NORTH EAST LAW REVIEW

North East Law Review

2025

Volume 11

Newcastle University

Foreword by the Editor-in-Chief

It is my honour as Editor-in-Chief to welcome readers to Volume 13, Issue 1, of the North East Law Review. Our mission remains to publish high-quality, thought-provoking student scholarship from Newcastle Law School to foster intellectual discourse and contribute to the broader legal community. As evident from the Contents Page, our authors have delivered rigorous and ambitious work across a diverse range of legal fields, with a particular emphasis on emerging technologies, mediation, and socio-legal analyses of cohabitation.

This paper would not be possible without the help of the Volumes Academic Lead, Dr Jiarong Zhang. She has been tremendous, from helping with mundane editorial tasks to organising editorial meetings and enabling editors with the freedom needed to meet their deadlines and contribute to this edition. Furthermore, I would like to thank my fellow Editors on the Editorial Board; without their relentless efforts, the continuation of the North East Law Review would be uncertain. Their attention to detail and professionalism are hopefully evident throughout this issue.

I thoroughly enjoyed my tenure as Editor-in-Chief of the North East Law Review and hope readers derive as much enjoyment and insight from this volume as I have from overseeing its creation. However, the ultimate judgement of this Volume rests with you, the reader.

Benjamin Holligon

The North East Law Review Board 2024-2025

Contents Page

Byte by Byte: Reshaping the European Union Artificial Intelligence Act

Kamya Chawla

1. Introduction

A 2023 TechBrew survey found 66% of European consumers supported "heavy government regulation of AI," revealing their skepticism about artificial intelligence (AI).[1] To develop an ecosystem of trustworthy AI,[2] the Commission proposed the Artificial Intelligence Act (AIA) — a Regulation harmonizing the development, deployment, and application of AI in the European Union's (EU) single market.[3] The Union addresses its AI regulatory void via a risk-based approach[4] — AI systems are ranked into categories reflecting unacceptable, high, limited or minimal risks depending on the threats posed to Union values and fundamental rights.[5] Evidently, the Union's framework acknowledges existing harms materializing from AI,[6] as supported by growing evidence of fundamental rights' breaches by AI.[7] Regardless, the Union merely legislates to contain these perils,[8] as opposed to eradicating them, by claiming such growing evidence is still scarce.[9] Hence, this article unveils robust data illustrating concrete risks posed to fundamental rights by AI. Particularly, the article demonstrates how the Union's regulation of remote biometric identification (RBI) and emotion recognition systems (ERS)[10]

---

[1] Maeve Allsup, 'US and European Consumers Agree on AI Concerns' (*TechBrew,* 26 July 2023) <https://www.emergingtechbrew.com/stories/2023/07/26/us-europe-consumers-ai-concerns> accessed 21 December 2023.

[2] European Commission, 'White Paper on Artificial Intelligence – A European Approach to Excellence and Trust' COM (2020) 65 final, 1.

[3] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM (2021) 206 final, 2.

[4] ibid 3.

[5] ibid 12; ibid Recital 15.

[6] European Parliament, 'EU AI Act: First Regulation on Artificial Intelligence' (*European Parliament,* 8 June, 2023) <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> accessed 14 November 2023.

[7] Jérôme De Cooman, 'Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act' (2022) 6 Market and Competition Law Review 49, 67.

[8] European Commission, 'Regulatory Framework Proposal on Artificial Intelligence' (*European Commission,* 15 November 2023) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai > accessed 27 December 2023.

[9] European Commission, 'Commission Staff Working Document Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down the Artificial Intelligence Act and Amending Certain Union Legislative Acts' SWD (2021) 84 final, 49.

[10] European Commission (n 3) article 5(d); European Commission, 'Annexes to the Proposal for a Regulation to the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM (2021) 206 final, Annex III(1)(a).

undermines free speech[11] and non-discrimination rights,[12] respectively. By conveying the AIA's insufficient protection of fundamental rights, the article calls for a prohibition of RBI in online spaces and on ERS.

2. RBI State of the Art

Presently, the AIA differentiates between 'real-time' and 'post' RBI — 'real-time' RBI is prohibited in publicly accessible spaces for law enforcement purposes, while 'post' RBI merely qualifies as high-risk.[13] Both identify natural persons remotely by comparing their biometric data to a reference database.[14] However, the former conducts instant identification.[15] Contrarily, 'post' RBI systems identify persons retrospectively.[16] Evidently, the distinction is merely technical — by scanning each person appearing in a surveillance feed non-consensually,[17] RBI in general constitutes mass surveillance.[18]

As both 'real-time' and 'post' RBI equally interfere with civil liberties, scholar Jakubowska advocates for an RBI prohibition extension to 'post' RBI and private actors,[19] aligning with the Civil Society Organizations' approaches.[20] This article concurs with Jakubowska, favoring a comprehensive RBI ban. However, the article finds the verification opportunities of biometric data analyzes in 'post' RBI systems more intrusive,[21] which exacerbates fundamental rights' threats in comparison to 'real-time' RBI. This is because retroactive footage review permits the identification of natural persons, even after months,[22] jeopardizing their autonomy.[23] In

---

[11] The Charter of Fundamental Rights of the European Union (CFR) article 11.
[12] ibid article 21.
[13] European Commission (n 10).
[14] European Commission (n 3) Recital 8.
[15] ibid.
[16] . European Digital Rights and others, 'Prohibit all Remote Biometric Identification (RBI) in Publicly Accessible Spaces' [2021] European Digital Risks 1, 2.
[17] ibid.
[18] Peter Königs, 'Government Surveillance, Privacy and Legitimacy' (2022) 35 Philosophy & Technology 7, 8.
[19] Ella Jakubowska, 'Remote Biometric Identification: A Technical and Legal Guide' (*European Digital Rights,* 23 January 2023) <https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/#:~:text=The%20distinction%20between%20%27real%2Dtime,how%20the%20system%20has%20been> accessed 15 November 2023.
[20] European Digital Rights and others (n 16) 4.
[21] Akın Ünver, 'Politics of Digital Surveillance, National Security and Privacy' (2018) 2 Centre for Economics and Foreign Policy Studies 1, 3.
[22] Jakubowska (n 19); Katrin Laas-Mikko and others, 'Promises, Social, and Ethical Challenges with Biometrics in Remote Identity Onboarding' in Christian Rathgeb and others (eds), Handbook of Digital Face Manipulation and Detection (Springer 2022) 444.
[23] Antoinette Scherz, 'How Should Personal and Political Autonomy Feature in the EctHR's Margin of Appreciation?' (2023) 5 Jus Cogens 149, 154.

further contributing to this RBI prohibition discussion, this article focuses on RBI conducted in online spaces, thereby addressing the current regulatory void and literature gap.

2.1 RBI in Online Spaces

In relation to online environments, the Union authorizes 'real-time' and 'post' RBI — the AIA's RBI prohibition merely applies to its notion of publicly accessible spaces.[24] Hence, the Act automatically excludes virtual spaces from the RBI prohibition because they are not physical.[25] However, the AIA fails to consider that online spaces may still constitute publicly accessible spaces,[26] thereby partly fulfilling the Act's notion of public spaces. Importantly, online forms of RBI share the very properties leading to RBI regulation in the AIA, namely the non-consensual mass surveillance of biometric data on continuous, scalable remote bases.[27] Thus, the intrusion levels of RBI are not mitigated in online contexts,[28] as incorrectly suggested by the Commission's lenient position. For example, RBI in online spaces still facilitates profiling which investigates individuals' behavior without their consent, often producing legal effects.[29] Arguably, distinguishing between 'real-time' RBI in online and offline contexts is irrelevant and contradictory — both pose the same, unacceptable risks,[30] meaning the AIA is inconsistent in its risk classifications. Therefore, the mere technical (instead of legal) justification[31] for precluding online environments from RBI's scope is insufficient. This section further explains why the RBI prohibition should extend to online spaces.

First, the Union's commitments in varying legal sources obliges the AIA to adopt a cautious approach to RBI in online environments. To begin, Recital 6 AIA pledges to address all risks arising from AI systems, including those influencing digital contexts.[32] This means the Union cannot exclude regulating RBI in online contexts simply because they do not constitute

---

[24] European Commission (n 3) Recital 9.
[25] ibid.
[26] Hilde Sakariassen and Irene Costera Meijer, 'Why So Quiet? Exploring Inhibition in Digital Public Spaces' (2021) 36 European Journal of Communication 494, 505.
[27] Elizabeth Stoycheff, 'Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects' (2019) 21 New Media and Society 602, 603-604.
[28] European Parliament, 'Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI' (*European Parliament,* 12 September 2023) <https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai> accessed 14 December 2023.
[29] Amnesty International, 'We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands' (Report) (15 July 2020) AI-Index EUR 35/2971/2020, 22.
[30] Rostam Neuwirth, 'Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA)' (2023) 48 Computer Law & Security Review 1, 10.
[31] European Commission (n 24).
[32] European Commission (n 3) Recital 6.

physical spaces. Furthermore, the General Data Protection Regulation (GDPR)'s Article 9(1) prohibits processing sensitive data, encompassing biometrics collected by RBI systems online.[33] To complement the GDPR, the AIA must also acknowledge the coerciveness of biometric processing in all public spaces,[34] including online environments. Moreover, at the international level, United Nations Security Council Resolution 2396 imposes a binding obligation to develop biometric capabilities in compliance with international human rights law.[35] This requires the Union to uphold self-determination and autonomy rights[36] which the AIA discards by permitting RBI online. To maintain consistency within the Act and other related frameworks, this article proposes including an RBI prohibition in online spaces via Article 7 AIA's procedure.

