ChatGPT

1. Liability for Robot-Caused Harm

EU: Under current EU law, robots are treated as "products." Victims can claim compensation under the Product Liability Directive (85/374/EEC) if a defect in the robot causes injury. In practice this means manufacturers (and sometimes importers) are strictly liable for defects in hardware or software, and operators/owners may be liable under general tort/negligence law. The European Parliament has noted that "robots cannot be held liable per se" – responsibility always falls on a human or corporate actor (manufacturer, owner, operator, etc.) [1]. Recent debates (e.g. the 2017 Parliament "Civil Law Rules on Robotics" resolution) considered new strict-liability rules and even a hypothetical "electronic person" status for AI, but these were not adopted [2] [1]. Instead, lawmakers focus on clarifying who "controls" the robot. For example, EU rules now make the vehicle's *keeper* (owner) strictly liable if an automated car causes harm, regardless of human control [3]. Revisions of the EU product-liability regime (and a proposed AI Liability Directive) are underway to extend strict liability to software and ease victims' burden of proof, but as of 2025 no special "robot law" exists beyond these general rules [4] [5].

United States: The U.S. has no robot-specific liability statute. Courts generally treat robots as consumer or industrial products. Manufacturers can be sued under state product liability (strict liability for defects) if a design or manufacturing flaw causes injury, and users/operators can face negligence claims if they misuse or fail to maintain a robot. Analysts note that "American legal frameworks still primarily treat AI-driven robotics as products, holding manufacturers liable for defects" [6]. (For example, debate over the 2018 Uber self-driving car crash centered on whether Uber, the carmaker, or the software was at fault.) Federal agencies like NHTSA (for vehicles) and the FTC are exploring AI safety, but no comprehensive federal law yet assigns robot liability. Victims often rely on existing consumer-safety and antitrust laws (e.g. the Consumer Product Safety Act for hazardous goods).

Japan: Japanese law similarly imposes strict product liability on robot makers. Under the Product Liability Act and Civil Code, a manufacturer is liable for injury or death caused by a defect ("a lack of safety the product should provide") [7]. Thus a defective robot (hardware or "intelligent" software) would render its maker strictly responsible. Operators also owe a duty of care: for example, Japan requires a human "driver" (or operator) to be present in certain automated vehicles, effectively ensuring a person retains final responsibility [8]. In practice, Japan has focused on human oversight and safety standards (e.g. mandated emergency stops, supervision protocols) rather than novel legal categories.

China: China's approach is evolving but largely rests on general product and tort law. Its Product Quality Law (supplemented by the 2020 Civil Code) imposes strict liability on producers of defective products [9]. An autonomous robot would likely be treated as a "product," making the manufacturer strictly liable for defects in design, manufacturing or warnings. (If an AI system were deemed a "service" instead, victims would need to prove the provider's negligence.) In recent practice, regulators have emphasized growth and control over AI but have begun applying product-safety rules to smart devices. For instance, a Chinese court suggested that AI chatbots could be classified as digital products, bringing them under the Product Quality Law [10]. Overall, Chinese policy emphasizes state-led AI deployment (e.g. in surveillance) with relatively few explicit liability rules, so injured parties typically rely on conventional defect/negligence claims under existing laws [11] [9].

In all these jurisdictions **the robot itself cannot be sued** or held criminally liable. Current frameworks assign blame to the human "owner" of the robot's intelligence – whether that is the manufacturer, programmer, owner or operator – using product-liability, negligence/tort, or contract law [1] [4]. Each

system grapples with proof-of-causation for complex AI behavior, but to date liability tracks human involvement, not the machine as an agent.

2. Jailbreaking and Misuse Protections

There is **no global law explicitly forbidding "jailbreaking" robots**, but several legal and technical mechanisms touch the issue. From a legal standpoint, general computer-crime and copyright rules can apply. For example, the U.S. Digital Millennium Copyright Act (DMCA) makes it unlawful to circumvent software copy-protection; in theory, this could cover unlocking a robot's firmware or AI module. Similarly, the EU Copyright Directive and the WIPO copyright treaties protect software under anti-circumvention rules. Thus, changing a robot's locked-down software or removing safety features might violate these laws – although many jurisdictions have exemptions (e.g. for security research or repair) that complicate enforcement.

