



VISUAAL

Privacy-Aware and Acceptable
Video-Based Technologies
and Services for Active and
Assisted Living

D1.7. Active Assisted Living – proposals *de lege ferenda* Guidelines for responsible research and innovation of monitoring technologies/AAL

Document information			
Deliverable ID	D1.7	Deliverable Title	Guidelines for responsible research and innovation of monitoring technologies/AAL
Deliverable type	Report	Release version	1.0
Due (month number)	42	Delivery date	20/12/2024

Status	RELEASED		
Authors	ZH	Zhicheng He	SU
	MK	Maksymilian Kuźmicz (editor)	SU
	IP	Irakli Pkhakadze	SU
Reviewers	LC	Liane Colonna	SU
	FFR	Francisco Florez-Revuelta	UA
	SG	Stanley Greenstein	SU
	PW	Peter Wahlgren	SU

Dissemination Level	
Restricted	
Public	X



This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 861091.

Universitat d'Alacant
Universidad de Alicante
Project Coordinator

RWTH AACHEN
UNIVERSITY

STOCKHOLM
UNIVERSITY

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

TU
WIEN

Version	Date issued	Milestone*	Release comments
0.1	09/12/2024	D	Initial draft by ESRs ZH, MK and IP
0.2	11/12/2024	I	Reviewed by their supervisors
0.3	19/12/2024	I	Final draft by ESRs ZH, MK and IP
1.0	20/12/2024	R	Final version

* Milestones names include abbreviations/terms as follows:

- Draft (D): describes planned contents and main structure of the different sections. Document is between 0% - 50% completed.
- Intermediate (I): document is approximately between 50% - 100% completed. It is the previous step before it could be released.
- Released (R): document is 100% completed, reviewed, and authorized for release by the partner responsible of the deliverable or the WP leader.

Table of contents

1.	Introduction and methodologies	3
2.	Product safety regulations.....	6
2.1.	EU Regulatory Framework in Product Safety Setting	6
2.2.	Stakeholders' Perspectives.....	12
2.3.	Technical and Operational Compliance	14
2.4.	Conclusions	14
3.	Medical Devices Regulation (MDR)	16
3.1.	AAL in the light of MDR.....	16
3.2.	MDR and other Laws	17
3.3.	Conclusions	19
4.	Cybersecurity	20
4.1.	Cybersecurity challenges.....	20
4.2.	Suggestions	21
5.	Competition law	24
5.1.	Market Dominance and Data-Driven Expansion	24
5.2.	Abuse of Dominance	25
5.3.	Cartels and Anti-Competitive Agreements	25
5.4.	Mergers and Concentrations.....	26
5.5.	Comparative Analysis with Other Jurisdictions	26
5.6.	Emerging Technologies and Future Trends.....	27
5.7.	Case Studies and Real-World Examples	29
5.8.	Policy Recommendations and Practical Implications	31
6.	Consumer law	33
6.1.	Consumer status.....	33
6.2.	Definition of vulnerable consumer.....	34
6.3.	Information obligations.....	36
7.	Contract law	38
7.1.	Introduction	38
7.2.	Contract Formation and Governing Law	39
7.3.	Specific Contractual Clauses in AAL Agreements	40
7.4.	Consumer Contracts and Unfair Terms	41
7.5.	Future Directions and Legal Innovations in Contract Law for AAL.....	43
7.6.	Practical Applications and Case Studies.....	44

7.7. Conclusions	45
8. Criminal law	47
8.1. Definition of nudity	48
8.2. Criminal liability of AAL providers	49
9. Data protection.....	51
9.1. Data privacy challenges.....	51
9.2. Suggestions	52
10. Conclusions	54
Bibliography.....	56
Legislation	56
Case law.....	59
Documents	60
Literature	62
Disclaimer.....	72

1. Introduction and methodologies

Active and Assisted Living (AAL) technologies emerge as a promising answer to ageing European society. AAL is a set of technologies incorporated together into computer systems aimed at offering essential support for daily tasks.¹ This assistance helps users maintain independence and prolong active participation in society. AAL systems are tailored to learn from and adapt to the unique needs and preferences of the individuals they assist, aligning closely with their specific requirements.² Extensive research confirms that AAL technologies are progressively improving their effectiveness in supporting older adults.³

AAL is a multidimensional phenomenon, raising numerous ethical, legal, and social questions. For example, although AAL systems can provide important functionalities like fall detection and medication reminders, they also have the potential to infringe on a person's privacy, especially when visual data is utilized.⁴ This trade-off is one of the most frequently discussed issues in the field.⁵

Another important issue connected with AAL is the applicable law. In this regard, Colonna reviewed the legal and regulatory challenges facing the use of lifelogging technologies for the frail and sick. Her work provides an analytical legal framework that is wide in scope and touches upon various legal domains, including data protection rules, cyber security laws, medical device regulations, general product safety regulations, consumer protection rules, criminal laws, intellectual property concerns,

¹ AGE Platform Europe. (2016). *Glossary & acronyms*. <https://www.age-platform.eu/glossary/active-and-assisted-living-programme-aal>.

² Blackman, S., Matlo, C., Bobrovitskiy, C., Waldoch, A., Fang, M., Jackson, P., Mihailidis, A., Nygård, L., Astell, A. & Sixsmith, A. (2016). Ambient Assisted Living Technologies for Aging Well: A Scoping Review. *Journal of Intelligent Systems*, 25(1), 55-69. <https://doi.org/10.1515/jisys-2014-0136>

³ See, for example: Aleksic, S., Atanasov, M., Calleja Agius, J., Camilleri, K., Čartolovni, A., Climent-Pérez, P., Colantonio, S., Cristina, S., Despotovic, V., Ekenel, H. K., Erakin, E., Florez-Revuelta, F., Germanese, D., Grech, N., Sigurðardóttir, S. G., Emirzeoğlu, M., Iliev, I., Jovanovic, M., Kampel, M., ... Zgank, A. (2022). State of the Art of Audio- and Video-Based Solutions for AAL. Zenodo. <https://doi.org/10.5281/zenodo.6390709>; and Choukou, M.-A., Shortly, T., Leclerc, N., Freier, D., Lessard, G., Demers, L., & Auger, C. (2021). Evaluating the acceptance of Ambient Assisted Living Technology (AALT) in rehabilitation: A scoping review. *International Journal of Medical Informatics*, 150, 104461. <https://doi.org/10.1016/j.ijmedinf.2021.104461>.

⁴ Arning, K., & Ziefle, M. (2015). "Get that camera out of my house!" Conjoint measurement of preferences for video-based healthcare monitoring systems in private and public places. *Inclusive Smart Cities and E-Health*, 152–164. https://doi.org/10.1007/978-3-319-19312-0_13, p. 161-162; and Maidhof, C., Ziefle, M., & Offermann, J. (2022). Exploring privacy: Mental models of potential users of AAL Technology. *Proceedings of the 8th International Conference on Information and Communication Technologies for Ageing Well and E-Health*. <https://doi.org/10.5220/0011046200003188>, p. 103.

⁵ Mujirishvili, T., Maidhof, C., Florez-Revuelta, F., Ziefle, M., Richart-Martinez, M., & Cabrero-García, J. (2023). Acceptance and privacy perceptions toward video-based active and Assisted Living Technologies: Scoping Review. *Journal of Medical Internet Research*, 25. <https://doi.org/10.2196/45297>, p. 10.

contract laws and health-care laws.⁶ Colonna observes that the current legal framework of lifelogging is a patchwork and is highly fragmented, and that coherent legal regulation is needed to ensure privacy protection and product safety.⁷

More recently, there were two White Papers examining the legal aspects of AAL. The GoodBrother COST Action's White Paper recognises seven legal aspects that are central to the use of video and audio-based AAL tools, including: (1) data protection and design requirements of data protection law; (2) cyber security; (3) medical device regulation and health laws; (4) general product safety regulation; (5) consumer protection; (6) intellectual property; and (7) AI Regulation.⁸ The White Paper of MSCA ITN visuAAL identifies other relevant legal domains: (1) competition law; and (2) criminal law.⁹

Building on the frameworks established in state-of-the-art research, this deliverable aims to identify possible improvements to the law. These *de lege ferenda* (Latin for “concerning the law how it should be”) conclusions stem from three years of research conducted in the framework of MSCA ITN visuAAL. The conclusions have a character of guidelines – they rather identify goals that should be achieved than propose particular solutions. This can make the deliverable more time-proof: recommendations set forth hereafter can inspire legislative changes, and serve as a point of reference to assess future legislative developments.

This contribution employs primarily legal methods. The suggested amendments are informed primarily by doctrinal legal research, which aims to present the law as it is (*lege lata*) as a network of principles, rules, metarules, and exceptions.¹⁰ Some inspirations for the improvements come from comparative legal studies. The comparative method allows seeing how a similar problem is addressed in different legal frameworks, which broadens the perspective of potential solutions. Additionally, this research is informed by materials gathered in the domains of computer studies. That is indispensable when discussing regulatory aspects of technology to understand

⁶ Colonna, L. (2019). Legal and regulatory challenges to utilizing lifelogging technologies for the frail and sick. *International Journal of Law and Information Technology*, 27(1), 50–74. <https://doi.org/10.1093/ijlit/eay018>.

⁷ Ibid.

⁸ Ake-Kob, A., Blazeviciene, A., Colonna, L., Čartolovni, A., Colantonio, S., Dantas, C., Fedosov, A., Florez-Revuelta, F., Fosch-Villaronga, E., He, Z., Klimczuk, A., Kuźmicz, M., Lukács, A., Lutz, C., Mekovec, R., Miguel, C., Mordini, E., Pajalic, Z., Pierscionek, B. K., ... Tamò-Larrieux, A. (2022). State of the art on ethical, legal, and social issues linked to audio- and video-based AAL solutions. Zenodo. <https://doi.org/10.5281/zenodo.6793617>.

⁹ Kuźmicz, M. M., & He, Z. (2022). *Active Assisted Living – legal tectonic plates: White paper on the legal framework for video-based assisted technologies [White paper]*. visuAAL.

¹⁰ Peczenik, A. (2001). A theory of legal doctrine. *Ratio Juris*, 14(1), 75–105. <https://doi.org/10.1111/1467-9337.00173>, p. 75, 79.

the phenomenon at hand, and situating it in the legal context.¹¹ Hence, the traditional legal approach is supplemented by the perspectives from computer studies, making this deliverable an interdisciplinary endeavour.

The following sections discuss the potential improvements in eight legal domains: (1) general product safety regulations, (2) medical device regulations, (3) cybersecurity, (4) competition law, (5) consumer law, (6) contract law, (7) criminal law, and (8) data protection. The lack of AI regulations is a strategic decision of the authors.¹² This contribution suggests amendments to the law. Meanwhile, AI laws are nascent in Europe, with the AI Act¹³ and the Council of Europe's Convention on AI adopted in 2024.¹⁴ Hence, it was decided to leave those pieces of legislation out of the scope, and wait till they are finally adopted and implemented.

¹¹ Cf. Ubena, J. (2015). *How to Regulate Information and Communications Technology? A Jurisprudential Inquiry into Legislative and Regulatory Techniques*. Jure.

¹² Yet, they are mentioned in the context of other relevant laws when necessary.

¹³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), PE/24/2024/REV/1, OJ L, 2024/1689, 12.7.2024.

¹⁴ Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Vilnius, 5th September 2024.

2. Product safety regulations

Active Assisted Living (AAL) systems represent a merging of hardware and software technologies aimed at supporting elderly and disabled individuals.¹⁵ Ambient Assisted Living (AAL) systems are developed to improve the quality of life for elderly by integrating advanced technologies. However, these systems present significant challenges to current regulatory frameworks. The convergence of products and services within AAL blurs traditional distinctions, creating complexities that existing regulations are not fully equipped to address. As a result, there is a critical need for a more refined and nuanced legal approach to effectively govern the multifaceted nature of AAL systems.

AAL systems integrate hardware components, such as sensors, assistive devices, and robotics, with software elements like artificial intelligence algorithms and monitoring platforms to provide continuous support and monitoring.¹⁶ These systems often rely on wireless communication, real-time data processing, and AI-driven decision-making, making them inherently hybrid in nature. The dynamic and interconnected characteristics of AAL systems present unique challenges for regulatory compliance, particularly in distinguishing between products and services.¹⁷

2.1. EU Regulatory Framework in Product Safety Setting

2.1.1. General Product Safety Regulation (GPSR)

The General Product Safety Regulation (GPSR),¹⁸ which entered into force in 2023 with a transitional period ending in December 2024, updates the EU's approach to product safety. As a horizontal legal framework, the GPSR applies to non-food consumer products, broadening the definition of a "product" to encompass any item, whether interconnected or not, including those integrated into services (Article 3(1), GPSR).

AAL systems, characterized by their integration of hardware and software, fall within the expanded scope of the GPSR. The regulation imposes safety obligations across

¹⁵ Cicirelli, G., Marani, R., Petitti, A., Milella, A., & D'Orazio, T. (2021). Ambient assisted living: a review of technologies, methodologies and future perspectives for healthy aging of population. *Sensors*, 21(10), 3549.

¹⁶ Jovanovic, M., Mitrov, G., Zdravevski, E., Lameski, P., Colantonio, S., Kampel, M., ... & Florez-Revuelta, F. (2022). Ambient assisted living: scoping review of artificial intelligence models, domains, technology, and concerns. *Journal of Medical Internet Research*, 24(11), e36553.

¹⁷ Colonna, L. (2019). Legal and regulatory challenges to utilizing lifelogging technologies for the frail and sick. *International Journal of Law and Information Technology*, 27(1), 50–74. <https://doi.org/10.1093/ijlit/eay018>.

¹⁸ Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC

the entire lifecycle of these systems, addressing concerns such as cybersecurity vulnerabilities and the safety risks associated with interconnectivity and real-time updates. Article 25 of the GPSR mandates that manufacturers proactively address potential vulnerabilities, particularly those related to cybersecurity. For AAL systems, this entails implementing robust security measures to safeguard against unauthorized access and ensuring that software updates do not compromise system integrity. Compliance measures may include regular security audits, adherence to ISO/IEC 27001 standards¹⁹ for information security management, and the implementation of secure coding practices.

However, while the GPSR extends product safety obligations to interconnected devices, it remains ambiguous in allocating liability for harm arising from service components. For instance, if a software malfunction in an AI-driven AAL system results in harm, the GPSR's broad definition of "product" may still inadequately address the nuances of liability for the service elements. To address this, the GPSR could be amended to include explicit provisions for service-related liabilities, guaranteeing comprehensive coverage of both hardware and software defects.

2.1.2. Product Liability Directive (PLD)

The original Council Directive 85/374/EEC²⁰ imposed strict, no-fault liability on manufacturers for harm caused by defective products, applying to "all movables" and holding producers accountable irrespective of fault (Article 1, PLD). Under Article 2 PLD, this included tangible items such as assistive devices and sensors found in Active Assisted Living (AAL) systems. However, the directive primarily addressed physical components and did not adequately consider intangible elements. As a result, software malfunctions or defects in AI-driven AAL functionalities were difficult to reconcile with the concept of "product" as originally conceived. Under this older regime, victims injured by software-induced defects faced uncertainty, and a clear liability framework for hybrid, hardware-software AAL systems was lacking.

For instance, if an AAL system's fall detection algorithm malfunctioned due to a software update, resulting in delayed emergency responses, it was unclear whether strict liability would apply. The PLD, as originally framed, focused on tangible goods, leaving a regulatory gap for intangible digital components and evolving AI functionalities. Some suggested amending the original PLD to explicitly include software as a product, while others proposed introducing a supplementary liability regime for intangible digital elements. In contrast, certain jurisdictions like the United

¹⁹ ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

²⁰ 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

States' Food and Drug Administration (FDA)²¹ already acknowledged software as integral to medical devices, subjecting it to validation and verification processes.

Recognizing these shortcomings, the EU fundamentally reformed its product liability landscape through Directive (EU) 2024/2853 (the “new PLD”), adopted on 23 October 2024. This new directive explicitly extends no-fault liability to software, stating that “no-fault liability ... should apply to all movables, including software” (Recital 6; Article 4(1)(1) new PLD). By expressly including software within the definition of “product,” the new PLD removes the previous ambiguity and aligns the law with the technological realities of contemporary AAL systems, where hardware and AI-driven software components are inextricably intertwined.

Under Article 7(1) of the new PLD, a product is defective if it fails to provide the safety that the public at large is entitled to expect. Crucially, Article 7(2)(c) adds that product defectiveness must consider “the effect on the product of any ability to continue to learn or acquire new features after it is placed on the market.” This is pivotal for AAL systems employing machine learning and continuous updates. Unlike static products, AI-driven AAL solutions can evolve post-deployment, altering their functionality and risk profiles over time. By incorporating continuous learning capabilities into the legal definition of defectiveness, the new PLD ensures that the changing nature of AI models and software updates is directly accounted for in assessing liability.

In addition, Article 4(5) of the new PLD introduces the concept of “manufacturer’s control.” Manufacturers remain liable if they retain the ability to supply software updates or authorize third-party integrations after the product’s initial placement on the market. This continuous control principle prevents manufacturers from attributing defects solely to later changes introduced post-sale. Given that modern AAL products often undergo iterative improvements, feature expansions, and new software integrations long after their initial release, maintaining manufacturer accountability throughout the product’s lifecycle is essential for consumer protection.

To address the evidentiary challenges posed by complex, adaptive technologies, Article 10 of the new PLD incorporates rebuttable presumptions for defectiveness and causation in scientifically challenging cases. For example, if an AI-driven fall detection algorithm fails and causes harm, these presumptions help claimants overcome the difficulty of proving the link between the algorithm’s defect and the resulting injury. Furthermore, Article 9 establishes disclosure obligations, ensuring that claimants can access key technical evidence (such as source code, update logs, and product documentation) controlled by the manufacturer. These measures promote

²¹ U.S. Food and Drug Administration. (n.d.). *Software as a medical device (SaMD)*. U.S. Department of Health and Human Services. Retrieved September 14, 2024, from <https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd>

transparency, fairness, and facilitate the effective enforcement of liability claims in an era of sophisticated digital products.

Comparing the old regime to Directive (EU) 2024/2853 highlights a significant advancement. Previously, intangible software defects and continuously learning AI functionalities often fell into a legal grey area, leaving victims vulnerable and uncertain about their rights. Now, by explicitly treating software and AI-driven components as integral product elements and recognizing their evolving nature, the new PLD offers a harmonized liability model that better supports the hybrid character of AAL systems. Strict liability no longer applies solely to tangible parts of AAL systems but extends seamlessly to intangible, adaptive digital elements as well. This integrated approach eliminates the need for supplementary liability regimes specifically for software and aligns EU product liability law with cutting-edge technological developments.

