technical capability that creates new risks and challenges for oversight.

i. Machine Learning

Machine learning is a branch of AI focused on algorithms that enable computers to learn from data and improve their performance over time without being explicitly programmed for each task. In ML, the system is "trained" on historical data so that it can detect patterns and make predictions or decisions when given new data (IBM 2021b). For example, a machine learning model can be trained to recognize images of cats versus dogs by learning from thousands of labeled images. After some time, the model "learns" the distinguishing features that separate the two categories.

Subtypes of Machine Learning include: supervised learning which is learning from labeled examples to predict labels on new data; unsupervised learning which is finding hidden patterns or groupings in unlabeled data; reinforcement learning which is learning through trial-and-error rewards in an environment.

Some real-world applications can be e-mail spam filters, recommendation systems, fraud detection systems, and autonomous driving systems in vehicles. However, it is important to note

that, some of them may be quite controversial, for instance, the autonomous driving systems contribute to many debates - since failures in such systems can pose grave safety risks, the AI Act explicitly classifies AI that enables autonomous driving as high-risk, subject to rigorous oversight. Thus, under the EU AI Act, many machine learning applications are deemed as high-risk depending on their use case (Gehrmann et al. 2024).

ii. Neural Networks and Deep Learning

Artificial Neural Networks, also known as ANNs, are computing architectures inspired by the neural structure of the human brain, consisting of interconnected nodes arranged in layers (Mitchell 2025). Each neuron processes inputs and passes an output to neurons in the next layer. Neural networks excel at learning complex, non-linear relationships in data. Deep learning refers to neural networks with multiple (often many) hidden layers – these deep networks can learn very intricate representations and have driven most of the recent breakthroughs in AI.

In practice, deep learning powers facial recognition systems, speech-to-text transcription, medical image analysis. Deep learning's "black-box" nature, meaning that the complexity makes the decision process opaque, poses challenges for transparency and explainability, which is why EU regulations push for algorithmic transparency especially for high-stakes AI.

iii. Natural Language Processing

Also known as NLP, it is a field of AI that enables computers to understand, interpret and generate human language. Modern usages of NLP heavily utilize machine learning to process text or speech. Key NLP capabilities include language translation, sentiment analysis, speech recognition, and text generation. An important example would be that NLP algorithms allow smart assistants like Siri or Alexa to interpret spoken commands and respond appropriately, or enable

Google Translate to convert text from one language to another. Real-world applications of NLP range from chatbots in customer service, which can handle routine inquiries, to document analysis tools that can automatically summarize or extract information from large text datasets (Stryker et al. 2024). The AI Act introduces specific rules for generative AI – requiring that AI-generated content be disclosed as such to prevent deception.

In general, NLP systems deployed for high-impact tasks (e.g. an AI system that evaluates job applicants' interview answers) would be scrutinized under the high-risk category due to the potential for significant effects on individuals' lives.

iv. Robotics and Autonomous Vehicles

Robotics is a branch of AI and engineering that deals with designing and building robots and machines capable of performing physical tasks in the world, often autonomously or semi-autonomously (Britannica 2025). These systems integrate AI algorithms for perception, navigation, and decision-making with hardware components like sensors and actuators. Examples include autonomous vehicles, industrial assembly robots, service robots (e.g., automated vacuum cleaners), and surgical assistants. In the EU, such applications are often classified as high-risk under the AI Act due to their direct interaction with humans and the physical environment, necessitating stringent safety standards and liability frameworks to ensure accountability and public trust (European Commission n.d.a)

C. Evolution of AI

Understanding this historical evolution provides context for why regulatory and liability frameworks are now urgently being developed. The field of AI was formally born in 1956 at the Dartmouth Conference – the term was coined by John McCarthy and his colleagues (Mitchell

2025). Early AI researchers pursued the vision of creating machines that could simulate human reasoning. This era relied on the symbolic AI; which uses explicit rules, logic, and representations of knowledge. Programs in this period tackled tasks like solving algebra word problems, proving logical theorems, or playing simplified games, all through hand-crafted rules and symbols. Later, in the 1970s, expert systems which are direct extensions of the symbolic approach emerged. These systems demonstrated that computers could mimic aspects of human expertise by following predefined rules. However, early AI also revealed fundamental challenges – symbolic systems struggled with ambiguity and the vast complexity of the real world that cannot be fully captured by rigid rules (Mitchell 2025).

By the late 1960s, the progress slowed and led to the first AI winter as the hype gave way to disappointment when the promises of AI did not materialize. However, during the same era, researchers like Geoffrey Hinton and Yann LeCun revitalized interest in neural networks and machine learning, developing algorithms like backpropagation that allowed computers to learn directly from data. Backpropagation is a method used in training neural networks, where the model adjusts its internal settings by calculating and minimizing errors from previous predictions. By the 1990s, this data-driven, statistical approach exemplified by machine learning methods such as decision trees, Bayesian networks, and support vector machines laid the groundwork for modern AI.

The early 2000s marked a transformative period for AI driven by abundant data availability and rapid advancements in computing power, notably GPUs that accelerated neural network training (Mitchell 2025). These developments culminated in the Deep Learning revolution of the early 2010s, exemplified by AlexNet's success in image recognition in 2012, showcasing deep neural networks' superiority over traditional algorithms. Subsequent breakthroughs in speech

recognition, generative adversarial networks (GANs), and landmark achievements like AlphaGo's victory further validated AI's powerful capabilities. Yet, these advances also revealed new challenges such as "black box" opacity, privacy concerns, and biases, prompting increased regulatory efforts to ensure transparency, safety, and accountability.

The current AI wave, defined by generative AI models and transformer architectures like GPT and BERT, has dramatically expanded AI's capabilities in language and content generation (Mitchell 2025). OpenAI's ChatGPT, along with image-generating models like DALL-E and Stable Diffusion, illustrate AI's newfound creativity, raising profound questions about authenticity, trust, and potential misuse.

These rapid technological advancements have compelled regulators, particularly in the EU, to swiftly update frameworks, such as introducing transparency obligations in the AI Act, to manage the emerging risks and complexities related to accountability and liability.

III. COMPARATIVE APPROACHES TO AI LIABILITY FRAMEWORKS

A. United States

Currently, the US lacks a comprehensive federal law or clear federal guidelines explicitly dedicated to regulating AI. However, there are ongoing efforts to introduce specific AI legislation and establish a federal regulatory authority for AI oversight. Until such federal legislation and guidelines are implemented, developers and deployers of AI systems must operate in compliance with applicable state and local laws, which can include privacy laws, data protection regulations, employment discrimination laws, and other technology-related local ordinances.

The change in the office in January made it harder to apply an AI directive for the USA. Before Biden left the office, he signed the Executive Order 14110; titled “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence”. The aim of it is to eliminate any societal harms during the usage of AI. However, with Trump coming back office in January 2025, he signed a new executive order, titled “Removing Barriers to American Leadership in AI” (The White House 2025). It is also known as the “Removing Barriers EO”. The executive order calls for federal departments and agencies to revise the policies, directives, regulations, and other actions that are taken by the Biden administration. Before the new formation of the Congress, the US Congress was considering numerous AI bills that were responsible for covering wide range of issues. However, with the new formation, the Congress was formed under a Republican-held Congress which may not enact the legislation regarding the AI and rather focus on the practices that goes accordingly to their priorities.

As stated before, currently, the US does not have a specific federal law dedicated solely to regulating AI. Existing federal laws that may apply indirectly to AI, such as competition law, consumer protection laws, and broader technology-related legislation, have limited and general applicability. For instance, the Federal Aviation Administration’s "Reauthorization Act" includes provisions requiring reviews specifically focused on the use of AI in aviation. Similarly, the "National Defense Authorization Act for Fiscal Year 2019" undertakes various AI-related activities, such as appointing a coordinator to oversee AI initiatives. Furthermore, the "National AI Initiative Act of 2020" aims to expand AI research and development, establishing the National Artificial Intelligence Initiative Office to oversee and implement the US national AI strategy (National Defense Authorization Act 2019).

i. Legal and Regulatory Framework

The White House Blueprint for an AI Bill of Rights, issued under the Biden administration, asserts a guidance around equitable access and the usage of AI systems. While the new executive order of Trump does not revoke the AI Bill of Rights, with the executive order titled Removing Barriers EO, it is unlikely to pursue the development of principles that were set out during Biden's administration. As Trump see them inconsistent with the enhancing America's global AI dominance, it is unlikely to be supported by the US government for the next four years. However, the AI developers may keep these the principles of the AI Bill of Rights in mind when designing such systems.

Even though the Trump administration has issued an executive order that limits the safe and effective systems and gives the freedom to developers to succeed in their respected topics, several companies that are in the leading positions for AI, such as Adobe, Amazon, Google, IBM, Nvidia, Open AI have committed to the executive order of Biden, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence". Most importantly, these technology companies have stated that they are committed on internal and external security testing of AI systems before their releases; as well as sharing information on managing the AI risks and investing in safeguards.

Another framework is the declaratory that was issued by the Federal Communications Commission, which states that the restriction on the use of "artificial or pre-recorded voice" messages that aligns with Telephone Consumer Protection Act of the 1990s include the AI technologies that generate human voices. This issue demonstrates that the regulatory agencies will be applying this existing law to AI (Federal Communications Commission 2024).

As can be seen from these examples, US' AI governance has emphasized a soft-law guidance and a sector-specific oversight, rather than a blanket regulation. Dozens of AI-related bills have been proposed in Congress, but as of 2025, none have passed.

ii. Civil Liability Approaches

Since there is an absent of new law from Congress or state legislatures, the tort law is in usage for AI liability cases. The issue within the context of the US is that the tort law is primarily a state law, and can vary from state to state, and there is no single tort law which is applied in all states of the US. Therefore, the specific tort law applied to AI will differ depending on which state's law is applied.

Most of the AI-related tort cases involve claims of negligence – that a party did not act with due care – by harmed plaintiffs against AI developers and deployers (Smith et al. 2024) However, negligence claims face challenges. Due to AI's complexity and how it often diffuses "supply chain" of vendors and components; this makes it harder to identify a specific act of negligence and the responsible party.

Thus, it leads to be an ongoing debate whether new liability frameworks might be needed as AI systems become more autonomous, but as can be seen from the examples, the legal system is adapting existing tort principles to AI cases (Marchisio 2021).

iii. Emerging Debates and Reforms

The rapid growth of AI has led to many debates in the US whether existing liability frameworks or laws are adequate. One of the key issues is about how to handle the black box nature of advanced AI in litigation. The main limitation on these regulations are caused by the ones that are inherent characteristics of AI including its complexity, autonomy and, as stated

before, the black box effect. It makes it difficult or unduly burdensome for the injured parties to identify the responsible subjects and prove to have met the requirement of tortious liability (Lusardi 2023). Discussions around the Section 230 broadens the topic. Section 230, also known as the Communications Decency Act, can be viewed as a shield for online platforms from liability for user-generated content. The discussion is that whether it should be applied when AI algorithms curate or generate harmful content. Plaintiffs in cases such as the chatbot suicide suit are attempting to attempting to bypass Section 230 by framing the AI as a product (Brannon et al. 2024).

Debate around the Section 230 criticizes that it promotes immunity to online platforms such as social media websites, forums, and blogs from civil liability for content posted by their users. So, in simple terms, it allows platforms like Facebook, X, etc. to be not sued for harmful and unlawful content created by their users. However, critics state that platforms remain liable for their own original content or content they directly create or substantially modify. As can be seen, this law also allows platforms to moderate or remove inappropriate content without automatically assuming liability for all other user-generated content. Questions such as whether do we still regard platforms as immune in the cases where a harmful content or misinformation is generated by AI systems owned or operated by the platform itself arose (Brannon et al. 2024).

On the other hand, reforms play crucial roles as well. The National Institute of Standards and Technology, also known as the NIST, released an AI risk management framework to guide industry best practices. The project on the AI liability may eventually lead to adjustments to the tort doctrine; however, in the meantime, the US approach still remains iterative, regulators like the Federal Trade Commission are pushing the envelope by enforcing existing laws, and courts will gradually build precedent as more AI-related cases appear (White & Case 2025).

As can be seen from the system of the USA, the overarching theme is the effort to fit AI into the existing legal mold – relying on common-law evolution and sectoral enforcement – rather than creating a new liability regime from whole cloth. However, as debates arose whether this strategy could address AI's unique challenges, it leaves an open question to debate in legal and policy circles.

B. China

i. National AI Legislation and Regulatory Framework

China has been rapidly developing a legal and regulatory framework to govern artificial intelligence in a safe and controlled manner. Although a comprehensive "AI law" is not yet enacted, China has issued a patchwork of national laws, administrative regulations, and guidelines to address AI safety, accountability, and liability mitigation (Chow et al. 2025). These efforts reflect Beijing's emphasis on centralized oversight of AI development to safeguard national security and the public interest, even as it promotes innovation. A notable development is the draft AI Law circulated by legal scholars, which foreshadows a comprehensive national law. The draft AI Law lays down broad principles and specifies various scenarios in which AI developers, providers, or users would be liable for the misuse of AI tools. While this draft is not yet enacted, it signals the direction of China's policy; namely, a unified statute to supervise AI research and development (R&D), deployment, and risk management at the national level.