Furthermore, via the AIA's maximum harmonization,[37] the Commission restricts Member States' competence to legislate in the field of online RBI, thereby deteriorating protection against RBI in online contexts,[38] as provided by existing EU national laws. For example, Germany's 'traffic light' coalition committed to prohibiting RBI online for surveillance purposes.[39] Similarly, the Italian Parliament introduced a prohibition on video surveillance systems using facial recognition technologies, in publicly accessible places like online environments.[40] In prohibiting Member States from exceeding the AIA's protection standards in relation to online RBI,[41] the EU disregards the Member States' calculation of risks posed by RBI systems online.

---

[33] 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) [2016] OJ L 119/1, article 9(1).

[34] Jakubowska (n 19).

[35] United Nations Security Council (UNSC) Res 2396 (21 December 2017) UN Doc S/Res/2396, 8.

[36] Micheal Wehmeyer, 'The Importance of Self-Determination to the Quality of Life of People with Intellectual Disability: A Perspective' (2020) 17 International Environment Public Health 257, 258.

[37] Lilian Edwards, 'Expert Explainer: The EU AI Act Proposal' (*Ada Lovelace Institute,* 8 April 2022) <https://www.adalovelaceinstitute.org/resource/eu-ai-act-explainer/> accessed 10 December 2023.

[38] Stephen Weatherill, 'The Fundamental Question of Minimum or Maximum Harmonization' in Sacha Garben and Inge Govaere (eds), The Internal Market 2.0 (Oxford Hart Publishing 2020) 6.

[39] Oliver Noyan, 'New German Government to Ban Facial Recognition and Mass Surveillance' (*Euractiv,* 26 November 2021) < https://www.euractiv.com/section/data-protection/news/new-german-government-to-ban-facial-recognition-and-mass-surveillance/> accessed 22 December 2023.

[40] European Digital Rights, 'Italy Introduces a Moratorium on Video Surveillance Systems that Use Facial Recognition' (*European Digital Rights,* 15 December 2023) <https://edri.org/our-work/italy-introduces-a-moratorium-on-video-surveillance-systems-that-use-facial-recognition/> accessed 22 December 2023.

[41] Micheal Veale and Fredrick Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22 Computer Law Review International 97, 108.

Among examples of RBI systems deployed online include Clearview AI, which utilizes facial recognition systems online for identifying natural persons remotely.[42] Scholars like Amariles argue risks arising from the automated recognition of human biometric features can be mitigated by human intervention.[43] However, this article argues human oversight is inadequately regulated in the AIA — in subjecting decisions regarding automated biometric identification to the verification by two natural persons,[44] the Act fails to regulate their independence, rendering its reliability meaningless. Additionally, this article argues human oversight in itself is fruitless. Particularly, natural persons often fall prey to automation bias — even as final decision-makers, humans follow automated identification decisions produced by RBI systems, ignoring any contradictions.[45] A 2023 study confirms such automation bias is related to the presence of low verification intensity, expressed by a lack of background information confirmation.[46] This is concerning since RBI in online systems constitute bases for legal decisions, including arrests.[47]

Such human oversight shortcomings also apply to self-certification for high-risk RBI conformity assessments, as companies engage in bluewashing, thereby portraying themselves in more fundamental rights-friendly lights than justified.[48] Lastly, this article suggests human oversight introduces individual biases,[49] meaning human supervision or interference in online RBI systems fails to guarantee an effective scrutinizing power.

To further advocate for the online RBI prohibition, this article demonstrates the international trend reflecting strict approaches to RBI, focusing on China. Particularly, China prohibits all forms of RBI in public spaces, except for public security purposes.[50] Contrarily, the Union

---

[42] Camilla Dul, 'Facial Recognition Technology vs Privacy: The Case of Clearview AI' (2022) 3 Queen Mary Law Journal 1, 1-2.

[43] David Amariles and Pablo Baguero, 'Promises and Limits of Law for Human-Centric Artificial Intelligence' (2023) 48 Computer Law & Security Review 1, 9.

[44] Mo Jones-Jang and Yong Jin Park, 'How Do People React to AI Failure? Automation Bias, Algorithmic Aversion, and Perceived Controllability' (2022) 28 Journal of Computer-Mediated Communication 1, 2.

[45] Cordula Kupfer, 'Check the Box! How to Deal with Automation Bias in AI-based Personnel Selection' (2023) 14 Organizational Psychology 1, 6.

[46] European Parliament, 'Biometric Recognition and Behavioral Detection: Assessing the Ethical Aspects of Biometric Recognition and Behavioral Detection Techniques with a Focus on their Current and Future Use in Public Spaces' (*European Parliament,* 01 August 2021) <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf> accessed 14 December 2023.

[47] De Cooman (n 7) 64.

[48] European Parliament (n 46).

[49] ibid.

[50] Rogier Creemers and Graham Webster, 'Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021' (*Stanford University,* 20 August 2021) <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> accessed 17 November 2023; Denis Sadovnikov, 'Real-Time Remote

permits 'post' RBI systems and RBI occurring online.[51] The Union's 'real-time' ban is also conditional — the Union formulates three, broad exceptions to its 'real-time' RBI ban in pursuing elastic public interest objectives, such as public safety and security.[52] This permits indiscriminate surveillance,[53] compromising the Union's proportionality obligations. To adopt a coherent approach, this article suggests the Union must limit RBI forms and legal bases upon which RBI may be deployed, similarly to China.

2.2 Free Speech Case-Study

This section explores how RBI conducted online infringes upon the Union's fundamental rights obligations, as derived from Article 19 International Covenant on Civil and Political Rights (ICCPR), protecting free expression.[54] Although the EU is not legally bound by the ICCPR itself, the convention still has legal relevance— (1) each Member State has ratified the ICCPR,[55] and (2) the ICCPR reflects customary international law.[56] Therefore, the ICCPR's General Comment 34, comprising an authoritative interpretation of minimum standards guaranteed by Article 19 ICCPR,[57] is of relevance to the EU's AIA. Particularly, General Comment 34 protects all forms of expression and the mediums of their dissemination, including electronic and internet-based forms of expression.[58] Hence, free expression rights are equally applicable to online communications,[59] meaning online environments do not invalidate EU Member State free speech protection obligations.

This article focuses on how RBI online contravenes free expression rights. A 2016 study confirms surveillance induces chilling effects on free speech,[60] directly countering the AIA's

Biometric Recognition: Where European and Chinese Regulatory Approaches Coincide'(*DPOrganizer*, 20 September 2023) < https://www.dporganizer.com/blog/real-time-remote-biometric-recognition-where-european-and-chinese-regulatory-approaches-coincide/> accessed 19 December 2023.

[51] European Commission (n 10).

[52] ibid.

[53] . Stoycheff (n 27) 605.

[54] . International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) article 19.

[55] United Nations Treaty Body Database, 'Ratification Status for CCPR - International Covenant on Civil and Political Rights' (*United Nations Treaty Body Database*, 2010) < https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CCPR&Lang=en> accessed 21 December 2023.

[56] . Rudy Baker, 'Customary International Law in the 21st Century: Old Challenges and New Debates' (2010) 21 European Journal of International Law 173, 174-175.

[57] Human Rights Committee 'General Comment No. 34' (2011) UN Doc CCPR/C/GC/34.

[58] ibid 3.

[59] Miloon Kothari, 'The Sameness of Human Rights Online and Offline' in Mart Susi (ed), Human Rights, Digital Society and the Law (Routledge 2019) 28.

[60] Ben Marder and others, 'The Extended 'Chilling' Effect of Facebook: The Cold Reality of Ubiquitous Social Networking' (2016) 60 Computers in Human Behavior 582, 583.

objective to garner public trust in AI.[61] When aware of surveillance in online spaces, minorities conform to majority opinions, threatening heterogeneity and democratic discourse online.[62] Additionally, persons are identified via their keyboard stroke patterns through RBI.[63] Therefore, especially considering the permanency of digital discussions, pseudonyms are used online in fear of silencing reactions and sanctions.[64] Arguably, RBI undermines privacy, the precondition to unrestrained expressions of free speech.[65] Such concerns heighten when biometric features convergence, like combining voice and facial recognition, occurs online.[66] Once compromised, biometrics cannot be reissued like passwords — irises cannot be changed once used by imposters.[67] Hence, the aggregation of biometric databases collected from online surveillance exacerbates hacking effects and increases false positive occurrences leading to the misidentification of persons.[68] Consequently, this contributes to hesitance in disseminating opinions, especially if such false positives lead to legal consequences.[69] To this end, this article argues facilitating free expression requires the protection of privacy and anonymity rights online.