In sum, Directive (EU) 2024/2853 ensures that AAL systems, which rely heavily on intelligent software and ongoing updates, fall squarely under a clear, no-fault liability standard. By fully incorporating intangible digital components and continuous learning capabilities into the product liability framework, the EU has created a more coherent, future-proof legal environment.

2.1.3. Medical Device Regulation (MDR)

The Medical Device Regulation (MDR)²² governs products intended for medical purposes, including those used for diagnosis, monitoring, or treatment (Article 2(1), MDR). AAL systems incorporating health-monitoring functionalities may fall under the MDR, subjecting them to stringent regulatory requirements such as clinical evaluations and ongoing risk assessments. The classification of AAL systems under the MDR hinges on whether their primary function relates to general wellbeing or medical support.

For instance, an AAL system that primarily assists with daily activities, such as medication reminders and mobility support, would likely fall under a lower classification (MDR Annex VIII, Rule 10). In contrast, a system providing real-time health monitoring and emergency medical interventions would require higher regulatory scrutiny. The MDR could introduce clearer guidelines describing the threshold between general wellbeing and medical support functionalities, enabling more precise classification and preventing non-medical AAL systems from being excessively burdened by strict regulatory requirements.

²² Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

2.1.4. Machinery Regulation and Radio Equipment Directive (RED)

The Machinery Regulation (EU) 2023/1230²³ and the Radio Equipment Directive (RED)²⁴ establish essential safety standards for mechanical and wireless communication components, respectively. AAL systems featuring robotic aids or fall detection capabilities must comply with the Machinery Regulation to ensure mechanical safety, while the RED ensures electromagnetic compatibility and safe wireless communication.

Compliance with these directives may involve following ISO 13482²⁵ for safety requirements of personal care robots and ensuring electromagnetic compatibility as per RED standards. Naturally, implementing safety features such as emergency stop mechanisms and fail-safes in robotic components is essential, however, while these directives address physical and communication aspects, they do not encompass software-driven functionalities like AI decision-making, which significantly impact system performance. This highlights the need for regulatory harmonization that integrates software safety into existing frameworks.²⁶

2.1.5. AI Act and AI Liability Directive

The AI Act²⁷ introduces stringent safety, transparency, and oversight requirements for high-risk AI systems, which are particularly relevant to AAL systems reliant on AI for critical functions. The Act mandates continuous risk management, guaranteeing high-quality training data, and effective human oversight mechanisms (Articles 6, 9, 10, and 14, AI Act). These provisions ensure that AI-driven AAL systems maintain high standards of safety throughout their lifecycle.

In addition, the proposed AI Liability Directive²⁸ will address liability issues specific to AI-related incidents by introducing a rebuttable presumption of causality when AI systems malfunction and cause harm (Article 4, AI Liability Directive). This eases the burden of proof on claimants, facilitating compensation in cases where AI malfunctions.

²³ Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC

²⁴ Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC

²⁵ ISO 13482:2014 Robots and robotic devices — Safety requirements for personal care robots

²⁶ For further reading, see Mahler, Tobias, Smart Robotics in the EU Legal Framework: The Role of the Machinery Regulation (May 30, 2024). Oslo Law Review, DOI: 10.18261/issn.2387-3299, Available at SSRN: <https://ssrn.com/abstract=4848905>

²⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

²⁸ Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)

The Directive also establishes a shared liability framework, holding both AI providers and users accountable for ensuring compliance with safety obligations.

For example, if an AAL system's AI algorithm inaccurately interprets health data, triggering inappropriate emergency alerts, the AI Liability Directive could hold both the provider (responsible for the algorithm's design) and the user (responsible for proper system monitoring) liable. To further bridge regulatory gaps, the AI Act and AI Liability Directive should incorporate explicit guidelines for hybrid systems like AAL, ensuring that both product and service components are adequately regulated and that liability is clearly delineated across different functionalities.²⁹

2.1.6. Practical Examples

2.2.1. Example 1: Fall Detection Failure in AAL Systems

Consider an Ambient Assisted Living (AAL) system equipped with fall detection sensors and an AI algorithm that misinterprets movement data, failing to trigger an emergency alert during a critical incident. Under the General Product Safety Regulation (GPSR) Article 5, the manufacturer's failure to ensure sensor accuracy could breach the general safety obligations required to place safe products on the market. Additionally, GPSR Article 9 mandates that manufacturers conduct thorough risk analyses and maintain technical documentation to ensure product conformity.

At the same time, the updated Product Liability Directive (PLD) Article 7 introduces strict liability for defective sensors, recognizing that such defects compromise the safety expectations of users. This provision reflects a commitment to ensuring that products meet the reasonable safety standards expected by the public. Furthermore, Articles 5 and 10 of the PLD work together to protect injured parties by removing the need to prove negligence on the part of the manufacturer. Article 5 establishes a clear right to compensation for harm caused by defective products, emphasizing the directive's focus on consumer protection. Complementing this, Article 10 alleviates the evidentiary burden on claimants, particularly in complex cases, by allowing the use of presumptions to establish defectiveness and causation, thereby ensuring access to justice even in technologically intricate disputes.

Additionally, the proposed AI Liability Directive might extend liability to both the manufacturer for the algorithm and the user for improper monitoring. To mitigate such risks, manufacturers could implement redundant sensor systems to enhance reliability, conduct regular software updates and algorithm validations, and perform comprehensive risk assessments in alignment with GPSR and AI Act requirements.

²⁹ Hacker, P. (2023). AI Regulation in Europe: From the AI Act to Future Regulatory Challenges. arXiv preprint arXiv:2310.04072.

2.2.2. Example 2: Medication Reminder Malfunction in AAL Systems

Another example is an AAL system's medication reminder feature malfunctioning due to a software glitch, resulting in missed doses for the user. If classified under the Medical Device Regulation (MDR) Articles 2 and 52, stringent conformity assessments as outlined in MDR Articles 50-60 and Annex IX would apply. Compliance with the AI Act Articles 13 and 14 would require robust data governance and transparent algorithmic decision-making, while adherence to the Radio Equipment Directive (RED) Articles 3 and 7 would ensure reliable wireless communication.

Manufacturers can address these challenges by following MDR conformity assessment procedures (MDR Articles 50-60), implementing robust data validation and error-handling mechanisms within the software (AI Act Article 13), and ensuring compliance with RED standards for wireless communication reliability (RED Articles 3 and 7). Additionally, establishing comprehensive user training and support systems can help mitigate improper usage that may lead to system malfunctions. These measures collectively highlight the importance of integrating regulatory compliance into the design and maintenance of AAL systems to ensure user safety and legal conformity.

2.2. Stakeholders' Perspectives

Understanding the perspectives of various stakeholders is fundamental to developing an effective regulatory framework for Ambient Assisted Living (AAL) systems.³⁰ Such a framework must ensure safety, reliability, and innovation to enhance the quality of life for end-users, including elderly individuals and people with disabilities, while also fostering technological advancement and market growth.³¹

Manufacturers of AAL systems navigate both product and service regulations, striving to streamline compliance processes to accelerate market entry. Their primary goal is to avoid excessive regulations that could hinder technological progress, allowing them to innovate and bring advanced AAL solutions to consumers swiftly. Service providers, on the other hand, are tasked with ensuring that their offerings meet stringent safety standards and effectively address user needs. They must balance the introduction of innovative features with the reliability required by consumers.³² Key priorities for service providers include maintaining operational flexibility to adapt to evolving

³⁰ KUŹMICZ, M. M. Who Should We Care About in the Digital World? Challenges of Stakeholders' Identification—The Case Study of AAL. *DATA PROTECTION AND PRIVACY*, 231.

³¹ Kastl, A., Rauner, Y. N., Mayer-Huber, S., Oestreich, C., Benstetter, F., & Fettke, U. (2024). Stakeholder needs assessment for developing ageing in place solutions—a qualitative study. *BMC geriatrics*, 24(1), 104.

³² Calvaresi, D., Cesarini, D., Sernani, P. et al. Exploring the ambient assisted living domain: a systematic review. *J Ambient Intell Human Comput* 8, 239–257 (2017). <https://doi.org/10.1007/s12652-016-0374-3>

regulations, managing data effectively to safeguard privacy while enabling comprehensive monitoring and analytics, and ensuring interoperability for seamless integration with various hardware and software platforms.³³

End-users and their caregivers prioritize the usability, data privacy, and dependability of AAL solutions. Their main concern is to improve their quality of life without introducing new risks, ensuring that the technologies are accessible, user-friendly, and reliable in performing as intended. Meanwhile, regulatory bodies seek clear guidelines on liability distribution to minimize legal uncertainties and ensure accountability among all parties involved. Their focus lies in comprehensive coverage of all aspects of AAL systems, adaptability to keep pace with technological advancements, and harmonization of EU regulations with international standards to facilitate market integration.³⁴

To develop an effective regulatory framework, it is crucial to balance the diverse priorities of all stakeholders. For manufacturers and service providers, streamlining compliance processes and fostering innovation are vital. Regulations should be designed to facilitate rather than impede technological advancements, allowing manufacturers to bring products to market efficiently while ensuring that service providers maintain high safety and reliability standards. For end-users and caregivers, ensuring that AAL systems are user-friendly, protect personal and health data, and are dependable is paramount. Accessibility and usability must be prioritized to meet the diverse needs of users effectively. For regulatory bodies, establishing clear liability guidelines and comprehensive coverage ensures that all aspects of AAL systems are adequately regulated.³⁵ Regulations must be adaptable to evolving technologies and harmonized with international standards to support market integration and global interoperability.

Engaging with stakeholders through consultations and collaborative platforms is essential to gather valuable insights and foster a regulatory environment that balances safety, innovation, and consumer protection. Facilitating ongoing dialogue among manufacturers, service providers, end-users, caregivers, and regulatory bodies helps inform regulatory decisions and address emerging challenges collaboratively. Developing adaptable regulations that can evolve with technological advancements is also crucial, incorporating mechanisms for regular review and updates to stay current

³³ Cicirelli, G., Marani, R., Petitti, A., Milella, A., & D'Orazio, T. (2021). Ambient Assisted Living: A Review of Technologies, Methodologies and Future Perspectives for Healthy Aging of Population. *Sensors*, 21(10), 3549. <https://doi.org/10.3390/s21103549>

³⁴ Queirós, A., Silva, A., Alvarelhão, J. *et al.* Usability, accessibility and ambient-assisted living: a systematic literature review. *Univ Access Inf Soc* 14, 57–66 (2015). <https://doi.org/10.1007/s10209-013-0328-x>

³⁵ Caballero, P., Ortiz, G. & Medina-Bulo, I. Systematic literature review of ambient assisted living systems supported by the Internet of Things. *Univ Access Inf Soc* 23, 1631–1656 (2024). <https://doi.org/10.1007/s10209-023-01022-w>

with industry developments. Additionally, aligning EU regulations with global standards enhances interoperability and market access, enabling cross-border collaboration and integration of AAL technologies. Creating a well-structured regulatory framework for AAL systems requires a nuanced understanding of stakeholder perspectives and a balanced approach to regulation. By engaging stakeholders and harmonizing safety, innovation, and consumer protection, regulators can support the growth and effectiveness of AAL technologies. Ongoing collaboration and adaptability will be key to addressing future challenges and ensuring that AAL systems continue to enhance the quality of life for their users.³⁶

2.3. Technical and Operational Compliance

AAL systems must follow to various technical standards and best practices to ensure regulatory compliance. Interoperability standards, such as ISO/IEC 27001³⁷ for information security and IEEE 11073³⁸ for health informatics, are essential for ensuring compatibility and data integrity. Compliance with the General Data Protection Regulation (GDPR)³⁹ is vital, particularly concerning the collection, processing, and storage of sensitive health data. Additionally, robust cybersecurity measures are required to protect against data breaches and unauthorized access, aligning with the GPCR's cybersecurity obligations.

Certification and testing play a critical role in ensuring that AAL systems meet all necessary safety and performance standards. Providers must obtain relevant certifications, such as CE marking under the MDR and RED, and conduct regular testing and validation of both hardware and software components. Implementing secure coding practices,⁴⁰ conducting vulnerability assessments, and adhering to standardized compliance protocols are essential steps in maintaining ongoing compliance and mitigating risks associated with AAL system functionalities.

2.4. Conclusions

Addressing the regulatory gaps in AAL systems requires a comprehensive and integrated approach. First, establishing an "Integrated Systems" classification

³⁶ Márquez, G., & Taramasco, C. (2023). Barriers and Facilitators of Ambient Assisted Living Systems: A Systematic Literature Review. *International Journal of Environmental Research and Public Health*, 20(6), 5020. <https://doi.org/10.3390/ijerph20065020>

³⁷ ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

³⁸ CEN ISO/IEEE 11073 Health informatics - Medical / health device communication standards

³⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

⁴⁰ For example, see OWASP Secure Coding Practices - Quick Reference Guide. Retrieved from: <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/>

acknowledges the inseparable combination of hardware, software, and services in AAL, ensuring all components are comprehensively regulated. To clarify liability, introducing a supplementary regime within the Product Liability Directive (PLD) and AI Liability Directive specifically for software and AI defects is essential.⁴¹

Creating cross-sectoral regulatory bodies focused on hybrid technologies like AAL systems would guarantee coordinated oversight across different domains. Additionally, implementing standardized compliance protocols that unify product safety, liability, data privacy, and AI governance would streamline regulations, reducing complexity for AAL providers.⁴² Balancing automation with human oversight maintains user autonomy and trust. Maintaining ethical standards requires integrating human oversight processes, increasing transparency in decisions driven by AI, and guaranteeing accountability.

⁴¹ Buiten, M.C. Product liability for defective AI. *Eur J Law Econ* 57, 239–273 (2024). <https://doi.org/10.1007/s10657-024-09794-z>

⁴² da Fonseca, A.T., Vaz de Sequeira, E., Barreto Xavier, L. (2024). Liability for AI Driven Systems. In: Sousa Antunes, H., Freitas, P.M., Oliveira, A.L., Martins Pereira, C., Vaz de Sequeira, E., Barreto Xavier, L. (eds) *Multidisciplinary Perspectives on Artificial Intelligence and the Law*. Law, Governance and Technology Series, vol 58. Springer, Cham. https://doi.org/10.1007/978-3-031-41264-6_16

3. Medical Devices Regulation (MDR)

Under the Medical Devices Regulation (MDR)⁴³, safety evolves from a theoretical concept into a legally binding standard that rigorously oversees the design, manufacturing, and implementation of medical devices, including those essential to Ambient Assisted Living (AAL) technologies. These technologies are increasingly integrated into home environments to enhance users' health and independence, necessitating strict adherence to the safety and performance standards set forth by the MDR. Ensuring the safety of AAL systems requires navigating a complex regulatory landscape, where each product's intended use and specific characteristics determine its classification and the corresponding legal requirements.

3.1. AAL in the light of MDR

3.1.1. Software as a Medical Device (SaMD)

A crucial aspect of the MDR is its governance over Software as a Medical Device (SaMD). It is imperative to distinguish that not all health-related software qualifies as SaMD. According to the International Medical Device Regulators Forum (IMDRF)⁴⁴, SaMD refers to software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device. For instance, a mobile application that analyses electrocardiogram (ECG) data to detect arrhythmias is classified as Software as a Medical Device (SaMD) under Article 2(1) and Article 2(2) of the MDR, thereby subjecting it to stringent regulatory scrutiny under Article 51 and the classification rules outlined in Annex VIII. In contrast, applications designed solely for general health or wellness, such as fitness trackers that monitor daily steps, do not meet the definition of a medical device as specified in Article 2(1) and thus are not regulated by the MDR.

3.1.2. Classification of AAL Technologies under MDR

Under the Medical Device Regulation (MDR), the intended use of a product is decisive in determining its classification into risk categories—Class I, IIa, IIb, or III—based on the potential harm it may pose to users (MDR, Article 51). Ambient Assisted Living (AAL) technologies designed for health monitoring, such as those tracking heart rates, predicting falls, or monitoring other vital health metrics, are typically classified as Software as a Medical Device (SaMD). This classification subjects them to stringent

⁴³ Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

⁴⁴ International Medical Device Regulators Forum. (2014). *Software as a medical device (SaMD): Key definitions*. <https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf>

regulatory requirements. Specifically, Rule 11 of the MDR addresses software-based medical devices, assigning higher risk categories to systems that monitor physiological processes or inform decisions that could have significant health implications. For instance, an AAL system utilizing artificial intelligence to predict health deterioration would be classified as a Class IIb medical device under the MDR.

Rule 11 plays a central role in the regulation of AAL technologies, particularly those involved in physiological monitoring or disease prediction. Devices categorized under Class IIa or IIb face substantial regulatory demands, including pre-market evaluations and ongoing post-market surveillance, all aimed at ensuring patient safety and the efficacy of the device. To effectively navigate these regulatory obligations, developers can adopt an integrated compliance framework that aligns the requirements of both the MDR and the AI Act. This approach enables systematic compliance to each regulatory mandate, thereby guaranteeing that AAL technologies meet the necessary standards for safety and performance.

3.1.3. Wellness and Medical Devices

The boundary between wellness and medical devices is increasingly indistinct, particularly as healthcare shifts from clinical settings to home-based environments. According to MDR, Article 2, a device intended for medical purposes is classified differently from those intended solely for general well-being. For instance, a smart bed that monitors sleep patterns for general well-being might be classified as a wellness device. However, under MDR, Article 3, if the same bed is utilized to detect sleep apnea by analysing breathing patterns, it would likely be reclassified as a medical device under the MDR, necessitating compliance with stricter regulatory standards as specified in Annex VIII of the MDR. This evolution raises critical questions about the scope of regulatory protection and whether such technologies fall under stringent medical device regulations or general product safety frameworks, as outlined in MDR, Article 5.