Meanwhile, China has relied on sectoral laws and new regulations to fill the gap. Key pillars include the Cybersecurity Law (2017), Data Security Law (2021), and Personal Information Protection Law (2021), which establish baseline obligations for data handling, security, and

privacy in all technologies, including AI (Creemers et al. 2022). These regulations, though narrow in scope, form a patchwork framework addressing different AI applications until a comprehensive law is in place. Each regulation delineates responsibilities for various AI stakeholders and imposes compliance duties aimed at ensuring AI does not threaten social order, national security, or individuals' rights.

China's AI governance features strong centralized oversight through mandatory algorithm registration and risk assessment. Providers of influential algorithmic services must file detailed reports, including algorithm purpose and safety evaluations, and publicly display official registration numbers. High-risk algorithms undergo regular state-mandated security assessments, particularly those affecting public opinion or societal stability. Generative AI services must comply with stringent content regulations, including mandatory clear labeling of AI-generated content, reflecting China's pioneering efforts in algorithmic transparency and user protection. This centralized control and comprehensive transparency aim to proactively manage AI-related risks before they cause significant societal harm (Creemers et al. 2022).

ii. Liability and Accountability Under Chinese Law

China's legal system does not recognize AI systems as bearing legal personhood, so liability for AI-caused harm rests with the human or corporate actors behind the AI (Chow et al. 2025). The PRC Civil Code enacted in 2020 provides the general tort framework: any person who through fault infringes another's civil rights causing harm must bear liability (fault-based negligence), and in some scenarios, liability can be strict or presumed by law; as can be seen, these principles apply to AI as well. In other words, if an AI malfunction or decision causes damage, a plaintiff must sue the relevant company or individual rather than the software or algorithm itself. Determining the responsible party can be complex and fact-specific; for example, if an

autonomous vehicle crashes, fault might lie with the manufacturer or the user, depending on circumstances (Chow et al. 2025).

iii. Data Protection and AI Governance

China's Personal Information Protection Law, also known as PIPL, plays a key role in AI accountability by imposing strict obligations on entities that collect, process, or use personal data (Chow et al. 2025). It mandates lawful grounds for data processing such as informed consent, and prohibits uses that violate agreed purposes or infringe on individual rights. Authorities actively enforce the law, signaling that improper data use in AI, such as unauthorized facial recognition, will result in legal and regulatory penalties.

iv. Enforcement and Emerging Case Law

China's centralized regulatory model allows rapid rulemaking and enforcement, with agencies like the Cyberspace Administration of China imposing fines, suspensions, or shutdowns for violations such as failing to register algorithms or monitor AI content (Chow et al. 2025). Courts are also shaping liability norms, ruling that AI-assisted works with human input can gain copyright, while fully autonomous outputs without human creativity cannot. Prosecutors have criminally charged individuals for abusing AI tools, reinforcing that human actors behind AI misuse will be held liable under civil and criminal law. Together, these developments form a robust, evolving AI liability framework driven by proactive state oversight and emerging jurisprudence.

C. International Institutions

i. OECD's AI Principles: Foundations for Trustworthy AI

The Organisation for Economic Cooperation and Development, also known as OECD, established the first intergovernmental standard on AI governance with its OECD AI Principles in May 2019 (OCED.AI n.d.). These principles were crafted to promote the innovative and beneficial use of AI while ensuring it remains trustworthy, respects human rights and democratic values. At their core, the OECD Principles set out five fundamental values to guide AI development and use: inclusive growth; sustainable development and well-being; human-centered values and fairness; transparency and explainability; robustness, security and safety; and accountability. These values-based tenets call for AI systems to be designed and deployed in a manner that upholds human dignity, prevents unfair bias or harm, and allows for appropriate oversight and explanation of algorithmic decisions. Notably, the principle of accountability explicitly states that AI actors should be accountable for the proper functioning of AI systems and for compliance with these principles (OECD n.d.b). Therefore, this emphasis on accountability links directly to liability: it implies that there must be identifiable persons or organizations responsible when AI systems cause harm or otherwise violate legal norms.

Although, the OECD principles are soft-law, meaning non-binding frameworks, they have had a significant influence on global thinking about AI governance and liability. Indeed, the OECD's definition of an "AI system" and its risk-based approach have been borrowed in legislative and regulatory frameworks around the world, including in the EU's AI Act, Council of Europe initiatives, U.S. guidance, and UN discussions.

ii. G7 and G20: Soft Law Leadership and Convergence

Group of Seven (G7) and the Group of Twenty (G20) member states have built upon the OECD's groundwork to forge broader international consensus on AI ethics and liability. In June 2019, just weeks after the OECD Principles were adopted, the G20 formally endorsed a set of AI Principles drawn from the OECD recommendation (Center for AI and Digital Policy n.d.). G20 leaders agreed to a "human-centered approach to AI" and welcomed these non-binding G20 AI Principles as a guide for fostering public trust and accountability in AI. This marked a significant moment: it signaled that not only Western OECD countries, but also large emerging economies recognized common values for AI. The G20's endorsement extended the OECD's influence on a global scale and affirmed that AI should be developed in line with principles like fairness, transparency, privacy, and safety, with mechanisms to hold developers and deployers accountable.

Recently, the G7 nations have taken a proactive role in developing voluntary codes of conduct and guiding principles to address cutting-edge AI challenges. Under Japan's G7 Presidency in 2023, the bloc launched the Hiroshima AI Process, which led to an International Code of Conduct for Organizations Developing Advanced AI Systems alongside a set of G7 Guiding Principles for Advanced AI (Carr et al. 2023). These G7 guidelines, which explicitly build upon the OECD AI Principles, urge AI developers and operators to implement robust risk assessments, transparency measures, and governance policies throughout the AI system lifecycle. Though adherence is voluntary, these measures reflect a shared commitment among leading democracies to prevent harm and ensure someone can be held responsible for AI-driven outcomes.

iii. United Nations and UNESCO: Toward Global Ethical Consensus

The United Nations, through United Nations Educational, Scientific, and Cultural Organization (UNESCO), has established the first global ethical framework for AI with its 2021 Recommendation on the Ethics of Artificial Intelligence, endorsed by 193 Member States (UNESCO 2023). This non-binding instrument promotes principles like transparency, accountability, and human rights, urging governments to implement legal frameworks aligned with these values. It serves as a global baseline that complements OECD standards, with UNESCO requiring regular progress reporting to encourage national compliance.

In parallel, the broader UN system is developing the Global Digital Compact (GDC) to harmonize global digital governance, including AI ethics (United Nations n.d.). The GDC aims to align AI with shared global values and has prompted discussions on creating international oversight bodies like an "AI Agency." Though still in early stages, UN resolutions now urge Member States to adopt national AI governance strategies, laying the groundwork for future international legal cooperation on AI liability and accountability. Although these UN efforts are still evolving soft-law discussions, they represent the inclusive, multilateral approach: engaging all countries in agreeing on ethical guidelines and potential norms for AI. The hope is that, through instruments like the UNESCO Recommendation and the forthcoming Global Digital Compact, the international community can establish common ground. Such common ground may be an agreement that AI should not violate human rights or be used in ways that undermine peace and sustainable development, which in turn lays the groundwork for more concrete cooperation, and possibly future international law, on issues like AI liability and accountability.

iv. Harmonizing AI Liability Standards Through Cooperation

Across these various forums, namely OECD, G7, G20, UNGA, a clear pattern emerges; international cooperation is building a shared framework of principles that can guide how AI is regulated and who is liable when plans may not go as expected. While hard law is still catching up to the fast pace of AI innovation, this soft law consensus is a critical first step toward harmonization. Common themes of transparency, accountability, safety, and human-centered approach now run through all major global AI initiatives, creating a baseline of agreement. This paves the way for more harmonized liability standards in the future. To truly harmonize AI liability, coordination is continuing on multiple levels. The OECD, working with over 100 countries, is actively aligning its guidance with other regimes, for example by mapping its risk-management framework to the G7's Code of Conduct, to promote interoperability and consistency across international AI governance mechanisms. (OECD 2025). This kind of alignment helps ensure that voluntary codes, national regulations, and industry standards are not working at cross purposes but rather complement each other. Over time, these efforts could yield a more formal convergence, such as the development of model laws or even international agreements that codify the currently non-binding principles on AI liability. Already, regional bodies like the EU are proposing legislation reflecting these global principles, such as easing the burden of proof on victims and mandating transparency, and such laws, if adopted, could become de facto standards that influence other countries. The collaborative work of the G20 and United Nations also points to potential future frameworks or treaties: a universally endorsed global AI governance framework under UN auspices could, for example, articulate how responsibility is apportioned among

developers, deployers, and users of AI, much like international environmental law assigns liability for transboundary harm.

IV. REAL-WORLD AI LIABILITY CASE STUDIES

A. Autonomous Vehicles and Accidents

On March 21, 2018, a woman was struck and killed by an autonomous car operated by Uber in Tempe, Arizona. The death of the 49-year-old woman, Elaine Herzberg, is believed to be the first pedestrian death associated with the self-driving technology (BBC 2020).

The problem regarding this situation arises with the decision by the Arizona prosecutors that ruled that Uber was not criminally responsible for the crash; rather, the back-up driver of the vehicle was charged with negligent homicide (BBC 2020). The investigation showed that the backup driver was watching an episode of a television show when the accident occurred. Later, the driver, Rafael Vasquez, pled guilty to endangerment, and was sentenced to three years' probation (Billeaud & Snow 2023). At the same time, Uber reached a settlement with the Herzberg's family within the two weeks of the incident to avoid a protracted litigation (Dandurand 2019).

Debates regarding the position of Uber created heavy criticism for the company's self-driving system. Michael Ramsey, a self-driving car expert with Gartner, has stated that the video that was taken by the car camera before the accident shows that there is a complete failure of the system to recognize an obviously seen person; later, a Silicon valley entrepreneur, Brad Templeton stated that the laser should have seen her presence; thus, there is a clear problem with the Uber's technology (Said 2018).

As can be seen from the incident, it leads to several challenges to AI liability such as causation and foreseeability which can be viewed as the hotly debated topics. The software in the modified Volvo XC90 did not properly identify Herzberg, the victim, as a pedestrian and did not address operators' automation complacency, as experts claim (Shepardson 2020). Thus, as can be seen from this, the vehicle's AI system saw Elaine Herzberg, but failed to recognize her as a pedestrian.

Yet under the existing law, those software design flaws did not translate into criminal liability for the company. The foreseeability of such an AI mistake was not clearly established in law, and the attribution of responsibility fell to the human operator who ultimately had a duty to monitor the vehicle. The legal system treated the incident similarly to a conventional car accident caused by a distracted driver, rather than as a product malfunction.

This reveals a liability gap: when an AI behaves in unpredictable ways, it can be difficult to assign fault to the algorithm's creator unless negligence in design can be proven. At the end, Uber was not prosecuted, and the courts never got to rule on product liability since the civil claim settled quickly out of court, as stated previously.

Similar issues have become the topic of debate with Tesla's Autopilot system, which is an AI-based driver-assistance system. A fatal crash in which the car to suddenly veer off the road in 2019 in California can be given as an example of the issues related to the Tesla's Autopilot system. In 2023, the jury found that the vehicle did not have a defect, effectively concluding that Tesla's software was not legally to blame; thus, the outcome in civil courts shows that when plans go unexpectedly on the road, the responsibility rests with the drivers (Levimne & Jin 2023). Another case occurred when Tesla's Model X swerved off the California highway while the autopilot was on and eventually led to a death of an Apple engineer. Tesla settled with the family of the victim

to avoid a jury examination of whether Tesla's system was unsafe. Thus, this underscores that the company was wary of a legal precedent finding its AI design at fault (Aljazeera 2024). Therefore, as can be seen from the example, the legal outcomes underscore the difficulty of applying traditional negligence and product liability standards to AI.

If a self-driving car makes a poor decision, is the "reasonable care" standard violated by the human supervisor, the programmers who coded the AI, or neither? The "black-box" nature of advanced driving algorithms, often based on machine learning, can make it hard in court to prove how or why the AI failed. As a result, responsibility often defaults to the nearest human agent.

Overall, autonomous vehicle accidents reveal how existing law struggles with foreseeability and causation when an AI's split-second decisions lead to harm, bolstering the case for updated liability frameworks.