Importantly, the freedom of expression is not absolute — limitations must be pursuant to law, proportionate, and fulfill general interest objectives.[70] However, RBI in online systems does not constitute targeted surveillance. By processing data from an indiscriminate number of data subjects, RBI online disproportionately infringes on individuals' private lives.[71] This article's perspective is supported by a range of national jurisprudence — For example, the UK court in *Bridges v the England and Wales Court of Appeal* held that indiscriminate mass surveillance extends beyond proportionality requirements.[72] For these reasons, the present article proposes a blanket prohibition on RBI conducted online.

---

[61] European Commission (n 2).

[62] Elizabeth Stoycheff, 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring' (2016) 93 Journalism & Mass Communication Quarterly 296, 305.

[63] Fabian Monrose and Aviel Rubin, 'Keystroke Dynamics as a Biometric for Authentication' (2000) 16 Future Generation Computer Systems 351, 353.

[64] David M. Tortell, 'Surfing the Surveillance Wave: Online Privacy, Freedom of Expression and the Threat of National Security' (2017) 22 Rev Const Stud 211, 214.

[65] ibid.

[66] Neuwirth (n 30) 11.

[67] Pablo Nebreda, 'Biometric Data Encryption: Protecting User Privacy' (*Alice Biometrics,* 23 March 2023) < https://alicebiometrics.com/en/biometric-data-encryption-protecting-user-privacy/> accessed 4 December 2023.

[68] De Cooman (n 7) 72.

[69] Marder (n 59) 583.

[70] CFR (n 11) article 52(1).

[71] Stoycheff (n 52).

[72] *Bridges v the England and Wales Court of Appeal* [2020] EWCA Civ 1058 [2019] EWHC 2341.

3. ERS

Under the AIA, ERS evaluating facial or other data (temperature, sweat, eye movements) to establish emotional states are classified as limited-risk in general.[73] In limited circumstances, where used by law enforcement, these systems pose high-risks.[74] As such, the perils are not mutually exclusive. By allocating these risks consistently over demographic groups,[75] the AIA fails to consider perils are contextual. Hence, this section demonstrates how historically marginalized groups are unequally affected in comparison to dominant, privileged groups by fundamental rights' threats emanating from ERS, focusing on the right to non-discrimination.[76] In conveying how this dilemma is rooted in structural inequalities,[77] this article shows the AIA inaccurately quantifies risks, calling to prohibit ERS.

This section illustrates how emotion recognition technologies facilitate marginalization and exclusion in the employment sector, wherein these systems aid the decision-making of recruiters.[78] By screening candidates through video assessments, ERS evaluates emotional intelligence,[79] as depicted in micro-expressions, indicators proven to be unreliable and discriminatory.[80] Since dominant groups define emotion categories of marginalized communities, minorities not conforming to developers' archetypal emotions are subject to discrimination.[81] For example, in cases where persons suffer from facial muscle paralysis, emotions may be misclassified by algorithms,[82] or where non-binary employees emotions' are not accounted for in algorithms reflecting gender binary divisions, marginalized groups face discrimination.[83] Furthermore, such emotion recognition surveillance is used for predictive

---

[73] European Commission (n 3) article 52(2).
[74] European Commission (n 3) annex III 6(b).
[75] European Commission (n 72).
[76] CFR (n 11) article 21.
[77] Lucy Barnes and others, 'The Structural Sources of Socioeconomic Inequalities in Health: A Cross-National Perspective' (2023) 9 Sage Journals 1, 3.
[78] European Data Protection Supervisor, 'Facial Emotion Recognition' (2021) 1 Tec Dispatch 1, 2.
[79] ibid.
[80] Vidushi Marda and Ella Jakubowska, 'Emotion (Mis)Recognition: Is the EU Missing the Point?' (*European Digital Rights,* 2 February 2023) < https://edri.org/our-work/emotion-misrecognition/> accessed 26 December 2023.
[81] ibid.
[82] European Data Protection Supervisor (n 77) 3.
[83] European Center for Not-for-Profit Law, 'Give a Smile, Get a Smile: The Human Rights Impacts of Emotion Recognition in the Workplace' (*European Center for Not-for-Profit Law,* 13 July 2021) <https://ecnl.org/news/give-smile-get-smile-human-rights-impacts-emotion-recognition-workplace> accessed 18 November 2023.

analysis purposes, meaning misinterpretations of marginalized groups' emotions often lead to penalties for these minority workers,[84] exacerbating employment relation asymmetries.

Regarding current literature, scholar Crawford explains why emotion recognition datasets are rooted in prejudices using the Japanese Female Facial Expression (JAFFE) database. [85] Further developing this notion, this article aims to demonstrate the inadequate protection provided by the AIA in respect to mitigating perils associated with ERS. Arguably, emotion recognition technologies are inaccurate, and based on pseudo-scientific architectures.[86] These systems assume a universal correspondence between emotions. However, emotions are culturally constructed.[87] For instance, the Western stereotypical expression of fear corresponds to an angered face in Malaysia.[88] Therefore, emotion recognition incites discrimination on ethnic origin grounds because the algorithms reflect the emotions of dominant groups, proving training datasets often underrepresent minorities, thereby violating Article 10(3) AIA's clause requiring datasets to be representative.[89] Moreover, anterior, facial expressions can fail to represent internal emotions, meaning the datasets cannot be 'free of errors,' as required by Article 10(3) AIA. [90] Importantly, technical aspects (varying camera angles or lighting conditions) diminish the qualities of captured facial expressions. [91] Hence, objective classifications and predictions of emotions are unreliable and arbitrary.[92] In merely requiring transparency as to gaps in datasets and relating theoretical solutions, [93] the AIA is silent regarding the implementation of such solutions. Hence, the Union's Regulation falls short of adequate protection against discrimination.

Scholar Hansen claims banning ERS would be a premature decision, considering it is an emerging technology.[94] Furthermore, Hansen posits even if emotion recognition technologies

---

[84] ibid.

[85] Kate Crawford and Trevor Paglen, 'Excavating AI: The Politics of Images in Machine Learning Training Sets' (2020) 36 AI & Society 1105, 1107.

[86] Access Now, 'Joint Statement: The EU AI Act Must Protect People on the Move' (*AccessNow,* 7 March 2023) < https://www.accessnow.org/press-release/joint-statement-ai-act-people-on-the-move/> accessed 14 December 2023.

[87] ibid.

[88] Hannah Devlin, 'AI Systems Claiming to 'Read' Emotions Pose Discrimination Risks' (*The Guardian,* 16 February 2020) < https://www.theguardian.com/technology/2020/feb/16/ai-systems-claiming-to-read-emotions-pose-discrimination-risks> accessed 27 December 2023.

[89] European Commission (n 3) article 10(3).

[90] ibid.

[91] European Data Protection Supervisor (n 77).

[92] European Center for Not-for-Profit Law (n 81).

[93] European Commission (n 3) article 10(2)(d)-(g).

[94] Rune Hansen, 'Emotion Recognition Tech Can Be Used For Good and For Bad' (*Date Ethics,* 21 April 2021) <https://dataethics.eu/emotion-recognition-tech-can-be-used-for-good-and-for-bad/> accessed 17 November 2023.

violate privacy rights, their deployment is not 'morally wrong.'[95] However, this article argues ERS go beyond infringing privacy — they unethically incite discrimination against marginalized groups. [96] In actively discriminating, these technologies translate existing structural inequalities in societies, ERS perpetuate societal biases.[97] Since this discrimination is not rooted in the technology itself,[98] this article posits no procedural or technical safeguards can mitigate the risks. Even seeking equal representation in datasets cannot eradicate these perils, considering computer scientists (from dominating groups) still subjectively categorize and label emotions of minorities based on historical, discredited assumptions, [99] thereby reinforcing systemic discrimination. Hence, this article proposes to prohibit ERS, upholding a human-centric approach.

3.1 Enforcement

The Union's choice of legal instrument to regulate AI, namely a Regulation, stems from aiming to formulate one uniform set of rules, guaranteeing legal certainty and precluding Member States from enacting divergent laws, thereby countering legal fragmentation.[100] In reinforcing consistency, this article argues the Union-level obligation for individual member states to implement 'effective, proportionate and dissuasive' penalties is inadequate.[101] Instead, the Act should criminalize infringements of this article's proposed emotion recognition ban at the Union level. Therefore, the AIA will guarantee equal degrees of enforcement throughout the EU, dissuading 'forum shopping,' wherein ERS is unlawfully deployed in States with the lowest possible penalties or prosecution chances.[102] To achieve policy coherence goals (beyond stating criteria relevant to penalties), the AIA should coordinate penalties in Article 71 AIA on the Union level.[103]

Furthermore, as this article suggests introducing a ban on ERS, it also proposes formulating legal bases to challenge any violations. To facilitate judicial remedies, this article advocates introducing an explicit right not to be subject to prohibited AI systems in the AIA. This way,

---

[95] ibid.
[96] Marda and Jakubowska (n 79).
[97] Margot Kaminski, 'Regulating the Risks of AI' (2023) 103 Boston University Law Review 101, 105
[98] Padmashree Gehl Sampath, 'Governing Artificial Intelligence in an Age of Inequality' (2021) 12 Global Policy 21, 25.
[99] Crawford and Paglen (n 84) 1113.
[100] European Commission (n 3) 6.
[101] ibid article 71(1).
[102] Viktor Szép and Kamya Chawla, 'The EU's 2022 Sanctions Against Russia: External Shocks Altering EU Restrictive Measure Practices?' (2023) The Hungarian Yearbook of International and European Law 196, 208.
[103] European Commission (n 3) article 71.

minorities subject to unilateral decisions by authorities that determine their emotions' validity can discredit such decisions.[104] To complement this actionable right, this article argues for introducing a redress mechanism in the AIA to lodge complaints with national supervisory bodies, aiding investigations conducted pursuant to Articles 65 and 67 AIA.[105] This will further develop standards for fundamental rights. By authorizing to contest ERS, the Union will actively fulfill its human rights obligations in technological spheres.[106]

4. Conclusion

This article illustrates how AI systems intrude and violate EU fundamental rights,[107] drawing attention to the AIA's shortcomings in adequately mitigating arising perils. The article particularly focuses on how RBI and ERS undermine free speech and non-discrimination rights.[108] In adopting a fundamental rights compliance approach, the article constructs legal arguments conveying the AIA's insufficient protection of fundamental rights. To conclude, this article calls for a prohibition of RBI in online spaces and ERS.