3.2. MDR and other Laws

3.2.1. General Data Privacy Regulation (GDPR)

Confirming compliance with data privacy regulations, particularly the General Data Protection Regulation (GDPR), is principal for Ambient Assisted Living (AAL) technologies. These devices routinely collect sensitive health-related data, making strict compliance to GDPR essential. Developers must guarantee that data processing is conducted lawfully, based on clear and informed user consent. Additionally, it is critical to implement robust data protection measures to safeguard user information against breaches and unauthorized access. This involves practices such as data minimization, obtaining explicit consent from users, and establishing ample data security protocols. By adhering to these principles, AAL technologies not only comply

with GDPR but also align with the requirements set forth by the Medical Device Regulation (MDR) and the Artificial Intelligence Act.⁴⁵

3.2.2. AI Act

The regulatory landscape is further complicated by the introduction of the EU's Artificial Intelligence (AI) Act in 2024. The AI Act complements the MDR by introducing a risk-based classification system for AI systems, categorizing them based on their potential risk to safety and fundamental rights (AI Act, Article 6). Article 5 outlines the classification criteria, ensuring a clear framework for risk assessment. High-risk AI systems, particularly those in healthcare and Ambient Assisted Living (AAL), must meet stringent requirements concerning safety (AI Act, Article 10), transparency (AI Act, Article 13), and human oversight (AI Act, Article 14). For example, an AAL system employing AI to predict health deterioration must follow both MDR classification as a Class IIb device (MDR, Article 51) and the high-risk criteria under the AI Act. MDR, Annex VIII details the classification rules for medical devices, ensuring that such devices meet the necessary safety and performance standards. This dual regulatory environment necessitates comprehensive compliance strategies to manage rigorous pre-market evaluations (AI Act, Article 19; MDR, Annex II), transparency obligations (AI Act, Article 13), and continuous post-market surveillance (AI Act, Article 21; MDR, Article 83) under both frameworks.

Under the MDR, manufacturers must establish a robust Post-Market Surveillance (PMS) system that continuously monitors the performance of AAL devices in the market.⁴⁶ For AI-driven systems, this includes tracking changes in algorithm performance over time and ensuring that updates do not introduce new risks. Regular reporting of adverse events and proactive risk mitigation strategies are essential components of effective PMS. Additionally, the AI Act emphasizes ongoing risk management and monitoring, particularly relevant for AI-driven AAL technologies operating in sensitive healthcare contexts.

3.2.3. Other

AAL devices often fall under multiple regulatory directives beyond the MDR and the AI Act. For instance, an AAL device incorporating wireless communication features must also comply with the Radio Equipment Directive (RED)⁴⁷. Similarly, the applicability of

⁴⁵ Meszaros, J., Corrales Compagnucci, M., & Minssen, T. (2021). The interaction of the medical device regulation and the GDPR: Do European rules on privacy and scientific research impair the safety & performance of AI medical devices?.

⁴⁶ Tecante, K. E., & Sokija, A. (2022). The periodic safety update report and post market surveillance report under the new EU Medical Device Regulation. *Medical Writing*, 31, 50-55.

⁴⁷ Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC

the General Product Safety Directive depends on the device's intended use and how it is marketed. Manufacturers should perform thorough regulatory assessments to identify all relevant directives and develop compliance strategies that address each requirement cohesively. This approach helps prevent regulatory overlaps and ensures a smooth entry into the market.

Although the primary focus is on EU regulations, it is important to acknowledge that AAL technologies often aim for global markets. Compliance with the Medical Device Regulation (MDR) and the AI Act typically aligns with standards established by other regulatory authorities, such as the U.S. Food and Drug Administration (FDA). By engaging with international standards organizations and keeping abreast of global regulatory developments, developers can enhance their market reach while maintaining compliance. Efforts to harmonize regulations across different regions are crucial for achieving global compliance and fostering innovation within the AAL sector.

3.3. Conclusions

The regulatory framework surrounding AAL technologies is increasingly intricate due to advancements in digital healthcare, AI integration, and the shift towards home-based care environments. The combined pressures of the MDR and the AI Act necessitate that developers engage in advanced legal reasoning and strategic planning to ensure both product safety and regulatory compliance. By implementing integrated compliance frameworks, adhering to data privacy regulations, and adopting flexible strategies to accommodate future regulatory changes, developers can effectively navigate this dual regulatory environment. Clear regulatory guidance and the harmonization of safety standards across jurisdictions will be essential in safeguarding user welfare while fostering innovation in this rapidly expanding field.

4. Cybersecurity

4.1. Cybersecurity challenges

We have observed that the security issues of AAL technologies have a dual nature, encompassing both product safety and cybersecurity. While the focus in the past was more on the physical safety of products, the importance of cybersecurity has increasingly been recognized with the rapid advancement of information technologies. Government agencies are beginning to pay attention to the cybersecurity concerns of digital health technologies and solutions.⁴⁸ For instance, a UK government-commissioned report found that consumer wearable health-tracking devices collect a large amount of health data, and these devices communicate via wireless protocols such as Wi-Fi and Zigbee, which are not adequately encrypted.⁴⁹ Additionally, a report by the European Union Agency for Network and Information Security (ENISA) highlighted that IoT products used in smart home environments may pose serious security risks, but the industry lacks the incentive to enhance security.⁵⁰ As a result, ENISA recommended that EU policymakers adopt clearer liability rules.⁵¹

In the face of these cybersecurity issues, a rapid regulatory response has become crucial. Legal scholars have also recognized that cybersecurity is an important legal issue closely related to the application of emerging information technologies, such as artificial intelligence, in healthcare.

Countries are actively taking action. In the EU, several relevant cybersecurity legal instruments have been introduced over the past decade, including the General Data Protection Regulation (GDPR), particularly Article 32,⁵² the Network and Information Systems (NIS) 2 Directive, which effectively obliges more organizations to implement cybersecurity measures. Incidents like the WannaCry attack on the UK NHS system

⁴⁸ Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, 35(6), 105336. <https://doi.org/10.1016/j.clsr.2019.06.007>

⁴⁹ Malan, J., Eager, J., Lale-Demoz, E., Cacciaguerra, G., & Brady, M. (2020). Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape. 102.

⁵⁰ European Union Agency For Network And Information Security. (2015). Security and Resilience of Smart Home Environments [Report/Study]. European Union Agency For Network And Information Security. <https://www.enisa.europa.eu/publications/security-resilience-good-practices>

⁵¹ European Union Agency For Network And Information Security. (2015). Security and Resilience of Smart Home Environments [Report/Study]. European Union Agency For Network And Information Security. <https://www.enisa.europa.eu/publications/security-resilience-good-practices>

⁵² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance), Regulation (EU) 2016/679 OJ L 119 (2016). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

motivated the creation of the new EU Cybersecurity Act, which established the European cybersecurity certification framework.⁵³

4.2. Suggestions

In response to the cybersecurity issues associated with AAL technologies, we believe that future legislation needs to be strengthened and improved from multiple angles to address the shortcomings of the current legal framework and ensure that the safety of users and systems is effectively protected in the context of rapid technological development.

First, future legislation should enhance proactive measures, such as further clarifying and strengthening the responsibilities of all parties involved in AAL technologies with regard to cybersecurity. This includes not only manufacturers and service providers but also all stakeholders related to AAL technologies.⁵⁴ To ensure the safety of products and services, it is recommended that stricter cybersecurity standards be established, requiring all AAL devices to meet minimum security requirements, such as mandatory encryption, regular security updates, and vulnerability patching. Additionally, the law should introduce clear liability provisions to ensure that if a data breach or system intrusion occurs due to insufficient cybersecurity measures, the responsible parties will be held legally accountable. This clarification of legal liability will incentivize businesses and organizations to invest more resources in improving cybersecurity, thereby enhancing security. In terms of proactive measures, the EU's AI Act has made some noteworthy attempts, such as implicitly presupposing risk identification and risk analysis,⁵⁵ offering valuable references.

Secondly, since AAL technologies and devices are typically developed and deployed through transnational supply chains and service networks, future legislation should promote broader international coordination and cooperation. In terms of cybersecurity standards, certification frameworks, and legal enforcement, cross-border cooperation is particularly important. It is recommended to promote unified global cybersecurity

⁵³ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA Relevance), 151 OJ L (2019). <http://data.europa.eu/eli/reg/2019/881/oj/eng>

⁵⁴ See on the complexity of stakeholders in a potential AAL scenario, Chen, J., Edwards, L., Urquhart, L., & McAuley, D. (2020). Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. *International Data Privacy Law*, 10(4), 279–293. <https://doi.org/10.1093/idpl/ipaa011>

⁵⁵ See generally EU's AI Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance) (2024). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

standards and enhance mutual legal recognition and enforcement cooperation between different countries.

Furthermore, in addition to proactive measures mentioned above, the legislation could also consider enhancing reactive measures, such as encouraging the establishment of cross-border cybersecurity emergency response mechanisms to enable rapid and effective responses to cybersecurity incidents occurring across borders. Such international cooperation would help improve global cybersecurity defences and ensure that countries can coordinate effectively when facing common threats.

To compensate for the current industry's lack of motivation to invest in cybersecurity, future legislation should introduce incentive mechanisms to encourage the industry to voluntarily strengthen cybersecurity measures. It is suggested to establish cybersecurity certification incentive programs that offer tax reductions or other economic incentives for products and services that meet or exceed cybersecurity standards. This not only incentivizes companies to raise security standards but also encourages more innovation and investment. Additionally, legislation should promote collaboration between the public and private sectors, the sharing of cybersecurity best practices, and the establishment of national cybersecurity capacity-building funds to support small and medium-sized enterprises (SMEs) in enhancing their cybersecurity defences, thereby raising the overall safety level of the industry.⁵⁶ Notably, the EU's Cyber Resilience Act (CRA) has made notable efforts in this regard.⁵⁷ The CRA enhances cybersecurity standards for digital products in the EU by introducing mandatory requirements for manufacturers and retailers. It addresses cybersecurity gaps, ensuring products are designed, developed, and maintained securely throughout their lifecycle. Critical products must undergo third-party assessment before being sold, and compliant products will carry the CE marking. The CRA shifts responsibility to manufacturers, enabling consumers and businesses to make informed decisions about secure products. Exemptions include certain open-source software and sectors covered by existing regulations. The act came into force on 10 December 2024, with obligations effective from 11 December 2027.⁵⁸

⁵⁶ See more on good security practices in: European Network and Information Security Agency. (2018). Good practices for security of Internet of things in the context of smart manufacturing. Publications Office. <https://data.europa.eu/doi/10.2824/851384>

⁵⁷ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA Relevance) (2024). <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>

⁵⁸ For detailed purposes and measures of the CRA, see generally recitals of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA Relevance) (2024). <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>

Finally, as emerging information technologies continue to develop, the existing cybersecurity legal framework also needs to be continually updated and expanded. For example, the legal frameworks should be monitored to make sure that they cover more types of AAL devices and technologies, ensuring that these new technologies comply with the highest cybersecurity standards during development and use.

5. Competition law

5.1. Market Dominance and Data-Driven Expansion

5.1.1. Defining the AAL Market

The AAL market includes a wide array of products and services designed to support individuals in their daily lives through technological means. This includes smart home devices, wearable health monitors, AI-driven personal assistants, and integrated healthcare platforms. Key players in this market range from established technology giants to innovative startups specializing in healthcare solutions. The market's scope is further defined by the types of data collected—ranging from health metrics to behavioural patterns—and the interoperability of devices and platforms that underpin effective AAL systems.

5.1.2. Data-Driven Market Power

Market dominance in the AAL sector is increasingly tied to the control and utilization of vast datasets. The European Court of Justice (ECJ) in *Hoffmann-La Roche & Co. AG v. Commission*⁵⁹ defines a dominant position as one of economic strength that allows a company to act independently of competitors and consumers. In AAL markets, dominance can stem not only from data possession but also from the capability to leverage this data through AI and machine learning, thereby enhancing service quality and creating formidable entry barriers.

Recent judgments, *Commission v Ireland*⁶⁰ and *Others and Google and Alphabet v Commission (Google Shopping)*⁶¹, have underscored the importance of data control in assessing market power. These rulings highlight that firms with extensive data repositories can perpetuate their dominance by continuously refining their algorithms, making it arduous for new entrants to compete on equal footing.

5.1.3. Network Effects and Data Accumulation

AI backed systems often exhibit strong network effects,⁶² where the utility of a service increases with the number of users. Dominant firms with access to expansive datasets can improve their offerings through superior AI capabilities, thereby attracting more users and further entrenching their market position. The Organisation for Economic

⁵⁹ Case 85/76, ECLI:EU:C:1979:36, para. 38

⁶⁰ Case C-465/20 P | *Commission v Ireland and Others*

⁶¹ Case C-48/22 P | *Google and Alphabet v Commission (Google Shopping)*

⁶² DiMaggio, P., & Garip, F. (2012). Network effects and social inequality. *Annual review of sociology*, 38(1), 93-118.

Co-operation and Development (OECD) notes that access to vast amounts of data can significantly boost AI development, creating competitive advantages.⁶³

This self-reinforcing cycle (AI flywheel effect) poses significant challenges for competition authorities, necessitating a forward-looking approach that considers both current market share and the potential for dynamic competition. The National Bureau of Economic Research emphasizes the importance of proactive competition policies in rapidly evolving AI markets to address these challenges.⁶⁴ Tackling these challenges allows policymakers to find a balance, one that supports innovation and technological growth while ensuring markets remain fair and competitive, ultimately serving the broader interests of society.

5.2. Abuse of Dominance

Article 102 of the Treaty on the Functioning of the European Union (TFEU) prohibits the abuse of a dominant position within the internal market. In the context of AAL systems, abuses may manifest as predatory pricing, exclusive agreements, or refusal to supply essential datasets or interoperability standards. For instance, a dominant AAL provider might refuse to share critical health data with competitors, thereby stifling innovation and limiting consumer choice.

The *Apple Inc. v. European Commission*,⁶⁵ where Apple was fined €1.84 billion for restricting music streaming app developers, serves as a pertinent example of how digital market abuses are scrutinized. Similarly, the recent judgments referenced above further delineate the boundaries of acceptable behaviour for dominant firms in data-driven markets. These cases reinforce the necessity for competition authorities to rigorously evaluate the impact of data control on market dynamics and consumer welfare.

5.3. Cartels and Anti-Competitive Agreements

Article 101(1) TFEU prohibits agreements that restrict competition within the internal market. In the AAL sector, this includes both explicit agreements, such as collusive pricing or market sharing, and tacit understandings that may arise from industry collaborations. The *Commission v. Anic Partecipazioni SpA* (Case C-49/92 P, ECLI:EU:C:1999:356, para. 115) illustrates that even informal agreements can constitute violations if they impede competition.

⁶³OECD (2024), "Artificial intelligence, data and competition", *OECD Artificial Intelligence Papers*, No. 18, OECD Publishing, Paris, <https://doi.org/10.1787/e7e88884-en>.

⁶⁴ Cockburn, I. M., Henderson, R., & Stern, S. (2018). *The impact of artificial intelligence on innovation* (Vol. 24449). Cambridge, MA, USA: National bureau of economic research.

⁶⁵European Commission. "Commission Fines Apple," March 4, 2024. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161.

Article 101(3) TFEU provides exemptions for agreements that enhance production or distribution, promote technical or economic progress, and allow consumers to benefit without eliminating competition. In the AAL context, collaborations on interoperability standards or joint R&D⁶⁶ initiatives may qualify for such exemptions. However, regulators must meticulously assess these collaborations to ensure they do not inadvertently create barriers to market entry or entrench dominant positions.

5.4. Mergers and Concentrations

The EU Merger Regulation (Article 1) oversees mergers and acquisitions to prevent significant impediments to competition. In the rapidly evolving AAL sector, characterized by high innovation cycles and substantial growth potential, merger control (Article 6) poses unique challenges. The designation of ByteDance as a "gatekeeper"⁶⁷ under the Digital Markets Act (Article 3 DMA) exemplifies how data control (Article 5 DMA) influences merger evaluations.

A notable concern is the phenomenon of "killer acquisitions," where large firms acquire smaller, innovative startups to pre-empt future competition. Recent judgments emphasize the importance of assessing not only the immediate market share but also the long-term implications for innovation and dynamic competition. Competition authorities are increasingly adopting a forward-looking approach (Article 4 EU MR), evaluating potential future market dynamics and the role of data accumulation in sustaining dominant positions.

5.5. Comparative Analysis with Other Jurisdictions

The United States employs a distinct antitrust framework compared to the EU, emphasizing consumer welfare and economic efficiency. The Sherman Act, Clayton Act, and Federal Trade Commission Act form the backbone of US antitrust law, focusing on preventing monopolistic practices and promoting competitive markets. In the context of AAL systems, US authorities are increasingly scrutinizing data monopolization and anti-competitive mergers, aligning with global trends towards stricter digital market regulation.

Major markets in the Asia-Pacific region, such as China and Japan, exhibit unique approaches to competition regulation in the digital and healthcare sectors. China's Anti-Monopoly Law (AML) addresses data-related competition issues, emphasizing state oversight and strategic sector regulation. Japan's Act on Prohibition of Private Monopolization and Maintenance of Fair Trade (Anti-Monopoly Act) similarly targets anti-competitive behaviours, with a growing focus on data-centric market practices.

⁶⁶ A joint research and development agreement

⁶⁷ Case T-1077/23, *Bytedance v. Commission*, , PRESS RELEASE No. 114/24 Luxembourg (2024, July 17).

These comparative insights highlight diverse regulatory strategies that can inform EU policy development in the AAL sector.

5.6. Emerging Technologies and Future Trends

Advancements in AI and machine learning are fundamental in enhancing AAL systems' capabilities. However, these technologies also pose new competition law challenges, such as algorithmic collusion and discriminatory practices.⁶⁸ The opacity of AI decision-making processes requires regulatory oversight to prevent anti-competitive outcomes and ensure transparency and fairness in AAL services.

The establishment of open interoperability standards is essential for promoting competition and preventing vendor lock-in within the AAL ecosystem. Integration between diverse devices and platforms, interoperability promotes a competitive environment where multiple providers can coexist and innovate. Further research indicates that pricing algorithms can learn to collude, leading to supra-competitive prices and reduced market competition.⁶⁹ Additionally, AI-enabled price discrimination allows firms to predict consumers' willingness to pay, potentially resulting in unfair pricing strategies that exploit consumer data.⁷⁰

Again, AAL systems operate at the intersection of technology and healthcare, needing compliance with healthcare-specific regulations. Patient privacy, data security, and medical device approvals are critical considerations that intersect with competition law. Harmonizing competition enforcement with healthcare regulations ensures that AAL innovations enhance care delivery without compromising regulatory standards or market fairness.