B. Facial Recognition and Wrongful Arrests

Another important category of real-world AI liability cases can be the problems related to the facial recognition systems and the wrongful arrests caused by it. In 2020, a wrongful arrest occurred in Detroit, USA. It was due to the facial recognition technology that was used by the Detroit Police Department. Even though Robert Williams, the victim of the wrongful arrest, later won the settlement in 2024, the issue depicts an issue regarding the efficiency and liability of such technologies (Golston & Komer 2024). Williams spent 30 hours in police custody after an algorithm listed him as a potential match for a suspect in a robbery committed a year and a half earlier. The AI technology stated that the expired driver's license photo of the victim in the state police database showed that he can be a possible match. However, Williams wasn't anywhere near

the store that was robbed on the day of the robbery. Thus, the arrest of Williams ultimately led to be the first public case of a wrongful arrest due to misuse of the facial recognition technology in policing (Gross 2025).

The issue regarding the arrest emphasizes several challenges regarding the legal, technical and ethical usage of the system. Attribution of responsibility was contentious. Detroit police officers arrested Williams, but they did so in reliance to a recommendation given by an AI system. The legal liability fell on the police, not the software vendor, because it was the police who decided to act on the AI's output without properly verifying or assessing it The lawsuit was framed as a violation of Williams's constitutional rights and police negligence, rather than product liability against the AI company. This indicates how, under current law, victims often must sue the human institution using the AI, since proving the fault of the algorithm itself can be difficult without access to its inner workings.

Another challenge of such systems is the bias and foreseeability of harm. Studies show that, like all AI technologies, facial recognition has been less accurate for darker-skinned and other minority populations; it was arguably foreseeable that deploying such a system without safeguards could lead to false accusation against African-American citizens – following Williams' incident, at least seven people across the country have been falsely arrested (Gross 2025).

Thus, overall, these cases depict that the black-box nature of AI and its errors can directly intervene with individual's rights; it overall shows that there is a need for a transparency and human oversight to ensure that the system works efficiently.

C. Generative AI "Hallucinations" and Defamation

The rise of the generative AI systems, meaning the systems that produce human-like text, images, or audio, has introduced new liability dilemmas. Walters v. OpenAI, a recent precedent case that occurred in 2023 depicts broader issues. The radio talk show host, Mark Walters, has sued OpenAI for defamation. In June 2023, radio host Mark Walters filed a defamation lawsuit against OpenAI in Gwinnett County Superior Court, alleging ChatGPT falsely accused him of embezzling funds from the Second Amendment Foundation (SAF). Walters claimed ChatGPT generated entirely fabricated details of a legal complaint, inaccurately stating he had manipulated financial records and misappropriated funds, despite no such allegations existing (Brown & Hummel 2024). Thus, as can be seen from this example, the fabricated complaint and the summary can be given as an example of a hallucination when a generative AI program makes up the facts (Brown & Hummel 2024). Walters only learned of this when the journalist, recognizing the claims were odd, contacted him. Disturbed by the potential damage to his reputation, Walters sued OpenAI for libel, arguing that the company published false and harmful statements about him by disseminating ChatGPT's response.

Many debates regarding the legal challenges arise. One major issue that the critics argue is that whether the existing defamation law and intermediary liability doctrines apply to AI. In its defense, OpenAI has suggested that they should not be held liable since ChatGPT is merely just a tool responding to the user prompts, and indeed in its Terms of Use, the system warns that the AI may produce some untrue information that is a need of a fact-check. Thus, they implied that the user's role matters. In addition to this, OpenAI believes that since there is no real publication from the journalists, no real publication of the libel occurred; thus, the defamation case is irrelevant to

the issue. However, on the other hand, Walters pressed that when an AI platform produces a detailed and authoritative-sounding false narrative about a private individual, it eventually effects the individual's life no different than a news outlet publishing a false story; thus, he states that the harm to one's reputation is done once the false information is conveyed, even if only to one person at first (Brown & Hummel 2024).

Attribution of responsibility in this case plays a crucial role. The question of should OpenAI be treated like a publisher, or the speaker of the AI's content contributes to greater issues. Thus, it ties to the Section 230 debate. As stated in the earlier chapters, Section 230 of the U.S. Communications Decency Act grants internet platforms immunity from liability for content provided by third-party users. However, in this case, the defamatory content was not written by a user; rather it was generated by the AI itself. Thus, it remains legally unresolved whether Section 230's immunity extends to AI-generated content as well. Therefore, if the court does not apply to the case, OpenAI may be seen as liable since they will be regarded as the publisher of the AI's statements (Brannon et al. 2024). Notably, in 2024, a Georgia judge denied OpenAI's motion to dismiss the defamation lawsuit. Thus, many critics signal that the judge's refusal to throw out the claim at a preliminary stage suggests that Walters' case raised a legally plausible argument that AI developers may bear responsibility for what their algorithms say (Scarcella 2025).

Thus, as can be seen from this example, this case is groundbreaking because it marks the first instance in which an AI company faced a defamation lawsuit specifically for a hallucination generated by its AI system. Although OpenAI has not yet been definitively found liable, the denial of OpenAI's motion to dismiss by the Georgia judge indicates the court's willingness to seriously consider holding AI companies accountable for such AI-generated falsehoods. The judge's decision to proceed with the case suggests that, at least for now, the judiciary views AI-generated

statements as potentially defamatory, even without direct human intent behind the false statements (Scarcella 2025).

D.Other Notable Cases and Issues

Beyond the issues that were discussed earlier in this chapter, there is a spectrum of other AI-related incidents that exemplify liability challenges across different sectors. For instance, in the healthcare systems, the use of AI diagnostic tools has prompted the question that when AI causes a medical error, who should be held liable. Even though any such case has not made it to headlines, under the current law, the likely outcome is that the patient would sue the treating physician or hospital for malpractice since the doctor relied on the AI's recommendation. Thus, legal experts suggest that if a doctor uses an AI tool for diagnosis or treatment, and if it goes wrong, the physician would likely to be held liable under the existing malpractice principles (Pearl 2024). Thus, the American Medical Association has started to call "AI", augmented intelligence, rather than artificial intelligence, to emphasize that physicians must not rely on it blindly, and conversely, AI developers should not be the final arbiters of life-and-death decisions (Payne 2024).

Another issue rises in the realm of commerce and finance; where AI systems are seen as producers of biased and discriminatory outcomes, leading to legal liability under anti-discrimination and consumer protection law. An example comes from the Apple Card controversy in 2019, where numerous customers observed that the Apple's new credit card, which was issued by Goldman Sachs, using an algorithmic credit decision process, was granting significantly higher credit limits to men than to woman. This has gained interest in the instances even when the women

had better credit scores or shared finances with their husbands. One example related to this issue was stated by a tech entrepreneur that he received a credit line 20 times higher than his wife's, despite their joint assets (Reuters 2019). Thus, this has ultimately sparked public outcry and a regulator investigation by the New York Department of Financial Services on an inquiry into whether the AI-driven credit scoring system was engaging in a sex discrimination (Reuters 2019). Apple and Goldman Sachs denied intentional bias, and an audit later claimed to find no deliberate gender discrimination. But the incident highlighted a key issue: AI algorithms can unintentionally reproduce or even amplify biases present in training data or historical human decisions. From a liability perspective, even unintentional disparate impact can violate laws, such as equal credit opportunity statutes or civil rights laws.

As can be seen from the real-world case studies, from self-driving car accidents to false arrests, AI libel, potential medical AI errors, and algorithmic bias, a common theme between those instances showed the challenge of pinning down legal responsibility when autonomous or opaque systems are involved. The black-box nature of the many commonly used AI systems complicates evidence and accountability, as injured parties may struggle to demonstrate how an AI's decision led to damage. Nevertheless, each incident is gradually shaping the evolving legal landscape for AI. They highlight an urgent need for clearer frameworks, which is precisely why the European Union is now advancing such initiatives such as the AI Liability Directives. Thus, as can be seen from the attempts, such efforts to aim to fill the gaps by adapting liability rules to the age of algorithms, and to ensure that those harmed ones by AI can find an effective remedy can be a subject to a legal framework that seeks the protection from AI content. In addition to this, it is important for the providers of such AI systems to know that they have appropriate responsibility. As policymakers negotiate the new rules, the lessons that can be learnt from the real-world case

studies like those above provide invaluable guidance on what works and what does not; moreover, it shows what principles a future-ready AI liability regime should encompass.

V. LEGAL AND PROCEDURAL ASPECTS OF AI LIABILITY IN THE EU

A. EU's Existing Liability Framework

i. Product Liability Directive (PLD)

The new Product Liability Directive (PLD) which came into force on 8th of December 2024 revises and adjusts the European Union's liability rules for emerging technologies, ensuring improved protection for victims and greater legal certainty for economic operators (European Commission n.d.b). The PLD, which guarantees that victims can claim compensation from the responsible party when they suffer damages caused by a defective product, is based on two main principles. The first of them is that the damage caused by the manufacturer's defective product must be compensated by the responsible party, the manufacturer. The other one is the victim must prove the specific product's defectiveness and the damage that was caused because of it (European Commission n.d.b).

According to the PLD, any and all persons who has suffered from damage that was caused by a defective product has the right to bring their claim to the national court, including a bystander, a family member, or the owner of the product itself. Even though some EU countries have established similar laws to cover the situations in which the victim is a company, the PLD mainly focuses on consumer protection. Damages that must be compensated vary from death or personal injury, which includes physical and/or psychological harm, to destruction or corruption of data.

The victim is entitled to claim compensation for any of the main forms of damage, as well as all the losses resulting from them (European Commission n.d.).

Objectives of the revision of the PLD range from digital technology to international frameworks. It ensures that rules are future-proof and suitable for cases involving any type of product, from traditional ones to the newest technologies, such as artificial intelligence. Its other provision is to be fit for global value chains. For example, even in situations where the manufacturer is not based in the EU, there shall always be an EU-based liable party for the victim to claim compensation. PLD assured better protection for victims and legal certainty by providing new tools for requesting evidence in court to ensure impartiality for both parties and reduce the burden of proof when it is necessary (European Commission n.d.).

The new PLD will apply to products placed on the market from 9 December 2026, the deadline for EU countries to transpose this directive into national law. The 1985 directive will continue to remain applicable for products placed on the market before the date (European Commission n.d.).

ii. Challenges of Applying Traditional Liability Laws to AI

a. Transparency and Complexity of AI Systems

AI systems complicate integrating traditional laws because of their black box algorithms. Since users cannot see the inner workings of the algorithm, it creates challenges in the areas of transparency, auditing, and data dependency (Arimetrics n.d.). Due to a lack of transparency, the opaque nature of these algorithms can undermine users who are unaware of the mechanisms' decision processes. This lack of clarity can raise doubts about the legitimacy and impartiality of the process. Particularly if the algorithmic decisions impact essential areas of peoples' lives.

The impossibility of accessing internal details contributes to the difficulty of auditing and critically analyzing these algorithms. This may create a challenge for entities that must abide by transparency and accountability regulations, which creates a difficult environment to identify and correct errors or prejudices. In cases where the used data are biased or deficient, the produced algorithms may result in inaccuracies. This data dependence can lead to unreliable decisions that sustain already existing prejudices or do not appropriately reflect reality.

b. Diffusing Responsibility

The diffusion of responsibilities creates major challenges in determining accountability. The more AI systems develop complexity, the more traditional liability frameworks combat difficulties in adjusting the subtle and varied roles of involved parties. These challenges need reconsideration of existing legal structures to ensure that the responsible party is being held liable while contemplating the exclusive characteristics of AI technologies.

This can be seen in the case of AI-driven accidents, which have become more pervasive. According to the report of a federal agency in the US, self-driving cars were involved in almost 400 car crashes in 2021 alone. However, the complexity and opacity of AI systems make the establishment of legal norms complicated. These systems also complicate the process of determination of who is liable. The development and implementation of AI involve numerous factors such as hardware manufacturers, software developers, and data trainers. This leads to a fragmentation of responsibility, which is commonly referred to as the "problem of many hands." It can even result in a situation where no one, or only factor with the lowest position in the chain of command, is held liable for harm. As expert observes show, the opacity of the outputs that are produced by these systems can make it more challenging for individuals to satisfy the traditional

conditions for moral and legal accountability which are intention, foreseeability, and control (Vasudevan 2023).

The responsible development and deployment of AI necessitate justice and accountability for the affected party of AI accidents. These intentions can only be achieved if the legal challenges of dealing with these swiftly advancing technological developments are addressed.

iii. Relevant EU Legislation

a. EU AI Act

The AI Act is a landmark EU regulation that established a horizontal framework for AI; aiming to ensure AI systems are safe, transparent, and respect the fundamental rights of individuals. Most importantly, it introduces a risk-based classification of AI systems (EU Artificial Intelligence Act 2024). Unacceptable risk AI are those that are prohibited for usage that violate the fundamental rights, such as social scoring systems or subliminal manipulation. High-risk AI are the systems that are allowed but heavily regulate, and it is subject to strict compliance requirements, some examples are AI in medical devices, hiring, critical infrastructure and law enforcement. Limited-risk AI systems are designed with specific transparency obligations, for example chatbots or deepfakes must disclose that they are AI-generated. Minimal-risk AI systems compromise all other AI systems, which face no new legal obligations beyond voluntary codes of conduct (EU Artificial Intelligence Act 2024).