---

[104] Marda and Jakubowska (n 79).
[105] European Commission (n 3) article 65, 67.
[106] European Commission (n 3) 7.
[107] European Commission (n 9).
[108] CFR (n 11) article 11, article 21.

Data Privacy Rights and Regulatory Challenges of Generative AI Models: A Case Study Approach

Ada Izuchukwu

1. Introduction

1.1 Background

The rapid advancement of generative AI (GAI) models such as Generative Adversarial Networks (GANs), GPT series, and DALL-E has transformed various industries by enabling sophisticated automation and enhancing creative processes. These models have become indispensable tools for content creation, driving innovation by reducing the need for human intervention in routine tasks.[109] Additionally, GAI technologies may also be employed to safeguard systems against malicious cyber-attacks,[110] further demonstrating their multifaceted utility. Notwithstanding its tremendous benefits and opportunities, the development and deployment of GAI technologies present significant concerns, including privacy concerns.

GAI models are pre-trained on massive amounts of data,[111] including unlabelled data scrapped from the internet,[112] which consists of personal and sensitive data that falls within the purview of personal data and privacy laws.[113] The utilisation of these data raises profound privacy concerns as it risks violating the privacy rights of individuals and exposing them to various privacy risks such as data breaches, identity theft, and social surveillance[114] and data

---

[109] Muhammad Hussain, 'When, Where, and Which?: Navigating the Intersection of Computer Vision and Generative AI for Strategic Business Integration' (2023) 11 Open Access Journal 127202, 127205 <https://ieeexplore.ieee.org/document/10316296> accessed 7 July 2024.

[110] Maanak Gupta, 'From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy' 11 Open Access Journal 80218, 80220 <https://ieeexplore.ieee.org/document/10198233> accessed 7 July 2024.

[111] ibid; Dang Minh, 'Explainable Artificial Intelligence: a Comprehensive Review' (2022) 55 Artificial Intelligence Review 3503 <https://doi.org/10.1007/s10462-021-10088-y> accessed 15 August 2024.

[112] European Data Protection Supervisor (EDPS), 'Generative AI and the EUDPR: First EDPS Orientations for ensuring data protection compliance when using Generative AI systems' (EDPS, 3 June 2024) 1, 4 & 5 <https://www.edps.europa.eu/data-protection/our-role-supervisor/first-edps-orientations-euis-using-generative-ai_en> accessed 30 July 2024.

[113] UK Information Commissioner Office (ICO), 'Joint Statement on Data Scraping and the Protection of Privacy (ICO UK, 24 August 2023) 1 <https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf> accessed 16 August 2024; European Data Protection Board (EDPB), ' Report of the Work Undertaken by the ChatGPT Taskforce' (EDPB, 23 May 2024) 1, 6 <https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf> accessed 16 August 2024.

[114] Jochen Wirtz and Valentina Pitardi, 'How Intelligent Automation, Service Robots, and AI will Reshape Products and their Delivery' (2023) 2023 Italian Journal of Marketing 289, 294 – 295.

leakages. [115]   GAI also enables the inadvertent [116] and malicious [117] generation of false information about individuals, including false images and texts, thereby posing a risk not only to the privacy of individuals but also undermining public trust and could lead to traumatic experiences, reputational damage or loss of life in extreme cases.[118]

In response to these challenges, various individuals and organisations have sought legal remedies through court actions, alleging unlawful collection of personal data[119] and defamation claims[120] or by filing complaints seeking regulatory intervention.[121] As several jurisdictions grapple with these concerns while seeking to ensure a balance between technological advancements and the risks associated with GAI technologies, the European Union (EU) continues to assume a leading position in regulating data privacy and artificial intelligence technologies, wielding significant influence over the digital regulatory landscape.[122]

The EU's data privacy framework, the General Data Protection Regulation (GDPR),[123] adopts a right-based approach to data protection [124] anchored on the idea of informational self-determination[125] and guaranteed under the EU Charter of Fundamental Rights[126] and the Treaty

---

[115] Tao Wang et al, 'Security and Privacy on Generative Data in AIGC: A survey' (*arXiv*, 18 December 2023) 1, 4 <https://arxiv.org/abs/2309.09435> accessed 21 July 2024.

[116] For instance, See NOYB, 'ChatGPT Provides False Information About People, and OpenAI can't Correct It' (NOYB, 29 April 2024) <https://noyb.eu/en/chatgpt-provides-false-information-about-people-and-openai-cant-correct-it> accessed 21 July 2024.

[117] See Felipe Romero Moreno, 'Generative AI and Deepfakes: a Human Rights Approach to Tackling Harmful Content' (2024) International Review of Law, Computers and Technology 1, 3 <https://www.tandfonline.com/doi/full/10.1080/13600869.2024.2324540> accessed 1 August 2024.

[118] ibid (n 9), 9.

[119] Christopher Valente et al, 'Recent Trends in Generative Artificial Intelligence Litigation in the United States' (K & L Gates, 5 September 2023) <https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023> accessed 17 August 2024

[120] James Vincent, 'OpenAI Sued for Defamation after ChatGPT Fabricates Legal Accusations against Radio Host (the Verge, 9 June 2023) <https://www.theverge.com/2023/6/9/23755057/openai-chatgpt-false-information-defamation-lawsuit> accessed 17 August 2024.

[121] NOYB (n 8); NOYB, 'NOYB Urges 11 DPAs to Immediately Stop Meta's Abuse of Personal Data for AI' (NOYB, 6 June 2024) <https://noyb.eu/en/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai> accessed 17 August 2024.

[122] European Commission, 'Shaping Europe's Digital Future' (*European Commission*, undated) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 16 August 2024; European Council on Foreign Relations (ECFR), 'The EU as a Digital Regulatory Superpower: Implications for the United States' (ECFR, 8 April 2020) <https://ecfr.eu/article/commentary_the_eu_as_a_digital_regulatory_superpower_implications_for_the_u/> accessed 16 August 2024.

[123] 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) [2016] OJ L199/1.

[124] ibid, recital 1.

[125] Ruben de Bruin, 'A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergences' (2022) 13 Hastings Science and Technology Law Journal 127, 134 & 135; General Data Protection Regulation (n 15), recital 7.

[126] Charter of Fundamental Rights of the European Union [2012] OJ C326/391(CFR), art 8 (1).

on the Functioning of the European Union.[127] This idea of informational self-determination, which upholds the right of individuals to exercise control over their data[128] – albeit not as an absolute right, but as a right to have a say in the processing of their data[129] – is protected within the GDPR through specific data processing principles, the obligations of data controllers, and the rights afforded to data subjects (DSRs). However, the efficacy of the GDPR in addressing privacy concerns and enforcing data privacy rights is significantly challenged by the inherent complexities of GAI technologies. These challenges include structural and systemic underpinnings of GAI technologies, which are averse to data processing principles, [130] inadequate enforcements, conceptual fallacies,[131] and the Regulation's failure to consider the severity or realisation of harm that privacy violations may occasion. [132] Furthermore, the GDPR's non-prohibitory approach,[133] which does not outrightly prohibit the processing of personal data but instead seeks to balance conflicting rights and interests, including the economic interest[134] of GAI developers, hamper the adequacy of the GDPR to provide robust privacy protection. These limitations underscore the need for additional regulatory frameworks and stricter enforcement to effectively address the unique privacy challenges posed by GAI technologies.

Although the recently enacted Artificial Intelligence Act [135] (AIA) is a vital AI-specific framework that shapes the EU's digital landscape and complements the GDPR [136] in safeguarding privacy rights, it falls short in adequately addressing privacy concerns and

---

[127] Consolidated version of the Treaty on the Functioning of the European Union (TFEU) [2012] OJ C326/171; see also General Data Protection Regulation (n 15), recital 1.

[128] General Data Protection Regulation (n 15), recital 7; Claudia Kodde, 'Germany's 'Right to be Forgotten' – between the Freedom of Expression and the Right to Informational Self-Determination' (2016) 30 International Review of Law, Computers & Technology 17, 18

[129] See Florent Thouvenin, 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?' (2021) 12 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 246, 248, para 6.