5.6.1. Data Protection

The General Data Protection Regulation (GDPR) intersects significantly with competition law, particularly through provisions like data portability (Article 20). Data portability facilitates consumer switching between service providers, potentially lowering entry barriers and enhancing competitive dynamics. However, it also

⁶⁸ See Picht, Peter Georg and Leitz, Anna-Katharina, Algorithms and Competition Law - Status and Challenges (February 5, 2024). Available at SSRN: <https://ssrn.com/abstract=4716705> or <http://dx.doi.org/10.2139/ssrn.4716705>

⁶⁹ Hanspach, Philip and Galli, Niccolò, Collusion by Pricing Algorithms in Competition Law and Economics (February 20, 2024). Robert Schuman Centre for Advanced Studies Research Paper No. 2024_06, Available at SSRN: <https://ssrn.com/abstract=4732527>

⁷⁰ Li, Q., Philipsen, N. & Cauffman, C. AI-enabled price discrimination as an abuse of dominance: a law and economics analysis. *China-EU Law J* 9, 51–72 (2023). <https://doi.org/10.1007/s12689-023-00099-z>;

also see De Hert, Paul and Papakonstantinou, Vagelis and Malgieri, Gianclaudio and Beslay, Laurent and Sanchez, Ignacio, The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services (2018). *Computer Law & Security Review* (2018) 193–203, Available at SSRN: <https://ssrn.com/abstract=3447060>

introduces complexities, as data protection and privacy concerns must be balanced against the imperative to maintain competitive markets.⁷¹

In Ambient Assisted Living (AAL) systems, data portability can empower consumers to transfer their health and behavioural data easily between different platforms, thereby encouraging competition.⁷² However, dominant firms with extensive resources can navigate GDPR compliance more efficiently, potentially reinforcing their market positions. This dichotomy necessitates a nuanced regulatory approach that harmonizes data protection with competition objectives, ensuring that data portability serves as a genuine tool for enhancing market competition without compromising consumer privacy.⁷³

Recent judgments have delved into the practical implications of GDPR provisions on competition. Notably, the European Court of Justice (ECJ) ruled in October 2024 that national laws may permit competitors to bring actions against companies for GDPR infringements under unfair competition practices.⁷⁴ This decision underlines the necessity for regulators to consider both data protection and competitive effects when evaluating business practices in data-intensive sectors like AAL. By addressing the interplay between these regulatory areas, courts reinforce the importance of a balanced approach that upholds both consumer rights and market integrity.

5.6.2. Digital Economy

The DMA and DSA, effective since 2023, introduce significant regulatory measures targeting large digital platforms. The DMA aims to prevent self-preferencing and mandates interoperability, ensuring smaller companies can compete on a level playing field. For AAL systems, these provisions are crucial as access to essential data and services is often concentrated among dominant players. The ByteDance case,⁷⁵ one of the initial applications of the DMA, emphasises the regulatory focus on safeguarding competition through stringent oversight of data practices.⁷⁶

⁷¹ Jeon, DS., Menicucci, D. Data portability and competition: Can data portability increase both consumer surplus and profits?. *Eur J Law Econ* **57**, 145–162 (2024). <https://doi.org/10.1007/s10657-023-09774-9>

⁷² Wilkowska, W., Offermann, J., Colonna, L. *et al.* Interdisciplinary perspectives on privacy awareness in lifelogging technology development. *J Ambient Intell Human Comput* **14**, 2291–2312 (2023). <https://doi.org/10.1007/s12652-022-04486-5>

⁷³ Wilkowska W, Offermann J, Spinsante S, Poli A, Ziefle M (2022) Analyzing technology acceptance and perception of privacy in ambient assisted living for using sensor-based technologies. *PLoS ONE* **17**(7): e0269642. <https://doi.org/10.1371/journal.pone.0269642>

⁷⁴ Case C-21/23, Lindenapotheker

⁷⁵ Case T-1077/23, Bytedance v. Commission, PRESS RELEASE No. 114/24 Luxembourg (2024, July 17).

⁷⁶ Moreno Bellosa, Natalia and Petit, Nicolas, The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove (April 5, 2023). (2023) 48 *European Law Review* 391, Available at SSRN: <https://ssrn.com/abstract=4411743>

The Digital Services Act (DSA) complements the Digital Markets Act (DMA) by improving transparency and consumer protection, particularly in data handling within digital services. The DSA establishes comprehensive transparency obligations for digital platforms, including requirements for clear terms and conditions, transparency reporting, and mechanisms for users to report illegal content.⁷⁷ These measures aim to empower consumers and ensure accountability in digital services.

Collectively, the DMA and DSA seek to mitigate the entrenched market positions of dominant firms by enforcing fair competition practices and promoting open standards. The DMA targets anti-competitive behaviours by large online platforms, known as "gatekeepers," imposing obligations to ensure fair and open digital markets. The DSA complements this by focusing on the responsibilities of digital services in content moderation and user protection, thereby fostering a safer and more transparent online environment.⁷⁸

The recent Apple⁷⁹ and Google judgments⁸⁰ further elaborate on the application of DMA and DSA provisions, potentially, within the AAL sector. These rulings highlight the judiciary's role in interpreting and enforcing competition laws in the context of data-driven technologies, reinforcing the necessity for continuous regulatory adaptation to emerging market realities.

5.7. Case Studies and Real-World Examples

ECJ decisions reveal how the EU tackles competition issues in digital and technology sectors. By looking at examples like Google's acquisition of Fitbit and Illumina's takeover of Grail, we see the complexities of managing market dominance and promoting innovation. These examples illustrate the EU's efforts to regulate data-driven companies, guarantee fair competition, and protect consumer interests in rapidly evolving industries. These cases also illustrate the balance regulators must maintain between promoting market competitiveness, promoting innovation, and safeguarding consumer choice, particularly in data-driven and technology-centric industries.

See also: Drewes, Helena and Kirk, Alexander, Extraterritorial Effects of the Digital Markets Act - The 'Elusive Long Arm' of European Digital Regulation (March 18, 2024). Available at SSRN: <https://ssrn.com/abstract=4763361> or <http://dx.doi.org/10.2139/ssrn.4763361>

⁷⁷ Nosák, D. (2021). *Overview of Transparency Obligations for Digital Services in the DSA*.

⁷⁸ See: EU Commission "The Digital Markets Act: ensuring fair and open digital markets" retrieved from: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en?

EU Commission "The Digital Services Act Ensuring a safe and accountable online environment" https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en?

⁷⁹ European Commission. (2024, March 4). *Commission fines Apple*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161.

⁸⁰ Case C-48/22 P | Google and Alphabet v Commission (Google Shopping)

In 2021, Google's acquisition of Fitbit attracted significant scrutiny from the European Commission.⁸¹ Google, a dominant entity in online advertising, sought to acquire Fitbit, a leading manufacturer of wearable health devices. The European Commission raised concerns that this merger could enable Google to utilize Fitbit's extensive health data to enhance its advertising algorithms, potentially disadvantaging competitors in the health data analytics and wearable technology markets. Furthermore, the consolidation posed risks of stifling innovation by restricting Fitbit's ability to collaborate with other technology firms, thereby diminishing consumer choices and slowing the advancement of new health-centric technologies. The merger also had the potential to reinforce Google's dominant market position, making it more challenging for new entrants to compete and thereby impacting overall market competitiveness. Following a comprehensive investigation, the Commission imposed conditions to mitigate these risks, including ensuring data portability and preventing Google from restricting Fitbit's access to other services.⁸²

The acquisition of Grail LLC by Illumina Inc. in 2020 serves as an important case in understanding the enforcement of merger controls, especially concerning "killer acquisitions." Grail, a biotech innovator, was targeted by Illumina, a company specializing in genetic analysis solutions. Under the EU Merger Regulation (EUMR),⁸³ the transaction did not meet the necessary jurisdictional thresholds for merger control review since Grail had no sales in Europe. Nonetheless, the European Commission (EC), prompted by referrals from national agencies under Article 22 of the EUMR, sought to block the acquisition, arguing that it could reduce future competition in cancer diagnostic testing within Europe. The EC imposed a fine exceeding €400 million on Illumina for proceeding without approval and ordered the unwinding of the acquisition.⁸⁴

However, on September 3, 2024, the European Court of Justice (ECJ) ruled that the EC had overstepped its authority by applying Article 22 to transactions that did not meet the relevant thresholds, emphasizing the importance of foreseeability and legal certainty in merger control. This decision has significant implications for future enforcement against "killer acquisitions" in Europe, highlighting the need for clear and

⁸¹ European Commission. (2020). Case M.9660 – Google/Fitbit: Commission Decision of 17 December 2020.

⁸² Vande Walle, S. (2021). The European Commission's Approval of Google/Fitbit—A Case Note and Comment. *CONCURRENCES COMPETITION LAW REVIEW*, (3-2021). See also Vande Walle, S. (2021). The European Commission Clears the Acquisition of a Maker of Fitness Trackers and Smartwatches by a Major Online Platform, Subject to Long-Lasting Behavioural Remedies (Google/Fitbit, M. 9660). *Concurrences Competition Law Review*, (3-2021), 123-127.

⁸³ Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation)

⁸⁴ European Court of Justice. (2024). *Illumina Inc. v. European Commission* (Joined Cases C-611/22 P and C-625/22 P). <https://curia.europa.eu/juris/document/document.jsf?docid=289718&doclang=EN>; for General court Judgement see *Illumina, Inc. v. European Commission*, Case T-227/21, ECLI:EU:T:2022:447 (General Court July 13, 2022). Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021TJ0227>

predictable rules. Antitrust agencies may need to reconsider their strategies, potentially amending EUMR thresholds or relying on post-closing investigations under EU antitrust laws. Additionally, EU Member States may continue to play an essential role through their national merger control laws, which vary in their capacity to review below-threshold transactions. The ECJ's ruling underscores the necessity for transparent and consistent regulatory frameworks to guarantee that businesses can ascertain the applicability of merger control measures without ambiguity.

Beyond mergers and acquisitions, interoperability issues are critical in maintaining competition within the AAL sector. In September 2024, the European Commission initiated proceedings to ensure that Apple complies with interoperability obligations under the Digital Markets Act (DMA).⁸⁵ The focus of these proceedings is to guarantee that Apple's iOS operating system effectively interoperates with third-party devices such as smartwatches and headphones. The Commission aims to ensure that Apple's process for handling interoperability requests from developers is transparent, timely, and equitable. These proceedings are anticipated to conclude within six months, with non-compliance potentially leading to formal investigations and significant fines.⁸⁶

Under the DMA, Apple is mandated to provide free and effective interoperability to third-party developers and businesses that utilize hardware and software features controlled by Apple's operating systems, iOS and iPadOS. The Commission has engaged in specification proceedings to formalize the regulatory dialogue with Apple, targeting specific compliance areas. The first proceeding addresses various iOS connectivity features and functionalities essential for connected devices, ensuring effective interoperability with functions such as notifications, device pairing, and connectivity. The second proceeding examines the process Apple has established to handle interoperability requests, aiming to make the process transparent and fair for all developers. These measures comply with the DMA's broader objective of promoting contestable and fair markets in the digital sector by regulating gatekeepers, large digital platforms that serve as critical gateways between business users and consumers.

5.8. Policy Recommendations and Practical Implications

To effectively address the unique aspects of AAL systems, competition laws may require specific adjustments. These could include provisions tailored to data monopolization, enhanced scrutiny of data-driven mergers, and explicit guidelines on

⁸⁵ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)

⁸⁶ *Commission starts first proceedings to specify Apple's interoperability obligations under the Digital Markets Act.* (2024). European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4761

interoperability requirements. Policymakers should consider sector-specific regulations that complement existing competition laws, ensuring comprehensive oversight of AAL market dynamics.⁸⁷

AAL companies must steer complex competition and data protection landscapes. Developing practical guidelines that emphasize proactive compliance, ethical data practices, and transparency can aid firms in adhering to regulatory requirements. Such guidelines should encourage best practices in data management, collaboration, and innovation while mitigating anti-competitive risks.⁸⁸

Regulatory approaches should balance competition enforcement with the promotion of innovation. By supporting collaborative initiatives that drive technological advancements and ensuring that competition laws do not stifle beneficial partnerships, regulators can create an environment conducive to both competitive integrity and technological progress in the AAL sector.⁸⁹

Due to the global scope of digital markets, competition authorities need to strengthen cross-border collaboration to effectively tackle anti-competitive practices in AAL systems. Aligning enforcement standards and coordinating investigations across jurisdictions, especially among the EU, US, and Asia-Pacific regions, is crucial to preventing regulatory arbitrage and ensuring uniform competition oversight.⁹⁰

By proactive and vigorous enforcement authorities should intensify their efforts in investigating practices such as predatory pricing, exclusionary agreements, and anti-competitive mergers. Enhanced vigilance, supported by international cooperation, can safeguard novelty and maintain competitive market structures in the face of evolving technological landscapes.

⁸⁷ Brown, I. (2020). Interoperability as a tool for competition regulation.

⁸⁸ Dantas, C., & Mackiewicz, K. (2022). Are we ensuring a citizen empowerment approach for health data sharing?. *Zagreb, Croatia*, 55.

⁸⁹ Cini, M., & Czulno, P. (2022). Digital single market and the EU competition regime: An explanation of policy change. *Journal of European Integration*, 44(1), 41-57.

⁹⁰ Furman, J. (2019). Unlocking digital competition: Report of the Digital Competition Expert Panel.

6. Consumer law

Consumer law is a critical legal issue related to AAL systems. Article 38 of the Charter of Fundamental Rights of the European Union (Charter) acknowledges consumer protection as a fundamental right, emphasising "a high level of consumer protection in Union policies."⁹¹ Achieving this goal involves two key components. Firstly, Article 169 TFEU emphasizes the protection of consumers' health, safety, and economic interests. These interconnected aspects are addressed through distinct legal acts, each requiring different approaches and measures. Secondly, consumer protection entails empowering consumers through information, education, and organization, as specified in Article 169 TFEU. These strategies collectively ensure comprehensive consumer protection via various secondary laws.⁹²

The visuAAL project research addressed three key issues within consumer law. The first issue pertains to the consumer status, which determines the legal rights and obligations of AAL stakeholders.⁹³ The second issue involves identifying the average and vulnerable consumers within the AAL context.⁹⁴ Lastly, the research examined the information obligation as a consumer protection tool.⁹⁵ This chapter summarizes the findings related to these issues and presents *de lege ferenda* conclusions.

6.1. Consumer status

The concept of the consumer is fundamental in consumer law. Individuals recognized as consumers enjoy specific rights that other entities may be obligated to satisfy. Thus, the legal status of AAL stakeholders hinges on who is designated as a consumer.

⁹¹ Cf. Weatherill, S. (2014). *EU Consumer Law and policy*. Edward Elgar.

⁹² Malczyńska-Biały, M. (2020). European Union consumer policy on product safety in years 2002–2014. *Przegląd Politologiczny*, (1), 93–102. <https://doi.org/10.14746/pp.2020.25.1.7>.

⁹³ Kuźmicz, Maksymilian M. (2024). Who Should We Care About in the Digital World? Challenges of Stakeholders' Identification – The Case Study of AAL. In H. Matsumi, D. Hallinan, E. Kosta, D. Dimitrova, & P. De Hert (Eds.), *Data Protection and Privacy. Ideas That Drive Our Digital World* (Vol. 16). essay, Bloomsbury Publishing.

⁹⁴ Ibid.

⁹⁵ Kuźmicz, Maksymilian Michał. (2022). Information Obligation as a Balancing Tool in the Context of Active and Assisted Living. In A. Petz, E.-J. Hoogerwerf, & K. Mavrou (Eds.), *ICCHP-AAATE 2022 Open Access Compendium "Assistive Technology, Accessibility and (e)Inclusion" Part II* (pp. 260–269). essay, Association ICCHP.; Kuźmicz, Maksymilian Michał. (2023). Inspirations from EU Financial Law for Privacy Protection by Information Obligations in Active and Assisted Living Technologies. In A. Gryszczyńska, W. Wiewiórowski, & G. Szpor (Eds.), *Internet. Hacking* (pp. 172–197). essay, C. H. Beck.; and Kuźmicz, Maksymilian Michał. (2023). Multilayer Information Obligation, and Why We Need I. *Journal on Technology & Persons with Disabilities*, 11, 43–59. <https://doi.org/http://hdl.handle.net/10211.3/225164>.

Legally, the term "consumer" refers to natural persons engaging in commercial activities, such as purchasing goods and services, outside their trade, business, craft, or profession (see Article 2(a) of the Unfair Commercial Practices Directive (UCPD)⁹⁶ and Article 3(17) of the General Product Safety Regulation (GPSR)⁹⁷). Crucially, consumer status is determined not by the actual use or benefit derived from a product but by participation in a transaction outside one's professional domain. Under EU consumer law, seniors buying AAL for personal use and informal caregivers procuring AAL solutions unrelated to their profession are classified as consumers. Conversely, if another individual, such as a family member, purchases the AAL product, that buyer is the consumer under EU law, not the older adult.⁹⁸ Consequently, older adults assisted by AAL do not receive the legal protections afforded to consumers.

This raises the question of whether the law should consider end-users of AAL as consumers, aligning with the economic definition where consumer classification is based on product usage. Recognising AAL users as consumers could help safeguard their interests.⁹⁹

6.2. Definition of vulnerable consumer

A special category of consumers in consumer law is vulnerable consumers. The concepts of the average consumer and the vulnerable consumer are pivotal. The average consumer is a theoretical construct representing an individual who is reasonably well-informed, observant, and circumspect, making decisions rationally (Recital 18 of the UCPD).¹⁰⁰ This construct serves as a benchmark for evaluating the

⁹⁶ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, p. 22–39.

⁹⁷ Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, OJ L 135, 23.5.2023, p. 1–51.

⁹⁸ Kuźmicz, Maksymilian M. (2024). Who Should We Care About in the Digital World? Challenges of Stakeholders' Identification – The Case Study of AAL. In H. Matsumi, D. Hallinan, E. Kosta, D. Dimitrova, & P. De Hert (Eds.), *Data Protection and Privacy. Ideas That Drive Our Digital World* (Vol. 16). essay, Bloomsbury Publishing, p. 244.

⁹⁹ Cf. Ibid., p. 257-258.