The Act places most obligations on providers of high-risk AI, with some duties also for users. Providers must implement rigorous safety and risk-management measures, maintain technical documentation and logs, ensure data quality, and build in human oversight and transparency features. For example, a high-risk AI system must have human interventions possible

and provide clear information for its capabilities as well as its limits (EU Artificial Intelligence Act 2024).

Although the AI Act itself does not create a civil liability scheme, its compliance obligations set a baseline for duty of care. Non-compliance can strongly influence fault in a lawsuit. Failing to meet the Act's safety, transparency or oversight requirements may constitute negligence or a breach of statutory duty in national courts. Notably, the proposed AI Liability Directive, the topic on the agenda for this meeting, would allow courts to presume causation if a defendant violated certain AI Act obligations and that lapse likely contributed to harm (AI Liability Directive 2022). In other words, if a provider ignores mandated safeguards and an accident occurs, that breach can be treated as evidence of fault and causation in civil proceedings.

To conclude, the AI Act's regulatory duties (on accuracy, transparency, human oversight, etc.) are poised to intersect with civil liability. Companies that flout these duties face not only administrative penalties but also greater exposure in civil lawsuits if their AI causes harm.

b. Digital Services Act (DSA)

The Digital Services Act is an EU regulation revamping intermediary liability and online platform accountability. The Digital Services Act (DSA) updates EU regulations on online platform accountability, preserving the safe harbor principle that exempts platforms from liability for user-generated content, provided they swiftly remove illegal content when notified (Algorithm Watch 2022). Importantly, the DSA prohibits mandatory pre-screening of all content but introduces due diligence obligations, such as content moderation systems and transparency reporting. For Very Large Online Platforms, also known as VLOPs, and search engines, it mandates annual assessments and mitigation of algorithmic risks related to harmful content and

fundamental rights. These platforms must transparently disclose AI-driven content curation methods, provide non-AI curated content options, and undergo independent annual audits, significantly increasing algorithmic transparency and accountability in EU law.

While the act primarily crates regulatory obligations, it indirectly shapes the AI liability by setting a standard of care for online platforms. Platforms deploying AI for content moderation or curation are expected to do so responsibly, for example by avoiding biased or unsafe algorithmic practices and promptly removing flagged illegal content. Thus, the DSA reinforces AI accountability through enforced diligence and oversight mechanisms.

c. Revised Product Liability Directive (PLD)

The EU's Product Liability Directive has been modernized to address the digital-age technologies, expanding strict liability to AI systems and software. Under the updated PLD, injured persons can claim compensation from manufacturers or suppliers without needing to prove fault, if a product is defective and causes damage. Furthermore, and crucially, the definition of "product" and "defect" is broadened for AI-era risks. The new PLD explicitly extends to intangible tech. This includes software, AI systems, and digital services; they are deemed products for liability purposes (Civatte et al. 2024) Liability no longer stops at the original manufacturer; Those who modify or deploy AI software, online marketplaces that present themselves as sellers, importers of AI systems, and others in the supply chain can be strictly liable if they put a defective AI product into circulation. Moreover, a product is considered defective not only when it falls short of ordinary safety expectations, but also if it fails to meet standards set by law. In addition to this, the revised PLD recognizes intangible harms. Victims can claim for destruction or corruption of data and for medically certified psychological harm, in addition to traditional injury or property damage .

The updated PLD establishes a robust no-fault route for AI liability, complementing the proposed AI Liability Directive's fault-based approach. This means a person harmed by AI has two avenues, either sue under product liability – if the injury was caused by a defective AI product – or sue under fault-based rules – if someone's negligence in designing, deploying, or controlling an AI system caused the harm (Civatte et al. 2024). Overall, the revised PLD significantly strengthens consumer protection in the AI context by ensuring AI systems and software are covered by strict liability.

VI. Proposed AI Liability Directive (AILD)

A. Presumption of Causality

One of the main initiatives hte proposed AI Liability Directive introduces is the presumption of causality. This will reduce the burden on victims to explain in detail how the damage has resulted from a specific defect or neglect. On the condition that the victims show someone was at fault for not abiding by their allocated responsibilities that led to the harm, and there's a chance that AI may have caused the situation. If this connection is not irrelevant, the court can presume that this failure of AI to follow rules and regulations caused the damage (European Commission 2022).

Nonetheless, the person held liable, the developer or manufacturer, can refute this presumption; this is called the rebuttal presumption of causality. In cases where AI provider fails to comply with their obligation to ensure safety, and the AI system's output creates damage, the assumption is that the violation of responsibility caused the damage (Clifford Chance 2025). To illustrate; if an autonomous delivery robot malfunctions, and it is demonstrated that the operator

had deactivated a safety feature, the presumption would link that fault to the accident unless the operator proves otherwise. This assumption is designed to assist the claimant in overcoming the technical difficulties of proving causation between the failure of the AI deployer to provide the flawed AI output that caused the damage (Clifford Chance 2025).

The presumption will only be applicable to systems that are considered extremely difficult for the claimant to prove, which are non-high-risk AI systems. As for high-risk AI systems, the presumption of causality will not be applicable if there is sufficient evidence for the claimant to prove the relevance between AI's failure and the damage created (Norton Rose Fulbright 2024).

B. Disclosure of Evidence

This provision grants individuals the right to claim disclosure of information from AI providers. These AI providers can be entities or persons who develop or produce AI systems for the market, as well as the ones who place them or put them into service. The aim of this grant is to identify potential claims and liable parties because of the damage they have suffered as a result of incorrect or harmful AI outcome. The AI providers are obliged to respond to the request accordingly (Clifford Chance 2025).

Through this approach of the AILD, courts can be empowered to order companies to disclose necessary information regarding their AI systems when high-risk AI is involved. However, under the current rules, victims may struggle to access the technical data and system records that are essential to prove the role of an AI system in causing damage since firms often hold these data as proprietary. When a victim that was harmed because of AI wants to prove the responsibility of the company through the technical details of the system, and the company does

not provide the information, in other words fails to comply with a disclosure order; the presumption of causality may be automatically applied in the victim's favor.

VI. CHALLENGES AND FUTURE CONSIDERATIONS

A. Addressing Cross-Border Liability

One of the significant issues regarding the liability for the AI systems operate or cause harm across multiple jurisdictions. Thus, cross-border liability issues arise because EU member states historically have had different tort laws and evidentiary standards; thus, leading to a fragmented outcome in the AI-related cases (Frattone 2025). An accident or harm caused by an AI system in a country might be subject to different liability standards than a similar incident in another country, leading to uncertainty for victims and businesses.

Prior to a unified framework, companies faced legal uncertainty in predicting how courts in various countries would handle AI-caused damage, especially for businesses trading across borders (AI Liability Directive n.d.). It is important to note that this fragmentation not only made it hard for the victims, but it also increased compliance costs for AI developers and deployers operating EU wide. Without harmonization, member states could develop inconsistent national AI liability laws, further complicating cross-border commerce and potentially encouraging uneven compensation for victims (Frattone 2025).

The proposed proposal seeks to harmonize how national courts across the EU handle the cases regarding AI. With varying legal interpretations and approaches in different member states, businesses and individuals face significant challenges as stated previously. Thus, the directive aims to provide clear guidelines that apply uniformly across the EU, fostering greater trust in the AI

technologies (Werner 2024). Clarity and uniformity would reduce compliance costs for companies and favor cross-border AI commerce by allowing businesses to operate under a predictable liability regime (Frattone 2025). In addition to this, uniform rules would facilitate mutual recognition of judgments and enforcement in cross-border cases, since courts would be applying aligned standards.

B. **Uncertainties in Causation and Enforcement**

AI systems present novel difficulties in proving causation and enforcing liability due to their complexity and opacity. The traditional tort law requires the injured party to identify a responsible actor, prove a wrongful action, and establish a causal link between the fault and the damage. However, with AI, each of these steps become uncertain. Modern AI models often function as black boxes; thus, making it difficult or prohibitively expensive for victims to identify the liable person and prove the requirements for a successful liability claim (AI Liability Directive n.d.). Even experts cannot always pinpoint exactly why an AI behaved a certain way due to its complexity and lack of transparency. This raises the problem of causation uncertainty: victims might suffer harm but be unable to trace it to a specific human or company's negligence under existing rules (Frattone 2025).

The AI Liability Directive introduces a "presumption of causality," allowing victims to establish causation by showing a defendant's likely non-compliance with legal obligations, thus significantly easing the burden of proof in complex AI-related cases. Defendants retain the right to refute this presumption by demonstrating alternative causes for the harm. Additionally, the directive empowers courts to order companies to disclose critical technical evidence, addressing information asymmetries while balancing confidentiality concerns.

Despite all the measures that the AI Liability Directive proposes, the uncertainties remain. The enforcement of liability judgments in AI cases might be problematic if the liable party is insolvent, not domiciled in the jurisdiction, or if multiple parties share responsibility. Therefore, this creates challenges in assigning liability. Regulators and legislators acknowledge that proving a causal chain in AI will never be as straightforward as in traditional cases; hence, ongoing discussions about possibly expanding strict liability to certain AI applications or creating insurance pools. For now, the directive's approach focuses on procedural relief to make enforcement of existing laws feasible. It stops short of redefining substantive causation rules (Frattone 2025).

C. **Regulatory Gaps and Overlaps**

The emergence of AI has exposed gaps in existing liability regimes as well as areas of potential overlap between new AI-specific rules and established laws. One gap is that traditional EU product liability law was not fully equipped to handle all AI-related harms. The recently updated Product Liability Directive imposes strict liability for defective products but historically applied mainly to tangible products causing physical injury or property damage. Purely digital or intangible AI systems, and harms such as discrimination or privacy infringements, fell outside its scope. The revised PLD is expanding the definition of "product" to include software and AI, and even covers data loss as a form of damage (Frattone 2025). However, important limitations remain, the PLD framework only covers certain harm categories such as personal injury, property damage, and data loss; while excluding other types of harm like violations of fundamental rights such as equality or privacy rights, as well as purely economic losses. Moreover, it also does not compensate damage to professional/commercial property and provides a "state of the art" defense shielding manufacturers from liability for risks that were not foreseeable given scientific knowledge at the time. These gaps mean that victims of AI-caused harms that are non-tangible,

such as being unfairly discriminated against by a hiring algorithm or having one's reputation harmed by an AI's output, might have no recourse under product liability law. Thus, the AI Liability Directive was designed to fill these gaps by covering cases outside the PLD's scope by essentially providing a path to compensation for harms caused by AI.

However, debates exist regarding the introduction of AI. On one hand, AILD raises concerns about regulatory overlaps and complexity. The AI system is already governed by multiple layers of regulation. Besides the updated version of PLD, the EU has the forthcoming AI Act, as well as horizontal frameworks that corresponds to issues regarding AI. Many of these instruments include their own enforcement and liability provisions. Thus, over-regulation could risk inconsistent or duplicative obligations and might even conflict with well-established national liability doctrines.

On the other hand, supporters argue that the AI Liability Directive provides a narrow, complementary framework, setting minimum harmonization standards for procedural aspects such as disclosure of evidence and easing the burden of proof, while leaving fundamental liability rules to national laws. The directive is designed as the "missing piece" to address gaps left by existing strict liability provisions under the Product Liability Directive, without creating a completely new liability system. However, it doesn't resolve all discrepancies between national tort laws, prompting future discussions on deeper harmonization or adopting a two-tiered liability system at the EU level (Frattone 2025). Policymakers also consider the potential shift from a directive to a regulation to enhance uniformity but must balance such measures against national sovereignty and subsidiarity principles.

D.Legal Personhood for AI

The concept of granting legal personhood to AI is a highly debated future consideration in AI liability discussions. It asks whether autonomous AI systems should, at some point, be treated not merely as products or tools of human operators, but as bearers of legal rights and obligations; in effect, as "electronic persons." In 2017, the European Parliament ignited this debate by suggesting the creation of a special legal status for very advanced robots and AI, drawing an analogy to corporate personhood (Dvorsky 2018). The idea behind this was that if an AI system operates with a high degree of autonomy and it becomes hard to pin liability on a specific human, perhaps the AI system itself could be deemed a legal entity that bears certain social responsibilities and obligations. Under such a scheme, liability for harms caused by the AI would reside with the AI agent itself, which in practical terms would mean requiring these AI entities to be insured or to maintain funds to pay out damages. Proponents of AI legal personhood suggest treating advanced autonomous AI systems similarly to corporations or individuals by granting them limited legal personhood, primarily as a pragmatic solution to complex liability issues such as clearly identifying defendants in incidents involving sophisticated AI, like self-driving vehicles.

However, the notion of AI legal personhood was met with strong opposition from legal experts, ethicists, and industry alike. Shortly after the Parliament's proposal, 156 AI experts from 14 countries signed an open letter warning that granting robots or AI systems legal personhood would be "inappropriate from a legal and ethical perspective." (Delcker 2018).