Technically, **robust security measures** are the norm. Manufacturers often use secure boot chains, signed firmware updates, encrypted operating systems and hardware Trusted Platform Modules to prevent unauthorized code modifications. Industry standards and best practices have emerged: for instance, ISO 10218 (robotics safety) and IEC 62443 (industrial control security) set guidelines that implicitly demand tamper-resistance. The Robot Operating System community, as well as independent initiatives like the Robot Security Framework, publish checklists for locking down sensors, networks and control software. In regulation, the EU's proposed AI Act (still under negotiation) would classify many robotics functions as "high-risk AI," requiring built-in cybersecurity and human oversight [12]. In the U.S., the NIST AI Risk Management Framework encourages robust design and patching of AI systems. North American and European cyber-security agencies are also beginning to issue guidance for robots (similar to IoT devices), though no binding robot-specific standard exists yet.

Analysts have noted that *removing* built-in safeguards is effectively a form of misuse. Recent research has shown that AI models (including embodied robots) can indeed be "jailbroken" via adversarial commands [13]. In response, experts have suggested frameworks like mandatory logging and incident reporting (analogous to anti-fraud or child-protection statutes) so that attempts to force a robot to do something unsafe can be detected and traced [13]. Some tech policy proposals urge requiring companies to monitor and report malicious AI use (drawing on analogies to bank secrecy or CSAM laws) [13]. However, these remain theoretical for now.

In practice, legal protection against misuse of robots relies on **existing cybersecurity and safety laws**. Unauthorized remote control of a robot would violate computer-fraud statutes; using a hacked robot to commit crime could incur liability under hacking or anti-tampering laws. Many countries have general cybercrime acts that forbid unauthorized access to computer systems, which would cover robots connected to networks. To date, no jurisdiction has passed a law specifically about "jailbreaking" AI robots beyond these broader provisions. In summary, the safeguards against jailbreaking are mostly technical and indirect: built-in security features, industry best practices, and general IP/cyber laws, rather than bespoke regulation [12] [13].

3. Transferring AI Agents to/From Physical Robots

This is largely **unregulated territory**. No country has specific rules for transferring a synthetic "AI companion" or virtual personality into a physical robot or vice versa. Such transfers would currently be

treated as software operations (downloading, installing AI code in a robot, or copying software to the cloud) rather than a legal "event" requiring a permit.

Ethical/Policy Guidance: While legal frameworks are silent, some ethical guidelines touch on related concerns. For example, the European Parliament's 2017 Robotics Charter emphasizes that robots (especially in caregiving/companion roles) **must be designed to respect human dignity, autonomy and self-determination** [14]. By analogy, if a user's personal AI (say, a virtual assistant or therapeutic chatbot) were given a robot body, designers should ensure the experience does not degrade human rights or mental well-being. But the Charter speaks to human dignity, not rights of the AI itself.

There is currently **no law granting any "rights" or protections to AI entities**. Notably, the idea of AI "consciousness" or "identity" being transferred isn't addressed by legislatures or regulators. Philosophical and ethical debates exist (some scholars advocate caution about "mind uploading"), but no standards. International AI ethics frameworks (e.g. UNESCO's Recommendation on Ethics of AI, OECD AI Principles) stress human control, transparency and avoidance of psychological harm to *people*, but do not regulate how AI programs are deployed.

As a result, there are **no mandatory protocols** for "reviewing" an AI when it is installed in a robot, nor any required procedures if an embodied agent is decommissioned or "traumatized." A manufacturer might voluntarily run diagnostics or data resets, but no law requires it. Conceptually, one could imagine guidelines (e.g. regular safety audits, user notifications, "digital welfare" checks) for transfer of human-like AI, but no jurisdiction has adopted such measures. In short, transferring an AI from software to hardware (or vice versa) is treated as an engineering matter, not a legal one, and no standards for "trauma recovery" of AI agents are established.