¹⁰⁰ In that way the average consumer is understood by the CJEU in, for example, Case C-210/96 Gut Springenheide and Tusky v Oberkreisdirektordes Kreises Steinfurt [1998] ECR I-4657, para. 31; Case C-51/94 Commission of the European Communities v Federal Republic of Germany [1995] ECR I-3599, para. 36. That approach has been criticised as it does not take into account contextual aspects and cognitive biases. Cf. Wilhelmsson, T. (2018). The informed consumer V the vulnerable consumer in European Unfair Commercial Practices Law — a comment. *The Yearbook of Consumer Law 2007*, 211–227. <https://doi.org/10.4324/9780429430862-8>, p. 218.

fairness and transparency of commercial practices and should be interpreted with consideration of social, cultural, and linguistic factors, as per the CJEU.¹⁰¹

In contrast, a vulnerable consumer is someone who, due to specific characteristics or circumstances, may struggle to understand and navigate commercial transactions, making them more susceptible to unfair or deceptive practices.¹⁰² The criteria for consumer vulnerability are specified in the law. Article 5(3) of the UCPD identifies three factors of vulnerability: mental or physical infirmity, age, and credulity. The UCPD's limited list of vulnerability factors has been criticized as paternalistic and arbitrary, as it overlooks the diversity within certain groups, such as older adults, and ignores factors like class-based and state-based vulnerability.¹⁰³

The distinction between average and vulnerable consumers is crucial in the AAL context. For instance, the average consumer might be an older individual or a relative of senior seeking AAL services or devices, needing clarity in the terms of a telehealth service contract. Conversely, a vulnerable consumer in the AAL context could be an elderly person with limited cognitive abilities (mental infirmity) who requires an AAL system for daily living. However, someone with limited technological literacy would rather not qualify as vulnerable under Article 5(3) UCPD.

The GPSR, however, considers "older people and persons with disabilities" as vulnerable consumers (Recital 5 and Article 6(1)(e)). Given that AAL technologies target senior citizens needing assistance due to their limited abilities, it can be argued that they are vulnerable consumers under both the UCPD and GPSR. Consequently, their specific needs must be considered when assessing the safety of AAL products (Article 6(1)(e) GPSR) and the fairness of commercial practices (Article 5(3) UCPD). Further legislative clarification of the distinction between average and vulnerable consumers would enhance legal clarity, ensuring proper allocation of rights and obligations.

¹⁰¹ For instance, Case T-363/04 Koipe Corporaci6n, SL v Office for Harmonisation in the Internal Market (Trade Marks and Designs) (OHIM) [2007] ECR 11-3355, para. 109; Case C-195/14 Bundesverband der Verbraucherzentralen und Verbraucherverbnde - VerbraucherzentraleBundesverband e. V. v Teekanne GmbH & Co KG. Cf. Purnhagen, K. (2017). More reality in the CJEU's interpretation of the average consumer benchmark – also more behavioural science in unfair commercial practices? *European Journal of Risk Regulation*, 8(2), 437–440. <https://doi.org/10.1017/err.2017.13>, p. 437.

¹⁰² European Commission, Consumers, Health, Agriculture and Food Executive Agency. (2016). *Consumer vulnerability across key markets in the European Union Final Report*. Publications Office, p. 41-43.

¹⁰³ Kaprou, E. (2020). The legal definition of 'vulnerable' consumers in the UCPD. *Vulnerable Consumers and the Law*, 51–67. <https://doi.org/10.4324/9781003104650-4>, p. 53-54.

6.3. Information obligations

One of the most critical tools of consumer protection is the informational obligation.¹⁰⁴ This obligation is regulated by various legal acts, including consumer protection directives, the GDPR, and the AI Act. Generally, producers or service providers must inform consumers about the main characteristics of goods or services, product functionality, safety measures, and necessary warnings.¹⁰⁵ The essence of the informational obligation is the consumer's right to know what they are purchasing.¹⁰⁶

Two essential elements of the informational obligation are content and form. The obligation must provide context-specific information that safeguards consumers' interests, and thus, the content depends on the circumstances.

The second element is the form of the information. Legislators often avoid specifying exact delivery methods, offering only general guidelines. However, the EU legislature increasingly emphasizes the importance of how information is presented to ensure consumer understanding.¹⁰⁷

In this regard, EU financial regulations can serve as a source of inspiration for other legal domains. The information obligations for financial products have evolved significantly, especially after the 2008 financial crisis,¹⁰⁸ moving from extensive prospectuses introduced in 1989¹⁰⁹ to concise Key Information Documents (KID) limited to three pages.¹¹⁰ This shift demonstrates the EU legislature's commitment to understandable information. The first component is the language of communication, which should avoid technical terms and jargon, use examples, and adopt a narrative

¹⁰⁴ Cf. Grundmann, S., Kerber, W., & Weatherill, S. (2012). *Party autonomy and the role of information in the internal market*. De Gruyter.

¹⁰⁵ Kuźmicz, Maksymilian Michał. (2022). Information Obligation as a Balancing Tool in the Context of Active and Assisted Living. In A. Petz, E.-J. Hoogerwerf, & K. Mavrou (Eds.), *ICCHP-AAATE 2022 Open Access Compendium "Assistive Technology, Accessibility and (e)Inclusion" Part II* (pp. 260–269). essay, Association ICCHP, p. 263-265.

¹⁰⁶ Beales, H., Craswell, R., & Salop, S. C. (1981). The efficient regulation of Consumer Information. *The Journal of Law and Economics*, 24(3), 491–539. <https://doi.org/10.1086/466997>, p. 492.

¹⁰⁷ Kuźmicz, Maksymilian Michał. (2023). Inspirations from EU Financial Law for Privacy Protection by Information Obligations in Active and Assisted Living Technologies. In A. Gryszczyńska, W. Wiewiórowski, & G. Szpor (Eds.), *Internet. Hacking* (pp. 172–197). essay, C. H. Beck, p. 188.

¹⁰⁸ Kuźmicz, M. M. (2023). Inspirations from EU financial law for privacy protection by information obligations in Active and Assisted Living technologies. In A. Gryszczyńska, W. Wiewiórowski, & G. Szpor (Eds.), *Internet. Hacking*. (pp. 172–197). essay, C.H. Beck., p. 180-188.

¹⁰⁹ Council Directive 89/298/EEC of 17 April 1989 coordinating the requirements for the drawing-up, scrutiny and distribution of the prospectus to be published when transferable securities are offered to the public (OJ L 1989 No. 124, 0008–0015).

¹¹⁰ Article 5 and 6 of the Regulation (EU) 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs) (OJ L 2014 No. 352, p. 1–23).

style¹¹¹ The second component involves the layout and structure, which should facilitate readability and comparability.¹¹²

The aim of the informational obligation is not just to provide information but to do so in a manner comprehensible to the average consumer. Research shows preferences for graphical forms, numerical scales, tables, and narrative language,¹¹³ though oversimplification remains a concern.¹¹⁴ To address this, a Multilayer Information Obligation (MIO) could be introduced, comprising three layers of information. Each layer would be more detailed than the previous one, using various communication forms such as graphic or numeric labels, "yes/no" questions, tables, narrative language, and examples.¹¹⁵

¹¹¹ Colaert, V. (2016). The regulation of PRIIPs: Great ambitions, insurmountable challenges? *Journal of Financial Regulation*, 2(2), 203–224. <https://doi.org/10.1093/jfr/fjw009>, p. 217.

¹¹² Kuźmicz, M. M. (2023). Inspirations from EU financial law for privacy protection by information obligations in Active and Assisted Living technologies. In A. Gryszczyńska, W. Wiewiórowski, & G. Szpor (Eds.), *Internet. Hacking*. (pp. 172–197). essay, C.H. Beck., p.188.

¹¹³ Lusardi, A. (2014). *Visual tools and narratives: New ways to improve financial literacy*. National Bureau of Economic Research., p. 301. Cf. Directorate-General for the Internal Market and Services , & London Economics. (2015). *Consumer Testing Study of the possible new format and content for retail disclosures of packaged retail and insurance based investment products*. Publications Office of the EU. <https://op.europa.eu/en/publication-detail/-/publication/ea428cc5-9e8f-11e5-8781-01aa75ed71a1/language-en/format-PDF/source-search>.

¹¹⁴ Directorate-General for the Internal Market and Services , & London Economics. (2015). *Consumer Testing Study of the possible new format and content for retail disclosures of packaged retail and insurance based investment products*. Publications Office of the EU. <https://op.europa.eu/en/publication-detail/-/publication/ea428cc5-9e8f-11e5-8781-01aa75ed71a1/language-en/format-PDF/source-search>, p. 110-113.

¹¹⁵ Kuźmicz, M. M. (2023). Multilayer Information Obligation, and Why We Need It. *Journal on Technology and Persons with Disabilities*, 11, 43–59. <https://doi.org/http://hdl.handle.net/10211.3/225164>, p. 47-48.

7. Contract law

7.1. Introduction

AAL contracts within the EU operate within a multifaceted legal structure that blends national contract laws with an array of EU regulations and directives. Central to this framework are the AI Act (Regulation (EU) 2024/1689),¹¹⁶ the NIS 2 Directive (Directive (EU) 2022/2555),¹¹⁷ the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679),¹¹⁸ the Medical Devices Regulation (Regulation (EU) 2017/745),¹¹⁹ and the Product Liability Directive (DIRECTIVE (EU) 2024/2853).¹²⁰ Additionally, foundational regulations such as the Rome I Regulation¹²¹ and the Brussels I Regulation¹²² play essential roles in contract formation and dispute resolution. This section aims to clarify the contractual obligations and legal considerations vital for AAL systems within the European Union (EU). By harmonizing national laws with relevant EU regulations and directives, the analysis explores the current legal background and suggests improvements to establish legally sound, consumer-friendly, and compliant AAL contracts.

7.1.1. Regulation and Directive Overview

For AAL systems in the EU, contract law delineates the roles and responsibilities of manufacturers, service providers, and consumers. AAL technologies often manage sensitive data, adhere to stringent safety standards, and operate across multiple jurisdictions, necessitating comprehensive contract provisions that address liability, data protection, and dispute resolution. The EU legal framework significantly shapes

¹¹⁶ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

¹¹⁷ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

¹¹⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

¹¹⁹ Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

¹²⁰ Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC

¹²¹ Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)

¹²² Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters

contractual norms, requiring the integration of various regulations and directives into agreements.

The AI Act establishes comprehensive rules for AI systems, categorizing them based on risk levels (Article 6). AAL systems typically fall under the high-risk category due to their impact on health and safety, necessitating stringent compliance measures such as transparency (Article 13), human oversight (Article 14), and robust risk management practices (Articles 17-18). Similarly, the NIS 2 Directive imposes enhanced cybersecurity obligations on essential service providers, including those offering AAL services, emphasizing the implementation of adequate security measures (Articles 21, 23) and incident reporting protocols (Article 20) to protect critical infrastructure and sensitive data (Smith & Nguyen, 2023).

GDPR provides a robust framework for data protection, which is particularly relevant to AAL systems that process sensitive health data. It outlines principles for lawful data processing (Article 5), data subject rights (Articles 12–23), and data security requirements (Article 32). For AAL systems classified as medical devices, the Medical Devices Regulation ensures compliance with rigorous safety and performance standards, including post-market surveillance (Articles 14-15) and continuous compliance monitoring (Article 10). The new Product Liability Directive extends producer liability to defective AAL systems (Article 7), imposing obligations on manufacturers and providers to guarantee product safety and address liabilities arising from defects (Jones, 2024).

Furthermore, the Rome I Regulation and the Brussels I Regulation govern the choice of law in contractual agreements and jurisdictional issues, respectively. These regulations are pivotal for cross-border AAL contracts, providing clarity in legal obligations and dispute resolution mechanisms. This overview underscores the significance of these regulations and directives in shaping the contractual landscape for AAL systems

7.2. Contract Formation and Governing Law

The formation of AAL contracts is primarily influenced by national laws; however, EU-level regulations play a significant role, especially in cross-border contexts. The Rome I Regulation facilitates the selection of applicable law in contracts, granting parties autonomy while safeguarding consumer protections. Specifically, Article 3 of Rome I allows parties to choose the governing law, whereas Article 6 mandates compliance with mandatory protections based on the consumer's habitual residence. This dual approach is particularly relevant for AAL contracts, where consumer safety and data protection are utmost.¹²³

¹²³ Schmon, C. (2020). *The Interconnection of the EU Regulations Brussels I Recast and Rome I*. TMC Asser Press. For further reading see: Siegmann, C., & Anderljung, M. (2022). The Brussels effect and

In addition, the Brussels I Regulation addresses jurisdictional matters by enabling parties to agree on competent courts for dispute resolution. Article 25 of Brussels I is instrumental in establishing jurisdiction clauses, ensuring efficient dispute handling in cross-border AAL agreements. These regulations collectively provide a structured framework for contract formation and governance, enhancing legal certainty and reducing potential conflicts

7.3. Specific Contractual Clauses in AAL Agreements

Effective AAL contracts must incorporate specific clauses that address licensing, service levels, data protection, termination, and remedies. These contractual components are essential for integrating relevant regulatory requirements and best practices, ensuring that both providers and consumers are adequately protected.

7.3.1. Licensing Agreements

Licensing agreements for AAL software must clearly define usage rights, intellectual property (IP) protections, and prohibitions on reverse engineering. Article 13 of the AI Act mandates transparency for high-risk AI systems, requiring comprehensive documentation within licensing agreements. This includes defining the scope of use, limitations, and permitted modifications, as well as safeguarding the provider's IP rights and prohibiting unauthorized use or distribution. Additionally, provisions preventing the deconstruction or replication of the software are essential to maintain IP integrity. Directive 2009/24/EC¹²⁴ on the Legal Protection of Computer Programs, particularly Articles 5 and 6, further governs the scope of software licenses, addressing the transfer of rights and reverse engineering restrictions, which must be harmoniously integrated into licensing agreements

7.3.2. Service Level Agreements (SLAs)

Service Level Agreements (SLAs) are critical in defining the performance standards of AAL systems, encompassing uptime, reliability, and response times. Article 9 of the AI Act emphasizes risk management for high-risk AI systems, which should be reflected in SLAs through clear definitions of performance metrics, including uptime percentages, service reliability benchmarks, and response time expectations. Additionally, SLAs should outline strategies for identifying, assessing, and mitigating risks associated with system performance, as well as specify the roles and

artificial intelligence: How EU regulation will impact the global AI market. *arXiv preprint arXiv:2208.12645*.

¹²⁴ Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs

responsibilities of human operators in cases of system malfunctions, as required by Article 16 of the AI Act.¹²⁵

The NIS 2 Directive further imposes cybersecurity obligations, compelling SLAs to incorporate security measures to protect against data breaches and cyber threats. This includes clear timelines and procedures for reporting security incidents, as stipulated in Article 21 of the NIS 2 Directive, and strategies for maintaining service continuity and mitigating disruptions in the event of security breaches or system failures.

7.3.3. Data Protection Clauses

Given the sensitive nature of health data processed by AAL systems, robust data protection clauses are indispensable. The General Data Protection Regulation (GDPR), particularly Articles 5, 6, and 32, provides a comprehensive framework outlining core principles of data processing, lawful bases for data processing, and conditions for processing special categories of data such as health information. Additionally, Article 10 of the AI Act mandates that high-risk AI systems safeguard data quality, accuracy, and integrity. Consequently, data protection clauses must encompass detailed protocols for safeguarding health data against unauthorized access and breaches, clear terms outlining the roles and responsibilities of data processors and controllers, and the integration of cybersecurity measures to protect sensitive personal data

7.4. Consumer Contracts and Unfair Terms

AAL contracts frequently involve consumers who may lack technical expertise, necessitating consumer protection measures to ensure fairness and transparency. This section examines the regulations governing unfair contract terms and information disclosure requirements, emphasizing the protection of consumer rights within AAL agreements.

The Unfair Terms in Consumer Contracts Directive¹²⁶ safeguards consumers from terms that create significant imbalances between them and service providers. In the context of AAL contracts, terms that limit liability or impose onerous obligations must be carefully scrutinized to prevent unfairness. Article 3 of the directive defines a term as unfair if it causes a significant imbalance, considering factors such as transparency and fairness. Terms must be clear and understandable, avoiding complex legal jargon, and provisions should not unduly favor the service provider at the expense of consumer rights.

¹²⁵ Nicolazzo, S., Nocera, A., & Pedrycz, W. (2024). Service Level Agreements and Security SLA: A Comprehensive Survey. *arXiv preprint arXiv:2405.00009*.

¹²⁶ Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts

Transparency is paramount in consumer contracts, especially for AAL systems involving complex AI technologies. The Consumer Rights Directive¹²⁷ mandates comprehensive pre-contractual disclosures, particularly Articles 6 and 7, including detailed explanations of the system's capabilities and intended use, transparent disclosure of all associated costs, and a thorough articulation of the contractual terms, including the rights and obligations of both parties. Article 13 of the AI Act complements these requirements by obligating providers to inform consumers about the capabilities and limitations of AI systems. Failure to provide adequate disclosure can result in legal consequences, such as contract nullification or extended withdrawal rights, underscoring the necessity for thorough and transparent information dissemination in AAL contracts.¹²⁸

Termination clauses and remedies for breach are critical components of AAL contracts, guaranteeing that both parties have clear expectations and recourse in the event of non-compliance or system failures. Effective termination clauses must safeguard consumers who depend on AAL systems for vital services, incorporating provisions that ensure continuity and support during transitions. This includes implementing measures such as backup plans that provide temporary alternatives or additional support to vulnerable users, and establishing clear timelines for notifying users about termination to allow sufficient time for transitioning to other services without undue hardship. Compliance with relevant regulations like the AI Act ensures that termination provisions protect consumer interests and maintain service continuity.

Enforcing AAL contracts across EU Member States presents unique challenges despite regulatory frameworks designed to streamline such processes. Procedural variations, language barriers, and differing legal interpretations can complicate cross-border contract enforcement. The Brussels I Regulation enables the recognition and enforcement of court decisions across EU Member States, but issues such as translation of legal documents and varying judicial efficiencies can impede the process. To address these challenges, strategic approaches such as utilizing neutral jurisdictions for dispute resolution and incorporating Alternative Dispute Resolution (ADR) mechanisms within contractual agreements are effective. ADR methods, including mediation or arbitration, typically require less time and incur lower costs

¹²⁷ Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights

¹²⁸ See also Ruggeri, F., Lagioia, F., Lippi, M. *et al.* Detecting and explaining unfairness in consumer contracts through memory networks. *Artif Intell Law* **30**, 59–92 (2022). <https://doi.org/10.1007/s10506-021-09288-2>

compared to traditional litigation, offering a more adaptable framework for resolving conflicts.¹²⁹

7.5. Future Directions and Legal Innovations in Contract Law for AAL

As AAL technologies continue to evolve, so must the legal frameworks governing their contractual arrangements. This section explores emerging legal innovations and future trends poised to shape AAL contract law.