Critics highlight that AI lacks consciousness, intent, and moral agency, making legal personhood philosophically problematic and potentially inappropriate. The EU has largely rejected the idea, emphasizing human-centric approaches to liability and focusing instead on procedural tools like transparency and burden-shifting under the AI Liability Directive, alongside practical

solutions such as mandatory insurance. While legal personhood remains mostly theoretical today, future developments in AI capabilities could reignite this debate, requiring ongoing regulatory attention and potential adjustments.

E.Emerging Global Trends

The EU's efforts on the AI liability are unfolding against a backdrop of global trends in AI governance. Approaches vary widely, reflecting different legal cultures and policy priorities. The global landscape is dynamic: the EU's comprehensive regulatory approach stands in contrast to the US and UK's more incremental or fragmented approach (Benizri et al. 2023), and to Asia's split between China's heavy regulation and others' soft guidance (Tan et al. 2024). These divergent models underscore an ongoing global dialogue and potential need for international harmonization, especially given AI's inherently cross-border nature, highlighting Europe's influential but challenging role in shaping global AI governance.

F.Balance Between Innovation and Consumer Protection

Policymakers designing the AI liability rules continually strive to balance the technological innovation with consumer protection. This balancing act is a central theme for the directive, since on one side, there is a need to foster vibrant AI industry in Europe by encouraging experimentation, and not suffocate startups or researchers with overly fearsome liability risks. On the other hand, there is the imperative to safeguard the public from harm, ensure users' rights and safety, and maintain trust in AI by providing adequate remedies when things go wrong. The equilibrium is challenging. The EU aims for a human-centric, risk-based approach to AI regulation, emphasizing

strict consumer protection for high-risk AI applications, such as those in healthcare and transport, to foster public trust and responsible innovation. The proposed AI Liability Directive sought to ensure consumer confidence through clear liability rules aligned with the AI Act's safety standards, incentivizing developers to create safer AI. However, critics argue stringent liability measures could stifle innovation, especially among small businesses, potentially driving companies away due to increased legal risks and insurance costs.

VII. PARTY STANCES

A. European Conservatives and Reformists Group (ECR)

The ECR group strongly rejected the AILD. ECR's rapporteur in IMCO, Kosma Złotowski (PL), drafted an opinion explicitly calling the directive "premature and unnecessary" since the AI Act and revised Product Liability Directive already raise safety and liability standards. (Werner 2025). ECR MEPs highlighted that imposing new presumptions or disclosure orders could unduly burden businesses, especially SMEs, and should be postponed. Their official line was to scrap the proposal: in practice ECR votes in committee and Plenary were grouped with other right wing parties against moving the file forward (Kroet 2025). ECR also questioned the directive's scope – noting that without a final EU definition of "AI system," it was unclear what new rules would cover.

B. Europe of Sovereign Nations

The ESN group – a right-wing sovereigntist bloc – did not take a supportive stance on the AI Liability Directive. ESN leaders consistently decry EU liability rules as excessive bureaucracy. The AI Liability directive would introduce features like rebuttable presumption of causality –

shifting the burden of proof onto AI operators – but the ESN made no public effort to defend or expand those provisions (Legorburu 2025). No ESN amendments or press statements advocate the directive's liability extensions or evidence-disclosure rules; on the contrary, ESN rhetoric suggests it opposed the AILD overall.

C. Group of European People's Party (EPP)

The center-right EPP generally viewed the AI Liability Directive with skepticism. Its IMCO committee members voted to drop the proposal, arguing that a full new liability regime was "premature" and could hurt European competitiveness (Sasdelli 2025). EPP coordinators emphasized first assessing how the new AI Act and updated product liability law play out before adding new rules; for example, EPP MEP Andreas Schwab said the legislature should focus on the AI Act now and revisit liability only in a couple of years (Kroet 2025). In sum, the EPP group's official line has been to delay or narrow the directive – prioritizing legal certainty for businesses – though there are dissenting voices within the group calling for strong AI accountability.

D.Group of the Greens/European Free Alliance (Greens/EFA)

The Greens/EFA group championed a strong liability framework and opposed scrapping AILD. MEPs like Kim van Sparrentak (NL/Green) warned that withdrawing the rules showed "a lack of understanding" of victims' needs – the directive was not meant to "bully companies" but to protect people and small businesses (Kroet 2025). Greens consistently joined S&D and The Left in advocating for AILD's provisions. They backed the proposal's disclosure orders and rebuttable "causality" presumption, especially for high-risk AI, arguing that complexity of AI demands easing the evidentiary burden on claimants. The Greens publicly supported the directive's focus

on critical AI systems and were among the groups writing to Parliament leaders to keep AILD alive.

E.Group of the Progressive Alliance of Socialists and Democrats in the European Parliament (S&D)

The center-left S&D group strongly backed the proposed directive. Shadow rapporteur Brando Benifei (IT/S&D) and his colleagues repeatedly urged that the AILD fill gaps in the AI Act and Product Liability regime. They criticized the Commission's withdrawal of AILD as "disappointing," saying harmonized liability rules would ensure clarity and fairness for consumers harmed by AI (Kroet 2025). S&D members supported key provisions like easier burden-of-proof and expanded disclosure obligations for high-risk AI, arguing these help ordinary people seek redress when opaque systems cause damage (Sasdelli 2025).

F.Patriots for Europe

Similar to the ESN, the far-right Patriots for Europe (PfE) group did not champion the AILD. No PfE press release or plenary speech endorses the directive; instead, PfE-linked MEPs participated in parliamentary debate but offered no text to broaden liability or ease proof. In fact, the Internal Market committee's draft opinion – reflecting center-right and conservative views – explicitly called the AILD "premature and unnecessary (Werner 2025). PfE opposes its broad causality presumption and onerous disclosure requirements.

G.Renew Europe Group

The liberal Renew group largely aligned with the EPP on AILD. In committee votes, Renew MEPs joined the center-right in opposing the draft directive, calling it unnecessary in light of the new AI Act and Product Liability overhaul (Sasdelli 2025). EU-wide AI liability could

overburden SMEs and innovators, according to Renew's views. While Renew did not issue a high-profile manifesto on specific AILD clauses, its coordinators in IMCO agreed to defer binding rules until after the AI Act takes effect.

H.The Left

The The Left bloc staunchly supported the directive. Left MEPs argued AILD was needed to fill accountability gaps left by the AI Act and product liability reforms. They joined Greens and S&D in urging Parliament not to abandon the file (Kroet 2025). The Left backed the core AILD provisions – especially the rebuttable presumption of causality and court-ordered disclosure of AI evidence – as essential tools for victims. They also endorsed a broad scope covering new high-risk categories and favored strict liability rules for the most critical AI uses

VIII. COUNTRY STANCES

A. Austria

Austria has created a comprehensive national AI strategy called Artificial Intelligence Mission Austria 2030, shortly referred to as AIM AT 2030, and is actively implementing the EU AI Act (Regulation (EU) 2024/1689). Finalized in 2021, this strategy focuses on promoting AI research, innovation, and ethical AI deployment while adhering to EU regulations. In order to provide guidance for AI policy decisions, Austria established a Council on Robotics and Artificial Intelligence. The nation places a high priority on reliable AI, guaranteeing adherence to moral standards, legal requirements, and safety regulations. AIM AT 2030 also highlights AI applications in industry, healthcare, education, and climate change mitigation, with the goal of making Austria a leader in AI-driven digital transformation. (Austria AI Strategy Report 2017).

B. **Belgium**

Currently, in Belgium, the term Artificial Intelligence does not have an official definition under the law (LexGO 2024). Although within the country, there are no guidelines, rules, or laws that have been adopted, different regional authorities have adopted their own strategy for the agenda. The government of Brussels created an institution called FARI (Fund for Artificial Intelligence Research and Innovation) in order to increase the number of research projects on AI, while adopting an AI policy. The Flemish AI plan was adopted by the authorities in Flanders in March 2019. The earliest step was taken by the Walloon government in 2015 with the creation of Agence du Numérique (AdN). This agency was launched to coordinate communicational or operational actions according to the Digital Wallonia strategy. The Walloon government did not end its programs with AdN: four years later, DigitalWallonia4.ai was introduced in July 2019. However, a collaborative framework was established in late 2022 by the government of Belgium. This plan includes 70 actions under 9 different goals. These aims include promoting a trustworthy AI, the usage of AI in the healthcare field, ensuring cybersecurity, providing better protection and services for the citizens, and preserving the environment.

C. **Bulgaria**

The Bulgarian Academy of Sciences (BAS) established a structure for the creation of National AI strategy, which was finalized by professionals from the Ministry of Transport, Information Technology and Communications (MTITC) of the country before being announced to the public in 2020 (European Commission 2021). The strategy includes extensive programs that will manage the development of AI in the country between the years 2020-2030, and highlights areas that will face significant outcome such as research and innovation capacity, as well as data availability. Some of the main goals of National AI strategy can be counted as financing AI

development to be sustainable, awareness and trust in society being raised, and essential services for AI development to be reliable. The need for educational reforms was also stated in the strategy. In order to increase the skills and knowledge for artificial intelligence, the Ministry of Education and Science (MON) implemented specific programs. These programs include enhancement of teachers' ability to work with digital technologies, including AI, application of AI tools in education to increase the efficiency of learning process, creation of suitable conditions for an increase in the number of students who will pursue their PhD in the topic or related to the topic of artificial intelligence, and improvement of students' abilities to use technology in an ethical way (European Commission 2021a).

D.Croatia

The National Plan for the Development of Artificial Intelligence that the Croatian government assigned several experts into a working group to establish the draft was expected to be concluded in 2021 which got delayed because of the COVID-19 pandemic (JustAI 2024). Currently, the country is advancing its strategy to utilize the capabilities of AI for supporting economic and societal development. Croatia's strategy is led by a various collaboration that includes the public sector, civil society and academia. The framework is expected to be introduced by the end of 2025, which is presumed to address environmental issues under the usage of AI since the Croatian Presidency of the Council of the EU gave notable attention to the topic.

E.Republic of Cyprus

Cyprus capitalizes on its National AI Strategy as well as its EU membership to create a reliable AI ecosystem aligning with the AI Act. Main objectives of the strategy are safeguarding and preserving fundamental rights while keeping regulations unified. In this strategy, the

government of Cyprus focuses on five topics: human capital, research& & innovation, infrastructure, ethics & governance, and international cooperation. The country released their implementation roadmap of their National AI Strategy. Roadmap of the plan starts with reviewing the gap between the country's AI systems and mandates of AI Act. After planning structure according to the gap, governance policies and documentation process starts. At the next step, high-risk AI undergoes an evaluation. Ongoing compliance is being maintained through annual reporting and audits to remain updated with the changes in standards (Doviandi 2025).

F.Czech Republic

The Czech government introduced the National Artificial Intelligence Strategy (NAIS) of the country, whose goal is to develop the Czech Republic's maximum efficiency from AI for both the economy and society until the year 2030. The strategy was a collaborative work between the private sector and public. It aimed to strengthen the country through improving research and education while assuring the process is ethical and secure. It also addresses expanding international initiatives for advancing AI and its various actor chain, from developers to users. NAIS has seven crucial goals from interrelated areas that include security aspects, industry and business, education and professional training, and public administration and services. The strategy was based on the result of expert research, analysis, and public consultation. In order to work on an update, a working group with academic attendants, non-profit organizations, ministries and economic partners were brought together in 2024 (Ministry of Industry and Trade 2024).

G.Denmark

With the support of Microsoft and significant Danish companies, Denmark has established a groundbreaking framework for AI governance and is actively implementing the EU AI Act (Regulation (EU) 2024/1689). In 2019, the nation unveiled its National AI Strategy, which

emphasizes business competitiveness, ethical AI research, and development. Adoption of AI in the public sector has been given top priority in Denmark, which ensures adherence to EU laws while promoting innovation (Denmark AI Strategy Report 2019).

In order to promote workforce development and education, the government has also set aside funds for AI research and digital transformation. Denmark's strategy maintains technological leadership while encouraging responsible AI use by ensuring a balanced integration of AI regulations.

H.Estonia

Estonia has been a steadfast supporter of AI-driven digital transformation and is actively implementing the EU AI Act (Regulation (EU) 2024/1689). First unveiled in 2019, the nation's National AI Strategy aims to promote AI research, innovation, and ethical AI implementation in the public and private sectors. With specialized programs at TalTech and the University of Tartu, including a Master's program in AI and data science, Estonia has made significant investments in AI education. In order to improve accessibility and efficiency, the government has also made AI adoption in the public sector a top priority. Estonia's strategy guarantees a fair incorporation of AI laws while encouraging creativity and competitiveness. (Estonia AI Strategy Report 2019).

