الدراسة الثامنة:

AI-related harm and civil liability law: Current challenges and the need for legislative reform

Ahmad Ali Bardan[1]

Introduction

Civil liability connotates the responsibility of a person or entity to compensate another for any harm they have caused[2]. It may be triggered by a breach of a contract, car accidents, professional malpractice, among other scenarios. It is thus viewed as being contingent on someone's failure to meet a certain obligation[3], or on an infringement of someone's legally protected interest. The type of liability that is imposed, however, varies with the specific duty that is breached. In other words, its nature is determined by the source of the obligation in question, whether it originates from an agreement or a statutory provision. Consequently, legal responsibility can vary between contractual and extracontractual (tortious) liability[4].

Meanwhile, the risk of AI causing or contributing to losses has become an undeniable issue for in today's society. Also, the legal

[1] Ph.D. candidate in Private Law at Université Panthéon-Assas, LL.M. in business law (LAU), and associate at Ali Bardan law office.
[2] Etier, G. & Sträuli, B. (2015), p. 14.
[3] Oman, N. (2014), p. 384.
[4] Al-Awji, M. (2019), p. 10; See Al-Sanhouri, A. (1952), p. 653.

system's ability to handle AI-induced damages is being put under scrutiny given the absence of a well-defined liability framework that specifically applies to AI. So far, an aggrieved party can only resort to existing civil liability rules to seek compensation.

The peculiarity of AI technology, nevertheless, has created a challenge in applying these rules that were established long ago and did not anticipate its impact on different stakeholders. Scholars contend that many of the relevant AI-associated lawsuits will be affected by novel and complex technical issues and therefore result in legal uncertainty at the level of courts and litigants alike(1).

Besides, as AI entities are viewed as objects rather than subjects of law to date, an injured party cannot directly sue these systems. Instead, they can only invoke legal actions against individuals or entities associated with the AI system. Accordingly, receiving compensation for the damage incurred hinges on the fulfillment of statutory requirements for the specific type of liability a claimant wishes to base his allegations on, which differs from one situation to another.

1. Contractual liability

Contractual liability is conditional on the occurrence of a breach of a valid contract(2). To be considered valid, the latter must be founded on specific elements. These include an agreement between the parties involved, a lawful reason for the contract, and a licit subject, among other things(3). In our following discussion, we will focus on two aspects of contractual liability. First, the liability that falls upon someone who

(1) See, generally, Pagallo, U. (2022). https://www.adalovelaceinstitute.org/blog/the-way-ahead-on-ai-liability/ (Accessed September 14, 2025).
(2) Kol B'Seder, Inc. v. Certain Underwriters at Lloyd's of London, 766 Fed. Appx. 795, 2019 U.S. App. LEXIS 7160, 2019 AMC 1039, 2019 WL 1130357.
(3) See Art 177, 189 LCOC ; Art 1128 FCC; See Tagnetics, Inc. v. Kayser, 842 Fed. Appx. 969, 2021 U.S. App. LEXIS 986, 2021 FED App. 0033N (6th Cir.), 2021 WL 129071.

uses the AI system to fulfill his contractual obligations (AI user). Second, liability issues related to cases where an AI entity is the subject-matter of contracts, notably in sales-related contexts.

1.1. AI integration into contract performance

Parties engaging in contractual relationships may fulfill their corresponding obligations either by themselves, through the assistance of others, or even by using an automated equipment, e.g., an AI system. Meanwhile, all contractual issues associated with AI systems can only be resolved through existing laws and legal institutions that best address the problem, even if such solution is not optimal(1).

An understanding of the distinct obligations imposed on a user, as a contracting party, is fundamental for determining if any breach has occurred. From a civil law standpoint, these obligations can be classified into two categories: effort obligations (obligations de moyen) and result obligations (obligations de résultat)(2). The former pertains to the obligation to use one's best efforts in carrying out an activity(3), whereas the latter refers to the duty of achieving a specific outcome. In light of that, a breach of contract occurs whenever the debtor's performance falls short of the one that is due.

That being noted, contractual liability is imposed when the following conditions are met: there is a contractual fault(4), damage has occurred, and there is a causal link between the fault and the damage.

From both contractual and non-contractual perspectives, the principal issue centers on the first and third elements. A contractual fault (or a breach) occurs when the party responsible for meeting a specific

(1) Pfeifer-Chomiczewska, K. (2022), p. 63.
(2) See Bellis, K. (2018), p. 327-328.
(3) DiMatteo et al. (2021), p. 41.
(4) A contractual fault typically corresponds to the notion of "breach" in common law systems.

obligation (debtor/obligor) does not perform it entirely, partially, or adequately. This, in turn, represents a violation of the contract's terms. It therefore leads to a failure in achieving the expected outcome as envisaged by the other party (creditor/obligee).

In practice, when it comes to result obligations, the injured party is only required to establish the non-compliance with the contract's provisions, not the debtor's conduct that led to the non- compliance, given the latter it is presumed, and the former is deemed a fault in itself(1). Accordingly, this scenario does not pose a serious hurdle for imposing liability on AI users.

Liability for effort obligations hinges on proving fault by the obligor, meaning the plaintiff must demonstrate a wrongful act by the AI user that leads to incomplete or inadequate performance(2). Legally, "fault" implies a conduct that is both harmful and unlawful(3), either as a breach of legal duties or social norms resulting in damage(4).

Negligence is the primary form of fault here(5), involving a failure to meet a duty of care owed to others. Whether such a duty exists is determined by national courts(6) and its standard is assessed objectively, based on how a reasonable person would have acted in similar circumstances. This is a principle widely applied in Europe(7), Lebanon(8), and the United States.

A clear example of how contractual liability might arise is a lawyer who uses an AI system during the due diligence process. The lawyer's

(1) See Sage, N. (2019), p. 460-61.
(2) Al-Awji, supra note 3, at 32-33; See also Art. 254-255 Lebanese code of obligations and contracts (Hereinafter LCOC).
(3) Syoufi, G. (1994), p. 395.
(4) Al Naqib, A. (1983), p. 123.
(5) Lee, R. (1918), at 725.
(6) Goldberg, J. & Zipursky, B. 2010, p. 77.
(7) Koziol, H. (Ed). (2015), no 8/ 229, p. 787.
(8) See Al-Awji, supra note 3, at 256-258.

obligation to the client remains one of reasonable effort rather than a guaranteed/specific outcome (e.g. securing a favorable verdict). This is because the nature of the obligation is defined by the activity itself, not by the tools employed. However, using AI introduces additional responsibilities specific to the technology. These include selecting a system appropriate for the intended purpose, operating it with the required technical competence, and maintaining its accuracy through timely updates and bug fixes as recommended. Liability could arise, for example, if the lawyer relies on an AI system that is inadequate for the task, especially considering the current limitations of the technology.

Furthermore, lawyers are obligated to thoroughly review and verify any AI-generated content before relying on or submitting it, as failure to do so can lead to liability for breaching the contractual duty of care owed to the client, in addition to facing administrative sanctions and professional malpractice claims. This obligation was confirmed in California, where an attorney was fined $10,000 for filing a state-court appeal containing fabricated ChatGPT-generated quotations that were not checked for accuracy before submission(1).

This incident has resulted in significant institutional reactions as the California judicial council has issued guidelines requiring judges and court staff either to prohibit generative AI outright or to adopt a formal AI use policy. In parallel, the California bar association is considering

(1) Attorneys from Butler Snow (Mississippi) were also caught submitting AI-generated fake case citations in court filings before U.S. District Judge Anna Manasco in Alabama. Similarly, in Mata v. Avianca, Inc., a case before the U.S. District Court for the southern District of New York, the court dismissed a personal injury claim against the airline and imposed a $5,000 fine on the plaintiffs' lawyer for submitting fake AI-generated quotations. See https://www.reuters.com/legal/government/trouble-with-ai-hallucinations-spreads-big-law-firms-2025-05-23/ and https://virtuositylegal.com/ai-in-court-when-legal-tech-goes-rogue-lessons-from-mata-v-avianca/(Accessed Nov 22, 2025). Also, Park v. Kim, No. 22-2057 (2d Cir. 2024).

amendments to its code of conduct to address the professional and ethical implications of AI use.

1.2. AI as the subject matter of the contract

The type of AI-related contracts varies according to the intent of the contracting parties. For instance, sale, lease, or license agreements are commonplace. Another possibility is to conclude contract for specific work (including service agreements) where one person undertakes to fulfill a particular task or render a service for another person in exchange for appropriate remuneration(1), e.g., creating a particular AI system. Alternatively, parties can opt for a sui generis contract that best regulates their needs.

Usually, the party that is contractually bound to provide an AI system undertakes a result obligation. This applies to sales agreements and even covers service contracts in which the client has relied on a contractor's experience in creating an AI system(2). Besides, the obligor-obligee relationship will be governed by the specific provisions such as those of named contracts. Otherwise, the general rules of contract law must apply(3).

Extending that logic, the obligor (seller, contractor, or a software provider) is expected to deliver a functional system in a timely manner pursuant to the contract provisions. Nevertheless, non/partial performance scenarios are not that relevant in the context of AI. These

(1) Art. 624 LCOC; Art. 1710 FCC (referred to as Louage d'ouvrage)

(2) Kindly note that it is generally understood that service contracts impose an obligation of effort, meaning that the obligor is not in breach of contract as long as they have used reasonable skill and judgement. However, the judicial trend in IT contracts, including those related to software development which encompass AI, implies the opposite in both common and civil law jurisdiction; See Schwenzer et al., 2019, p. 318.

(3) Townsend v. Little, 109 U.S. 504, 3 S. Ct. 357, 27 L. Ed. 1012, 1883 U.S. LEXIS 992 (Highlighting that specific provisions serve to qualify and provide exceptions to general provisions)

cases do not really challenge liability rules and can be resolved by referring to the general rules of contract law discussed in the previous section. Consequently, the focus will be on non-conforming AI systems.

Imagine an AI system that was delivered by the debtor, accepted by the creditor, however it turned out that this system failed to meet the anticipated performance standards and subsequently caused harm to the user. This case can illustrate a sub-par contractual performance on the part of the debtor. One might therefore ask: What legal options are available for the damaged to recover compensation?

One potential solution is to invoke express warranties. These are factual affirmations or promises that the debtor has made and are a crucial part of the contract(1). If there are none, implied warranties (guaranties légales) may be used as a safeguard against any defects in the product or service provided(2). These are legal obligations upon the AI provider that exist does not depend on any contractual terms(3). As a result, both types of warranties trigger a compensation scheme for any non-conforming AI.

On the other hand, a defect denotes an imperfection or abnormality that impedes the quality, function, or usefulness of the AI system.(4). Not all flaws, however, are covered by implied warranties. For instance, the ones that are deemed acceptable, or minor, are typically excluded. Courts hence will evaluate the implications of each defect on a case-by-case basis.

---

(1)See Jones, W. (1990), p. 733.

(2) See Art. 442-664 LCOC; Art. 1641 FCC; § 2-314, 2-315 UCC.