4. Manufacturer Responsibilities (Maintenance, Parts, Updates, Recalls)

Manufacturers of robots are increasingly subject to obligations typical of other consumer/industrial goods. In the EU, for example, recent laws strengthen **repair and maintenance duties**. The 2024 EU "Repair Directive" (effective 2026) requires manufacturers of certain durable goods to offer repair services within a reasonable time and price, and even bans any design or software locks that **impede repairs** [15] [16]. For listed products, makers must also make spare parts available at fair prices and provide repair information. Similarly, the EU's Ecodesign regulations now require manufacturers to supply security updates: for instance, smartphones/tablets must receive at least 5 years of software/security updates, and have critical parts (batteries, screens, cameras, etc.) available to repairers for up to 7 years [17]. If robots are categorized under such rules (e.g. as ICT or "monitoring/control equipment"), those obligations could apply: robot makers might have to commit to long-term support and spare components to comply with these green-consumption directives.

In practice today, obligations vary by product type and jurisdiction. In the **EU**, a manufacturer releasing a consumer robot must comply with the Sale of Goods Directive (minimum 2-year warranty) and with any applicable sector rules (e.g. medical or toy standards if it's a robot toy or surgical robot). If a design flaw endangers users, the EU General Product Safety Directive or Machinery Directive can force a recall. In the **US**, no federal "right to repair" law exists, but the Federal Trade Commission has signaled it will crack down on unfair repair restrictions (and many state laws require provision of service manuals or parts for electronics). Robot firms selling to consumers or businesses are also subject to product warranties (often 1–2 years) and must comply with voluntary standards (like UL for safety) that can influence maintenance expectations. For industrial robots, manufacturers routinely provide service

contracts, updates, and spare parts, though this is more contract law and insurance practice than binding law. Both EU and US regulators expect companies to initiate recalls of dangerous products: e.g., a faulty household or medical robot would fall under the Consumer Product Safety Commission's recall regime in the US, or a safety recall under EU law.

No **robot-specific** recall statute exists, but general product-liability and safety rules fill the gap. For example, the U.S. CPSC and Japan's Consumer Safety Act empower agencies to order recalls or bans of any consumer product (robots included) that poses an "unreasonable risk." Likewise, robotics sold as industrial machinery may fall under workplace-safety regulations (e.g. OSHA requirements to fix hazardous equipment). In summary, while specific "robot maintenance laws" are rare, manufacturers are increasingly expected by law and policy to provide long-term support, spare parts, and updates for electronic products [15] [17].

5. Environmental and End-of-Life Regulations

Robots, being electrical/electronic equipment (EEE), generally fall under existing e-waste and circular-economy laws. In the **EU**, the Waste Electrical and Electronic Equipment (WEEE) Directive requires that producers of EEE finance the collection and recycling of waste devices [18]. Although robots are not always listed as a separate category, they contain batteries, metals and electronics, so they are subject to WEEE if covered by national laws. The Directive mandates separate collection targets and proper treatment of WEEE, effectively forcing manufacturers or importers to join compliance schemes for take-back and recycling [18]. The EU's broader Circular Economy Action Plan also encourages eco-design: for instance, some member states and industry groups are already discussing "ecological criteria" for robot design (durability, recyclability).

In **Japan**, multiple recycling laws exist. The Home Appliance Recycling Law (2001) obliges companies to recycle certain large appliances (TVs, ACs, refrigerators, washing machines). More recently, laws like the 2013 Act on Promotion of Recycling of Small WEEE require manufacturers to recycle smaller electronic goods as well [19]. While robots are not specifically singled out, a personal robot could be classified as electronic equipment and enter these programs. In practice, Japanese robot makers often participate in existing recycling schemes or offer buy-back for obsolete units, but no robot-specific take-back regulation is known beyond these general e-waste laws.