I.Finland

Finland’s age of artificial intelligence began in October 2017, when its national AI strategy was published by the Finnish Ministry of Economic Affairs and Employment. The report, also labelled as AI Finland, aims to make AI and robotics major parts of success for Finnish companies. The strategy underlines Finland’s place in the global market, not just with its strengths but also with its weaknesses. In order to be a success in AI development, the Finnish government has

adopted an open date policy. Moreover, the strategy aims to increase competition in the industry, integrate AI skills into lifelong learning systems, research for the development of AI technologies and their application process. The strategy was lastly updated in November of 2020: the Artificial Intelligence 4.0 Programme focuses on AI's role in the public sector, such as AI-powered public services and the importance of the definition of strong ethics for the usage of AI. (NordForsk 2024)

J.France

The national AI Strategy of France is mostly influenced by the report "For a meaningful artificial intelligence: Towards a French and European Strategy" and its recommendations. The report took six months to finalize with the efforts of Cédric Villani, who is a French mathematician and member of the Parliament, and his team. Key proposals ot eh Villani Report on AI were various and included boosting the potential of French research, planning for the impact of AI on labour, making AI more environmentally friendly, and ensuring that AI is supportive of inclusivity and diversity. The report also underlines that AI should be targeting four strategic sectors: health, transport the environment, and defence & security (Ambassade de France au Royaume-Uni n.d.).

K.Germany

The German government established its National AI strategy in the November of 2018. The strategy was developed by the efforts of three different ministries: the Federal Ministry of Education and Research, the Federal Ministry of Labour and Social Affair, and the Federal Ministry for Economic Affairs and Energy. The strategy's goals include increasing Germany's competitiveness, and making Germany, and Europe, a leading center in AI, ensuring the AI developments to serve for the society, and integrating AI in society through cultural, legal, and ethical terms for a comprehensive societal dialogue and political measures. In October 2019, an

ethical guideline and certain recommendations for artificial intelligence were released by the Federal Governments Data Ethics Commission. One year later, final document produced by the Study Commission of AI was announced, and in December 2020, the updated version of the AI strategy was adopted. According to OECD (n.d.a), during this period, the funds allocated for artificial intelligence by the German government made a major increase. It can be added that no decrease is expected in the near future (European Commission 2021b).

L.Greece

Greece is proactively developing its AI governance structure to conform to the AI Act of the European Union. Regarding high-risk AI systems, the Ministry of Digital Governance has appointed national authorities to supervise adherence to fundamental rights. The Greek Ombudsman, the Hellenic Authority for Communication Security and Privacy, the Hellenic Data Protection Authority, and the National Commission for Human Rights are some of these authorities. (Milosevic 2024).

Furthermore, the goal of Greece's national AI strategy is to democratize AI in a sustainable manner. Key players and experts from Greece and the EU are involved in the strategy, which is coordinated by the Hellenic Ministry of Digital Governance. To ensure responsible AI development, the nation is concentrating on ethical principles, data policy, and trust frameworks. (Greece AI Strategy Report 2021).

M.Hungary

The government of Hungary introduced its National AI strategy that outlines its visions and the necessary actions for AI development between 2020-2030 in 2020. Hungary's National AI strategy was designed by the Ministry of Innovation and Technology through an "AI Coalition"

established in October 2018 with partnerships between the Ministry and experts from academics, leading IT companies, and state institution, including over 320 members. Hungary's strategy for artificial intelligence is about supporting AI and its relevant sectors by means of extensive goals. These goals are designed to sort out specific sectors and prioritize the ones the country has most potential to grow and launch programs accordingly that will benefit the public. It should be noted that in order to remain aligned with technological developments, the strategy should be examined every two years (European Commission 2021c).

N.Ireland

The first National Artificial Intelligence Strategy of Ireland is named "AI - Here for Good", which was introduced in July 2021. The strategy can be classified as a manual for how Ireland can strengthen its potential to use AI in the most beneficial way for public services, business, and the public. The strategy underlines how crucial it is to create a reliable, ethical, and civilization-focused artificial intelligence. "AI - Here for Good" has got certain strategic action to take. Some of these are initiating a study to examine the effects of AI, as well as generative AI, developing a country-wide campaign in order to raise awareness, reserving a place where government officials are supported to experiment with artificial intelligence, and ensuring Ireland's leadership in the EU for AI standards and certification (Department of Enterprise, Trade and Employment 2024).

O.Italy

Only recently, on 20 March 2025, the AI Bill was approved by the Italian Senate, which authorized the Italian government to adopt the Bill in a twelve-month period. The intention of the AI Bill is not to coincide with the EU's AI Act, but accompanying its legal structure. The AI Bill underlines the significance of fundamental rights under both the Italian and EU law, such as

security, transparency, data protection, non-discrimination and gender equality, while reaffirming preservation of confidentiality for personal data and information. Additionally, promotion and advancement of AI technologies is highlighted. The bill consists of detailed arrangements for particular sectors. These sectors include health and disability, labour law, intellectual professions, research and experimentation. For copyright law and the code of civil and criminal procedure, amendments were proposed, and now adopting the Bill is waited from the Italian government (Rinaldi & Breschi 2025).

P.Latvia

The government of Latvia published its national AI strategy, Developing artificial intelligence solutions, in February 2020. The strategy outlines the promotion for growth of AI in the country's economy. The main goal of the strategy includes various areas, including developing an ethical and legal framework for artificial intelligence, raising awareness in AI across communities through reforms in education, and actively engaging in both national and international collaboration for AI and related fields. The strategy is promised to be monitored on a non-specified regular basis (European Commission 2021d).

Q.Lithuania

In 2019, Lithuania became the second EU country to release an AI strategy. The strategy aims to be a regional leader in the topic through engaging in the global AI ecosystem. An Action Plan for Development of Lithuanian AI Technologies was created cover the goals between the years 2023-2026, whose main goal is to provide the necessities for high-tech AI development. The Vice-Minister of the Economy and Innovation, which is the ministry that prepared the previously mentioned plan, states that they are working to establish an appropriate environment for companies

to develop this technology in their country (Ministry of the Economy and Innovation of the Republic of Lithuania 2024).

R.Luxembourg

Strategic Vision for AI in Luxembourg has three particular ambitions. The country aims to be one of the most developed digital societies, especially in the EU. Luxembourg's second goal is to achieve transitioning to a data-driven economic model that is also sustainable. Last one is human-centric AI development, AI that is supportive of and respects human rights. The strategy focuses on crucial areas such as ethics, privacy, and security, AI for the public sector, skills and lifelong learning, and international cooperation. Luxembourg states that its AI strategy is a living document, thus, it is intended to be updated according to the received feedbacks and new developments (Digital Watch Observatory 2019).

S.Malta

Malta's national AI strategy, Strategy and Vision for Artificial Intelligence in Malta 2030, was developed by the Maltese government in order to focus on resources and investment needed to maximize the AI benefits for the country. The strategy's aim is Malta to gain advantage to lead the AI field while focusing on three different major steps which are boosting investment, innovation, and adoption. Thus, it is believed that the strategy's aforementioned extensive impact is inclusive and does not let any part of the society to be left behind (Malta Digital Innovation Authority 2019).

T.Netherlands

The Netherland's national AI strategy called The Netherlands Strategic Action Plan for Artificial Intelligence highlights the government's plan of developing and regulating AI. The

action plan centers on education, innovation, and research on AI while keeping ethical and societal criteria under consideration. The plan mentions the cruciality of international collaboration as well as public and private sector cooperation. Primary goals of the plan are regulatory framework, economic and social benefits, infrastructure and data, and enhancing AI capability (Digital Watch Observatory 2019).

U.Poland

Policy for the development of artificial intelligence in Poland from 2020, Poland's national AI strategy, was adopted by the Council of Ministers in December 2020. Main focuses of the strategy are education, business, society, and international relations. The Polish strategy aims to meet objectives with their AI ecosystem. These objectives include reforming the educational system for learning AI technologies, increasing partnership in AI for both national and international fields, and establishing trustworthy data. The Polish government reserved a spot at the governance center for its national AI strategy under the chair of the Minister of Digital Affairs and the Council of Ministers Committee for Digital Affairs. The strategy is decided to be evaluated each year (European Commission 2021e).

V.Portugal

Although the Artificial Intelligence Act of the EU, first extensive regulation for artificial intelligence in the world, directly affects Portugal, the country has not yet launched its national AI strategy. Portugal must adopt a regulatory act by August 2, 2025. This act must include at least one control mechanism for the market, and regulations governing sanctions, such as administrative fines (Lexology 2024).

W.Romania

In July 2024, the Romanian government authorized the National Artificial Intelligence Strategy for 2024-2027. The strategy summarized Romania's integration of AI technologies into multiple sectors such as public administration, which aligns with the EU's approach. It emphasizes the significance of developing a regulatory framework customized for the country's national needs through a cooperation among business, research facilities, and academia for both the investment and innovation to reach their maximum potential. The strategy focuses on five key fields, which are digital education, digital economy, digital public administration, emerging technologies and cybersecurity. The Romanian government expects AI technologies to contribute to the country's improvement on economic and social areas (Digital Watch Observatory 2024).

S. Slovakia

Action plan for the digital transformation of Slovakia for 2019-2022 was introduced in July 2019 by the Slovakian Government. This plan focuses on how to create a trustworthy, human-centric, and sustainable AI ecosystem under the long-term national strategy for AI, the Strategy of the digital transformation of Slovakia 2030. The short-term policy actions of the Slovakian Action Plan includes supporting the AI ecosystem and digital transformation for education to promote technological skills, strengthening the data economy, and improving the potential of public administration's usage of data for the public benefit. The Action plan is funded by the Analysis for budgetary implications for public administration of the Slovakian government (European Commission 2021f).

X.Slovenia

The Slovenian government published its draft National AI programme in the August of 2020, which endorsed the advancement of AI usage in Slovenia until the year 2025, with plans of

making the programme official in 2021. The programme was created with the collaborative efforts of certain ministries, industrial representatives, and national experts. Republic of Slovenia's national AI strategy focuses on Slovenia's capacity of innovation and research, as well as its place in the global competition in the sector between the years 2020-2025. The strategy targets the creation of a supportive environment for AI development, enhancement for productive international collaboration, launching a National AI Observatory, and improvement go industrial capacities. The Slovenian government plans to revise the education system in order to include digital thinking skills and AI related topics to the curriculums of schools from primary level to secondary level. Implementation of the National AI Programme is classified as dynamic by the government. Thus, periodic updates will be made along the way (European Commission 2021g).

Y.Spain

The Spanish government implemented its National Artificial Intelligence Strategy during 2020 with a goal to achieve AI leadership in five years. A partnership between ministries along with academic institutions and industry representatives and civil society members was responsible for creating this strategic plan. Spain's national AI strategy focuses on three main areas which include strengthening research and innovation capabilities and building ethical trustworthy AI systems as well as promoting digital transformation in the economy and public administration. The strategic objectives focus on improving AI talent development and helping small and medium-sized enterprises adopt AI while developing international AI research and regulatory partnerships. The national government plans to transform education through the integration of AI literacy and digital skills across all educational stages beginning with primary grade through higher education. The government designed the implementation process to remain adaptable through continuous

evaluation and revision to match changing technology and social requirements (Digital Watch Observatory 2020).

Z.Sweden

Although Sweden does not have a legal definition for artificial intelligence, it has introduced its national AI strategy that focuses on education, research and the usage of AI for public services. AI usage is pervading in the country, especially in sectors such as manufacturing, healthcare, and finance. There are no additional restrictions for AI, except EU's laws and regulations. The integration of AI is promoted through funding and supporting research, innovation, and considering ethical standards. Sweden is currently an active contributor in EU-led programs and is committed in research and development in AI (The Legal 500 Country Comparative Guides 2024).

IX. QUESTIONS TO BE ADDRESSED IN THE DIRECTIVE

1. Should the AI Liability Directive incorporate a strict liability regime for certain AI systems – especially high-risk AI, or maintain a fault-based approach for all related harms? What criteria or risk threshold could determine when each liability model applies?

2. How can the Directive alleviate the burden of proof on victims of AI-caused damage, given the opacity and complexity of AI "black box" systems? In what ways might traditional requirements of proving fault and causation be adjusted for AI cases?

3. Should the AILD's special liability measures apply only to high-risk AI systems, or be extended to AI systems of all risk levels?

4. What role should a presumption of causality play in the AILD to help victims link harm to an AI system's failure or a provider's wrongdoing? Under what conditions should courts presume a causal connection between an AI operator's non-compliance and the damage caused, and how can defendants effectively rebut such presumptions?

5. Should the Directive impose transparency or evidence disclosure obligations on AI developers and deployers to ensure victims can access necessary technical information to support their claims? How can such measures be balanced with protecting companies' trade secrets and confidential information?

6. What legal gaps in the current EU framework does the AI Liability Directive need to fill regarding AI-caused harm?

7. How should the Directive address the diffusion of responsibility when multiple parties are involved in designing, training, deploying, or operating an AI system?

8. How will the Directive ensure harmonized rules across all EU member states for AI liability and handle cross-border cases of AI-induced harm? What mechanisms could facilitate mutual recognition of judgments and effective enforcement of liability decisions when an AI system causes damage across different jurisdictions or when the liable party is based in another country?