(3) Tharp v. Allis-Chalmers Mfg. Co., 42 N.M. 443, 1938-NMSC-044, 81 P.2d 703, 1938 N.M. LEXIS 42, 117 A.L.R. 1344; Bekkevold v. Potts, 173 Minn. 87, 216 N.W. 790, 1927 Minn. LEXIS 1122, 59 A.L.R. 1164

(4) Merriam Webster's definition of defect,
https://www.merriam-webster.com/dictionary/defect (Accessed April 13, 2023);
See also Ibrahim, A. (2018), p. 183; Note that we will address the types of defects in our discussion on the role of product liability law to prevent any redundancy.

In contrast, only significant defects that are unknown to the damaged party may qualify for coverage. These usually reduce the value of the AI system or make it unsuitable to use according to its ordinary purpose. This is known as an implied warranty of merchantability, which is generally determined by comparing a specific good to others of similar kind and price in the market(1). Though this type of warranty typically applies to physical products, courts might use analogies to extend it to non-embedded AI systems(2). Besides, in theory, mass-produced AI systems such as Alexa Echo may not be problematic in this regard, but bespoke systems can pose challenges as there may not be a practical or meaningful point of comparison(3).

In this respect, some critics take an opposite view and argue that the concept of merchantability cannot be applied to software and algorithms as intangible elements, considering that they represent unique ideas and cannot be qualitatively compared to one another(4).

Furthermore, the provider guarantees that the AI system exhibits the necessary features when they had or ought to have had knowledge of the customer's intended use. This is referred to as a warranty for a specific purpose which is recognized in both common and continental legal systems. Courts may be more lenient in applying this type of warranty to software transactions(5), which can cover the software component of an AI system.

Nevertheless, the claimant is required to prove that the defect was present at the time of purchase or delivery, particularly in sales and

(1) Gomulkiewicz, R. W. (1997), p. 396.
(2) Ibid., at 397.
(3) Alces, P. (1999), p. 272.
(4) See Durney, E. (1983), p. 522-23.
(5) Ibid., at 529 (Highlighting that courts have applied this warranty to architectural design, which could apply by analogy to software transactions)

specific work contracts[1]. France, however, adopted a more friendly position towards consumers. If a defect arises within a period 12 months following the supply of digital content (including AI development services) [2], or within 24 months after the delivery of goods containing digital content[3], there is a rebuttable presumption that the flaw existed at the time of delivery or supply. Indeed, such a presumption simplifies the burden of proof placed on the damaged party. Whenever an AI system is defective, determining the time of defect's occurrence is a challenging task for consumers. These systems can learn from new data from the moment they are put into circulation and may change their behavior accordingly.

Though uncommon[4], contracts may specify remedies for AI system failures, which courts will enforce. Absent such terms, law and jurisprudence define available remedies: fixing or replacing the system or seeking a refund or price reduction. The claimant must notify the provider and respect the applicable limitation periods, which vary by jurisdiction[5].

Apart from the previous remedies, the injured party can be awarded compensatory damages. This may apply on the national level when the provider is aware of the defect which is presumed whenever the latter is an expert retailer or manufacturer[6]. In AI cases, however, this presumption might be contested because of the technology's complexity and ongoing development.

---

[1] Art. 445 LCOC; See Abdel-Razak Al-Sanhouri, 1952, part 7 vol.1, p. 99-100; See Ernest E. Fadler Co. v. Hesser, 166 F.2d 904, 1948 U.S. App. LEXIS 2390

[2] Art. L.224-25-16 FCDLC

[3] Art. L.217-7 FCDLC

[4] Chapman, K. & Meurer, M. J. (1989), p. 110.

[5] 30 days in Lebanon (Art 463 LCOC); 4 years pursuant to UCC § 2-725 (yet it varies across different states); Mainly 5 years in France (Art. L110-4 FCCm; Art. 2224 FCC). Kindly note that bodily harm claims are not subject to these periods.

[6] Ibrahim, supra note 26, at 220.

Furthermore, if the provider has explicitly stated that the system is defect-free, or if the client has specifically requested a particular feature to be present in the AI system, compensatory damages are likely to be granted(1). In practice, the first scenario is unlikely to occur as no one will guarantee the absence of any AI-related flaws.

A final point to consider is that there is a significant degree of overlap between the remedies outlined in contract law and those found in the consumer protection regulations(2). The latter play an instrumental role in complementing the liability rules discussed earlier by regulating the unbalanced contractual relationship between two economic actors. On the one hand, the first contracting party encompasses those who distribute, sell, rent, or provide AI products and services as their primary occupation, known as professionals. On the other hand, individuals who purchase or rent products or services for personal use are regarded as consumers, a vulnerable contracting party(3).

These consumer-friendly provisions impose certain obligations on professionals that are of considerable relevance in the realm of AI. For instance, one key principle in comparative consumer law is the duty to provide information to consumers about the optimal way of using the AI system(4), as well as any possible associated risks and limitations(5). This obligation is undoubtedly paramount given the relative novelty of AI technology(6), potential hazards associated with its use, and the high expectations consumers may have of what the purchases system can do.

(1) Ibid, at 221-222.
(2) See Art. 28-29-31-32-33 LCPL (Establishing provisions regarding implied warranty, option of a full refund, etc.)
(3) See 15 U.S. Code § 2301; Art.2 EU Directive 2000/31/EC; Art.2 LCPL.
(4) See Larsen, G. & Lawson, R. (2013), p. 516; Art.4 LCPL; Art. L111-1 FCDLC
(5) Art. 36-37 LCPL
(6) See, generally, Ebers, M. (2021).

Put differently, the compliance with the pre-contractual obligations to inform and inquire placed upon providers and clients respectively, particularly in B2C contracts, can dilute the implications of AI technology by safeguarding the mutual interests of the contracting parties before the occurrence of harm. Therefore, an emphasis should be made on the instructions of use that must elaborate the optimal ways for deploying the system, its main characteristics, its core architecture and functioning structure, in addition to the nature of input data that are compatible with the system's intended purpose.

AI providers should therefore ensure that their system, whether mass produced or custom-made, meets the general safety requirements and sector-specific regulations prior to its deployment. Such compliance entails a conformity assessment, whenever applicable, to ensure that the system is fit for public or professional use. Failure to meet these requirements, resulting in physical harm, constitutes a solid basis for contractual liability against the AI provider[(1)], given that they are legally bound to ensure the safety of consumers when the AI system is properly used.

To conclude, it is inevitable that AI systems will encounter operational inconsistencies, failures, and glitches and therefore we must acknowledge that the perfect design does not and may not ever exist. As a corollary, contracting parties are highly encouraged to agree what does constitute a design defect that qualifies for a warranty, or at least to settle on clear standards based on which defectiveness could be assessed. (e.g., comparing the performance of the system in the situation under investigation with that of another in the same situation

[(1)]Art 46 LCPL; See Al-Awji, supra note 3, at 41.

- comparing the overall outcomes of the system with those of another system[1]).

2. Non contractual liability

As is often the case, the damaged party may not have a contractual tie with the seller, manufacturer, or user of the AI system. Therefore, there won't be any contract-related provisions to govern the harm induced by the said system. Nevertheless, seeking compensation is still possible if a breach of non-contractual obligations occurs. The latter are prescribed by the law, and they are not contingent upon any voluntary transactions[2]. They safeguard individuals' legally protected status quo, including their bodily and personality integrity, property rights, and other similar interests.

In essence, three primary regimes fall within the scope of extra-contractual: liability for one's own actions, for the actions of things or animals, and for the actions of others. In this section, we will analyze the applicability of each regime on AI-related damages, either by direct reference or by employing an analogical reasoning.

2.1. Liability for one's own actions

This liability regime is recognized as being the default option by which a victim can seek compensation[3]. As it is based on fault, it serves a twofold purpose. From one angle, it provides compensation to victims

[1] See Borghetti, J. S. (2019), p. 98-99 (These options were discussed in the context of product liability. Borghetti contends that defectiveness should not be assessed according to the above standards. However, pursuant to the principle of contractual freedom, contracting parties can introduce such a criterion which could ease the assessment of defectiveness in design)

[2] Jansen, N. (2010).

[3] Zech, H. (2021), p. 151.

of reproached conduct ex post. From another angle, it essentially guides the public's conduct to prevent any potential damage ex ante[1].

Accordingly, individuals are responsible for compensating any losses that result from their wrongful actions, irrespective of whether such deeds are intentional or not (délit / quasi-délit)[2]. Nevertheless, a successful fault-based claim entails that the claimant provides evidence of the existence of three elements: an unlawful act, a damage, and a causal link between the first two.

In this respect, Article 122 LCOC laid down the following general rule: Whenever a person causes an illicit harm to someone else's interests, they must compensate for the damages if they had the ability to discern such consequences. Moreover, the following article clarifies that a person is also liable if their negligence or lack of prudence results in harming others. The same rules can be also found under French law[3]. As such, faulty behavior and causal nexus considerations prove to be key factors in establishing civil liability for someone's actions or omissions[4].

The Lebanese civil code permits compensation for both direct and indirect harm, provided the delict or quasi-delict can be linked to it. This suggests the adoption of the productive (or adequate) cause theory. To clarify, the event that made the damage objectively foreseeable qualifies as a legal cause of the harm. An individual therefore is liable for his actions if they directly contributed to or resulted in the occurrence of damage provided that this outcome materialized in the ordinary courses of events.

---

[1] See, generally, Askeland et al. (2015).
[2] Evas, T. (2020), p. 12.
[3] Art. 1240-1241 FCC.
[4] Kindly refer to section 1.1, as the principles and challenges surrounding fault in effort obligations also apply to non-contractual liability.

Conversely, the concept of equivalency of causes was rejected in civil matters, although being recognized in criminal law[1]. This theory identifies the legal cause as any event without which the damage would not have occurred, which is known as "conditio sine qua non" principle. This doctrine is equivalent to the "but for" test used in the United States[2].

Expanding on this comparative viewpoint, French courts tend to take a pragmatic approach. The Court of Cassation may apply either theory depending on the desired result: when it wishes to find a tortfeasor at all costs, the causality concept is extended by invoking the theory of equivalence of conditions[3].

The applicability of the standard fault-based liability (liability for one's own action) to any AI-associated loss depends on whether there are any alternative and more suitable legal option for the aggrieved party to exercise. If strict liability rules have a limited scope or are absent, one can only invoke this default principle as a foundation for any claim.

Nonetheless, not every fault-based claim is bound to be successful. If the AI system requires minimal or no human intervention at all, then the fault may not be attributed to the human user. Besides, even if a fault can be attributed, the determination that a specific wrongful act done by the user, such as lack of monitoring or maintenance, is the reason behind the occurrence of harm seems problematic.

When an AI system functions, it includes inherent processes that accompany and follow the human user's actions. These processes are in turn influenced by both internal and external factors that are totally

[1] Art. 204 Lebanese Penal Law.
[2] See Wright, R. (1985), p. 1775.
[3] French Court of Cassation, civil chamber 2, 27/3/ 2003, No. 01-00.850.

independent from the conduct of the operator[1]. As a consequence, it may be challenging to prove the existence of a causal connection between that conduct and the damage.