The development of model contracts is instrumental in establishing a uniform legal framework that simplifies compliance with a broad spectrum of EU regulations. These model contracts typically include accurately drafted template clauses and thorough compliance checklists. Template clauses provide standardized legal language addressing critical contractual elements such as intellectual property rights, data protection obligations, cybersecurity measures, liability allocations, and dispute resolution mechanisms. This standardization reduces the likelihood of contractual ambiguities and disputes. Compliance checklists are employed to systematically verify that contracts adhere to all pertinent regulatory standards, including those established by GDPR, the Medical Devices Regulation, and sector-specific guidelines (De Almeida, 2020).

The significance of standardized contractual clauses in safeguarding fairness and compliance within the EU legal framework is well-documented. For example, De Almeida (2020)¹³⁰ examines how standard contracts in EU energy exchanges incorporate EU legal norms to promote fairness and transparency. Similarly, the European Commission's study on model contract terms highlights the role of standardized agreements in simplifying fair data-sharing practices.¹³¹ In the realm of data protection, standardized contractual clauses are essential in ensuring compliance with GDPR. The European Commission has developed standard contractual clauses to facilitate lawful international data transfers, providing a mechanism for meeting data protection obligations.¹³²

¹²⁹ Alashqar, Y. (2024). The Comparative View: Mediation, Negotiation and Arbitration. In: AlDajani, I.M., Leiner, M. (eds) Reconciliation, Conflict Transformation, and Peace Studies. Springer, Cham. https://doi.org/10.1007/978-3-031-47839-0_7

¹³⁰ De Almeida, L. (2020). Standardization of standard contracts: fairness in EU energy exchanges. In M. C. Gamito, & H.-W. Micklitz (Eds.), *The role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes* (pp. 155–179). (Private Regulation). Edward Elgar. <https://doi.org/10.4337/9781788118415.00015>

¹³¹ European Commission, Directorate-General for Justice and Consumers, Graux, H., Somers, G., Van Camp, S., Morel, S., Herrera, F., Maridis, G., Di Giacomo, D., & Vassot, S. (2022). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights : executive summary*, Publications Office of the European Union. <https://data.europa.eu/doi/10.2838/462588>

¹³² European Commission. *Standard contractual clauses (SCC)*. European Commission. Retrieved from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

The enactment of new regulations, such as the Data Governance Act (Regulation (EU) 2022/868), alongside rapid advancements in artificial intelligence, necessitates the continual revision and adaptation of AAL contracts. Key considerations include establishing secure and legally compliant data-sharing protocols that align with Article 9 of the Data Governance Act. Furthermore, compliance with the Medical Devices Regulation (Regulation (EU) 2017/745) is essential. Article 10 of this regulation requires that AAL contracts guarantee ongoing compliance with safety and performance standards throughout the product's lifecycle. This includes obligations related to post-market surveillance, timely reporting of adverse events, and the implementation of corrective actions when necessary. Consequently, contracts must incorporate clauses that obligate parties to maintain these standards, facilitating regulatory compliance and promoting user safety.

7.6. Practical Applications and Case Studies

To illustrate the practical application of these legal frameworks, consider a scenario in which a German AAL provider offers health monitoring services to consumers in France and Italy. The contractual agreement involves AI-driven health analytics, requiring strict compliance with the European Union's AI Act, GDPR, and the Medical Devices Regulation. In accordance with the Rome I Regulation, the contract explicitly designates German law as the governing legal framework, ensuring uniformity and consistency in regulatory compliance across all involved jurisdictions and reducing the risk of conflicting legal requirements. The Brussels I Regulation allows the contractual parties to agree that German courts shall have jurisdiction over any disputes arising from the contract, centralizing dispute resolution within a specified jurisdiction and facilitating a streamlined and predictable legal process.

To address data protection concerns, the contract incorporates comprehensive GDPR provisions, ensuring that all data processing activities meet EU-wide standards for personal data protection. Supplementary safeguards mandated by the AI Act are also included to address specific challenges associated with AI-driven data analytics, such as algorithmic transparency, accountability, and bias mitigation. Service continuity is secured through Service Level Agreements (SLAs) that integrate the requirements of the NIS 2 Directive, ensuring the implementation of strong cybersecurity measures and effective incident response protocols. These provisions maintain uninterrupted service delivery and enhance the resilience of AAL systems against cyber threats, exemplifying how comprehensive legal compliance can be effectively integrated into practical contractual arrangements

7.6.1. Building Clear, Compliant, and Adaptive Contracts for AAL

Confirming clarity and transparency is vital in contract drafting. Employing plain language enables consumers and other stakeholders to fully comprehend the terms and conditions, which promotes fairness and reduces the potential for misunderstandings or disputes. Clearly articulated obligations, rights, and remedies enhance contractual certainty and foster trust between parties. Building Clear, Compliant, and Adaptive Contracts for AAL Technologies.

Comprehensive compliance is achieved by incorporating detailed provisions that systematically address all relevant legal and regulatory requirements. This includes not only adherence to overarching EU regulations but also compliance with national laws and sector-specific guidelines. Designing contracts with flexibility and adaptability is essential to accommodate evolving regulations and technological advancements. Including clauses that allow for contractual amendments in response to legislative changes or technological innovations ensures that the agreements remain relevant and effective over time. This proactive approach secures the long-term viability of contractual relationships in a dynamic legal and technological landscape.

Collectively, these best practices establish a solid foundation for equitable and sustainable contractual relationships, balancing the interests of all parties and fostering the responsible deployment of AAL technologies.

7.7. Conclusions

The contract law framework governing Ambient Assisted Living (AAL) systems within the European Union (EU) is notably complex, shaped by a combination of national legislations and specific EU regulations. Contracts related to AAL must navigate a diverse selection of legal instruments that address technological innovations, privacy concerns, security measures, and medical requirements. Prominent among these are the Artificial Intelligence (AI) Act, which oversees the deployment of AI technologies in AAL systems; the NIS 2 Directive, which emphasizes cybersecurity and the safeguarding of critical infrastructures; the General Data Protection Regulation (GDPR), which regulates the handling of personal data; and the Medical Devices Regulation (MDR), which ensures the safety and efficacy of health-related technologies.

Furthermore, foundational EU regulations such as Rome I and Brussels I are crucial for establishing jurisdiction, determining applicable laws, and facilitating the cross-border enforcement of contracts. These regulations are particularly relevant for AAL systems, which typically involve collaboration across multiple countries and among various stakeholders, including service providers, healthcare institutions, technology developers, and end-users.

To effectively navigate this intricate legal landscape, stakeholders can adopt standardized model contracts that incorporate provisions from the aforementioned regulations. Additionally, the implementation of legal innovations like smart contracts, which can automate and enforce contractual terms, may enhance both efficiency and transparency. Developing best practices that account for the rapidly evolving nature of AAL technologies, the shifting regulatory environment, and potential risks is essential for ensuring that contracts remain legally robust and compliant.

As AAL technologies continue to advance, it is essential to anticipate future legislative changes. Addressing challenges such as cross-border enforcement and ensuring that contracts can adapt to new legal requirements and technological developments will be critical for maintaining the long-term viability and compliance of AAL systems within the EU. By proactively addressing these factors, stakeholders can support the sustainable integration of AAL technologies, ultimately enhancing the quality of life for users across Europe.

8. Criminal law

AAL technologies implicate criminal law in multiple ways. For example, in the EU, AAL-providing companies classified as telecommunication providers may be obliged to retain data and then turn this data over to law enforcement agencies. The Convention on Cybercrime requires that countries have legal provisions "to order or similarly obtain the expeditious preservation of specified computer data, including traffic data" (Article 16).¹³³ In this way, AAL systems may facilitate the government's access to its citizens, subjecting citizens to additional scrutiny and approbation, potentially compromising the autonomy of AAL users.

The research conducted within the framework of the visuAAL project discussed two main problems in the domain of criminal law. The first issue concerned the protection of privacy through the criminalisation of the production and dissemination of intimate pictures without consent. In this context, the main research problem was how nudity is defined by criminal law, as it determines the scope of legal protection.¹³⁴ The second problem was the criminal liability of AAL providers for the production or dissemination of intimate pictures without the consent of the depicted people.¹³⁵

Prospective users of AAL solutions and other assistive technologies have voiced substantial concerns regarding their privacy, which is a significant impediment to the sustainable adoption and acceptance of these innovative technologies.¹³⁶ Privacy, a multidimensional concept encompassing facets beyond data protection, also includes the safeguarding of intimacy and nudity. To ensure privacy, especially in contexts involving nudity, it becomes imperative to comprehend the multifaceted meaning of nudity, not solely from a social sciences perspective¹³⁷ but also within the realm of law.

The studies on the legal definition of nudity investigated relevant provisions of EU law juxtaposed against the criminal laws of Ireland and Poland. These two countries embody diverse legal traditions, with Ireland adhering to the common-law tradition,

¹³³ Convention on Cybercrime, Budapest 2001.

¹³⁴ Cf. Kuzmicz, M. M. (2023). Naked in the eyes of the law. *European Journal of Crime, Criminal Law and Criminal Justice*, 31(3–4), 325–345. <https://doi.org/10.1163/15718174-bja10049>.

¹³⁵ Cf. Kuźmicz, Maksymilian M. (2023). Video-based AAL and intimate pictures – criminal liability in European, Irish, and Polish law. *Studies in Health Technology and Informatics*, 306, 105–112. <https://doi.org/10.3233/shti230603>.

¹³⁶ Arning, K., & Ziefle, M. (2015). "Get that camera out of my house!" Conjoint measurement of preferences for video-based healthcare monitoring systems in private and public places. *Inclusive Smart Cities and E-Health*, 152–164. https://doi.org/10.1007/978-3-319-19312-0_13, 152–164.

¹³⁷ See, for example, Maidhof, C., Hashemifard, K., Offermann, J., Ziefle, M., & Florez-Revuelta, F. (2022). Underneath your clothes: A social and technological perspective on nudity in the context of Aal Technology. *Proceedings of the 15th International Conference on Pervasive Technologies Related to Assistive Environments*, 47, 439–445. <https://doi.org/10.1145/3529190.3534733>.

while Poland adheres to civil law. Despite cultural similarities, primarily stemming from the historical influence of Catholicism, these nations exhibit divergent socio-economic contexts.¹³⁸ Additionally, the familiarity of the authors with these legal frameworks and their linguistic accessibility informed this choice.

8.1. Definition of nudity

The conducted study showed that legal perspectives on nudity are different in studied jurisdictions. Article 7(a) of the proposed Directive on combating violence against women and domestic violence concerns dissemination through ICT's "intimate images, or videos or other material depicting sexual activities, of another person."¹³⁹ The scope of the norm is unclear, as it may be limited only to the representations of sexual activities, or cover also images deemed intimate because of nudity.¹⁴⁰ Still, there is no legal definition of nudity in the proposed directive or other pieces of EU legislation.

Irish law offers a more comprehensive and precise definition of "intimate pictures." This definition encompasses not only images of completely unclothed individuals but also those depicting "what is, or purports to be" intimate body parts, even if they are covered with underwear. As a result, edited pictures and deepfake content fall within the scope of the Irish legislation. In contrast, Polish regulations do not provide a specific definition of nudity, and legal scholars generally associate it with genitals and female breasts being "recognizable". Furthermore, Polish law requires that a victim be identifiable for an offence to be established. Oppositely, Irish law does not impose such a requirement. Instead, causing or intending harm is a crucial element in determining the criminality of an act under Irish legislation. However, this emphasis on harm can potentially impede prosecution efforts and weaken the overall protection afforded to victims. Conversely, Polish law operates under the assumption that the mere capture or dissemination of an intimate picture is inherently harmful, as it infringes upon an individual's freedom and privacy. This perspective underscores the significance attributed to the act itself, independent of any specific harm caused.

Proposed European legislation concerning intimate pictures could combine the best elements of two investigated approaches. The Directive shall clearly define intimate pictures, possibly with a list of parts of the body considered intimate. Such a definition may also include "what appears to be an intimate part of the body" to cover technically

¹³⁸ Cf. Cullen, P., & Korolczuk, E. (2019). Challenging abortion stigma: Framing abortion in Ireland and Poland. *Sexual and Reproductive Health Matters*, 27(3), 6–19. <https://doi.org/10.1080/26410397.2019.1686197>.

¹³⁹ Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence, com/2022/105 final.

¹⁴⁰ Cf. Rigotti, C., & McGlynn, C. (2022). Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse. *New Journal of European Criminal Law*, 13(4), 452–477. <https://doi.org/10.1177/20322844221140713>.

rendered pictures, especially constantly more popular deepfakes. In the Directive, there should be no requirement of additional harm to not hinder possible prosecution for the crime.

8.2. Criminal liability of AAL providers

The second problem investigated within the visuAAL project concerns the criminal liability of AAL providers in the case of the production or dissemination of intimate pictures. Both Irish and Polish laws contain provisions about the criminal liability of people other than just the direct perpetrators. Section 6(1) of the Irish Harassment, Harmful Communications and Related Offences Act (Act) states that in some circumstances the managers of a company are liable for acts of the body corporate.¹⁴¹ To apply that provision, an offence must be committed by a body corporate, and it must be proven that the offence can be attributed to “any wilful neglect” or was committed with the consent or connivance of a manager. In the context of section 6(1) Act, “managers” refers to the directors, managers, secretaries, or other officers of the body corporate or of a person purporting to act in such a capacity. Similarly, in Polish law, every person who was both in a position to and legally obliged to prevent the crime but did not do so is criminally liable as an associate (Article 18 §3 KK).¹⁴² Additionally, whenever a special duty of care exists, a person may be held liable on the grounds of negligence (Article 2 KK). In the context of a company providing AAL, these rules may be applied to managers on various levels of management, but also to employees working on the development of technology.

Additionally, in some cases, legal persons may also be held criminally liable. According to Section 6(1) Act, if the conditions discussed in the relations to managers are satisfied, the corporate body itself is guilty of an offence and subject to prosecution and punishment. Thus, the AAL provider as a company, not just its employees, may be held criminally liable. Similarly, Polish law allows for the criminal prosecution of a legal person if three requirements are met. The first condition requires the identification and conviction of the natural person who committed the prohibited act under Article 4 of the Act of 28 October 2002 on the Liability of Collective Entities for Prohibited Acts [30]. The second condition is that the convicted natural person acted in the name or interest of the legal entity, and the act itself must have potentially benefited the legal person in any way under Article 3. Finally, the legal entity must have failed to exercise due diligence in selecting or supervising employees or other agents who committed the prohibited act, under Article 5. All three conditions must be met simultaneously for a natural person to be criminally liable. This high bar for criminal liability means that, in

¹⁴¹ Harassment, Harmful Communications and Related Offences Act 2020, <https://www.oireachtas.ie/en/bills/bill/2017/63/>.

¹⁴² Act of June 6, 1997 – Kodeks karny (Penal Code), Dz.U. 1997 nr 88 poz. 553, <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19970880553>.

most cases, the AAL provider would not be criminally liable under Polish law. Conversely, Irish regulations make it easier to hold the company responsible for the crime of producing or disseminating intimate images.

The significant disparities observed among the examined Member States necessitate a cohesive and uniform approach within EU law. The EU legislature shall decide if and under what circumstances an AAL provider may be criminally liable for depiction and dissemination of intimate pictures, and if legal persons can be liable too. Currently, only five EU Member States preclude criminal liability of legal persons: Bulgaria, Germany, Greece, Latvia, and Sweden.

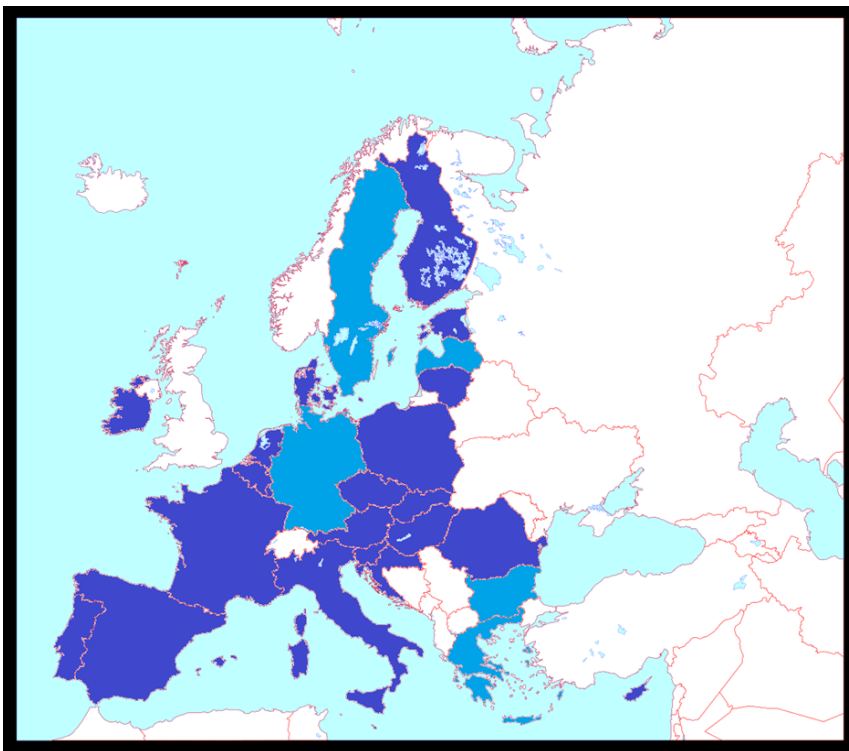


Figure 1. EU countries with criminal liability of legal persons (dark blue), and without (light blue)

9. Data protection

9.1. Data privacy challenges

In AAL technologies, data protection faces a series of complex challenges. Firstly, advances in computer science have made it increasingly easy to re-identify data that was supposedly protected through pseudonymization and anonymization.¹⁴³ Since AAL technologies may require highly personalized services, the application of pseudonymization is often limited. Additionally, the types of data collected are rich and multidimensional, making it more difficult to assess the sensitivity of the data, thereby increasing the risk of data breaches and misuse.

Secondly, transparency and consent mechanisms in the context of AAL technologies are particularly vulnerable. User interfaces may struggle to effectively provide the necessary privacy notices, especially when sensors are seamlessly integrated into users' private or semi-private environments.¹⁴⁴ In such cases, users may find it challenging to fully understand and manage their privacy rights, while the processing of third-party data and obtaining informed consent from individuals with diminished cognitive abilities also pose significant challenges, increasing the risk of unintentional privacy violations.