9. Should the EU consider granting AI systems themselves a form of legal personality so that they can bear liability directly, or should responsibility for AI-caused harm remain exclusively with human actors?

10. Is there a need for mandatory insurance or other financial security requirements for AI operators or producers under the Directive?

BIBLIOGRAPHY FOR AGENDA ITEM II

Ada Lovelace Institute. 2025. AI Liability in Europe. https://www.adalovelaceinstitute.org/resource/ai-liability-in-europe.

Advanced Modules on Digital Rights and Freedom of Expression—Module 5: Trends in Censorship by Private Actors / Intermediary Liability. n.d. Media Defence. Accessed May 19, 2025. https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-5-trends-in-censorship-by-private-actors/intermediary-liability.

AlgorithmWatch. 2022. "DSA Explained." AlgorithmWatch. https://algorithmwatch.org/en/dsa-explained.

Al Jazeera. 2024. "Tesla Settles Lawsuit over Fatal Car Crash for Undisclosed Amount." Al Jazeera Economy. https://www.aljazeera.com/economy/2024/4/9/tesla-settles-lawsuit-over-fatal-car-crash-for-undisclosed-amount.

Ambassade de France au Royaume-Uni. n.d. "France's AI Strategy." Accessed June 1, 2025. https://uk.ambafrance.org/France-s-AI-strategy

AIBC. n.d. “AI Winter History.” AIBC Learn Crypto Hub. Accessed May 19, 2025 https://aibc.world/learn-crypto-hub/ai-winter-history.

Arimetrics. n.d. “What is Black Box Algorithm.” Accessed April 6, 2025. https://www.arimetrics.com/en/digital-glossary/black-box-algorithm#:~:text=A%20black%20box%20algorithm,data%20leaks%20and%20unfair%20competition.

Artificial Intelligence Liability Directive. 2022. https://www.ai-liability-directive.com/Artificial_Intelligence_Liability_Directive_Preamble_21_to_33_(Proposal_28.9.2022).

Artificial Intelligence Act. n.d. “High-Level Summary.” ArtificialIntelligenceAct.eu. Accessed May 19, 2025. https://artificialintelligenceact.eu/high-level-summary.

Associated Press. 2021. “Autonomous Vehicle Death: Uber Charge Backup Driver.” AP News. https://apnews.com/article/autonomous-vehicle-death-uber-charge-backup-driver-1c711426a9cf020d3662c47c0dd64e35.

AI-Liability-Directive.com. n.d. AI-Liability-Directive.com. Accessed May 19, 2025. https://www.ai-liability-directive.com.

BABL AI. n.d. “European Parliament Committee Opposes AI Liability Directive, Citing Innovation Risks.” BABL AI. Accessed May 19, 2025. https://babl.ai/european-parliament-committee-opposes-ai-liability-directive-citing-innovation-risks/.

Badman, Annie. 2024. “AI Risk Management.” IBM Think. https://www.ibm.com/think/insights/ai-risk-management.

Batbatzul, Amar. 2024. “Legal Personality for AI in EU Law.” Medium.. https://amarbatbatzul.medium.com/legal-personality-for-ai-in-eu-law-28c13f8fb338.

BBC News. 2020. “US Regulators Approve First Facial Recognition Ban in Technology.” BBC News. https://www.bbc.com/news/technology-54175359.

BBMRI-ERIC. n.d. “Guidelines for Good Research.” ELSI Knowledge Base. Accessed June 10, 2025. https://www.bbmri-eric.eu/elsi-knowledge-base/guidelines-for-good-research.

Berger, Paul. 2019. “What Is Symbolic Artificial Intelligence?” BD Techtalks. https://bdtechtalks.com/2019/11/18/what-is-symbolic-artificial-intelligence.

Brannon, Valerie C., and Eric N. Holmes. “Section 230: An Overview”. CRS Report R46751. Washington, DC: Congressional Research Service, February 2, 2024. Congress.gov. Accessed June 8, 2025. https://www.congress.gov/crs-product/R46751.

Britannica. n.d. “Robotics.” Encyclopaedia Britannica. Accessed May 19, 2025. https://www.britannica.com/technology/robotics.

Britannica. n.d. “Jurisprudence.” Encyclopaedia Britannica. Accessed June 10, 2025. https://www.britannica.com/science/jurisprudence.

BSA & Industry Groups. 2025. “BSA and Industry Groups Call on EU to Withdraw AI Liability Directive.” Business Software Alliance. https://www.bsa.org/news-events/news/bsa-and-industry-groups-call-on-eu-to-withdraw-ai-liability-directive.

Byrne Wallace Shields. n.d. “Withdrawal of the AI Liability Directive.” Byrne Wallace Shields. Accessed May 19, 2025. https://byrnewallaceshields.com/news-and-recent-work/publications/withdrawal-of-the-ai-liability-directive.

CAIDP. n.d. “G20.” CAIDP Resources. Accessed May 19, 2025. https://www.caidp.org/resources/g20/.

Clifford Chance. 2025. “The EU Introduces New Rules on AI Liability.” Accessed April 6, 2025. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2025/01/the-eu-introduces-new-rules-on-ai-liability.pdf

Cornell Law School. n.d. “Tort.” Legal Information Institute, Wex. Accessed June 10, 2025. https://www.law.cornell.edu/wex/tort.

DLA Piper. 2023. “G7 Publishes Guiding Principles and Code of Conduct for Artificial Intelligence.” DLA Piper AI Outlook. https://www.dlapiper.com/en/insights/publications/ai-outlook/2023/g7-publishes-guiding-principles-and-code-of-conduct-for-artificial-intelligence.

Department of Enterprise, Trade and Employment. 2024. “National AI Strategy Refresh 2024.” Accessed May 19, 2025. https://enterprise.gov.ie/en/publications/national-ai-strategy-refresh-2024.html

DLA Piper. n.d. “Liability for Damages Caused by AI.” DLA Piper Law in Tech. Accessed April 6, 2025. https://www.dlapiper.com/en/insights/publications/law-in-tech/liability-for-damages-caused-by-ai.

Dialzara. 2024. “AI Transparency & Accountability: Principles, Differences.” Last modified May 18, 2024. https://dialzara.com/blog/ai-transparency-and-accountability-principles-differences/

Digital Watch Observatory. 2019. “Artificial Intelligence: A Strategic Vision for

Luxembourg." https://dig.watch/resource/artificial-intelligence-a-strategic-vision-for-luxembourg

Digital Watch Observatory. 2019. "Netherlands Strategic Action Plan for Artificial Intelligence." https://dig.watch/resource/netherlands-strategic-action-plan-for-artificial-intelligence

Digital Watch Observatory. 2024. "Romania's National Artificial Intelligence Strategy for 2024-2027." Accessed May 19, 2025. https://dig.watch/resource/romanias-national-artificial-intelligence-strategy-for-2024-2027

Digital Watch Observatory. 2020. "Spain's National Artificial Intelligence Strategy." https://dig.watch/resource/spains-national-artificial-intelligence-strategy

Droese Warns Against Brussels Overreach. n.d. ESN Group News. Accessed May 19, 2025. https://esn-group.eu/news

Doviandi. 2025. "The EU AI Act and Its Implementation in Cyprus." https://www.doviandi.com/eu-ai-act-implementation-cyprus/#

Elastic. n.d. "Artificial Intelligence Regulation in Asia: A Comparative Analysis." Elastic Blog. Accessed May 19, 2025. https://www.elastic.co/blog/artificial-intelligence-regulation-asia-comparative-analysis.

Electropages. 2025. "History of AI: Key Milestones & Impact on Technology." Electropages Blog.https://www.electropages.com/blog/2025/03/history-ai-key-milestones-impact-technology.

Euronews Next. 2025. "European Parliament to Grill Commission over Ditched AI Liability

Rules." Euronews. https://www.euronews.com/next/2025/02/26/european-parliament-to-grill-commission-over-ditched-ai-liability-rules.

European Center for Constitutional and Human Rights (ECCHR). n.d. "Hard Law/Soft Law." ECCHR Glossary. Accessed June 10, 2025. https://www.ecchr.eu/en/glossary/hard-law-soft-law.

European Commission. 2019. "What is an algorithm in AI?." Last modified August 26, 2019. https://ec.europa.eu/futurium/en/european-ai-alliance/what-algorithm-ai.html

European Commission. 2021a. "Bulgaria AI Strategy Report." Last updated September 1, 2021. https://ai-watch.ec.europa.eu/countries/bulgaria/bulgaria-ai-strategy-report_en

European Commission. 2021b. "Germany AI Strategy Report." Last updated September 1, 2021. https://ai-watch.ec.europa.eu/countries/germany/germany-ai-strategy-report_en

European Commission. 2021c."Hungary AI Strategy Report." Last updated September 1, 2021. https://ai-watch.ec.europa.eu/countries/hungary/hungary-ai-strategy-report_en

European Commission. 2021d. "Latvia AI Strategy Report." Last updated September 1, 2021. https://ai-watch.ec.europa.eu/countries/latvia-0/latvia-ai-strategy-report_en

European Commission. 2021e. "Poland AI Strategy Report." Last updated September 1, 2021. https://ai-watch.ec.europa.eu/countries/poland/poland-ai-strategy-report_en

European Commission. 2021f. "Slovakia AI Strategy Report." Last updated September 1, 2021 https://ai-watch.ec.europa.eu/countries/slovakia/slovakia-ai-strategy-report_en

European Commission. 2021g. "Slovenia AI Strategy Report." Last updated September 1, 2021. https://ai-watch.ec.europa.eu/countries/slovenia/slovenia-ai-strategy-report_en

European Commission. 2022. “Questions & Answers: AI Liability Directive.” Last modified September 28, 2022. https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5793

European Commission. n.d.a. "AI Act." Accessed June 5, 2025. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

European Commission. n.d.b. “Liability for defective products.” Accessed April 6, 2025. https://single-market-economy.ec.europa.eu/single-market/goods/free-movement-sectors/liability-defective-products_en

Eurostat. n.d. “Glossary: Information and communication technology (ICT).” Accessed March 20, 2025. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_(ICT)

EU AI Act. 2024. “High-Risk AI Systems Under the EU AI Act.” Last modified August 1, 2024. https://www.euaiact.com/blog/high-risk-ai-systems-under-the-eu-ai-act

Federal Communications Commission. 2024. “FCC Confirms that TCPA Applies to AI Technologies that Generate Human Voices”. https://www.fcc.gov/document/fcc-confirms-tcpa-applies-ai-technologies-generate-human-voices

Fox2Detroit. 2020. “Facial-Recognition False Arrest: Man Detroit Police Wins Settlement.” Fox 2 Detroit. https://www.fox2detroit.com/news/facial-recognition-false-arrest-man-detroit-police-wins-settlement.

Ganon, Dan. 2018. “Uber Video Shows Robot Car in Fatal Accident – Did Backup Driver Miss Red Light?” SFGATE. https://www.sfgate.com/business/article/Uber-video-shows-robot-car-in-fatal-accident-did-12771938.php.

Generative AI Licence & Libel. 2023. Addleshaw Goddard. https://www.addleshawgoddard.com/en/insights/insights-briefings/2023/technology/generative-ai-licence-libel.

Global Legal Insights. n.d. "China: AI, Machine Learning, and Big Data – Laws and Regulations." Global Legal Insights. Accessed May 19, 2025. https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/china.

Gorny & D'Andurand. n.d. "Who Is Responsible after a Collision in a Self-Driving Car?" Gorny & D'Andurand. Accessed April 6, 2025. https://gornydandurand.com/who-is-responsible-after-a-collision-in-a-self-driving-car.

Google Cloud. n.d.a. "What is Machine Learning?." Accessed March 30, 2025. https://cloud.google.com/learn/what-is-machine-learning

Google Cloud. n.d.b. "What are AI hallucinations?." Accessed March 21, 2025. https://cloud.google.com/discover/what-are-ai-hallucinations#

Google Cloud. n.d.c. "GPU for AI." Google Cloud Documentation. Accessed June 10, 2025. https://cloud.google.com/discover/gpu-for-ai.

G2 Learning Center. 2021. "Training Data." G2 Learn. https://learn.g2.com/training-data.

Gozun, Olga. 2018. "Experts Sign Open Letter Slamming Europe's Proposal to …" Gizmodo. https://gizmodo.com/experts-sign-open-letter-slamming-europe-s-proposal-to-1825240003.

History of AI: Key Milestones & Impact on Technology. 2025. Electropages

Blog. https://www.electropages.com/blog/2025/03/history-ai-key-milestones-impact-technology.

IBM. 2021a. “Computer Vision.” IBM Think. https://www.ibm.com/think/topics/computer-vision.

IBM. 2021b. “Machine Learning.” IBM Think. https://www.ibm.com/think/topics/machine-learning.

IBM. 2021c. “Neural Networks.” IBM Think. https://www.ibm.com/think/topics/neural-networks.

IBM. 2023. “Internet of Things (IoT).” IBM Think. https://www.ibm.com/think/topics/internet-of-things.