Another point to consider is that the response of the AI system to the user's input is not foreseeable as much as it is in the case of traditional IT applications. Courts may thus face difficulties in determining the applicable standard of care (the behavior of the average person) in such cases, as well as any deviation from such a standard.

To illustrate these principles in practice, consider a recent case from Sorbonne University involving the use of an AI-generated content detector. A student was suspended for six months after allegedly using an AI system to write her master's thesis and the administrative court of Montreuil upheld the university's decision. In fact, the university relied on an AI-detection tool that indicated a 99.2% probability the abstract was AI-generated, a finding the student did not contest[2]. However, the thesis' supervisor also noted a writing style inconsistent with the student's usual proficiency, further supporting the suspicion.

This case raises questions on the ethical use of AI and the reliability of such detection tools in academia. A 2023 Stanford study revealed significant limitations, showing that these detectors often misclassify non-native English writing as AI-generated, falsely flagging over 61% of TOEFL essays, while demonstrating near-perfect accuracy with native texts[3]. From a technical perspective, such false positives can occur across languages, underscoring the risk of erroneous conclusions if reliance on these technologies is uncritical.

---

[1] European Commission, Karner et al. (2021), p. 48, https://data.europa.eu/doi/10.2838/77360 (Accessed September 14, 2025)
[2] Administrative Court of Montreuil, 8th Chamber, October 8, 2025, No. 2405656.
[3] Liang, W., et al. (2023). GPT detectors are biased against non-native English writers. https://arxiv.org/abs/2304.02819 (Accessed Nov 22, 2025)

We can also draw of the same lawsuit to conclude how a fault-based liability claim could arise in a non-contractual setting between a student and a professor, where the professor is expected to exercise a duty of care by using up-to-date AI detection tools responsibly and by supplementing their assessment with additional methods rather than relying exclusively on AI results.

Another relevant case from China, although arising as a copyright infringement dispute, this type of liability is rooted in fault-based liability (A plaintiff must show that the defendant committed a wrongful act: reproduction, distribution, etc..). In this case, the court treated the AI operator as having a duty of care to prevent its generative AI system from producing infringing outputs.

To summarize, the Guangzhou internet court held that the AI operator[(1)]:

a. Should have reasonably foreseen the risk that generative AI may produce infringing derivative works (foreseeability);
b. Had the technical ability to prevent the harm through filtering or monitoring mechanisms (preventability);
c. Failed to adopt reasonable safeguards to address these risks (wrongful act); and
d. This failure directly resulted in the generation of infringing outputs (causation).

[(1)] Guangzhou Internet Court. (2024, Feb. 8). Shanghai Character License Administrative Co., Ltd. v. Anonymous AI Company (Case No. 2024 Yue 0192 Minchu 113). Similarly in the U.S, Andersen v. Stability AI Ltd., No. 23-cv-00201-WHO, 2024 WL 3823234 (N.D. Cal. Aug. 12, 2024) where the court permitted key copyright infringement claims to move forward, with trial currently scheduled for Sep. 2026. Similar cases also in Disney & Universal v. Midjourney (AI image generator produces unauthorized images of copyrighted characters) ; UMG, Sony, Warner Recording Labels v. Suno & Udio. (AI generated songs that closely resemble copyrighted recordings)

2.2. Liability for things' actions

The strict liability model represents a deviation from the standard regime of fault. It usually entails a presumption of a fault against someone whenever a certain damage occurs. In other instances, it may not even be contingent upon the concept of fault per se. Considering that it is an exception, strict liability only applies in specific and well-defined scenarios. As for its purpose, it simplifies the legal process, eases the compensation of victims, and ensures accountability.

Under Lebanese law, the liability arising from the actions of things is founded on the concept of guardianship. It is deemed an objective liability (responsabilité objective) and therefore it is not contingent upon the existence of a fault(1). The custodian of the thing is presumed to be liable whenever a damage occurs from the thing's actions, regardless of whether he committed a wrongful act(2).

From a comparative perspective, some jurisdictions justify imposing this type of liability based on the theory of risk which is a doctrine that holds someone liable because of his engagement in activities that present a risk to others(3). In other legal systems, this liability is based on an irrefutable fault of the part of the custodian(4).

The foundation thus varies although the implications are quite the same. A damaged party is entitled to remedies if it identifies the guardian of the thing, while establishing the causal link between the act of the thing in question and the resulting damage.

(1) Art.131 LCOC: The custodian of inanimate things is responsible for the resulting damages, even if they are not under his actual control or supervision …This objective liability shall only be lifted if the custodian proves the existence of irresistible force or the fault of the victim. It is not sufficient for the custodian to prove that he did not commit a fault".
(2) See Reid, E. (1999), p. 743; Also Al-Awji, supra note 3, at 592.
(3) Buyuksagis, E. & Van Boom, W. (2012), p. 612.
(4) See Al-Awji, supra note 3, at 593-596, citing H.L.J. Mazeaud, Leçons de droit civil, tome 2, no. 539; Al-Sanhouri, supra note 3, at 1096; In Italy and Portugal, this is a presumed fault-based liability.

2.2.1. The notion of "thing"

The Lebanese legislator did not provide any indication of what can fall under the category of things. One can conclude that this notion encompasses both tangibles and intangibles without regard to any risk and defectiveness considerations. Also, it extends to cover objects that may independently cause harm as well as the ones operated by humans[1]. Accordingly, an AI system falls within this notion, irrespective of whether it is embodied or not.

In terms of comparison, the regulations in France are quite similar. Art.1242 FCC laid down a general clause for strict liability [2], although it does not cover defective products and motor vehicles which are subject to specific provisions[3]. Meanwhile, in some EU jurisdictions, a thing can only be of a tangible nature [4], thereby software or non-embodied AI systems falls outside this notion.

Meanwhile, holding someone liable for the actions of a thing require that the latter has actively contributed to the incurred harm[5], meaning that the latter would not have occurred without the thing's action. A thing can also be viewed as having an active role when it behaves abnormally or in an unconventional manner[6], even if a physical contact is lacking, provided that it contributes to the occurrence of damages.

2.2.2. The concept of guardianship

(1) See Viney, G. & Jourdain, P. (2006), p. 682.
(2) Art.1242 FCC: "We are responsible not only for the damage caused by our own act, but also for that which is caused by the act.. of things that are in our custody".
(3) Art. 1245 FCC regulates defective products, while the Badinter Law governs land motorized vehicles.
(4) See Evas, supra note 49, at 14-17.
(5) Hoteit, A. (2006), p. 356.
(6) Van Dam, C. (2013), p. 63.

The second element of this liability regime revolves around guardianship. Legal scholarship has highlighted that this concept entails the following attributes: The power to use, control and oversight the actions of the thing in question. Being a guardian therefore can be described as playing a factual role rather than a legal one, which does not always require a constant physical possession of the thing(1).

As such, the person who was able to manage and direct the thing before the occurrence of the harm will be strictly liable. Nonetheless, jurisprudence has distinguished between two settings: custodianship of conduct and that of composition or structure(2). In most cases, these two attributes are tied with a single person, who is usually the owner.

In contrast, courts may hold either of the previous custodians liable. To illustrate, a manufacturer, as guardian of composition, will remain responsible for any harm incurred due to an inherent flaw in the product they made. Therefore, one can conclude that whenever the user has a limited control on the conduct of the thing, liability may shift towards the custodian of structure.

A similar approach to the division of guardianship was adopted by the EU Parliament with respect to AI technology. A recent resolution has introduced the notion of operator which encompasses the front-end operator, akin to the guardian of conduct, who controls to a certain degree the risks of the AI system while gaining from its operation(3). In parallel, the back-end operator, like the guardian of structure, defines the features of the said system, while also supplying data and support and supervising the risk associated with its functioning.

(1) Al-Awji, supra note 3, at 544-546.
(2) Abou Diya, W. (2014) (referring to Cour de cassation (LB), decision dated 10/6/1969, published in the Bulletin, 1970, p. 1159);
(3) Art.3, EU parliament resolution of 20/10/2020 with recommendations to the Commission on a civil liability regime for AI.

2.2.3. The guardian of AI systems

At the outset, strict liability for things seems more appropriate to apply in the context of AI technology when compared to the default delictual liability given that proving fault is not required. However, with the increasing autonomy of AI systems, liability is likely to shift from the guardian of conduct to the guardian of composition. This might be justified by the fact that it would be unfair to hold ordinary users (Front-end operators) liable for a behavior they could not control nor prevent. Nevertheless, such a shift might disincentivize innovation which is necessary to the development of the AI field.

Moreover, there exist various actors who can fit the description of a guardian of composition. For instance, each of the manufacturing companies, the software designer and the person providing the learning data (Back-end operators) exercises a degree of control on the risks related to the operation of the AI system. Accordingly, unless we treat the final producer who put the system into the market as a guardian of structure, it appears challenging for the damaged party to identify the true guardian. Adding to this complexity, the liability of that guardian, at least in Lebanon, is contingent upon proving the existence of an inherent defect, which could also be hard to establish(1).

2.3. AI deployment as a high-risk activity

The rules concerning dangerous activities are not expressly articulated in the Lebanese civil code. One can justify this reality in view of the provisions governing the liability for things which can be extended by courts to encompass such activities if needed. Regardless, these activities hold a significant position in foreign legislation in the

(1) Kindly refer to section 1.2. on the hurdles of proving a defect.

context of AI, particularly because of the EU proposal to adopt a risk-based approach with respect to AI systems.

US legislators have not applied strict liability in a broad manner, and instead, recognized a limited number of activities that are highly dangerous(1). Courts, however, can broaden the scope of this concept to novel scenarios if needed. At present, only a restricted number of activities are covered, especially those that pose a risk that cannot be entirely controlled by humans, e.g., nuclear power generation, blasting, hazardous waste processing(2).

In reference to the EU, countries can be divided into two main groups in the context of dangerous activities. The first one represents the open legal systems within which dangerous activities can be interpreted broadly by the courts such as Italy and Portugal. On the other hand, the second group applies strict liability in limited cases including technological risks and dangerous products, e.g., France, Germany, Spain(3).

The no-fault liability concept may apply prima facie in the case of harm caused by AI if it is linked to any of the previously mentioned hazardous activities.

Moreover, some have suggested that the AI technology can be interpreted to fit the description of a significant source of danger(4). To clarify, over the course of the system's operation, it analyzes vast amounts of data, reaches conclusions, and then acts appropriately while exhibiting a black box effect. This can be regarded as a dangerous activity by courts, especially within open legal systems.

(1) See Restatement (third) of torts, § 20; Restatement (second) of torts § 519(1); § 520.
(2) Green, B. (2022), p. 490.
(3) Evas, supra note 49, at 19-22 (e.g. pharmaceutical manufacturing, electricity and atomic energy, explosives and toxic substances..).
(4) See Čerka et al., p. 386.

2.4. The analogy of AI systems and animals

AI entities are already demonstrating risky, erratic, and unpredictable conduct in various fields of application. In this sense, this conduct resembles that of an animal. In addition, both cannot fully communicate with humans given their limited abilities. Besides, these entities are intentionally designed to look and behave like animals, as exemplified by the Boston Dynamics Robot Dog and Paro the baby seal.