Moreover, there may be tension between data minimization and purpose limitation in AAL technologies. To deliver better health and well-being services, it may be necessary to store user data for extended periods, but this also raises the risk of long-term storage of sensitive information, potentially leading to its misuse or abuse. In particular, the difficulty of automatically discarding non-essential data in video and audio monitoring increases the risk of inadvertently retaining unnecessary data, which violates the principle of data minimization.

Lastly, while the concept of Data Protection by Design and by Default (DPbDD) is considered a crucial strategy in AAL technologies, its implementation remains challenging. DPbDD requires systems to consider privacy protection from the design phase and to adopt the most privacy-friendly settings by default. However, there is a lack of effective methodologies to apply this concept in the context of AAL, leading to less than satisfactory privacy protection outcomes. These issues highlight the importance of strengthening data protection regulations and technical measures in

¹⁴³ Ohm, P. (2009). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57(6), 1701–1778.

¹⁴⁴ See advances in ambient sensors, Haque, A., Milstein, A., & Fei-Fei, L. (2020). Illuminating the dark spaces of healthcare with ambient intelligence. *Nature*, 585(7824), 193–202. <https://doi.org/10.1038/s41586-020-2669-y>

AAL technologies to ensure the security of user privacy amid technological advancements.

9.2. Suggestions

To address these challenges, we believe that future legislation needs to be strengthened and improved in several areas to ensure that the law effectively protects user privacy alongside AAL technological advancement.

Firstly, with the advancement of computer science, the risk of data re-identification is increasing, even with the use of pseudonymization and anonymization techniques.¹⁴⁵ Therefore, future legislation should re-examine the definition of “personal data”, especially “health data” in the AAL context.¹⁴⁶ Given that privacy risks may be contextual,¹⁴⁷ alternative mechanism can be considered, such as a dynamic data classification mechanism. This mechanism would allow the protection level of data to be flexibly adjusted based on the technological environment and specific data processing conditions. Particularly in AAL technologies, the highly personalized and multidimensional datasets increase the complexity of data protection, and current measures may not be sufficient to address these challenges.

Secondly, existing transparency and consent mechanisms in the application of AAL technologies show significant shortcomings. To enhance transparency and ensure that users can effectively manage their privacy, future legislation may consider requiring the embedding of real-time feedback and visual privacy notification tools in all sensor devices involved in personal data collection. These tools should clearly display the data collection and processing processes and provide convenient control options, enabling users to manage their data privacy in real time. Additionally, the law should particularly address the issues of third-party data processing and obtaining informed consent from individuals with diminished cognitive abilities by establishing specific legal provisions that mandate stricter protection measures, such as mandatory third-party reviews and guardian consent.

Thirdly, the principles of data minimization and purpose limitation also need to be further strengthened in AAL technologies. To balance data storage with privacy protection, future legislation may consider mandating that all data processing activities undergo strict necessity and proportionality assessments, ensuring that only data necessary for the consented service is collected and stored. The law should also

¹⁴⁵ Ohm, P. (2009). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57(6), 1701–1778.

¹⁴⁶ Schäfke-Zell, W. (2021). Revisiting the definition of health data in the age of digitalized health care. *International Data Privacy Law*, ipab025. <https://doi.org/10.1093/idpl/ipab025>

¹⁴⁷ Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press. <https://doi.org/10.1515/9780804772891>

require developers to incorporate automated data filtering and deletion features during the design phase to ensure that non-essential information is not improperly retained. Moreover, for potential secondary data processing, legislation should require explicit informed consent from users and, where possible, the adoption of techniques such as differential privacy and data sandboxes to limit the scope and purpose of data processing.¹⁴⁸

In terms of data protection by design and by default (DPbDD), future legislation should fully implement this concept and introduce standardized data protection design requirements.¹⁴⁹ Methodologies that help implement DPbDD are encouraged.¹⁵⁰ It is recommended to mandate privacy impact assessments (PIAs), especially in the early stages of AAL technology development, to ensure that all technology designs and developments involving personal data consider privacy protection. Additionally, the law should encourage the widespread adoption of privacy-enhancing technologies (PETs) and require developers and suppliers to ensure that their products, by default, are equipped with the strictest data protection settings.¹⁵¹ The law should also stipulate that developers must regularly review and update their privacy protection measures to keep pace with rapid technological development and ensure these measures remain effective throughout the technology's lifecycle.

¹⁴⁸ Regarding the secondary use of health data, see major legislative development in the EU: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space COM/2022/197 Final, No. COM(2022) 197 final (2022). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197>

¹⁴⁹ It is now already a legal requirement in the EU's GDPR.

¹⁵⁰ Mihaildis, A., & Colonna, L. (2020). A Methodological Approach to Privacy by Design within the Context of Lifelogging Technologies. *Rutgers Computer and Technology Law Journal*, 46(1), 1–52.

¹⁵¹ See development in this connection, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space COM/2022/197 Final, No. COM(2022) 197 final (2022). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197>

10. Conclusions

In this deliverable, we delve deeply into the legal risks associated with AAL technologies and offer specific *de lege ferenda* suggestions to address the obstacles and gaps within the current legal framework.

AAL integrate multiple technologies to help the elderly and other groups in need of support maintain independence in their daily lives and extend their active participation in society. However, as AAL technologies rapidly develop, their multidimensional nature has also sparked numerous ethical, legal, and social issues. For instance, while AAL systems perform excellently in providing functionalities such as fall detection and medication reminders, their use of visual data may infringe on personal privacy, which has become one of the most discussed topics in the field, and this work.

Based on a comprehensive review of the existing legal framework, this deliverable incorporates several cutting-edge research findings, including those from the MSCA ITN Visual and GoodBrother projects, to propose future legislative recommendations across multiple legal domains. First, in general product safety regulations, it is recommended to enhance safety standards for AAL devices to ensure that products meet the highest safety requirements both in design and use. In medical device regulation, it is suggested that AAL technologies be aligned with medical device regulations, while also considering their unique technological characteristics. Cybersecurity issues are of paramount importance, necessitating proactive measures such as enhancing risk assessment and standard-setting, and adopting forward-looking cybersecurity legislation, as exemplified by the EU's AI Act¹⁵² and Cyber Resilience Act.¹⁵³ In the areas of competition law and consumer protection law, recommendations include protecting vulnerable consumers, clarifying consumer status, and strengthening information obligations to ensure that fair market competition and consumer rights are upheld with the growing use of AAL technologies. Additionally, this deliverable explores the application of contract law and criminal law to AAL technologies, offering specific suggestions for improving contractual obligations and criminal liability to better protect user rights and ensure legal fairness. In particular, it clarifies the definition of nudity and the criminal liability of AAL providers. Finally, in data protection, considering the extensive collection and use of personal data by AAL

¹⁵² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance) (2024). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

¹⁵³ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA Relevance) (2024). <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>

technologies, it is recommended to strengthen data protection measures to ensure that user privacy is fully safeguarded amid technological advancements.

By comprehensively utilizing doctrinal legal methods and knowledge from the field of computer science, this deliverable not only highlights the shortcomings of the current legal framework but also provides suggestions for future legislation. These recommendations are intended to offer valuable reference points for legislators and policy makers, enabling them to draft more consistent and effective laws that protect users' rights in the face of ongoing AAL technological progress. In doing so, this deliverable aims to promote the widespread application of AAL technologies in Europe's aging society and beyond, while ensuring that technological development remains aligned with ethical and legal standards.

Bibliography

Legislation

Act of June 6, 1997 – Kodeks karny (Penal Code), Dz.U. 1997 nr 88 poz. 553, Poland, <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19970880553>.

Act on Prohibition of Private Monopolization and Maintenance of Fair Trade (Anti-Monopoly Act). (n.d.). Retrieved from https://www.iftc.go.jp/en/policy_enforcement/cartels_bidriggings/anti_cartel_files/The_Antimonopoly_Act.pdf

Anti-Monopoly Law of the People's Republic of China. (2022). Retrieved from <https://www.chinalawtranslate.com/en/anti-monopoly-law-2022/>

Clayton Act, 15 U.S.C. §§ 12–27 (1914).

Convention on Cybercrime, Budapest 2001.

Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, OJ L 347, 11/12/2006, p. 1.

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, OJ L 210, 07/08/1985, p. 0029 - 0033.

Council Directive 89/298/EEC of 17 April 1989 coordinating the requirements for the drawing-up, scrutiny and distribution of the prospectus to be published when transferable securities are offered to the public (OJ L 1989 No. 124, 0008–0015).

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation), OJ L 24, 29.1.2004, p. 1–22.

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Vilnius, 5th September 2024.

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 On liability for defective products and repealing Council Directive 85/374/EEC

Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ L 136, 22.5.2019, p. 28–50.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 011, 15/01/2002, p. 0004 - 0017.

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, p. 22–39.

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs.

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, p. 64–88.

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space COM/2022/197 final 2022 [COM(2022) 197 final]

Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (1914).

Harassment, Harmful Communications and Related Offences Act 2020, Ireland, <https://www.oireachtas.ie/en/bills/bill/2017/63/>.

Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177, 4.7.2008, p. 6–16.

Regulation (EU) 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs) (OJ L 2014 No. 352, p. 1–23).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) 2016 OJ L 119

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117, 5.5.2017, p. 1–175.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) 2019 (OJ L)

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC.

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital

Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA Relevance) (2024). <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>

Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 351, 20.12.2012, p. 1–32.

Sherman Act, 15 U.S.C. §§ 1–7 (1890).

Case law

C-597/19, *M.I.C.M.*, EU:C:2021:492.

C-623/17 *Privacy International*, EU:C:2020:790.

Case C-195/14 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e. V. v Teekanne GmbH & Co KG.

Case C-210/96 Gut Springenheide and Tusky v Oberkreisdirektor des Kreises Steinfurt [1998] ECR I-4657.

Case C-410/19, TSI v CA, ECLI:EU:C:2021:742.

Case C-465/20 P, Commission v. Ireland and Others, Judgment issued September 10, 2024 (European Court of Justice, 2024).

Case C-48/22 P, Google LLC and Alphabet, Inc. v. Commission, , Appeal filed January 20, 2022 (European Court of Justice, 2022).

Case C-502/13, Commission v Luxembourg, ECLI:EU:C:2015:143.

Case C-51/94 Commission of the European Communities v Federal Republic of Germany [1995] ECR I-3599.

Case C-511/18, La Quadrature du Net and Others, EU:C:2020:791.

Case C-85/76, *Hoffmann-La Roche*, ECLI:EU:C:1979:36.

Case C-T-8/89, DSM NV v Commission of the European Communities, ECLI:EU:T:1991:76.

Case T-1077/23, Bytedance v. Commission, , PRESS RELEASE No. 114/24 Luxembourg (2024, July 17).

Case T-363/04 Koipe Corporaci6n, SL v Office for Harmonisation in the Internal Market (Trade Marks and Designs) (OHIM) [2007] ECR I-3355.

Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Watson and others*, EU:C:2016:970.

European Commission. (2020). Case M.9660 – Google/Fitbit: Commission Decision of 17 December 2020.

European Court of Justice. (2024). *Illumina Inc. v. European Commission (Joined Cases C 611/22 P and C 625/22 P)*.

Documents

AGE Platform Europe. (2016). *Glossary & acronyms*. <https://www.age-platform.eu/glossary/active-and-assisted-living-programme-aal>.

Australian Human Rights Commission, *Euthanasia, human rights and the law*, 2016.

CEN ISO/IEEE 11073 Health Informatics - Medical/Health Device Communication Standards. <https://www.iso.org/standard/77338.html>

Directorate-General for the Internal Market and Services , & London Economics. (2015). *Consumer Testing Study of the possible new format and content for retail disclosures of packaged retail and insurance based investment products*. Publications Office of the EU. <https://op.europa.eu/en/publication-detail/-/publication/ea428cc5-9e8f-11e5-8781-01aa75ed71a1/language-en/format-PDF/source-search>.

European Commission, Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps (EU Framework Working Document), COM (2014) 219 final.

European Commission, Consumers, Health, Agriculture and Food Executive Agency. (2016). *Consumer vulnerability across key markets in the European Union Final Report*. Publications Office.

European Commission. (2024, March 4). *Commission fines Apple*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161.

EU Commission “The Digital Services Act Ensuring a safe and accountable online environment” https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en?

EU Commission “The Digital Markets Act: ensuring fair and open digital markets” retrieved from: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en?

European Network and Information Security Agency. (2018). *Good practices for security of Internet of things in the context of smart manufacturing*. Publications Office. <https://data.europa.eu/doi/10.2824/851384>.

European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence, 2020/2014(INL)

European Union Agency For Network And Information Security. (2015). *Security and Resilience of Smart Home Environments* [Report/Study]. European Union Agency For Network And Information Security. <https://www.enisa.europa.eu/publications/security-resilience-good-practices>.

European Commission, Directorate-General for Justice and Consumers, Graux, H., Somers, G., Van Camp, S., Morel, S., Herrera, F., Maridis, G., Di Giacomo, D., & Vassot, S. (2022). *Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights : executive summary*, Publications Office of the European Union. <https://data.europa.eu/doi/10.2838/462588>

European Commission. *Standard contractual clauses (SCC)*. European Commission. Retrieved from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

International Medical Device Regulators Forum. (2014). *Software as a medical device (SaMD): Key definitions*. Retrieved from <https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf>.

ISO 13482:2014 Robots and Robotic Devices — Safety Requirements for Personal Care Robots. <https://www.iso.org/standard/53820.html>

ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. <https://www.iso.org/standard/27001>

Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive).

Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law, COM/2011/0635 final - 2011/0284 (COD).

Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, COM/2021/346 final.

U.S. Food and Drug Administration. (n.d.). *Software as a medical device (SaMD)*. U.S. Department of Health and Human Services. Retrieved September 14, 2024, from <https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd>.

World Health Organization, *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance* (World Health Organization 2021) <https://www.who.int/publications/i/item/9789240029200>

Literature

Ake-Kob, A., Blazeveciene, A., Colonna, L., Čartolovni, A., Colantonio, S., Dantas, C., Fedosov, A., Florez-Revuelta, F., Fosch-Villaronga, E., He, Z., Klimczuk, A., Kuźmicz, M., Lukács, A., Lutz, C., Mekovec, R., Miguel, C., Mordini, E., Pajalic, Z., Pierscionek, B. K., ... Tamò-Larrieux, A. (2022). State of the art on ethical, legal, and social issues linked to audio- and video-based AAL solutions. Zenodo. <https://doi.org/10.5281/zenodo.6793617>.

Aleksic, S., Atanasov, M., Calleja Agius, J., Camilleri, K., Čartolovni, A., Climent-Pérez, P., Colantonio, S., Cristina, S., Despotovic, V., Ekenel, H. K., Erakin, E., Florez-Revuelta, F., Germanese, D., Grech, N., Sigurðardóttir, S. G., Emirzeoğlu, M., Iliev, I., Jovanovic, M., Kampel, M., ... Zgank, A. (2022). State of the Art of Audio- and Video-Based Solutions for AAL. Zenodo. <https://doi.org/10.5281/zenodo.6390709>.

Andersson B and others, *Healthcare and Care through Distance-Spanning Solutions – 24 Practical Examples from the Nordic Region* (Nordic Welfare Centre 2020)

Andoulsi I., Wilson P., “Understanding Liability in eHealth: Towards Greater Clarity at European Union Level” [in:] *eHealth: Legal, Ethical and Governance Challenges*, (eds.) George C., Whitehouse D., Duquemois P., 2012.

Arning, K., & Ziefle, M. (2015). “Get that camera out of my house!” Conjoint measurement of preferences for video-based healthcare monitoring systems in private and public places. *Inclusive Smart Cities and E-Health*, 152–164. https://doi.org/10.1007/978-3-319-19312-0_13.

Alashqar, Y. (2024). The Comparative View: Mediation, Negotiation and Arbitration. In: AlDajani, I.M., Leiner, M. (eds) *Reconciliation, Conflict Transformation, and Peace Studies*. Springer, Cham. https://doi.org/10.1007/978-3-031-47839-0_7

Ahmed, Mukarrum, *The Validity of Choice of Court Agreements in International Commercial Contracts under the Hague Choice of Court Convention and the Brussels Ia Regulation* (February 17, 2020).

Beales, H., Craswell, R., & Salop, S. C. (1981). The efficient regulation of Consumer Information. *The Journal of Law and Economics*, 24(3), 491–539. <https://doi.org/10.1086/466997>.

Brown, I. (2020). Interoperability as a tool for competition regulation.

Buiten, M.C. Product liability for defective AI. *Eur J Law Econ* 57, 239–273 (2024). <https://doi.org/10.1007/s10657-024-09794-z>

Caballero, P., Ortiz, G. & Medina-Bulo, I. Systematic literature review of ambient assisted living systems supported by the Internet of Things. *Univ Access Inf Soc* 23, 1631–1656 (2024). <https://doi.org/10.1007/s10209-023-01022-w>

Calvaresi, D., Cesarini, D., Sernani, P. et al. Exploring the ambient assisted living domain: a systematic review. *J Ambient Intell Human Comput* 8, 239–257 (2017). <https://doi.org/10.1007/s12652-016-0374-3>

Campo Comba, M. (2021). The Rome I Regulation and Its Mechanisms of Protection of Consumers and Employees. In: *The Law Applicable to Cross-border Contracts involving Weaker Parties in EU Private International Law*. Springer, Cham. https://doi.org/10.1007/978-3-030-61481-2_3

Chen, J., Edwards, L., Urquhart, L., & McAuley, D. (2020). Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. *International Data Privacy Law*, 10(4), 279–293. <https://doi.org/10.1093/idpl/ipaa011>.

Choukou, M.-A., Shortly, T., Leclerc, N., Freier, D., Lessard, G., Demers, L., & Auger, C. (2021). Evaluating the acceptance of Ambient Assisted Living Technology (AALT) in rehabilitation: A scoping review. *International Journal of Medical Informatics*, 150, 104461. <https://doi.org/10.1016/j.ijmedinf.2021.104461>.

Cicirelli, G., Marani, R., Petitti, A., Milella, A., & D'Orazio, T. (2021). Ambient assisted living: A review of technologies, methodologies and future perspectives for healthy aging of population. *Sensors*, 21(10), 3549. <https://doi.org/10.3390/s21103549>

Cini, M., & Czulno, P. (2022). Digital single market and the EU competition regime: An explanation of policy change. *Journal of European Integration*, 44(1), 41-57.

Cockburn, I. M., Henderson, R., & Stern, S. (2018). *The impact of artificial intelligence on innovation* (Vol. 24449). Cambridge, MA, USA: National bureau of economic research.