IBM. 2024a. “Big Data.” IBM Think. https://www.ibm.com/think/topics/big-data.

IBM. 2024b. “Deep Learning.” IBM Think. https://www.ibm.com/think/topics/deep-learning.

IBM. 2024c. “Natural Language Processing.” IBM Think. https://www.ibm.com/think/topics/natural-language-processing

IBM. 2024d. “What is artificial general intelligence (AGI)?.” Last modified September 17, 2024. https://www.ibm.com/think/topics/artificial-general-intelligence

Inside Global Tech. 2025. “The Future of the AI Liability Directive.” Inside Global Tech. https://www.insideglobaltech.com/2025/03/10/the-future-of-the-ai-liability-directive.

Investopedia. n.d. “Tort Law.” Investopedia. Accessed May 19, 2025. https://www.investopedia.com/terms/t/tort-law.asp.

Investopedia. n.d. “Weak AI.” Investopedia. Accessed May 19, 2025. https://www.investopedia.com/terms/w/weak-ai.asp.

Invoca. n.d. “What Is Black-Box AI?” Invoca Blog. Accessed May 19, 2025. https://www.invoca.com/blog/what-is-black-box-ai.

Information Commisioner’s Office. n.d. “What is personal data?.” Accessed March 21, 2025. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/#:~:text=%E2%80%9C'personal%20data'%20means%20any,location%20data%2C%20an%20online%20identifier.

Investopedia. 2025. “Burden of Proof: Meaning, Standards and Examples.” Last modified February 3, 2025. https://www.investopedia.com/terms/b/burden-proof.asp

JustAI. 2024. “AI Regulations and Policies in Croatia.” Accessed May 15, 2025. https://justai.in/ai-regulations-and-policies-in-croatia/

Kennedys Law. 2024. “A New Liability Framework for Products and AI.” Kennedys Thought Leadership. https://kennedyslaw.com/en/thought-leadership/article/2024/a-new-liability-framework-for-products-and-ai/

Kroet, Cynthia. 2025. “Lawmakers Reject Commission Decision to Scrap Planned AI Liability Rules.” Euronews. https://www.euronews.com/next/2025/02/18/lawmakers-reject-commission-decision-to-scrap-planned-ai-liability-rules.

Krol, Evan. 2025. “Expert System.” TechTarget SearchEnterpriseAI. https://www.techtarget.com/searchenterpriseai/definition/expert-system.

Lawfare Media. 2023. “A Comparative Perspective on AI Regulation.”

Lawfare. https://www.lawfaremedia.org/article/a-comparative-perspective-on-ai-regulation.

LexGO. 2024. “ArtificiaI Intelligence in Belgium | Legal State of Play in 2024.” Accessed May 13, 2025. https://www.lexgo.be/en/news-and-articles/13743-artificiai-intelligence-in-belgium-legal-state-of-play-in-2024#

Lexology. 2024. “A general introduction to Artificial Intelligence Law in Portugal.” https://www.lexology.com/library/detail.aspx?g=5708966e-0e5a-4c74-bf6e-015225088cbd

Lexology. 2025. “EU Advances AI Liability Directive to Strengthen Accountability and Harmonize Civil Liability Rules.” Lexology. https://www.lexology.com/library/detail.aspx?g=b890109e-304e-448a-846d-38c54f0c9569.

Liability Based on Fault. 2020. In Light of Law. https://www.inlightoflaw.com/2020/09/liability-based-on-fault.html.

Malta Digital Innovation Authority. 2019. “Malta AI Strategy and Vision.” https://mdia.gov.mt/national-strategies/malta-ai-strategy-and-vision/

Masterson Hall Injury Law. n.d. “Civil vs. Criminal Liability: Key Denver Insights.” Masterson Hall. Accessed June 10, 2025. https://www.mastersonhall.com/civil-vs-criminal-liability-key-denver-insights.

McCarter & English, LLP. 2024. “Artificial Intelligence & Product Liability.” Last modified August 20, 2024. https://www.mccarter.com/insights/artificial-intelligence-product-liability/#:~:text=The%20fundamental%20theory%20of%20product,the%20person%20or%20their%20property.

Ministry of the Economy and Innovation of the Republic of Lithuania. 2024. “Lithuania Aims to Become the Most Favourable Country for the Development of Artificial Intelligence Technologies.” Accessed May 19, 2025. https://eimin.lrv.lt/en/structure-and-contacts/news-1/lithuania-aims-to-become-the-most-favourable-country-for-the-development-of-artificial-intelligence-technologies/

Ministry of Industry and Trade. 2024. “Czechia as a technological leader. Government approved the National Strategy for Artificial Intelligence pf the Czech Republic 2030.” Accessed May 16, 2025. https://mpo.gov.cz/en/guidepost/for-the-media/press-releases/czechia-as-a-technological-leader--government-approved-the-national-strategy-for-artificial-intelligence-of-the-czech-republic-2030--282278/

National Center for Biotechnology Information (NCBI). 2020. Machine Learning in Health Care: A Critical Appraisal of Ethical and Trust Issues. PubMed Central. https://www.ncbi.nlm.nih.gov/articles/PMC7851658.

National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018).

National Law Review. n.d. “Understanding Scope: Artificial Intelligence (AI) System Definition – Key Insights.” The National Law Review. Accessed May 19, 2025. https://natlawreview.com/article/understanding-scope-artificial-intelligence-ai-system-definition-key-insights?amp.

NordForsk. 2024. “Annex 2: National AI Strategies in the Nordic Countries.” https://www.nordforsk.org/node/1377

Norton Rose Fulbright. 2024. “Artificial intelligence and liability: Key takeaways from recent

EU legislative initiatives." Accessed April 7, 2025. https://www.nortonrosefulbright.com/en/knowledge/publications/7052eff6/artificial-intelligence-and-liability

OECD. n.d.a. "AI in Germany." Accessed May 16, 2025. https://oecd.ai/en/dashboards/countries/Germany

OECD. n.d.b. "AI Principles." OECD Topics. Accessed May 19, 2025. https://www.oecd.org/en/topics/sub-issues/ai-principles.

OECD. 2024. "Explanatory Memorandum on the Updated OECD Definiton of an AI System.". https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_3c815e51/623da898-en.pdf

OECD. 2025. "OECD Launches Global Framework to Monitor Application of G7 Hiroshima AI Code of Conduct." OECD News. -https://www.oecd.org/en/about/news/press-releases/2025/02/oecd-launches-global-framework-to-monitor-application-of-g7-hiroshima-ai-code-of-conduct.html

Pearl, R. 2024. "If AI Harms a Patient, Who Gets Sued?" Forbes. https://www.forbes.com/sites/robertpearl/2024/05/06/if-ai-harms-a-patient-who-gets-sued/.

PwC. n.d. "Algorithmic Bias and Trust in AI." PwC Tech Effect. Accessed May 19, 2025. https://www.pwc.com/us/en/tech-effect/ai-analytics/algorithmic-bias-and-trust-in-ai.html.

Politico. 2025. "Europe Divided Over Robot/AI Artificial Intelligence Personhood." Politico

Europe. https://www.politico.eu/article/europe-divided-over-robot-ai-artificial-intelligence-personhood.

Politico. 2024. “Who Pays When Your Doctor’s AI Goes Rogue?” Politico. https://www.politico.com/news/2024/03/24/who-pays-when-your-doctors-ai-goes-rogue-00148447.

RAND Corporation. 2020. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. https://www.rand.org/pubs/research_reports/RRA3243-4.html.

ResearchGate. n.d. “Sketch of the ordinary legislative procedure.” Accessed June 8, 2025. https://www.europarl.europa.eu/cmsdata/293607/Diagram.pdf

Reuters. 2020. “Safety Driver in Fatal Arizona Uber Self-Driving Car Crash Charged with Homicide.” Reuters. https://www.reuters.com/article/world/asia-pacific/safety-driver-in-fatal-arizona-uber-self-driving-car-crash-charged-with-homicide-idUSKBN26708O.

Reuters. 2023. “Tesla Wins Autopilot Trial Involving Fatal Crash.” Reuters.https://www.reuters.com/business/autos-transportation/tesla-wins-autopilot-trial-involving-fatal-crash-2023-10-31 .

Rinaldi, Gian Marco, and Marta Breschi. 2025. “Italian Rules on AI as a Supplement to the AI Act.” *Bird & Bird,* April 29, 2025. https://www.twobirds.com/en/insights/2025/italian-rules-on-ai-as-a-supplement-to-the-ai-act

Robotics-Openletter.eu. n.d. Robotics Open Letter. Accessed May 19, 2025. https://robotics-openletter.eu.

SAS. n.d. “Big Data: What it is and why it matters.” Accessed March 30, 2025.

https://www.sas.com/en_us/insights/big-data/what-is-big-data.html

Sasdelli, Paolo. 2025. “Proposed EU AI Liability Rules Withdrawn.” Bird & Bird. https://www.twobirds.com/en/insights/2025/proposed-eu-ai-liability-rules-withdrawn.

Scarcella, M. 2025. “OpenAI defeats radio host's lawsuit over allegations invented by ChatGPT”. *Reuters*. https://www.reuters.com/legal/litigation/openai-defeats-radio-hosts-lawsuit-over-allegations-invented-by-chatgpt-2025-05-19/

Stanford University. “Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022.” https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022.

Stateline. 2025. “Facial Recognition in Policing Is Getting State-by-State Guardrails.” Stateline. https://stateline.org/2025/02/04/facial-recognition-in-policing-is-getting-state-by-state-guardrails.

SudSud. n.d. “External Commercial Borrowings Framework and Challenges.” SudSud. Accessed June 10, 2025. https://www.sudsud.in/post/external-commercial-borrowings-framework-and-challenges.

Taylor Wessing. 2024. “High-Risk AI Systems.” Taylor Wessing Insights. https://www.taylorwessing.com/en/insights-and-events/insights/2024/11/high-risk-ai-systems.

Taylor Wessing. 2025. “AI Liability: Who Is Accountable When Artificial Intelligence Malfunctions.” Taylor Wessing Insights. https://www.taylorwessing.com/en/insights-and-events/insights/2025/01/ai-liability-who-is-accountable-when-artificial-intelligence-malfunctions.

The Guardian. 2019. “Apple Card Issuer Investigated after Claims of Sexist Credit Checks.” The Guardian. https://www.theguardian.com/technology/2019/nov/10/apple-card-issuer-investigated-after-claims-of-sexist-credit-checks.

The Law Dictionary. n.d. “Contentious.” TheLawDictionary.org. Accessed June 10, 2025. https://thelawdictionary.org/contentious/.

The Legal 500 Country Comparative Guides. 2024. “Sweden: Artificial Intelligence.” Accessed May 19, 2025. https://www.legal500.com/guides/chapter/sweden-artificial-intelligence/

The White House. 2025. “Removing Barriers to American Leadership in Artificial Intelligence”. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

TrustPath. n.d. “AI transparency vs. AI explainability: Where does the difference lie?.” Accessed March 30, 2025. https://www.trustpath.ai/blog/ai-transparency-vs-ai-explainability-where-does-the-difference-lie

UNESCO. n.d. Recommendation on the Ethics of Artificial Intelligence: Key Facts. Accessed May 19, 2025. https://unesco.org.uk/site/assets/files/14137/unesco_recommendation_on_the_ethics_of_artificial_intelligence_-_key_facts.pdf.

United Nations. n.d. “Global Digital Compact.” UN Digital & Emerging Technologies. Accessed May 19, 2025. https://www.un.org/digital-emerging-technologies/global-digital-compact.

U.S. Federal Register. 2023. “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.” Federal Register. https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

Werner, J. 2024. “EU Advances AI Liability Directive to Strengthen Accountability and Harmonize Civil Liability Rules”. Babl. https://babl.ai/eu-advances-ai-liability-directive-to-strengthen-accountability-and-harmonize-civil-liability-rules/

White & Case. n.d. AI Watch: Global Regulatory Tracker – United States. Accessed April 6, 2025. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states.

Vasudevan, Amrita. 2023. “Who Is Liable for AI-Driven Accidents? The Law Is Still Emerging.” Centre for International Governance Innovation. Last modified June 21, 2023. https://www.cigionline.org/articles/who-is-liable-for-ai-driven-accidents-the-law-is-still-emerging

Voigt, Daniel. 2023. “Verfassungskonforme Anatomie eines Falls ?: AI Act, AILD, PLD.” Verfassungsblog. https://verfassungsblog.de/anatomy-of-a-fall-aiact-aild-pld.

INTRODUCTION BIBLIOGRAPHY

European Parliament. 2024a. “The Council of the European Union.” Accessed June 8, 2025. https://www.europarl.europa.eu/factsheets/en/sheet/24/the-council-of-the-european-union

European Parliament. 2024b. “The Ordinary Legislative Procedure - step by step.” Accessed June 8, 2025. https://www.europarl.europa.eu/olp/en/ordinary-legislative-procedure/overview

EUROsimA
2025