As such, some scholars have suggested treating these intelligent systems as animals in the context of civil liability(1). This proposal implies that the legal system needs to classify them as either pets or wild animals. This distinction is somehow founded on how predictable the behavior of these animals is, especially since the behavior of pets is generally more predictable. Accordingly, the predictability factor can also be applicable in the context of AI, as there exists a wide range of AI applications and techniques.

In Lebanon and several European Union (EU) countries, including France and Italy, animal keepers are subject to strict liability for damages caused by their animals(2). This liability is mainly based on the principle of guardianship, which is analogous to liability for the actions of things. As a result, the aforementioned rules also apply in this case.

Things are nevertheless different in the US. The foundation of this liability varies depending on the type of animal involved(3). For wild animals, strict liability is justified because their owners expose others to abnormal risks. In contrast, for pets, liability is determined under the concept of scienter. If the owner of a pet has knowledge of its dangerous

(1) See U.S. Chamber Institute for Legal Reform, p. 18, https://instituteforlegalreform.com/wp-content/uploads/2020/11/EU-AI-Paper-Final.pdf (Accessed September 14, 2025).
(2) Art. 129 LCOC; See Evas, supra note 49, at 23.
(3) See U.S Restatement (Second) of torts, § 506.

propensity to cause harm or damage to humans, they will be held strictly liable [1]. The owner's liability also extends if they should have known or had reason to believe that the animal possessed a dangerous trait or propensity that was not typical of its species.

The distinction between domesticated and non-domesticated animals has no legal consequence within our legal system. The reason for this is that strict liability applies to keepers irrespective of the type of animal involved, therefore it will apply to all guardians of AI systems. Nevertheless, this distinction can complicate matters in jurisdictions that embrace such a differentiation[2].

First, it appears unjust to automatically treat all AI entities as if they were inherently dangerous, especially the ones whose functions are limited and subsequently do not harm any risk to humans. Besides, the main cause for the recognition of animals' liability by most jurisdictions was the increasing bodily harm caused by animals, whereas AI systems can trigger all sorts of harm including pure economic loss.

Furthermore, one may question how the hazardousness of these systems will be evaluated. Some experts have already proposed that this distinction should be founded on either the intended function of the system in question, or on its operational history[3]. However, it remains challenging to embrace a well-defined and widely recognized criteria.

Lastly, determining that AI entities' behavior inclines towards aggressive and harmful actions is complicated. In many instances, the inner workings of the system are not transparent. Also, the latter might exhibit an unexpected behavior as a result of its learning process or because of a malfunction[4].

---

[1] Scherer, M. (2018), p. 282.
[2] Example: countries like the US, Estonia, Slovenia, Hungary, and Germany; See Evas, supra note 51, at 25.
[3] Scherer, supra note 80, at 283.
[4] Chopra & White (2011), p. 131.

2.5. The applicability of vicarious liability

A proposition has been put forth suggesting that people who use AI-based technologies should be liable for any harm incurred on the basis of an analogy to the concept of vicarious liability(1), which entails being held responsible for the actions of another person(2). Proponents of this proposal contend that if a person can be liable for the wrongdoing of a human assistant, then there is no reason why we should impose the same liability regime if such a person benefits from the operations conducted by a non-human auxiliary(3).

As per the Lebanese civil code, the list of cases where vicarious liability apply is exhaustive. It is thus restricted by legal parameters that courts cannot deviate from (4). Courts cannot extend the application of this legal regime to new scenarios beyond those enumerated hereinafter.

Art. 125 LCOC stipulates that a person is liable for the harm caused by a specific group of people for whom they are responsible. According to the subsequent two articles, this group encompasses the following:

a- The responsibility of parents and custodians for minors under their supervision or authority.
b- Teachers and craftsmen are responsible for their students or trainees.
c- Masters and employers are liable for the harm caused by employers and agents whenever they are conducting a work-related task (Respondeat Superior Doctrine).

The first two cases do not directly pertain to the said proposal; hence they will be disregarded. As for the third case, although it is the most appropriate analogy, it still introduces some challenges. This can be

(1) See, generally, Diamantis, M. (2021); Glavaničová, D. & Pascucci, M. (2022), p. 28; Čerka et al., (2015).
(2) Giliker, P. (2010), p.10.
(3) See Beckers, A. & Teubner, G. (2021), p. 139.
(4) Art. 126-127 LCOC.

reasoned by the fact that this approach comes with its own limitations, particularly since it represents an attempt to make a connection between two heterogenous things. In other words, it remains an analogy that is not fully customized to address the subject under scrutiny.

In any case, this liability framework assumes the existence of certain conditions. At the outset, a relationship of subordination between the principal (master/employer) and the AI entity(1). In general, such a relationship can be found in employment agreements. The latter entails the authority of the principal to supervise and manage the auxiliary (employee/agent) while tasking them with various work-related assignments. Meanwhile, the auxiliary is usually hired given that they possess the required qualifications or capabilities to complete the job.

This scenario can be mirrored in many current applications of AI. One can argue that subordination can be triggered when the system is deployed by the owner. Besides, the said entity can demonstrate some autonomous behavior, all while being tasked with duties that are compatible with its design, purpose, and limitations, which is also applicable with regard to any human auxiliary.

Nevertheless, some contend that the principal-agent relationship in the context of AI is unpalatable, especially with the lack of explicit employment regulations for machines. The EU parliament, however, has suggested the expansion of vicarious liability to include AI-applications whenever they are used in lieu of human agents. This suggestion introduces the principle of functional equivalence, which implies that if the AI entity is used akin to individuals from a functional perspective, vicarious liability could apply.

Regardless, one should bear in mind that the subordination relationship exists solely between a legal person, acting as a principal,

(1) See Al Naqib, A. (1987), p. 113.

and a natural person, serving as an agent. As such, vicarious liability does not cover non-human agents according to the established legal guidelines. Therefore, without amending the relevant provisions, it appears that AI entities cannot fit within this framework. This, in turn, requires ascribing legal personhood to these systems.

Also, vicarious liability is contingent upon proving a fault on the part of the auxiliary, such as negligence. This requirement is valid within Lebanon, France, and the USA[1]. In consequence, the following question arises: How can the fault of these systems be determined?

Tortious liability (Responsabilité délictuelle) primarily focuses on human conduct given that notions like prudence, care, recklessness, and intention play critical roles in liability law. Besides, when courts assess the fault of someone, they compare their conduct to the average person as stated earlier, therefore one may question the applicable reference in the case of AI systems. Should we compare them to humans regardless of the inherent differences?

In this respect, there are calls to evaluate the performance of these systems by comparison to the standard set of human auxiliaries, and if their capabilities exceed that of humans, the focus should move toward comparing them with the performance of available technology[2].

3. Product liability

Product liability represents a comprehensive and technology-neutral framework designed to safeguard consumers and ensure the safety of products[3]. This principle has been embraced at both the national level and in Europe through the Product Liability Directive (PLD) of 1985,

---

[1] Giliker, supra note 101, at 27.
[2] See Abbott, R. (2018), p. 35-36.
[3] See, generally, Com. staff working document, Evaluation of council Directive 85/374/EEC, 2018.

as well as in the United States via the Restatement (Second) of Torts[1]. Historically, this regime focused on imposing legal accountability on manufacturers of finished products or component parts, and in some cases, sellers or distributors, for harm caused to consumers due to defective products. Accordingly, those may be held liable irrespective of any contractual ties existing between them and the injured party. The latter, however, must prove the existence of a defect, the occurrence of harm, and a causal connection between the two[2].

3.1. Scope of applicability

Nationally, the main function of the consumer protection law is to regulate the legal relationship between consumers and manufacturers, or professionals. Although it primarily addresses the contractual aspect of this relationship[3], it also carries a non-contractual dimension as it regulates the legal implications of defective products or services.

The LCPL defines a product as any movable or immovable property (bien), whereas a service denotes any work that involves technical, artisanal, or intellectual activities[4]. Such a differentiation does not provide any legal significance because the same liability rules apply, no matter whether the harm was caused by a flawed product or service[5].

Under the 1985 European product liability directive, the definition of a product aligned closely with national approaches but explicitly excluded services, leaving service provider liability unaddressed[6]. This limitation created legal uncertainty regarding non-tangible items

[1] Scherer, supra note 80, at 280 citing US Restatement (2nd) of torts, § 402A(1)–(2).
[2] See Art.43-106 LCPL; Art.10 EU Directive 2024/2853.
[3] Kindly refer to section 1.2 which touches upon the contractual aspect of the LCPL.
[4] Art.1 LCPL.
[5] Art. 106 LCPL.
[6] Bertolini, A. (2020), p 57 (Although the Court of justice has held that the PLD's provisions apply to products used while providing any service).

such as non-embedded software and algorithms, which were not considered products. The U.S. approach similarly focuses on tangible personal property, although courts have occasionally expanded this to include non-tangible items, which could encompass non-embodied AI systems(1).

The revised PLD, however, have broadened the concept of "product", explicitly including all movables, electricity, raw materials, digital manufacturing files, software (with AI systems included as a corollary), even when integrated or interconnected with other products(2). This expansion closes gaps for non-tangible and digital products, ensuring liability for emerging technologies and aligning EU law with modern innovation. It also broadened the scope of recoverable damages considering the addition of non-material harm and loss/corruption of personal data to the old list which once only covered material harm caused by death, personal injury, or property damage (excluding the defective product itself). Also, the minimum threshold of 500 euros for material damage has been removed(3).

The LCPL, in turn, allows compensation for all types of harm, including pure economic loss, provided it arises from a defective product or service. The U.S. system shares limitations and damages caps with pure economic loss being typically excluded(4).

However, the 2024 EU Directive broadened recoverable damages, adding non-material harm, in so far as they can be compensated for

(1) Armour, J. & Humphrey, W. (1993), p.7.
(2) Art.4 EU Directive 2024/2853.
(3) Art. 9 of the 1985 PLD vs Art. 6 (1) a-b-c of the revised PLD.
(4) See Product liability laws and regulations USA, https://iclg.com/practice-areas/product-liability-laws-and-regulations/usa (Accessed September 14, 2025). Although a recent decision from a US Court demonstrates its willingness to consider AI software and applications as products under strict products liability principles. Garcia v. Character Technologies, Inc., 6:24-cv-01903, (M.D. Fla.), filed Oct. 22, 2024.
https://www.mofo.com/resources/ insights/250618-software-gains-new-status-as-a-product-under-strict-liability-law(Accesses Nov 23, 2025)

under national law, and, reflecting the realities of AI and digital products[1].

3.2. Nature of defects

Legal scholarship emphasizes three primary factors for product liability: manufacturing defects, failure to provide adequate instructions or warnings to users, and design defects[2]. In each one of these scenarios, defectiveness is closely related to the concept of safety that an average consumer would typically expect[3], rather than the fitness for use which is tied with contractual liability.

Meanwhile, if an item deviates in some material way from the intended design or performance standard and fails to align with the remaining products within the same series, it would be classified as a manufacturing defect[4]. The likelihood of such occurrences, however, has significantly diminished nowadays due to the use of advanced manufacturing software.