[130] See Hannah Ruschemeier, 'Generative AI and Data Protection' in Handbook on Generative AI and the Law, (Cambridge University Press, 2024) (forthcoming)
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4814999> accessed 28 June 2024.

[131] See Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why A 'Right to An Explanation' Is Probably Not the Remedy You Are Looking For' (2017) 16 (1) Duke Law and Technology Review 15, 66-67.

[132] Thouvenin (n 21) 256.

[133] Paul De Hert and S. Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action' in S Gutwirth et al (eds) *Reinventing Data Protection* (Springer, 2009) 3
<https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_1> accessed 16 August 2024.

[134] As in Case C-131/12 *Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD)* EU:C:2014:317, [2014] QB 1022.

[135] 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] OJ L1689/1.

[136] Artificial Intelligence Act (n 27), recital 9.

violations associated with GAI technologies. This is especially evident in the context of the case study analysed in this research paper, where it exhibits specific limitations that hinder its effectiveness in addressing these issues.

The complexities of regulating GAI technologies underscore the need for a more nuanced understanding of how privacy rights can be safeguarded. Case studies provide a valuable approach to exploring these issues, offering insights into specific instances where GAI models intersect with privacy concerns and existing regulatory frameworks. This approach enables the examination of the adequacy of these frameworks in addressing privacy issues associated with technological advancements and in identifying potential solutions to better protect individual privacy in this digital age.

1.2 Significance of the research

This research aims to contribute to the ongoing discourse on privacy and GAI regulation by analysing two case studies that exemplify the privacy challenges posed by GAI models. Through this approach, the research will explore the effectiveness of existing regulatory frameworks, identify existing gaps in current practices and propose recommendations for enhancing data privacy protection in the context of generative AI. The findings not only add to the academic understanding of these issues but may also have practical implications for policymakers and the relevant regulatory bodies seeking to navigate the complex landscape of GAI regulation.

1.3 Statement of research question

How do Generative AI models pose privacy risks, and to what extent are current regulatory frameworks effective in addressing these risks and protecting the data privacy of individuals?

1.4 Aims and objectives

1. To investigate the privacy risks associated with generative AI models.
2. To evaluate the intersection of generative AI models and data privacy by examining select case studies.
3. To assess the effectiveness and adequacy of current EU regulatory frameworks in addressing generative AI-related privacy risks and protecting privacy rights.

4. To provide recommendations for enhancing privacy protection in Generative AI.

1.5 Research methodology

Generally, this research employs a socio-legal and qualitative document research methodology to collect and analyse data.

Socio-legal research methodology was adopted to examine how privacy-related regulatory frameworks (law) interact with technological advancements (social phenomenon), collecting and analysing both legal and non-legal source data.[137] This methodology is relevant to this research as it enables the study of the practical implication and effectiveness of privacy laws on social interactions and developments in the EU.

On the other hand, qualitative research methodology is most suitable for answering 'what' and 'how' questions,[138] which are the basis upon which my main research question (*see 1.3. above*) is framed. This method is also instrumental in exploring how 'social phenomena arise' in social interactions.[139] Hence, it was useful in uncovering how GAI models/technologies expose individuals to privacy risks (RA 1).

1.5.1 Part-based methodology

Parts one and two are, respectively, the introductory and foundational parts of this research. Hence, they do not directly address any of the research aims and objectives.

---

[137] Laura Lammasniemi, *Law Dissertations: A Step-by-Step Guide* (2nd edn, Routledge 2021) 67 & 68.
[138] David Silverman, *Doing Qualitative Research* (6th Edn, SAGE 2022) 25.
[139] ibid, 10.

1.5.1.1 Part 2 employed a qualitative document method

Data collection

This involved the collection of both primary and secondary legal and non-legal documents. Given the socio-legal nature of this research, there was heavy reliance on non-legal secondary documents (including books and articles) for the definition/understanding of technical terminologies and techniques underpinning GAI models. This method was pivotal as it is advantageous for researchers with limited/novice knowledge about research,[140] as was the case here. Legal primary and secondary documents were also collected – to the extent that they defined relevant terminologies – to examine how relevant terminologies are defined in the legal parlance.

Data analysis

The data analysis is conducted by reviewing the collected literature (data) to establish a solid foundation for advancing knowledge[141] in the fields considering the intersection of GAI and privacy. It adopts a conceptual analytical framework, helpful in reflecting on and clarifying multiple descriptions of concepts, particularly in emerging fields[142] such as the GAI field.

---

[140] Hani Morgan, 'Conducting a Qualitative Document Analysis' (2022) 27(1) The Qualitative Report 64, 71 <https://hanimorgan.com/wp-content/uploads/2022/01/Hani-Morgan-Conducting-a-Qualitative-Document-Analysis-1.pdf> accessed 20 August 2024.

[141] Hannah Snyder, 'Literature Review as a Research Methodology: An Overview and Guidelines' (2019) 104 Journal of Business Research 333 <https://www.sciencedirect.com/science/article/pii/S0148296319304564> accessed 20 August 2024.

[142] Jaana Tahtinen and Virpi Havila, 'Conceptually confused, but on a field level? A method for conceptual analysis and its application' (2019) 19(4) Marketing Theory 533 <https://journals.sagepub.com/doi/full/10.1177/1470593118796677> accessed 20 August 2024.

1.5.1.2 Part 3 addresses RA1

Data collection

It involved the collection of primary and secondary documentary data, including non-legal textual data such as articles and case study analysis, and primary legal data such as case laws and legislation. The variety of source data reflects the socio-legal nature of this research. Cutting across several GAI case usage to present a holistic view of privacy issues associated with GAI. This generic classification was pivotal for understanding which privacy risk the selected case studies (part 4) fall under.

Data analysis

This part employed qualitative content analysis in investigating privacy risks associated with GAI models, it was pivotal to systemically identify and categorise the identified risks. Content analysis enables the systemic and objective identification of the characteristics of messages.[143] Beyond textual counting, content analysis enables the consideration of the substance of the text to be analysed and allows for a review of how various authors and sources view social occurrences, in this case, privacy risks.[144] This analytical method enabled this research to consider both aligning and divergent views on privacy risks associated with GAI models and to synthesise these opinions to arrive at the researcher's opinion on privacy risks associated with GAI models.

1.5.1.3 Part 4 addresses RA 2 & 3

This part employs case studies and Legal qualitative document methods.

Case studies are instrumental in making discoveries[145] and allow for detailed and intensive analysis of selected case(s).[146] This part takes on a representative/typical case study type,[147] epitomising broader privacy risks and challenges of current regulatory frameworks in the EU to address privacy infringements emanating from the development of and use of GAI models.

---

[143] Bruce Berg, *Qualitative Research Methods for the Social Sciences* (7th edn, Pearson 2009) 341.
[144] ibid, 343.
[145] ibid, 329.
[146] Tom Clark et al, Bryman's Social Research Methods (6th edn, Oxford University Press 2021) 59.
[147] Ibid 60

Data collection

Case study data was collected from secondary sources, including prominent news sources such as BBC, websites of regulatory bodies, and websites of an organisation (Meta) under study. Primary and secondary legal documents were also collected, including statutory laws, case laws, regulatory bodies' guidelines and opinions.

Data analysis

This part employs discourse analysis as its primary methodology. This is because critical discourse analysis is crucial for policy analysis, as it allows for an in-depth examination of the connection between language and broader social processes, moving beyond mere speculations and providing evidence of how effectively texts within policies and legislation function,[148] thereby addressing RA 2 and 3. It also analyses based on the context of social interactions with GAI models and privacy rights.

1.5.1.4 Part 5 addresses RA 4

This is the concluding part, and it draws from findings made in parts 3 and 4.

1.6 Overview of the article structure

Part one provides a background to the study, highlighting its significance, research questions, aims and objectives, and the research methodology adopted in conducting it.

Part two provides an overview of generative AI (GAI) models by defining generative AI and highlighting some of the generative modelling techniques that underpin GAI models.

Part three highlights some of the privacy risks associated with GAI models.

Part four provides 2 case study analyses highlighting the risks and examining the efficiency of current regulatory frameworks to address them; and

---

[148] Sandra Taylor, 'Researching Educational Policy and Change in 'New Times': Using Critical Discourse Analysis' (2004) 19(4) Journal of Education Policy 433, 436.

Part five synthesises my research findings and recommendations and concludes by reflecting on how the research responds to the research question and its aims and objectives.

2. An Overview of generative AI models

Generative AI (GAI) models have emerged as transformative foundational tools trained to comprehend intricate data distributions and produce outputs that densely mimic real-world data.[149] They are significant components that enable interactions and applications within GAI systems. GAI systems, on the other hand, encompass the entire GAI infrastructure, including the model, data processing, and user interface.[150]

Although generative AI gained prominence in recent times, it is said to date back to the 1950s with the development of Gaussian Mixture models and Hidden Markov networks, which were used to generate structures of data in the form of 'time series or speeches'.[151] However, the current break in GAI models and their ability to produce high-quality content is attributed to leveraging advancements in deep learning and their reliance on neural networks.[152]

This foundational part seeks to provide an overview of Generative AI models. Particularly, it explores definitions of the umbrella term 'Generative AI' (GAI), highlighting major commonalities shared across the definitions offered by diverse scholars, despite the lack of a generally accepted definition.[153] It also provides a general understanding of the term 'generative AI models' setting the tone for the usage of GAI-related terms throughout this research paper. It proceeds to cite examples of generative AI models, and their case uses and ends by providing a summative overview of some prominent generative modelling techniques underpinning GAI models to provide an understanding of some of their operational mechanisms and transformative potential.