In **China**, the 2020 amendment to the Solid Waste Law established an Extended Producer Responsibility (EPR) system for electronics and batteries [20]. This means producers must set up recycling and take-back systems for their products at end-of-life. Although aimed at items like PCs and batteries, a robot's electrical components would fall under this rule, so robot manufacturers in China will ultimately be expected to reclaim and recycle robots (or their parts) they place on the market [20]. The government's plan calls for formal EPR systems (e.g. deposit-return or recycling fees) by around 2025, which could extend to robotics.

In the **United States**, e-waste regulation is mostly at the state level. Some states (e.g. California, Maine, Minnesota) require manufacturers to finance recycling of covered electronics (like TVs, computers). A robot might not fit neatly into those categories unless explicitly included. There is no federal law yet obligating manufacturers to reclaim e-waste, but voluntary programs (Industry councils like ARCA) handle many electronics. Additionally, the Basel Convention (international treaty, which the US has signed) restricts export of hazardous e-waste. These frameworks imply that robotmakers should consider end-of-life planning, but as of 2025 no widely applied law forces them to "reclaim" used robots.

Summary: In effect, robots are treated as complex electronic products in regulatory frameworks. Environmental rules for electronics (WEEE, RoHS, EPR laws) apply by analogy: manufacturers bear general responsibility for recycling their devices [18] [20]. Emerging policies (like the EU's repair and ecodesign laws) increase pressure on companies to design robots for longevity and recyclability. However, formal take-back schemes tailored to robotics are still nascent, so this remains an area of policy development and perceived gap in global robot regulation.

Sources: Authoritative legal analyses and policy documents from the EU, OECD, government agencies, and legal scholarship have been cited for each point, as detailed above [1] [4] [6] [7] [9] [15] [16] [17] [18] [20].

---

[1] [14] C_2018252EN.01023901.xml
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017IP0051

[2] [3] [4] [5] Who is liable when robots cause damage? | Munich Re
https://www.munichre.com/en/insights/digitalisation/who-is-liable-when-robots-cause-damage.html

[6] [8] [11] Navigating Liability In Autonomous Robots: Legal And Ethical Challenges In Manufacturing And Military Applications - The Yale Review Of International Studies
https://yris.yira.org/column/navigating-liability-in-autonomous-robots-legal-and-ethical-challenges-in-manufacturing-and-military-applications/

[7] AI, Machine Learning & Big Data Laws 2025 | Japan
https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/japan/

[9] [10] Determining liability in first AI chatbot lawsuit | China | Law.asia
https://law.asia/first-ai-chatbot-lawsuit/

[12] Why We Need Cybersecurity Rules for Humanoid Robots and AI Agents - Latest News on Cybersecurity, Ethical Hacking, and Technology Trends
https://www.hackers4u.com/why-we-need-cybersecurity-rules-for-humanoid-robots-and-ai-agents

[13] Balancing safety and privacy: regulatory models for AI misuse - Institute for Law & AI
https://law-ai.org/balancing-safety-and-privacy-regulatory-models-for-ai-misuse/

[15] [16] Directive on repair of goods - European Commission
https://commission.europa.eu/law/law-topic/consumer-protection-law/directive-repair-goods_en

[17] Ecodesign for Smartphones: Two Steps Forward, One Step Back - iFixit
https://www.ifixit.com/News/111220/ecodesign-for-smartphones-now-in-effect

[18] Waste from Electrical and Electronic Equipment (WEEE) - Environment
https://environment.ec.europa.eu/topics/waste-and-recycling/waste-electrical-and-electronic-equipment-weee_en

[19] Act on Promotion of Recycling of Small Waste Electrical and Electronic Equipment - English - Japanese Law Translation
https://www.japaneselawtranslation.go.jp/en/laws/view/3209/en

[20] Extended Producer Responsibility | RKC-MPD
https://rkcmpd-eria.org/extended-producer-responsibility-detail/china