The second scenario represents cases where the provision of adequate instructions and warnings could have reduced or avoided product risks. Thus, failure to do so would result in an information defect[5]. In contrast, the third trigger of liability is the actual design of the product that fails to ensure the necessary level of safety that a typical consumer would expect or poses an unreasonable risk[6].

One of the challenges that arises when applying product liability to AI harm revolves around the concept of unpredictability. When it comes

(1) Art.6 EU Directive 2024/2853.
(2) Rachum-Twaig, O. (2020), p. 1155; Bertolini, supra note 97, at 52.
(3) Art. 43 LCPL; Art.6 PLD.
(4) See Wheeler v. Ho Sports, Inc., 232 F.3d 754, 2000 U.S. App. LEXIS 27820, CCH Prod. Liab. Rep. P15,946, 2000 Colo. J. C.A.R. 6159.
(5) See Pittenger, M. (1992), p. 1509.
(6) Owen, D. G. (2008), p. 929-930 (Note that the consumer expectation test is widely recognized in common law systems, along with the risk-utility test).

to information defects, claiming that users should have been informed about the risky behavior of an AI system implies that such risks were foreseeable, which is often not the case. The AI component is capable of learning and evolving from the moment the product is activated, which can lead to unexpected behavior(1). Producers thus may be held liable even if they were unable to take sufficient precautions to mitigate the risk through ex ante warnings, as these risks were unpredictable. In contrast, producers could list all sorts of potential risks and flaws associated with the use of the AI system, thereby nullifying the basis of this argument.

The second predicament concerns the uncertainty and ambiguity that surrounds the ceiling of consumers' expectations. It is arguable, for example, if there exists a criterion for determining how an AI system would be deemed safe from the perspective of an average consumer(2). This point may be subject to open interpretation and lead to future disputes concerning the appropriate benchmark. Besides, one should consider the fact that AI systems are diverse, ranging from low to high complexity. The same can be said about consumers, who cannot be simply deemed as average rational adults.

Given these facts, one can argue that the standard for assessing defectiveness should be based on a different criterion. For instance, the intended functionality of the system serves as a potential reference. This is rooted in the fact that when dealing with a complex AI system, we cannot understand what level of safety to expect, however its purpose is easy to identify a priori, as well as any abnormality in its functioning.

What is more, proving a design defect and subsequent a causal nexus with the resulting harm may be an arduous task given the need for

(1) Lemley, M. & Casey, B. (2019), p. 1324-1326.
(2) Buiten et al. (2023), p. 105794.

technical expertise and data access[1]. The former can be costly for consumers, whereas the latter may not be guaranteed. Also, some AI entities perform in an interconnected environment, where their normal functioning relies on various and possibly AI-based machines[2]. This can add another layer to the liability puzzle as the damage may be caused by an external defect, let alone the evolving nature of these systems, such as the ones founded on deep learning techniques, which hinders proving the existence of an inherent flaw that emerged before the product was put into circulation[3].

To address these challenges, the EU legislator has introduced targeted mechanisms in the new product liability directive. It established a disclosure of evidence obligation, which empowers courts to require defendants to provide evidence relevant to the claim. It also allowed defendants to request evidence from claimants that it is necessary to defend against the action[4].

This disclosure, however, is strictly limited to what is necessary and proportionate, with safeguards to protect trade secrets and confidential information. Additionally, courts may require that evidence be presented in a clear, accessible, and understandable format. Consequently, the technical complexity inherent in AI systems may not obstruct fair adjudication.

The EU legislation has also introduced presumptions, which represent an exception to traditional liability principles governing the burden of proof, where claimants are required to prove defectiveness and causation. The new Directive established these presumptions to

(1) Kindly note that in the US, the claimant may be required to show that a safer alternative design is feasible; See Wade, J. (1980), p. 575.
(2) See Buiten et al. (2021), p. 26.
(3) Benhamou, Y., & Ferland, J. (2021)., p. 171.
(4) Art. 9 of the revised EU product liability directive.

alleviate the evidential challenges faced by the damaged party, which may prove useful in cases involving AI systems as products.

Accordingly, a defect may be presumed if the defendant fails to disclose relevant evidence as stipulated in the new directive, provided the claimant has presented sufficient facts and evidence to support the plausibility of their claim. Presumptions may also apply if the product violates mandatory safety requirements or if the damage results from an obvious malfunction during ordinary use.

Moreover, courts shall presume defectiveness or causation, or both, in situations where technical or scientific complexity makes proof excessively difficult, provided that the claimant demonstrates that it is likely the product is defective or that a causal link exists, or both. At the same time, defendants retain the right to rebut these presumptions, ensuring a fair balance between consumer protection and the rights of defendants.

These provisions are complemented by transparency obligation for AI producers, including documentation of algorithms, training datasets, and software updates, which enhance accountability and facilitate litigation. Collectively, the directive establishes a balanced framework that protects consumers from the unique risks of AI systems, ensures fairness in the evidentiary process, and recognizes the evolving nature of modern technology, positioning it ahead of Lebanon's and the United States' regulations.

A recent case brings these issues into focus, with claims of defective design and negligence brought against OpenAI, the company behind ChatGPT[1]. Plaintiffs argue that the AI's design led to the suicide of a young boy considering it lacked the necessary safeguards to prevent the

[1] Shamblin et al. v. OpenAI, Inc. et al., No. 25STCV32382 (filed on Nov 06, 2025 before the Superior court of California, county of Los Angele).

AI system from providing encouraging responses when the boy expressed suicidal thoughts and emotional distress. It remains to be seen, nevertheless, how defectiveness and the scope of the duty of care imposed on the developers will be evaluated by the court.

4. Shaping effective policy for AI-induced harm

The impact of AI on liability law can be viewed in a binary manner. The first problem revolves around the legal uncertainty surrounding the allocation of AI-risks. The implications resulting from the application of the general rules of proof amid the lack of AI-specific regulations are unpromising to say the least. In practice, these obstacles affect the victim, the potential liable person, and courts alike, as the application of traditional liability rules to AI technology continues to be complex and open to varying interpretations.

The second downside relates to the lack of social trust among the public, especially AI users, which prevents or hampers both the emergence and uptake of AI-applications(1). When compared with traditional technologies, the damaged party is concerned about the lack of compensation for harm incurred in view of the application of current liability regimes, high cost of litigation and the required technical and legal expertise to establish certain liability conditions.

Now that the potential impact of AI on liability law is identified, the research's interest shifts towards the adaptation of liability rules to transcend the hurdles at stake.

(1) See Mosoreanu et al. (2022). Behavioural study on the link between challenges of artificial intelligence for Member States' civil liability rules and consumer attitudes towards AI-enabled products and services.p.24-28.

4.1. Proactive regulatory measures for risk mitigation

Safety regulations and liability rules work in tandem in reducing the risk associated with the use of AI systems. The former mainly plays a preemptive role as it delineates the safety requirements for a given product or service below which the system is deemed dangerous, or not fit for consumers' use, and therefore cannot be placed into circulation. The latter, on the other hand, have an ex post deterrent effect, as their enforcement should encourage a greater level of diligence and care, and therefore directs individuals' conduct towards considering the necessary precautions in conducting their activities.

Most jurisdictions have established provisions relating to product and services safety. Nationally, relevant regulations can be primarily found in the LCPL which imposes several obligations on professionals and manufacturers(1). In short, it is strictly forbidden to put into the market a product/service that does not comply with the safety specifications in force. Also, whenever applicable, professionals must, among other things, obtain certificates that ensure the conformity of products and services to the approved specifications.

On the other hand, the EU product safety legislation comprises general provisions set out by the general product safety regulation (henceforth GPSR) along with sector-specific provisions pertaining to automobiles, pharmaceuticals, and medical devices. Art. 3 of the GPSR defines a safe product as follows:

"'Any product which, under normal or reasonably foreseeable conditions of use, including the actual duration of use, does not present any risk or only the minimum risks compatible with the product's use, considered acceptable and consistent with a high level of protection of the health and safety of consumers"

(1) See Art. 40-41-42 LCPL.

Additionally, the safety assessment should take into consideration the characteristics of the product, its composition, its effects on other products, and the categories of users at risk. Also, the conformity of the product to the general safety requirement can be assessed based on product safety codes of good practice in the relevant sector, state of the art technology, or reasonable consumer expectation regarding safety(1). The directive embraces similar provisions stipulated by the LCPL with respect to the obligations imposed on manufacturers as the product should meet the relevant or sector-specific safety requirements.

These provisions appear to be of dynamic nature. They are flexible enough to ensure a medium level of safety for consumers and the public alike. However, there is still a need to adjust the manufacturers' obligations in light of AI advancements.

To start with, one can think of equipping AI systems with automatic means of recording data pertaining to their functioning and operation. This record-keeping feature ensures a level of traceability of the system's functioning throughout its lifecycle which may lead to the identification of the possible reasons behind the occurrence of harm. Yet, this should be done after assessing the technical and economic feasibility considering the wide range of AI applications that can vary from an AI-based vacuum cleaner to an AI-based attack drone. Moreover, the availability of other methods to collect such data must be taken into consideration(2).

At first glance, this suggestion may not prevent the harm, yet when the operation's history is scrutinized, the identification of the actual cause of harm, whether it is a defect, faulty human input, or a mixture

(1) Additional duties/requirements include the following: Informing consumers about the product's risk, withdrawal of unsafe products, obtaining CE mark for certain products. See Art.6-8-9 European Regulation 2023/988.

(2) Expert Group on Liability and New Tech., Liability for AI and other emerging digital technologies, 2019, p. 47.

of both, can help in improving the system' safety features at a later stage and thence reduce the likelihood of harm occurrence.

Secondly, the black-box phenomena can be mitigated through the implementation of AI transparency guidelines which increase the likelihood of understanding the workings of the system(1). These proactive measures could enable all stakeholders, especially users, to learn about the system's development and training history, how it processes input data and why it generated a particular result or course of action(2). Practically, achieving this objective requires the introduction of certain measures such as traceability and documentation, auditability, and best practices for testing, along with transparent communication on potential capabilities and limitations. Nevertheless, given that the complexity of these systems varies, the level of transparency and explicability should depend on the context in which they are used and the severity of the implications if their output is flawed(3).

Thirdly, central to risk reduction is the concept of human oversight which appears to be of great importance in the context of AI. To that end, legal scholarship calls for the oversight of AI systems' functioning by natural persons and therefore urges developers to implement the appropriate means to achieve such a purpose. Accordingly, the human user, who is supposedly competent and trained, should be able to monitor the AI system while in operation and intervene whenever needed(4). For instance, they should be able to press a built-in stop button or follow a certain procedure so that the act or omission of the system at hand will no longer pose a risk of harm (mandatory

(1) See Wachter et al. (2017).
(2) Hickman, E. & Petrin, M. (2021), p. 597; See, generally, Smuha, N. (2019).
(3) AI HLEG, Ethics guidelines for trustworthy AI, 2019, p. 13.
(4) See Koulu, R. (2020), p. 728.

backdoors). In this sense, the oversight feature will prove effective if it allows users to override, ignore, or modify any undesired, risky, or faulty output(1).