---

[149] Leonardo Banh and Gero Strobel, 'Generative artificial Intelligence' (2023) 33 Electronic Markets 63, 66.

[150] Stefan Feuerriegel et al, 'Generative AI' (2023) 66(1) Business Information Systems Engineering 111, 112.

[151] Marcello Mariani and Yogesh Dwivedi, 'Generative Artificial Intelligence in Innovation Management: A Preview of Future Research Developments' (2024) 175 Journal of Business Research 114542, 114545.

[152] Banh and Strobel (n 41); see also Ian Goodfellow et al, 'Generative Adversarial Networks' (2020) 63(11) Communications of the ACM 139 <https://dl.acm.org/doi/abs/10.1145/3422622> accessed 14 August 2024.

[153] Francisco José García-Peñalvo, Andrea Vázquez-Ingelmo, 'What Do We Mean by GenAI? A Systematic Mapping of The Evolution, Trends, and Techniques Involved in Generative AI' (2023) 8(4) International Journal of Interactive Multimedia and Artificial Intelligence 7,8.

2.1 Definitions and examples of generative AI

In the EU, there seems to be no legal definition of Generative AI. The European Parliament's 2023 version of the draft EU AIA proposed defining Generative AI as "… *AI systems specifically intended to generate, with varying levels of autonomy, content such as complex text, images, audio, or video.*"[154] However, this definition has been ostensibly removed from the approved EU AI Act, which merely describes 'Large generative AI models' as a concrete example of general-purpose AI models[155] because of the flexibility it provides for content generation and their readiness to accommodate a diverse range of tasks.[156]

The adoption of a broader terminology, GPAI, as opposed to a streamlined terminology, GAI, may be attributed to the need to prevent the Act from early obsolesce resulting from a confined definition in an ever-evolving field.

Notwithstanding a lack of legal definition, the European Data Protection Supervisor (EDPS) has offered some definitions for the term GAI, which align with definitions by several authors. The EDPS define GAI as:

> "Generative AI is a subset of AI that uses specialised machine learning models designed to produce a wide and general variety of outputs, capable of a range of tasks and applications, such as generating text, image or audio."[157]

As is suggestive of the word 'generative' and as defined by several authors,[158] generative AI has three core characteristics: it is a class of artificial intelligence, it involves the generation or

---

[154] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD) Amendment 399, Art 28 (b)(4) <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html> accessed 25th June 2024.

[155] Please refer to the definition of general-purpose AI in part 4 of this article, page 66 for space/word count constraint.

[156] EU AI Act, Recital 99; see also Anton Korinek, 'Generative AI for Economic Research: Use Cases and Implications for Economics' (2023) 61(4) Journal of Economic Literature 1281.

[157] European Data Protection Supervisor (n 4) 4.

[158] See Cecilia Ka Yuk Chan and Tom Colloton, *Generative AI in Higher Education: The ChatGPT Effect* (Routledge 2024) 9; Anjana Susarla et al, 'The Janus Effect of Generative AI: Charting the Path for Responsible Conduct of Scholarly Activities in Information Systems' (2023) 34(2) Information Systems Research 399; Feuerriegel et al, (n 42) 111; Cecilia Ka Yuk Chan and Wenjie Hu, 'Students' voices on generative AI: perceptions, benefits, and challenges in higher education' (2023) 20(1) International Journal of Educational Technology in Higher Education 40 <https://doi.org/10.1186/s41239-023-00411-8> accessed 26 June 2024; Faisal Kalota, 'A Primer on Generative Artificial Intelligence' (2024) 14 (2) Education Sciences 172, 178 <https://doi.org/10.3390/educsci14020172> accessed 26 June 2024; Carmen Ungureanua and Aura Amironeseia, 'Legal issues concerning Generative AI technologies' (2023) 14(2) Eastern Journal of European Studies 45, 47;; Stephanie Houde et al, 'Business (mis)Use Cases of Generative AI' (*arxiv org*, 2 March 2020)

creation of new content, and it transcends the analysis of already existing data. While all authors agree on the first two characteristics, only about one-sixth highlight the third, which is a crucial feature. Summatively, Generative AI relies on foundational models, usually generative AI models, such as Large Language models (LLMs), which are crucial for the functioning of GAI systems.[159] GAI models leverage neural networks to discern patterns and structures in existing data, enabling the creation of new and original content.[160]

Some examples of Generative AI models include the GPT series by OpenAI widely known for their text generation abilities and other advanced versions such as GPT-4o which supports a multimodal input system – of any combination of audio, images, text and video – and also generates any combination of image, text, audio and video as output in response to prompts.[161] Other examples are DALL.E 3 by Open AI[162] which enables the translation of prompts to images, DeepAI[163] for text, image, video and music generation, styleGAN3 by NVidia[164] for image generation, Midjourney, a text-to-image AI generator,[165] AVIA[166] for music generation, stable diffusion and stable video diffusion by stability AI,[167] and Open AI codex[168] and GitHub Copilot[169] for the generation of codes.

Generative AI models exemplify the broad spectrum of capabilities. These advancements underscore the profound impact of techniques enabling the generation of new data. The

<https://arxiv.org/abs/2003.07679> accessed 26th June 2024; Ömer Aydin and Enis Karaarslan, 'Is ChatGPT Leading Generative AI? What is Beyond Expectations?' (2023) 11(3) Academic Platform Journal of Engineering and Smart Systems 118, 119 <https://dergipark.org.tr/en/pub/apjess/issue/80086/1293702> accessed 28 June 2024; Michael Muller et al, 'GenAICHI: Generative AI and HCI' (*ACM Digital Library*, April 2022) <https://doi.org/10.1145/3491101.3503719> accessed 28 June 2024; Akshay Kulkarni et al, *Applied Generative AI for Beginners: Practical Knowledge on Diffusion Models, ChatGPT and other LLMs* (Springer 2023) 2 <https://link.springer.com/book/10.1007/978-1-4842-9994-4> accessed 25th June 2024; Weng Marc Lim et al, 'Generative AI and the Future of Education: Ragnarok or Reformation? A Paradoxical Perspective from Management Educators' (2023) 21(2) The International Journal of Management Education 100790, 100791.

[159] EDPS (n 4); also see Feuerriegel et al (n 42) for more details on GAI systems.

[160] Kulkarni et al (n 50) 3; Yan Chen and Pouyan Esmaeilzadeh, 'Generative AI in Medical Practice: In-Depth Exploration of Privacy and Security Challenges' 2024) 26 Journal of Medical Internet Research 1, 2 <https://doi.org/10.2196/53008> accessed 4 July 2024.

[161] See OpenAI, 'Hello GPT-4o' (OpenAI, 2024)< https://openai.com/index/hello-gpt-4o/ > accessed 25 March 2025.

[162] See OpenAI, 'DALL·E 3' (OpenAI, 2025) <https://openai.com/index/dall-e-3/> accessed 25 March 2025.

[163] See DeepAI (DeepAI.org) <https://deepai.org/?ref=prototypr.io> accessed 25 March 2025.

[164] See NVIDIA, *StyleGAN3* (GitHub, 2021) <https://github.com/NVlabs/stylegan3> accessed 25 March 2025.

[165] See Discord, 'MidJourney Invite Link' (Discord, 2025) <https://discord.com/invite/midjourney> accessed 25 March 2025.

[166] See Aiva Technologies, 'Aiva: Artificial Intelligence Virtual Assistant' <https://www.aiva.ai/> accessed 25 March 2025.

[167] See Stability AI, 'Home' (Stability AI, 2025) <https://stability.ai/> accessed 25 March 2025.

[168] See OpenAI, 'OpenAI Codex' (OpenAI, 2025) <https://openai.com/index/openai-codex/> accessed 25 March 2025.

[169] See GitHub, 'GitHub Copilot' (GitHub, 2025) <https://github.com/features/copilot> accessed 25 March 2025.

succeeding sub-section gives an overview of some prominent techniques underpinning the development of GAI models.

2.1.1 Generative modelling techniques underpinning generative AI models

Generative AI models adopt varying generative modelling techniques, which enable and facilitate the data generation capabilities of generative AI models and allow for the creation of new data points.[170] García-Peñalvo and Vázquez-Ingelmo, in a systematic mapping, categorise the major techniques found in reviewed articles as follows: Generative Adversarial Networks (GANs), Encoder-Decoder Networks, other Neutral Networks, other techniques and transformers.[171]

2.1.1.1 Generative Adversarial Networks (GANs)

As represented in the chart above, GANs are one of the most adopted generative modelling techniques adopted by GAIs.[172] They have transformed machine learning and computer vision domains[173] and enable the creation of 'realistic stimulations'.[174] GAN is an unsupervised model,[175] which consist of two neural networks – the generator and the discriminator– adverse to each other. The generator works to create and improve the quality of its 'synthetic data samples' by introducing noise to real data (RD) while the discriminator works to evaluate the authenticity of the synthetic samples with the aim of distinguishing the synthetic sample from the real data. This process is iterated until both components reach a point of equilibrium, wherein it becomes difficult for the discriminator to distinguish between the synthetic data and the real data.[176] GANs are primarily used in generating images, illustrations, videos, and audio

---

[170] Staphord Bangesi et al, 'Review of GANs, GPT, Autoencoders, Diffusion Model, and Transformers' (2024) 12 IEEE Access 69812 <https://ieeexplore.ieee.org/document/10521640> accessed 8 July 2024.