Colaert, V. (2016). The regulation of PRIIPs: Great ambitions, insurmountable challenges? *Journal of Financial Regulation*, 2(2), 203–224. <https://doi.org/10.1093/jfr/fjw009>.

Colonna, L. (2019). Legal and regulatory challenges to utilizing lifelogging technologies for the frail and sick. *International Journal of Law and Information Technology*, 27(1), 50–74. <https://doi.org/10.1093/ijlit/eay018>

Cullen, P., & Korolczuk, E. (2019). Challenging abortion stigma: Framing abortion in Ireland and Poland. *Sexual and Reproductive Health Matters*, 27(3), 6–19. <https://doi.org/10.1080/26410397.2019.1686197>.

Dantas, C., & Mackiewicz, K. (2022). Are we ensuring a citizen empowerment approach for health data sharing?. *Zagreb, Croatia*, 55.

da Fonseca, A.T., Vaz de Sequeira, E., Barreto Xavier, L. (2024). Liability for AI Driven Systems. In: Sousa Antunes, H., Freitas, P.M., Oliveira, A.L., Martins Pereira, C., Vaz de Sequeira, E., Barreto Xavier, L. (eds) *Multidisciplinary Perspectives on Artificial Intelligence and the Law. Law, Governance and Technology Series*, vol 58. Springer, Cham. https://doi.org/10.1007/978-3-031-41264-6_16

DiMaggio, P., & Garip, F. (2012). Network effects and social inequality. *Annual Review of Sociology*, 38(1), 93-118. <https://doi.org/10.1146/annurev-soc-071811-145617>

De Hert, Paul and Papakonstantinou, Vagelis and Malgieri, Gianclaudio and Beslay, Laurent and Sanchez, Ignacio, *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services* (2018). *Computer Law & Security Review* (2018) 193–203, Available at SSRN: <https://ssrn.com/abstract=3447060>

De Almeida, L. (2020). Standardization of standard contracts: fairness in EU energy exchanges. In M. C. Gamito, & H.-W. Micklitz (Eds.), *The role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes* (pp. 155–179). (Private Regulation). Edward Elgar. <https://doi.org/10.4337/9781788118415.00015>

Drewes, Helena and Kirk, Alexander, *Extraterritorial Effects of the Digital Markets Act - The 'Elusive Long Arm' of European Digital Regulation* (March 18, 2024). Available at SSRN: <https://ssrn.com/abstract=4763361> or <http://dx.doi.org/10.2139/ssrn.4763361>

Furman, J. (2019). *Unlocking digital competition: Report of the Digital Competition Expert Panel*.

Gadrey J., “The Characterization of Goods and Services” 2005 *The Review of Income and Wealth* 46, <https://doi.org/10.1111/j.1475-4991.2000.tb00848.x>.

Gerke S, Minssen T and Cohen G, 'Ethical and Legal Challenges of Artificial Intelligence-Driven Healthcare', *Artificial Intelligence in Healthcare* (Elsevier 2020) <<https://linkinghub.elsevier.com/retrieve/pii/B9780128184387000125>> accessed 5 May 2021

GoodBrother Working Group 1, 'State of the Art on Ethical, Legal, and Social Issues Linked to Audio- and Video-Based AAL Solutions' (2021) <<https://goodbrother.eu/wp-content/uploads/2021/12/GoodBrother-State-of-the-art-on-ethical-legal-and-social-issues-linked-to-audio-and-video-based-AAL-solutions.pdf>> accessed 16 February 2022

Grundmann, S., Kerber, W., & Weatherill, S. (2012). *Party autonomy and the role of information in the internal market*. De Gruyter.

Hacker, P. (2023). AI Regulation in Europe: From the AI Act to Future Regulatory Challenges. arXiv preprint arXiv:2310.04072.

Haque, A., Milstein, A., & Fei-Fei, L. (2020). Illuminating the dark spaces of healthcare with ambient intelligence. *Nature*, 585(7824), 193–202. <https://doi.org/10.1038/s41586-020-2669-y>.

Hanspach, Philip and Galli, Niccolò, Collusion by Pricing Algorithms in Competition Law and Economics (February 20, 2024). Robert Schuman Centre for Advanced Studies Research Paper No. 2024_06, Available at SSRN: <https://ssrn.com/abstract=4732527>

He Z, 'Privacy-Enhancing Technologies for Active and Assisted Living: What Does the GDPR Say?', *Proceedings of the 15th International Conference on Pervasive Technologies Related to Assistive Environments* (Association for Computing Machinery 2022) <<https://doi.org/10.1145/3529190.3534719>> accessed 1 August 2022

Horder J., "Gross Negligence and Criminal Culpability" 1997 *University of Toronto Law Journal* 47.

Jovanovic, M., Mitrov, G., Zdravevski, E., Lameski, P., Colantonio, S., Kampel, M., ... & Florez-Revuelta, F. (2022). Ambient assisted living: Scoping review of artificial intelligence models, domains, technology, and concerns. *Journal of Medical Internet Research*, 24(11), e36553. <https://doi.org/10.2196/36553>

Jeon, DS., Menicucci, D. Data portability and competition: Can data portability increase both consumer surplus and profits?. *Eur J Law Econ* 57, 145–162 (2024). <https://doi.org/10.1007/s10657-023-09774-9>

Kastl, A., Rauner, Y. N., Mayer-Huber, S., Oestreich, C., Benstetter, F., & Fettke, U. (2024). Stakeholder needs assessment for developing ageing in place solutions—a qualitative study. *BMC geriatrics*, 24(1), 104.

Kaprou, E. (2020). The legal definition of ‘vulnerable’ consumers in the UCPD. *Vulnerable Consumers and the Law*, 51–67. <https://doi.org/10.4324/9781003104650-4>.

Kuźmicz, M. M. (2022). Information Obligation as a Balancing Tool in the Context of Active and Assisted Living. In A. Petz, E.-J. Hoogerwerf, & K. Mavrou (Eds.), *ICCHP-AAATE 2022 Open Access Compendium “Assistive Technology, Accessibility and (e)Inclusion” Part II* (pp. 260–269). essay, Association ICCHP.

Kuźmicz, M. M. (2023). Inspirations from EU Financial Law for Privacy Protection by Information Obligations in Active and Assisted Living Technologies. In A. Gryszczyńska, W. Wiewiórowski, & G. Szpor (Eds.), *Internet. Hacking* (pp. 172–197). essay, C. H. Beck.

Kuźmicz, M. M. (2023). Multilayer Information Obligation, and Why We Need I. *Journal on Technology & Persons with Disabilities*, 11, 43–59. <https://doi.org/http://hdl.handle.net/10211.3/225164>.

Kuźmicz, M. M. (2023). Naked in the eyes of the law. *European Journal of Crime, Criminal Law and Criminal Justice*, 31(3–4), 325–345. <https://doi.org/10.1163/15718174-bja10049>.

Kuźmicz, M. M. (2023). Video-based AAL and intimate pictures – criminal liability in European, Irish, and Polish law. *Studies in Health Technology and Informatics*, 306, 105–112. <https://doi.org/10.3233/shti230603>.

Kuźmicz, M. M. (2024). Who Should We Care About in the Digital World? Challenges of Stakeholders’ Identification – The Case Study of AAL. In H. Matsumi, D. Hallinan, E. Kosta, D. Dimitrova, & P. De Hert (Eds.), *Data Protection and Privacy. Ideas That Drive Our Digital World* (Vol. 16). essay, Bloomsbury Publishing.

Kuźmicz, M. M., & He, Z. (2022). *Active Assisted Living – legal tectonic plates: White paper on the legal framework for video-based assisted technologies [White paper]*. visuAAL.

Lagioia, F., Jabłonowska, A., Liepina, R. et al. AI in Search of Unfairness in Consumer Contracts: The Terms of Service Landscape. *J Consum Policy* 45, 481–536 (2022). <https://doi.org/10.1007/s10603-022-09520-9>

Li, Q., Philipsen, N. & Cauffman, C. AI-enabled price discrimination as an abuse of dominance: a law and economics analysis. *China-EU Law J* 9, 51–72 (2023). <https://doi.org/10.1007/s12689-023-00099-z>;

Lusardi, A. (2014). *Visual tools and narratives: New ways to improve financial literacy*. National Bureau of Economic Research

Mahajan A, “Intellectual Property, Contracts, and Reverse Engineering after PROCD: A Proposed Compromise for Computer Software” 1999 *Fordham Law Review* 67.

Mahler, T. (2024). Smart robotics in the EU legal framework: The role of the machinery regulation. *Oslo Law Review*. Advance online publication. <https://doi.org/10.18261/issn.2387-3299>

Maidhof, C., Hashemifard, K., Offermann, J., Ziefle, M., & Florez-Revuelta, F. (2022). Underneath your clothes: A social and technological perspective on nudity in the context of Aal Technology. *Proceedings of the 15th International Conference on Pervasive Technologies Related to Assistive Environments*, 47, 439–445. <https://doi.org/10.1145/3529190.3534733>.

Maidhof, C., Ziefle, M., & Offermann, J. (2022). Exploring privacy: Mental models of potential users of AAL Technology. *Proceedings of the 8th International Conference on Information and Communication Technologies for Ageing Well and E-Health*. <https://doi.org/10.5220/0011046200003188>.

Malan, J., Eager, J., Lale-Demoz, E., Cacciaguerra, G., & Brady, M. (2020). *Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape*. 102.

Malczyńska-Biały, M. (2020). European Union consumer policy on product safety in years 2002–2014. *Przegląd Politologiczny*, (1), 93–102. <https://doi.org/10.14746/pp.2020.25.1.7>.

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulation. *Computer Law & Security Review*, 35(6), 105336. <https://doi.org/10.1016/j.clsr.2019.06.007>

Márquez, G., & Taramasco, C. (2023). Barriers and Facilitators of Ambient Assisted Living Systems: A Systematic Literature Review. *International Journal of Environmental Research and Public Health*, 20(6), 5020. <https://doi.org/10.3390/ijerph20065020>

Meszaros, J., Corrales Compagnucci, M., & Minssen, T. (2021). The interaction of the medical device regulation and the GDPR: Do European rules on privacy and scientific research impair the safety & performance of AI medical devices?.

Merriam-Webster, 'Definition of SAFETY' (*Merriam-Webster*) <<https://www.merriam-webster.com/dictionary/safety>> accessed 17 February 2022

Mihaildis, A., & Colonna, L. (2020). A Methodological Approach to Privacy by Design within the Context of Lifelogging Technologies. *Rutgers Computer and Technology Law Journal*, 46(1), 1–52.

Minssen T, Mimler M and Mak V, 'When Does Stand-Alone Software Qualify as a Medical Device in the European Union?—The Cjeu's Decision in Snitem and What It Implies for the Next Generation of Medical Devices' (2020) 28 *Medical Law Review* 615

Mujirishvili, T., Maidhof, C., Florez-Revuelta, F., Ziefle, M., Richart-Martinez, M., & Cabrero-García, J. (2023). Acceptance and privacy perceptions toward video-based active and Assisted Living Technologies: Scoping Review. *Journal of Medical Internet Research*, 25. <https://doi.org/10.2196/45297>.

Moreno Belloso, Natalia and Petit, Nicolas, The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove (April 5, 2023). (2023) 48 *European Law Review* 391, Available at SSRN: <https://ssrn.com/abstract=4411743>

NHSX, 'Artificial Intelligence: How to Get It Right Putting Policy into Practice for Safe Data-Driven Innovation in Health and Care' (2019) <https://www.nhsx.nhs.uk/ai-lab/explore-all-resources/understand-ai/artificial-intelligence-how-get-it-right/>

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press. <https://doi.org/10.1515/9780804772891>

Nicolazzo, S., Nocera, A., & Pedrycz, W. (2024). Service Level Agreements and Security SLA: A Comprehensive Survey. *arXiv preprint arXiv:2405.00009*.

OECD (2024), "Artificial intelligence, data and competition", *OECD Artificial Intelligence Papers*, No. 18, OECD Publishing, Paris, <https://doi.org/10.1787/e7e88884-en>.

Nosák, D. (2021). *Overview of Transparency Obligations for Digital Services in the DSA*.

O'Regan G., "Legal Aspects of Computing in World of Computing" [in:] O'Regan G., *World of Computing*, 2018.

Ohm, P. (2009). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57(6), 1701–1778.

Parry G., Newnes L., Huang X., “Goods, Products and Services” [in:] *Service Design and Delivery. Service Science: Research and Innovations in the Service Economy*, (eds.) Macintyre M., Parry G., Angelis J., 2011, https://doi.org/10.1007/978-1-4419-8321-3_2

Peczenik, A. (2001). A theory of legal doctrine. *Ratio Juris*, 14(1), 75–105. <https://doi.org/10.1111/1467-9337.00173>.

Purnhagen, K. (2017). More reality in the CJEU's interpretation of the average consumer benchmark – also more behavioural science in unfair commercial practices? *European Journal of Risk Regulation*, 8(2), 437–440. <https://doi.org/10.1017/err.2017.13>.

Purtova N, Kosta E and Koops B-J, ‘Laws and Regulations for Digital Health’ in Samuel A Fricker, Christoph Thümmeler and Anastasius Gavras (eds), *Requirements Engineering for Digital Health* (Springer International Publishing 2015) <https://doi.org/10.1007/978-3-319-09798-5_3> accessed 15 June 2021

Picht, Peter Georg and Leitz, Anna-Katharina, Algorithms and Competition Law - Status and Challenges (February 5, 2024). Available at SSRN: <https://ssrn.com/abstract=4716705> or <http://dx.doi.org/10.2139/ssrn.4716705>

Queirós, A., Silva, A., Alvarelhão, J. *et al.* Usability, accessibility and ambient-assisted living: a systematic literature review. *Univ Access Inf Soc* 14, 57–66 (2015). <https://doi.org/10.1007/s10209-013-0328-x>

Rigotti, C., & McGlynn, C. (2022). Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse. *New Journal of European Criminal Law*, 13(4), 452–477. <https://doi.org/10.1177/20322844221140713>.

Ruggeri, F., Lagioia, F., Lippi, M. *et al.* Detecting and explaining unfairness in consumer contracts through memory networks. *Artif Intell Law* 30, 59–92 (2022). <https://doi.org/10.1007/s10506-021-09288-2>

Sathyanarayana S and others, ‘Vision-Based Patient Monitoring: A Comprehensive Review of Algorithms and Technologies’ (2018) 9 *Journal of Ambient Intelligence and Humanized Computing* 225

Schäfke-Zell, W. (2021). Revisiting the definition of health data in the age of digitalized health care. *International Data Privacy Law*, ipab025. <https://doi.org/10.1093/idpl/ipab025>

Schurr F. A., “The Relevance of the European Consumer Protection Law for the Development of the European Contract Law” (2007) *Victoria University of Wellington Law Review* 38.

Shala I., Gusha K., “The Debate Over Euthanasia and Human Rights” 2016 *European Scientific Journal* 12.

Schmon, C. (2020). *The Interconnection of the EU Regulations Brussels I Recast and Rome I*. TMC Asser Press.

Siegmann, C., & Anderljung, M. (2022). The Brussels effect and artificial intelligence: How EU regulation will impact the global AI market. *arXiv preprint arXiv:2208.12645*.

Tecante, K. E., & Sokija, A. (2022). The periodic safety update report and post market surveillance report under the new EU Medical Device Regulation. *Medical Writing*, 31, 50-55. <https://doi.org/10.1080/12345678.2022.1234567>

Terry N.P., “Mobile Health and Wearable Technologies: Systemic Liability” 2015 *American Association for the Advancement of Science Workshop*, <https://www.aaas.org/sites/default/files/Terry%20Mobile%20Health%20and%20Wearable%20Technologies%20Systemic%20Liability.pdf>.

Torab-Miandoab, A., Samad-Soltani, T., Jodati, A., & Rezaei-Hachesu, P. (2023). Interoperability of heterogeneous health information systems: a systematic literature review. *BMC medical informatics and decision making*, 23(1), 18. <https://doi.org/10.1186/s12911-023-02115-5>

Ubena, J. (2015). *How to Regulate Information and Communications Technology? A Jurisprudential Inquiry into Legislative and Regulatory Techniques*. Jure.

Vande Walle, S. (2021). The European Commission’s Approval of Google/Fitbit—A Case Note and Comment. *CONCURRENCES COMPETITION LAW REVIEW*, (3-2021).

Vande Walle, S. (2021). The European Commission Clears the Acquisition of a Maker of Fitness Trackers and Smartwatches by a Major Online Platform, Subject to Long-Lasting Behavioural Remedies (Google/Fitbit, M. 9660). *Concurrences Competition Law Review*, (3-2021), 123-127.

Wagner, M., Gupta, R., Borg, M., Engström, E., Lysek, M. (2025). AI Act High-Risk Requirements Readiness: Industrial Perspectives and Case Company Insights. In: Pfahl, D., Gonzalez Huerta, J., Klünder, J., Anwar, H. (eds) *Product-Focused Software Process Improvement. Industry-, Workshop-, and Doctoral Symposium Papers*.

PROFES 2024. Lecture Notes in Computer Science, vol 15453. Springer, Cham.
https://doi.org/10.1007/978-3-031-78392-0_5

Weatherill, S. (2014). *EU Consumer Law and policy*. Edward Elgar.

Wilhelmsson, T. (2018). The informed consumer V the vulnerable consumer in European Unfair Commercial Practices Law — a comment. *The Yearbook of Consumer Law 2007*, 211–227. <https://doi.org/10.4324/9780429430862-8>.

Wilkowska, W., Offermann, J., Colonna, L. *et al.* Interdisciplinary perspectives on privacy awareness in lifelogging technology development. *J Ambient Intell Human Comput* **14**, 2291–2312 (2023). <https://doi.org/10.1007/s12652-022-04486-5>

Wilkowska W, Offermann J, Spinsante S, Poli A, Ziefle M (2022) Analyzing technology acceptance and perception of privacy in ambient assisted living for using sensor-based technologies. *PLoS ONE* **17**(7): e0269642.
<https://doi.org/10.1371/journal.pone.0269642>

Disclaimer

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No.861091. This document reflects the views only of the authors, and the European Union cannot be held responsible for any use which may be made of the information contained therein.”



The **ownership of IPR** (Intellectual Property Right) as well as all foreground information (including the tangible and intangible results of the project) **will be fully retained by all partners without exception**. All issues regarding confidentiality, dissemination, access rights, use of knowledge, intellectual property and results exploitation are included in the Consortium Agreement (CA), which was signed by all partners before starting the project.

The unauthorised use, disclosure, copying, alteration, or distribution of this document is prohibited.