The previous suggestions gained significant traction in the field of liability law, especially since any measure that minimizes or eradicates AI risk will impact AI-related litigations' rate. Still, each option comes with its own set of problems that mainly revolve around technical feasibility issues, cost to benefits analysis as well as the extent of transparency and oversight required in view of myriad systems. Moreover, the aspired trustworthy AI might have a negative effect on innovation, especially with respect to deep learning techniques that are responsible for the most capable yet unexplainable and opaque AI-applications.

Besides, effective forms of human oversight are difficult to establish in practice, let alone that such supervision is not always reliable given that humans may not correctly evaluate the quality of AI recommendations and therefore prevent the harmful conduct. That is why we need to put this option under further scrutiny and research to structure the optimal measures for human-AI system interactions.

Fortunately, some countries have already begun implementing proactive legislative measures to address AI safety concerns across various sectors, especially healthcare. Some jurisdictions in the United States, for example, have already enacted laws that prohibit AI systems from being used in ways that incite or encourage self-harm, harm to others, or criminal activity(2). Others have introduced strict restrictions on the disclosure of user information by mental health chatbots and therefore require clear disclosures that these chatbots are AI systems,

(1) See Etzioni, A. & Etzioni, O. (2016), p. 133; Taddeo, M. & Floridi, L. (2018), p. 751.
(2) Texas Responsible AI Governance Act, 2025 (effective date January 1, 2026).

not humans[1]. Additionally, some laws have banned AI chatbots from representing themselves as capable of providing professional mental health care, which prevents misleading claims about AI's therapeutic capabilities[2].

4.2. AI governance policy

It is evident from the outset that any discussion about the optimal regulatory framework should disregard the idea of a one-size-fits-all solution. AI technology and its diverse applications should not be regulated in the same manner. On the other hand, any effective policy must be technology neutral in terms of ensuring the same level of protection for victims regardless of whether the harm was caused by an AI system or a traditional IT system.

4.2.1. Risk classification as a guiding principle

The EU has been a pioneer in implementing an intuitive approach to classify AI-applications according to a set of predetermined criteria. The AI Act introduced a risk-based approach to AI technology, and the proposal for an AI Liability Directive was initially designed to support this approach, but it was later withdrawn in February 2025. Certainly, this approach is not new for many legal regimes, particularly since it already has parallels in other cross-border AI regulations[3].

This classification recognizes the heterogeneity of AI systems and their underlying techniques as well as the discrepancy between their impact and risk from a legal, social, and economic standpoint. By doing so, policymakers could determine the level of oversight and rules that apply to the use and development of each AI sub-class.

---

[1] Utah House Bill 452, 2025.
[2] Nevada Assembly Bill 406, 2025.
[3] Chamberlain, J. (2023), p.4 (e.g., the US Algorithmic Accountability Act).

The proposal prohibits certain practices that are considered a significant concern without explicitly assigning them a risk level, but it can be concluded that they pose an unacceptable level of risk from a risk management perspective, e.g., putting into circulation an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behavior that results in a physical harm(1).

On the other hand, high-risk AI systems are those presenting a high likelihood of causing harm or violating the rights of individuals(2), all while considering the sector in which such risks can be expected along with the nature of activities undertaken. Basically, when labelling a system as high risk, specific obligations are imposed on producers so that the system meets the appropriate requirements. However, these guidelines are outside the scope of this paper(3).

Additionally, despite the fact that the AI Act does not explicitly attribute a specific risk status to the third category of AI systems, the latter is often known as "limited risk systems"(4). These fall below the high-risk threshold(5). Their key features revolve around interacting with people, generating or manipulating images, audio, or video. Finally, if the system does fit within any of the previous sub-classes, it will be deemed as posing minimal risk.

(1) Art.5(1)(a), Commission proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on AI (The AI Act) and amending certain union legislative acts, COM 206 final, 2021.
(2) See Art. 4, European Parliament Resolution of 20/10/2020 with recommendations to the commission on a framework of ethical aspects of AI, robotics and related technologies.
(3) The definition of high-risk AI is outlined in Art.6 and is based on the list provided in Annex III of the AI Act which could be updated pursuant to the process described in Art.7.
(4) Excellence and Trust in AI, European Commission, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_en (Accessed Nov 22, 2025)
(5) Mahler, T. (2021), p. 249.

At a first glance, this approach appears to be plausible as it takes into consideration the severity of the possible harm and its probability of occurrence as well as the domain in which the system is employed(1). However, we can criticize it on multiple grounds. First, distinguishing between high- and low-level risk is founded on the magnitude and frequency of harm with no clear and systematic procedures applicable to the assessment of such a severity or rate of occurrence. Furthermore, as AI technology is still in its infancy stage, comprehensive statistical data on the risk that could potentially arise from the application of AI system is surely missing or insufficient and therefore any assessment scheme may be inaccurate.

Second, the enumeration of systems or applications falling under the high-risk category is not exhaustive given that the list encompassing said systems can be subject to a periodic update. It is thought that this will create a degree of uncertainty on the part of developers as regards the classification of their system and the scope of safety features that should be embedded.

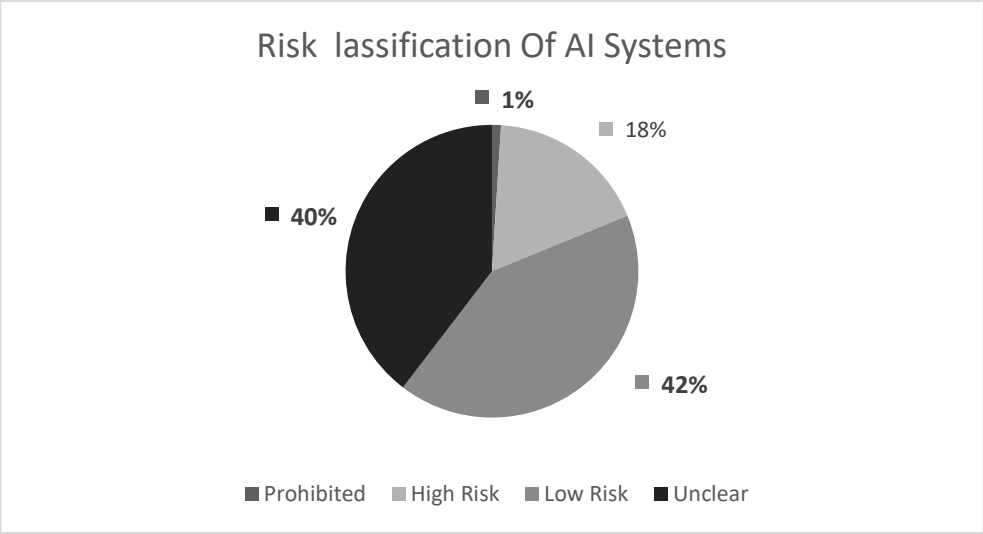
Moreover, the EU parliament suggested that the operator of a high-risk system is strictly liable while adopting a fault-based liability with respect to low-risk ones(2). This seems problematic from a regulatory perspective as liability is not supposed to be contingent on the severity of harm at hand. In other words, the optimal liability regime to govern AI harm should not discriminate between major and minor damages(3).

In line with the previous criticisms are the findings of a recent study published in March 2023. The study aimed at identifying the

(1) The AI Act, p. 26.
(2) Art. 4-8 of EU parliament resolution of 20/10/2020 with recommendations to the Commission on a civil liability regime for artificial intelligence.
(3) See Bertolini, A. & Episcopo, F. (2021), p. 649-652.

uncertainties of AI users based on the risk classification of 106 AI systems(1). Results are presented in the following figure.

Figure 1: Risk classification of 106 AI systems from the publicly available risk-classification database by the applied AI Institute for Europe gGmbH



4.2.2. A sector-specific approach

In contrast to the EU's legislator positioning, Professor Andrea Bertolini suggests a more thorough approach to classifying AI for liability purposes. Instead of the risk-based approach, he recommends a more pragmatic avenue by categorizing AI according to a class-of-application-by-class-of-application (CbC) approach(2). In modern legal systems, many areas where AI is used or could be deployed already fall under the purview of specific regulations which resemble the CbC approach.

(1) Liebl, A. & Klein, T. (2023), p. 12-13.
(2) Bertolini, supra note 97, at 96.

This proposal entails a technology-specific framework which identifies AI classes of applications that share common technological traits and have a uniform socio-economic impact.

To explain the rationale behind this recommendation, one can imagine the case of autonomous terrestrial and aerial vehicles. Both systems are designed to operate in open environments, exhibit a certain level of autonomy, and may cause severe harm to the public. Also, these systems may be classified as high-risk systems if the requirements stipulated in Art.6 of the AI act are met.

Yet, the technology underlying each system is distinct and their diffusion varies as well as the context in which they are employed. Moreover, the characteristics of the party operating these systems differ in terms of qualifications and capabilities (e.g., the operator could be a professional user or a mere average consumer). This raises the question of whether it is adequate for both systems to be governed by the same framework (high-risk), especially in terms of safety requirements.

Following the CbC approach, the authorities need first to identify a class of AI-applications that exhibits common attributes, techniques, and regulatory concerns such as surgical robots. Afterwards, the existing legal framework should be evaluated with respect to its adequacy and robustness in view of AI characteristics. In light of this analysis, regulators will be able to decide if any statutory amendments and ad hoc regulations are needed(1).

Moreover, for this classification to be ideal in terms of liability assignment, it should be founded on a risk management criterion. This means that the potential liable party should be the one who is in the best position to identify, minimize, control, and manage the risk while benefiting from the deployment of the AI system. Consequently, this

(1) Whittam, S. (2022), p. 261.

classification will be principle-based yet flexible enough to ensure predictability and legal certainty for all parties concerned.

Overall, the technology-specific risk management approach provides for a promising solution to the opacity, complexity, and interconnectivity of AI in an extra-contractual context. It allows the identification of a single entry point for litigation purposes instead of establishing a generic term like operator as the legal system will choose one responsible party from a pool of multiple potential stakeholders (user, infrastructure provider, producer, custodian)[1]. This party, however, could vary according to the class of application and the degree of autonomy at issue. In some classes, legislators may deem it more appropriate to hold the user, while in other cases, imposing liability on the producer or the business entity that benefits from the system's functioning may appear to be a better option.

4.2.3. A targeted liability regime for high-risk AI systems

Andrea Bertolini's 2025 analysis of AI liability frameworks has shifted towards a strict liability regime tailored specifically for high-risk AI systems[2]. This approach, in his opinion, may establish clear, uniform, and efficient legal standards across EU Member States, which will reduce regulatory fragmentation and provide stronger protection for AI users while simultaneously fostering innovation. By holding operators automatically responsible for damages caused by their AI systems, except in cases of force majeure, without requiring proof of fault, this regime would offer greater legal certainty and minimize costly litigation. Furthermore, by focusing solely on clearly defined high-risk AI applications, the framework avoids over-regulating lower-

(1) Bertolini & Episcopo, supra note 135, at 651.
(2) See Bertolini. A. (2025), p 127.

risk systems and allows for flexibility to accommodate future technological developments.