[171] José García-Peñalvo and Vázquez-Ingelmo (n 45) 14.

[172] Kulkarni et al (n 50) 155; Mlađan Jovanović and Mark Campbell, 'Generative Artificial Intelligence: Trends and Prospects' (2022) 55(10) Computer 107 <https://doi.org/10.1109/MC.2022.3192720> accessed 9 July 2024.

[173] Ajay Bandi et al, 'The Power of Generative AI: A Review of Requirements, Models, Input–Output Formats, Evaluation Metrics, and Challenges' (2023) 15(8) Future Internet 260, 275 <https://www.mdpi.com/1999-5903/15/8/260> accessed 9 July 2024.

[174] Staphord Bengesi et al, 'Advancements in Generative AI: A Comprehensive Review of GANs, GPT, Autoencoders, Diffusion Model, and Transformers' (2024) 12 IEEE Access 69812,69813 <https://ieeexplore.ieee.org/document/10521640> accessed 9 July 2024.

[175] ibid, 69814.

[176] ibid, 158; Tom Taulli, *Generative AI: How ChatGPT and Other AI Tools Will Revolutionize Business* (2023 Apress) 81 -82.

samples and have been adopted by Generative AI models such as CycleGAN, text-2-image,[177] and StyleGAN. The integrity of GANs is confronted with certain limitations such as training instability and non-convergence as well as 'mode collapse', which could inter alia lead to homogeneity of output data.[178] However, GAN variants such as Conditional Generative Adversarial Network (cGAN), Wasserstein GAN (WGAN) and StarGAN have emerged to address some of these limitations.[179]

2.1.1.2 Encoder-decoder networks

Encoder-decoder architectures enable Recurrent Neural Networks (RNNs) in mapping input sequences to output sequences of varying lengths. The encoder processes the input sequence into a fixed-length context vector, encapsulating the entire input sequence, which the decoder then uses to generate the output sequence.[180] Modern encoder-decoder architectures enable the performance of sequence-to-sequence applications such as speech-to-text translations,[181] 'language modelling',[182] and machine translations.[183] Some encoder-decoder network models include attention-based sequence-to-sequence models (seq2seq), Variational Autoencoders (VAEs) and Transformers.

Seq2seq models are applicable for various use cases including natural language generation, summarisation, machine translations, text translations,[184] and speech recognition.[185] VAEs also leverage encoder-decoder architecture by utilising an additional sampling layer from a latent distribution to learn to generate data.[186] Unlike traditional autoencoders, VAEs adopt a

---

[177] Tom Taulli , *Generative AI: How ChatGPT and Other AI Tools Will Revolutionize Business* (2023 Apress) 81, 82.

[178] ibid, 83; Bengesi et al (n 66) 69818 - 69819.

[179] Bengesi et al (n 66) 69819 – 69822.

[180] Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep Learning* (MIT Press, 2016) 370 - 371.

[181] Kyle Aitken et al, 'Understanding How Encoder-Decoder Architectures Attend' (*arXvi*, 28 October 2021) <https://arxiv.org/abs/2110.15253> accessed 9 July 2024; Willam Chan et al, 'Listen, attend and spell: A neural network for large vocabulary conversational speech recognition' (IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP, March 2016) <https://ieeexplore.ieee.org/xpl/conhome/7465907/proceeding> accessed 9 July 2024.

[182] Aitken (n 73); Colin Raffel, ' Exploring the Limit of Transfer Learning with a Unified Text-to-Text Transformer' (2020) 21 The Journal of Machine Learning Research 5485 <https://dl.acm.org/doi/10.5555/3455716.3455856> accessed 9 July 2024.

[183] Goodfellow (n 72) and Aitken (n 73).

[184] Hendrik Strobelt et al, 'SEQ2SEQ-VIS: A Visual Debugging Tool for Sequence-to-Sequence Models (2019) 25(1) IEEE Transactions on Visualization and Computer Graphics 353.

[185] Chung-Cheng Chiu, 'State-of-the-Art Speech Recognition with Sequence-to-Sequence Models' (International Conference on Acoustics, Speech, and Signal Processing (ICASSP), April 2018) <https://ieeexplore.ieee.org/xpl/conhome/8450881/proceeding> accessed 9 July 2024.

[186] Bengesi (n 66), 69815

probabilistic approach within the encoder-decoder architecture, enabling them to capture the structure and variability of the data, and to 'generate new data samples from the learned latent' representation.[187] VAEs have versatile case usage and are applicable in audio, image and video processing, image classification,[188] financial activity monitoring[189] and anomaly detection.[190]

2.1.1.3 Transformers

Transformer models have emerged as highly scalable and powerful generative modelling techniques in natural language processing (NLP) and have also found applications in other domains such as computer vision.[191] They build upon the encoder-decoder architecture and owe their scalability, concurrency, and enhanced functionality to the incorporation of 'attention mechanisms'. These mechanisms, which have proven successful such as reading apprehension and summarisation, enable the efficient computation of contextual representations of both input and outputs, while eliminating the need for sequential data processing inherent in traditional models.[192] Some notable GAI models built with the transformer model include Google's bidirectional encoder representations from transformers (BERT), a language representation model used for a wide range of NLP tasks[193] as well as the Open AI's Generative Pre-trained Transformer (GPT) model[194] which gained prominence with the release of ChatGPT-3 in November 2022.[195]

---

[187] Feuerriegel et al (n 42) 115.

[188] Bengesi (n 66) 69815; see also Haleh Akrami et al, 'Brain Lesion Detection Using a Robust Variational Autoencoder and Transfer Learning' (IEEE 17th International Symposium on Biomedical Imaging (ISBI), May 2020) <https://ieeexplore.ieee.org/document/9098405> accessed 9 July 2024; Hugo Mak et al, 'Application of Variational AutoEncoder (VAE) Model and Image Processing Approaches in Game Design' (2023) 23(7) Sensors 3457 <https://www.mdpi.com/1424-8220/23/7/3457> access 9 July 2024.

[189] Bengesi (n 66) 69815; Nguyen Thi Ngoc Anh, 'Fraud Detection via Deep Neural Variational Autoencoder Oblique Random Forest' (IEEE-HYDCON, November 2020) <https://ieeexplore.ieee.org/document/9242753> accessed 9 July 2024.

[190] Longyuan Li, 'Anomaly Detection of Time Series with Smoothness-Inducing Sequential Variational Auto-encoder' (2021) 32(3) IEEE Transactions on Neural Networks and Learning Systems 1177.

[191] Bengesi (n 66) 69816; Salman Khan et al, 'Transformers in Vision: A Survey' (2022) 54(10) ACM Computing Surveys 200 <https://dl.acm.org/doi/10.1145/3505244> accessed 10 July 2024; Kai Han et al, 'A Survey on Vision Transformer' (2023) 45(1) IEEE Transactions on Pattern Analysis and Machine Intelligence 87 <https://ieeexplore.ieee.org/document/9716741> accessed 10 July 2024.

[192] Ashish Vaswani et al, 'Attention is All You Need' (31st Conference on Neural Information Processing Systems (NIPS), Long Beach, June 2017) <https://arxiv.org/abs/1706.03762> accessed 10 July 2024.

[193] Jacob Devlin, 'BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding' (*arXiv*, 2019) <https://arxiv.org/abs/1810.04805> accessed 10 July 2024.

[194] Gokul Yenduri, 'GPT (Generative Pre-Trained Transformer) – A Comprehensive Review on Enabling Technologies, Potential Applications, Emerging Challenges, and Future Directions' (2024) 12 IEEE Access 54608 <https://ieeexplore.ieee.org/document/10500411> accessed 10 July 2024.

[195] José García-Peñalvo and Vázquez-Ingelmo (n 45).

2.1.1.4 Other techniques

Some other generative modelling techniques include the diffusion model, which are probabilistic generative models that generate new sample data by introducing 'Gaussian' noise to training data (called the forwarding diffusion process) and then denoises it in stages (the reverse diffusion process).[196] This technique is used by several GAI models including Stability AI's stable diffusion and Midjourney for image generation.[197] However, a study has revealed that diffusion models are more susceptible to privacy risks than GANs.[198] Autoregressive Models are another generative technique that generates data by predicting the next value in a sequence based on previous values and is used across several models including GPTs, BERT, and audio generation models such as WaveNet and SampleRNN.[199] Some others include Normalising Flows, Energy-based Models.[200] and Recursive Neural Networks.

Generative AI stands as a transformative force in the field of artificial intelligence, capable of producing novel and diverse content across multiple media. These models are driven by sophisticated generative modelling techniques such as GANs, encoder-decoder networks, and transformers, enabling their content generation capabilities. While they bring significant benefits, including enhanced creativity and productivity, they also pose unique challenges, risks and limitations that require careful consideration. The next part will examine some of these risks, with a focus on data privacy risks.