However, Bertolini acknowledges the significant political challenges and resistance such a strict liability regime might encounter. Therefore, he supports an alternative, although less effective, fault-based liability framework that maintains the provisions that were set out by the AI liability directive. The less optimal solution lies in introducing a special fault-based liability rule exclusively for high-risk AI applications only. In his opinion, this approach, unlike strict liability, requires proving negligence or failure to fulfill specific operator obligations, and therefore aligns with the existing EU regulatory ecosystem, particularly the AI Act. Consequently, policymakers can balance user protection with political feasibility, as well as reduce legal uncertainty.

4.3. Adapting liability rules to AI-related harm

The ultimate AI legal governance policy entails that liability rules will ensure an optimal deterrent effect and offer damaged parties proper ex post remedies and suitable access to justice. While contractual liability is less problematic, traditional fault-based liability (non-contractual liability) falls short of achieving these two objectives when an AI element is involved.

4.3.1. Reinforced fault-based liability regime

As the system's conduct or output becomes more detached from being influenced by human input, the orthodox fault-based rules appear to be less suitable to identify the deviation from the required standard of conduct. One option to address this gap is by contemplating the adaptation of fault-based liability provisions which will be followed by

an assessment of their impact on liability claims from a victim's perspective.

First, Courts should expect a heightened level of care from users and providers. The standards based on which fault is assessed are thereby extended taking into consideration novel duties that should accompany the use and manufacturing of AI. An acceptable standard of conduct will thence suggest an increased vigilance in deploying, servicing, and manufacturing AI systems which could also vary according to the underlying technology and context in which they are used.

This suggestion is crucial in legal systems that do not recognize a general rule of strict liability for the actions of things such as the USA as opposed to Lebanon and France.

Moreover, a rebuttable presumption of causality may ease the burden of proof if the plaintiff succeeds in providing evidence for the failure to meet that enhanced duty of care by the, or if they cannot access to evidence due to the high complexity of the system at hand(1), on the condition that the technical expertise asserts affirm the existence of a connection between the harm and the AI system's conduct or output.

Another inference can be considered in the case of non-compliance of providers with the required duty of care when they fail to disclose relevant evidence (logs, training data, etc.) at their disposal(2). Assuming that clear procedures concerning the court's right to request the disclosure of evidence are in place, these two options will ease and shift the burden of proof effectively and therefore can be considered as a quasi-safe harbor in safeguarding the interests of damaged parties.

(1) See, generally, Ziosi et al. (2023).

(2) See Art. 4 of the withdrawn proposal for the AI Liability Directive (its principles remain relevant, particularly the emphasis on holding providers accountable for failing to disclose critical evidence).

The term “quasi” is used considering that establishing an efficient benchmark of care may be hard to pinpoint for AI on a general level, let alone that the defendant can adhere to the elevated standard of conduct by taking the necessary precautions and duties or by complying with ex ante safety rules. Thereby, a key element of fault-based liability will be missing which will neutralize the presumption of causality as the human conduct was not blameworthy.

4.3.2. Reinforced strict liability approaches

A. Product liability rules reform

One possible solution is for the Lebanese legislator to follow the example set in the new EU PLD which introduced a rebuttable presumption of defectiveness in the case of non-compliance with safety rules, failure to disclose relevant data, occurrence of an obvious malfunction or even if the system exhibits a black-box effect[(1)].

The same approach could be embraced regarding the causality requirement which could be alleviated when the inner workings of the system cannot be deciphered with technical expertise and there is a reasonable reason to think that the said system played an active role in the harm suffered.

B. Independent strict liability regime

Alternatively, another paradigm of strict liability could be founded on the sector-specific risk management approach (RMA). Simply put, after the introduction of ex ante regulations to govern a certain class of AI applications, the RMA would attribute strict liability to the person best placed to identify and reduce the risk as previously noted.

(1) Art. 6 & 9 of the revised PLD.

An alternative iteration of this approach involves policymakers adopting a sector specific approach that entails assigning liability for AI harm to the entity with the most cost-effective capability of harm reduction that receives, at the same time, the highest level of benefits from the use or deployment of the AI system.

Certainly, some may argue that strict liability addressees would be exposed to a significant legal liability, thereby such a regime might reduce the public's desire to purchase novel AI-applications or hinder the development of new technologies. However, this is not accurate as there exist some feasible mechanisms that work in tandem with this liability regime to achieve a balance between the interests of all stakeholders.

One of the instruments to manage the financial consequences associated with AI harm is through insurance. The latter denotes a contract whereby a person (insurer) undertakes, in exchange for a premium, certain obligations (typically to pay money) in the event that certain contingencies related to another person (insured) or their property occur(1).

What concerns strict liability is third-party insurance, also known as liability insurance. This type may secure natural or juridical persons against the risk of being responsible for the economic consequences of accidents caused during the coverage period(2). It generally covers bodily injury and property damage, thereby shielding the insured person from paying damages in such scenarios.

This practice is not unfamiliar within jurisdictions as it already complements delictual liability in various fields either through mandatory or optional insurance. For instance, this is the case of the

(1) Art. 950 LCOC.
(2) Winter, R. (1991), p. 117.

national traffic law which mandates an insurance coverage for physical and material harm(1). Similarly, France and most US States recognize the same concept regarding motor vehicles. Furthermore, mandatory insurance is required in other instances in some legal systems, such as malpractice or negligence insurance for lawyers or within the medical industry respectively(2).

One-size-fits-all insurance, nevertheless, is not a viable solution as not all damages inflicted are identical, and therefore it is unpractical for a single insurance policy to risk pool and cover all AI applications. Meanwhile, it would be relatively easy for insurance companies already providing their services in established sectors to accommodate relevant AI applications in their pools. Yet, they will need to put additional effort into adapting with the AI market in light of its novelty and lack of statistical data pertaining to AI risk which would likely lead to high premiums for early adopters.

On the other hand, another tool to mitigate the repercussions of strict liability is the systematic pricing of products and services. This market mechanism allows producers to transform the uncertainty surrounding AI into ex post cost that will be transferred to all people benefiting from a certain application.

Conclusion

The rapid pace at which AI technology is developing, and the growing complexity of its systems, will render the identification of the responsible party more difficult in the future. And despite any prospective legal reform, particularly in light of the previous recommendations, complete remedies in all cases of AI-related harm

(1) Art. 353 Law No.243/2012.
(2) Art. L1142-2 French Code of public health.

might not be guaranteed. Some losses, such as pure economic losses or immaterial damage that may not be covered or difficult to measure or assess, and thence the damaged party may be left under or uncompensated.

It should therefore be emphasized that the two approaches discussed (A and B) ought to be combined rather than treated as alternatives as their scope of applicability is different. Also, product liability remains quasi-fault-based liability regime, considering that it still requires a proof of defectiveness and therefore cannot operate as a genuine strict liability framework. Also, litigation is likely to remain complex and costly, particularly due to disclosure and causation difficulties, and the product liability rules were not made to handle AI performance failures or damages arising from AI-based services. By contrast, a dedicated strict liability regime offers clearer allocation of responsibility, reduces litigation burdens, and enhances the insurability of AI-related risks.

The question regarding what liability regime is optimal remains theoretical until tested in practice. It is essential to assess how the law impacts AI users and developers, the scope of compensation for damaged parties, the cost of litigation, and the impact on innovation. The various proposals offered in this paper reflect ongoing efforts to address existing gaps in liability law. What is clear, however, is that a fragmented, inconsistent legislation, as well as preserving the current system, fails to establish the coherent liability rules needed for any effective AI governance.

Bibliography

- Abbott, R. (2018). The Reasonable Computer: Disrupting the Paradigm of Tort Liability. George Washington Law Review, 86(1), 1-45.
- Abou Diya, W. (2014). Al-masouleya al-najema aan hawades al-masaed [The liability arising from elevator accident]. Al-Diyar Newspapers.

- Administrative Court of Montreuil, 8th Chamber, October 8, 2025, No. 2405656
- AI HLEG, Ethics guidelines for trustworthy AI, 2019, p. 13.
- Al-Awji, M. (2019). Al-qanoun al-madani: Al-aakd (Vol.1) [The civil law: The contract]. Al-Halabi legal publications.
- Al-Awji, M. (2019). Al-qanoun al-madani: Al-masouleya al-madaneya (Vol. 2) [The civil law: civil liability]. Al-Halabi legal publications.
- Alces, P. A. (1999). W (h) ither warranty: the b (l) oom of products liability theory in cases of deficient software design. Cal L. Rev., 87, 269.
- Al-Naqib, A. (1983). Al-nazareya al-aama lel masouleya al-najema aan al-fe'el al-shakhsi [The general theory of liability arising from personal actions]. Oueidat publications.
- Al-Naqib, A. (1987). Al-nazareya al-aama lel masouleya al-najema aan al-fe'el al-ghayr [The general theory of liability arising from the actions of others]. Oueidat publications.
- Al-Sanhouri, A. (1952). Al-Waseet Fe Sharh Al-Qanoun Al-Madani [The intermediate in the explanation of civil law], part 7 vol.1, p. 99-100.
- Andersen v. Stability AI Ltd., No. 23-cv-00201-WHO, 2024 WL 3823234 (N.D. Cal. Aug. 12, 2024),
- Armour, J., & Humphrey, W. S. (1993). Software product liability. Software Engineering Institute, TR CMU/SEI-93-TR-13, ESC-TR-93, 190(3).
- Artificial Intelligence and Other Emerging Digital Technologies: a critical assessment. Cambridge University Press.
- Askeland, B., Yamamoto, K., Oliphant, K., Moréteau, O., Menyhárd, A., Ludwichowska-Redo, K.,.. . & Cardi, W. J. (2015). Basic questions of tort law from a comparative perspective. Jan Sramek Verlag.
- Beckers, A., & Teubner, G. (2021). Three liability regimes for artificial intelligence: algorithmic actants, hybrids, crowds. Bloomsbury Publishing.
- Bekkevold v. Potts, 173 Minn. 87, 216 N.W. 790, 1927 Minn. LEXIS 1122, 59 A.L.R. 1164.
- Bellis, K. (2018). Contrat et responsabilité civile: pour un système juste en droit des obligations. Revue Juridique Thémis, 52(2).

- Benhamou, Y., & Ferland, J. (2021). AI & Damages: Assessing liability and calculating the damages, Thomson Reuters - Yvon Blais.
- Bertolini A and Episcopo F (2021). The Expert Group's Report on Liability for
- Bertolini, A. (2020). Artificial intelligence and civil liability. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf (Accessed September 14, 2025)
- Buiten, M., De Streel, A. and Peitz, M., 2023. The law and economics of AI liability. Computer Law & Security Review, 48, p.105794.
- Buiten, M., De Streel, A., & Peitz, M. (2021). EU liability rules for the age of artificial intelligence. Available at SSRN 3817520.
- Buyuksagis, E., & Van Boom, W. H. (2012). Strict liability in contemporary European codification: Torn between objects, activities, and their risks. Geo. J. Int'l L., 44, 609.
- Čerka, P., Grigienė, J., & Sirbikytė, G. (2015). Liability for damages caused by artificial intelligence. Computer law & security review, 31(3), 376-389.
- Chamberlain, J. (2023). The risk-based approach of the European Union's proposed artificial intelligence regulation: Some comments from a tort law perspective. European Journal of Risk Regulation, 14(1), 1-13.
- Chapman, K., & Meurer, M. J. (1989). Efficient remedies for breach of warranty. Law & Contemp. Probs., 52, 107.
- Chopra, S., & White, L. F. (2011). A legal theory for autonomous artificial agents. University of Michigan Press.
- Commission proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on AI (The AI Act) and amending certain union legislative acts, COM 206 final, 2021.
- Cooter, R. D. (1988). Punitive damages for deterence: When and how much. Ala. L. Rev., 40, 1143.
- Cooter, R., & Eisenberg, M. A. (1985). Damages for breach of contract. Calif. L. Rev., 73, 1432.
- De Graaf, T. J., & Wuisman, I. S. (2022). Contractual Liability for the Use of AI under Dutch Law and EU Legislative Proposals. In Law and Artificial

Intelligence: Regulating AI and Applying AI in Legal Practice (pp. 259-277). The Hague: TMC Asser Press.

- Diamantis, M. (2021). Vicarious Liability for AI. Cambridge Handbook of AI and Law (Kristin Johnson & Carla Reyes eds., 2022), U Iowa Legal Studies Research Paper, (2021-27).
- DiMatteo, L. A., Infantino, M., Wang, J., & Monaco, P. (2021). Once More Unto the Breach: A Comparative Analysis of the Meaning of Breach in Contract Law. Transnat'l L. & Contemp. Probs., 31, 33.
- Disney & Universal v. Midjourny.
- Doughman, M. (2017). Al qanoun al tobbi [Medical law]. The modern book institution.
- Durney, E. G. (1983). The Warranty of Merchantability and Computer Software Contracts: A Square Peg Won't Fit in a Round Hole. Wash. L. Rev., 59, 511.
- Ebers, M. (2021). Liability for artificial intelligence and EU consumer law. J. Intell. Prop. Info. Tech. & Elec. Com. L., 12, 204.
- Ernest E. Fadler Co. v. Hesser, 166 F.2d 904, 1948 U.S. App. LEXIS 2390
- Etier, G., & Sträuli, B. (2015). Responsabilité civile - Responsabilité pénale. Journée de la responsabilité civile 2014. Schulthess, éditions romandes.
- Etzioni, A., & Etzioni, O. (2016). Keeping AI legal. Vand. J. Ent. & Tech. L., 19, 133.
- EU parliament resolution of 20/10/2020 with recommendations to the Commission on a civil liability regime for artificial intelligence.
- EU Regulation 2023/2152 on General Product Safety.
- European Commission, Excellence and Trust in AI, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_en (Accessed Nov 22, 2025).
- European Commission. (2018). Commission staff working document: Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (SWD(2018) 157 final).

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52018SC0157 (Accessed September 14, 2025)

- European Commission. (2021). Directorate-General for Justice and Consumers, Karner et al., Comparative law study on civil liability for AI. https://data.europa.eu/doi/10.2838/77360 (Accessed Oct 10, 2023).
- European Parliament Resolution of 20/10/2020 with recommendations to the commission on a framework of ethical aspects of AI, robotics and related technologies.
- Evas, T. (2020). Civil liability regime for artificial intelligence: European added value assessment. European Parliament.
- Expert Group on Liability and New Tech., Liability for AI and other emerging digital technologies, 2019, p. 47.
- Garcia v. Character Technologies, Inc., 6:24-cv-01903, (M.D. Fla.), filed Oct. 22, 2024
- Giliker, P. (2010). Vicarious liability in tort: A comparative perspective. Cambridge University Press.
- Glavaničová, D., & Pascucci, M. (2022). Vicarious liability: a solution to a problem of AI responsibility?. Ethics and Information Technology, 24(3), 28
- Globe Refining Co. v. Landa Cotton Oil Co., 190 U.S. 540, 23 S. Ct. 754, 1903 U.S. LEXIS 1557, 47 L. Ed. 1171
- Goldberg, J. C., & Zipursky, B. C. (2010). The Oxford introductions to US law: Torts. Oxford University Press.
- Gomulkiewicz, R. W. (1997). The Implied Warranty of Merchantability in Software contracts: A Warranty No One Dares to Give up and How to Change That. J. Marshall J. Computer & Info. L., 16, 393.
- Gotanda, J. Y. (2006). Damages in Lieu of Performance because of Breach of Contract. Public Policy Research Paper, (2006-8).
- Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. Computer Law & Security Review, 45, 105681.
- Guangzhou Internet Court. (2024, February 8). Shanghai Character License Administrative Co., Ltd. v. Anonymous AI Company (Case No. 2024 Yue 0192 Minchu 113)

- Hickman, E., & Petrin, M. (2021). Trustworthy AI and corporate governance: the EU's ethics guidelines for trustworthy artificial intelligence from a company law perspective. European Business Organization Law Review, 22, 593-625.
- Hoteit, A. (2006). Al-qanoun al-madani [The civil law]. Dar Al-Mu'allif Al-Jami'I.
- Ibrahim, A. (2018). Al-oukoud al-mosamat [The named contracts].
- Jansen, N. (2010). The Concept of Non-Contractual Obligations: Rethinking the Divisions of Tort, Unjustified Enrichment, and Contract Law. JETL, 1, 16.
- Jones, W. K. (1989). Product Defects Causing Commercial Loss: The Ascendancy of Contract over Tort. U. Miami L. Rev., 44(3), 731
- Kol B'Seder, Inc. v. Certain Underwriters at Lloyd's of London, 766 Fed. Appx. 795, 2019 U.S. App. LEXIS 7160, 2019 AMC 1039, 2019 WL 1130357
- Koulu, R. (2020). Proceduralizing control and discretion: Human oversight in artificial intelligence policy. Maastricht Journal of European and Comparative Law, 27(6), 720-735.
- Koziol, H. (Ed.). (2015). Basic questions of tort law from a comparative perspective. Jan Sramek Verlag.
- Larsen, G., & Lawson, R. (2013). Consumer rights: An assessment of justice. Journal of business ethics, 112, 515-528.
- Lee, R. (1918). Torts and delicts, Yale Law Journal, 27(6), 722-724.
- Lemley, M. A., & Casey, B. (2019). Remedies for robots. The University of Chicago Law Review, 86(5), 1311-1396.
- Liang, W., Yuksekgonul, M., Mao, Y., Wu, E., & Zou, J. (2023). GPT detectors are biased against non-native English writers. arXiv. https://arxiv.org/abs/2304.02819.
- Liebl, A. & Klein, T. (2023). AI Act: Risk classification of AI systems from a practical perspective. https://shorturl.at/MODnn (Accessed Nov 23, 2025).
- Mahler, T. (2021). Between risk management and proportionality: The risk-based approach in the EU's Artificial Intelligence Act Proposal. Nordic Yearbook of Law and Informatics.
- Markoff, J. (2013). Essay-grading software offers professors a break. The New York Times, 20(3), 1-4.

https://www.nytimes.com/2013/04/05/science/new-test-for-computers-grading-essays-at-college-level.html (Accessed September 14, 2025).
- Mata v. Avianca, Inc., No. 1:22-cv-01461 (PKC), Doc. 54 (S.D.N.Y. June 22 , 2023)
- Mosoreanu et al. (2022). Behavioural study on the link between challenges of artificial intelligence for Member States' civil liability rules and consumer attitudes towards AI-enabled products and services.p.24-28.
- Nevada Assembly Bill 406, 2025.
- Oman, N. B. (2014). A Theory of Civil Liability. 21 George Mason Law Review, 381-408.
- Owen, D. G. (2008). Design Defect Ghosts. Brook. L. Rev., 74, 927.
- Pagallo, U. (2022). The way ahead on AI liability issues. https://www.adalovelaceinstitute.org/blog/the-way-ahead-on-ai-liability/ (Accessed September 14, 2025).
- Park v. Kim, No. 22-2057 (2d Cir. 2024).
- Pfeifer-Chomiczewska, K. (2022). Artificial Intelligence and contractual liability under Polish law. Selected issues. Studia Prawno-Ekonomiczne, (124), 59-80.
- Pittenger, M. A. (1992). Reformulating the Strict Liability Failure to Warn. Wash. & Lee L. Rev., 49, 1509.
- Product liability laws and regulations USA, https://iclg.com/practice-areas/product-liability-laws-and-regulations/usa (Accessed September 14, 2025).
- Reid, E. (1999). Liability for dangerous activities: a comparative analysis. International & Comparative Law Quarterly, 48(4), 731-756.
- Sage, N. (2019). Contractual Liability and the Theory of Contract Law. King's Law Journal, 30(3), 459-488.
- Schwartz, A. (1979). The case for specific performance. Yale LJ, 89, 271.
- Shamblin et al. v. OpenAI, Inc. et al., No. 25STCV32382 (Superior Court of California, County of Los Angeles, filed Nov 06, 2025)
- Shanghai Character License Administrative Co., Ltd. v. Anonymous AI Company

- Sharkey, C. M. (2003). Punitive damages as societal damages. Yale LJ, 113, 347.
- Syoufi, G. (1994). Al-nazareya al-aama lel moujebat wal-oukoud (2nd ed.) [The general theory of obligations and contracts]
- Tagnetics, Inc. v. Kayser, 842 Fed. Appx. 969, 2021 U.S. App. LEXIS 986, 2021 FED App. 0033N (6th Cir.), 2021 WL 129071.
- Texas Responsible AI Governance Act, 2025.
- Tharp v. Allis-Chalmers Mfg. Co., 42 N.M. 443, 1938-NMSC-044, 81 P.2d 703, 1938 N.M. LEXIS 42, 117 A.L.R. 1344;
- UMG, Sony, Warner Recording Labels v. Suno & Udio.
- Utah House Bill 452, 2025.
- Van Dam, C. (2013). European tort law. OUP Oxford.
- Van Vliet, B. E. (2012). Systematic finance: Essays on ethics, methodology and quality control in high frequency trading. Illinois Institute of Technology. ProQuest Dissertations Publishing.
- Viney, G., & Jourdain, P. (2006) Les conditions de la responsabilité, Traité de Droit civil, dir. J. Ghestin, LGDJ, 3.
- Von Bar, C., & Drobnig, U. (2004). The Interaction of contract law and tort and property law in Europe: A Comparative Study. Sellier - European Law Publishers GmbH.
- Wachter et al. (2017).Transparent, explainable, and accountable AI for robotics. Science Robotics, 2(6).
- Wade, J. W. (1980). On product design defects and their actionability. Vand. L. Rev., 33, 551.
- Whittam, S. (2022). Mind the compensation gap: towards a new European regime addressing civil liability in the age of AI. International Journal of Law and Information Technology, 30(2), 249-265.
- Wright, R. W. (1985). Causation in tort law. Calif. L. Rev., 73, 1735.
- Youssef, C. (2020). Al-masouleya al-madaneya aan fe'el al-zakaa al-estenaii [Civil liability for artificial intelligence acts]. [Master's Thesis, Lebanese University].
- Zech, H. (2021, April). Liability for AI: public policy considerations. ERA Forum, 22, 147-158. Springer Berlin Heidelberg.