2.1.1.5 Privacy risks associated with generative AI models

The rapid advancements and widespread adoption of Generative AI models have yielded numerous benefits, such as task automation and productivity enhancement[201] and present tremendous opportunities across several sectors, including healthcare, business, education,

---

[196] Bengesi (n 66) 69822.

[197] Ayush Parti, 'Diffusion Models: A Beginners Guide (2024)' (*Pareto AI,* February 2024) <https://pareto.ai/blog/diffusion-models> accessed 9 July 2024.

[198] Nicholas Carlini et al, 'Extracting Training Data from Diffusion Models' (*arXiv*, 30 January 2023) <https://arxiv.org/abs/2301.13188> accessed 13 July 2024.

[199] Ran Song, Hao Zhang, and Wei Zhang, '3D Generative Network', in Zhihan Lyu (Ed) *Applications of Generative AI* (Springer 2024) 477, 489.

[200] See Sam Bond-Taylor et al, 'Deep Generative Modelling: A Comparative Review of VAEs, GANs, Normalizing Flows, Energy-Based and Autoregressive Models' (2021) 44 (11) IEEE Transactions on Pattern Analysis and Machine Intelligence <https://ieeexplore.ieee.org/document/9555209> accessed 9 July 2024.

[201] Korinek, (n 48) 1282; Ethan Mollick and Jam Euchner 'The Transformative Potential of Generative AI' (2023) 66(4) Research-Technology Management 11.

and the media.[202] These models have become essential tools for content creation, driving innovation, and fostering creativity. However, GAI models also introduce significant risks including, job displacement[203] and breach of trust,[204] undermining institutional integrity.[205] Copyright infringement has also been at the centre of associated risks, garnering considerable scholarly[206] and judicial attention[207] and enormous legislative consideration in the recently passed EU AI Act.[208] Moreover, the foundational reliance of these models on vast amounts of data,[209] which encompasses personal and sensitive data, raises severe concerns about privacy risks[210] throughout the GAI models' lifecycle.[211]

This part explores some of the key privacy risks associated with GAI models, focusing on data breaches, data leakages, memorisation, data misuse, and inaccuracy. It also serves as a prelude for examining existing regulatory frameworks for addressing these concerns in Part 4 and lays the foundation for the case study analysis of the intersection of generative AI and data privacy in Part 5.

---

[202] Bangesi (n 66).

[203] Pawan Budhwar et al, 'Human Resource Management in the Age of Generative Artificial Intelligence: Perspectives and Research Directions on ChatGPT' (2023) 33(3) Human Resource Management Journal 606 <https://doi.org/10.1111/1748-8583.12524> accessed 17 July 2024.

[204] Yuntao Wang et al, 'A Survey on ChatGPT: AI–Generated Contents, Challenges, and Solutions' (2023) 4 IEEE Open Journal of Computer Society 280, 282 <https://ieeexplore.ieee.org/document/10221755> accessed 2 July 2024.

[205] Yueye Wang et al, 'Towards Regulatory Generative AI in Ophthalmology Healthcare: A Security and Privacy Perspective' (2024) British Journal of Ophthalmology <https://doi.org/10.1136/bjo-2024-325167> accessed 6 July 2024.

[206] See Ryan Webster, 'A Reproducible Extraction of Training Images from Diffusion Models' (arXiv, May 2023) <https://arxiv.org/abs/2305.08694> accessed 15 July 2024; Nicola Lucchi, 'ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems' [2023] European Journal of Risk Regulation 1, 3; Henrik Skaug Sætra, 'Generative AI: Here to stay, but for good?' (2023) 75 Technology in Society 1, 3; Pamela Samuelson, 'Generative AI meets Copyright' (2023) 381 Science (American Association for the Advancement of Science) 158.

[207] Lisa Oratz, 'Recent Rulings in AI Copyright Lawsuits Shed Some Light, but Leave Many Questions' (Perkins Coie, 14 December 2023) <https://www.perkinscoie.com/en/news-insights/recent-rulings-in-ai-copyright-lawsuits-shed-some-light-but-leave-many-questions.html> accessed 16 July 2024.

[208] Hannah Ruschemeier, 'Generative AI and Data Protection' in Handbook on Generative AI and the Law, (Cambridge University Press, 2024) (forthcoming) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4814999> accessed 28 June 2024.

[209] Philipp Hacker et al, 'Regulating ChatGPT and other Large Generative AI Models' (FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, New York, June 2023) 1112 <https://dl.acm.org/doi/abs/10.1145/3593013.3594067> accessed 9 July 2024.

[210] Fiona Fui-Hoon Nah et al, 'Generative AI and ChatGPT: Applications, Challenges, and AI-Human Collaboration' (2023) 25(3) Journal of Information Technology Case and Application Research 277, 286; Wirtz and Valentina, (n 6) 294.

[211] Chen and Esmaeilzadeh, (n 52) 7.

3.   An Examination of Privacy Risks Associated with Generative AI Models

3.1 Data Breach

The use of personal and sensitive data in training GAI models presents significant privacy risks, potentially exposing individuals to unauthorised access and misuse of their data.[212] Despite the implementation of data anonymisation or pseudonymisation techniques and the use of synthetic data samples to obscure personal data, GAI models remain susceptible to privacy attacks.[213] For instance, during the implementation phase, membership inference attacks may be employed to determine whether specific data points were part of the training dataset by querying and analysing the outputs. Similarly, by systematically querying GAI models, model inversion attacks may be used to reverse-engineer the original data and reconstruct sensitive training data, revealing personal information about individuals.[214]

To circumvent or mitigate these risks, some privacy-preserving techniques, such as differential privacy and decentralised learning systems have been introduced.[215] However, although some strides have been made, vulnerabilities can still be exploited. For instance, Wang[216] notes that while federated learning technique makes it difficult to target individual data curators, advanced adversarial GANs can be utilised to construct class representatives of the 'global data distribution' among data curators. Further experiment revealed the possibility of an attacker GAN (multi-task GAN for Auxiliary Identification (mGAN-AI) to invisibly access, identify

---

[212] Kerstin Denecke et al, 'Transformer Models in Healthcare: A Survey and Thematic Analysis of Potentials, Shortcomings and Risks' (2024) 48(1) Journal of Medical Systems 23, 29; Wirtz and Pitardi (n 6); Benjamin Alarie and Rory McCreight, 'The Ethics of Generative AI in Tax Practice' (2023) 180 Tax Notes Federal 785, 788; Chen and Esmaeilzadeh, (n 52) 7; Wang (n 96) 281; Inyoung Cheong, 'Safeguarding Human Values: Rethinking US Law for Generative AI's Societal Impacts' (2024) AI and Ethics 1, 4 <https://link-springer-com.libproxy.ncl.ac.uk/article/10.1007/s43681-024-00451-4> accessed 6 July 2024.

[213] Ajay Bandi et al, 'The Power of Generative AI: A Review of Requirements, Models, Input–Output Formats, Evaluation Metrics, and Challenges' (2023) 15(8) Future Internet 260, 273 <https://www.mdpi.com/1999-5903/15/8/260> accessed 9 July 2024; Ziqi Zhang, 'Membership inference attacks against synthetic health data' (2022) 125 Journal of Biomedical Informatics 103977; Bengesi et al, (n 66); Ghadeer Ghosheh et al, 'A Survey of Generative Adversarial Networks for Synthesizing Structured Electronic Health Records' 56(6) ACM Computing Surveys 147,167 <https://dl.acm.org/doi/10.1145/3636424> accessed 10 July 2024.

[214] Chen and Esmaeilzadeh, (n 52); Wang et al (n 95) 281; Ghosheh et al (n 105).

[215] Remya Raveendran and Ebin Deni Raj, Deep Generative Models Under GAN: Variants, Applications, and Privacy Issues in Vikrant Bhateja et al (Eds) (Springer 2022) 93, 103; Chen and Esmaeilzadeh, (n 52) 5; Tara Templin et al, 'Addressing 6 challenges in generative AI for digital health: A scoping review' (2024) 3(5) PLOS Digit Health 1, 6 <https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000503> accessed 5 July 2024.

[216] Zhibo Wang et al, 'Beyond Inferring Class Representatives: User-Level Privacy Leakage From Federated Learning' (IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, Paris, April/May 2019) <https://ieeexplore.ieee.org/document/8737416> accessed 11 July 2024.

and recover specified personal data from the server's side.[217] The very nature of GANs, which enable the generation of synthetic sample data that closely resembles the patterns observed in the training data, accentuates the risk of re-identification. [218] Additionally, although compressive privacy GAN (CPGAN) aim to eliminate 'sensitive' information during the pre-training stage, other personal data may risk being exposed and accessed.[219]

These ongoing privacy vulnerabilities, despite advancements in protective measures, raise dire concerns about privacy breaches and their potential legal and ethical implications, particularly in sensitive sectors including healthcare[220] and education sectors.[221]

3.1.1 Data Leakages

The potential for GAI models to disseminate or transfer personal and sensitive data, whether inadvertently[222] or intentionally through malicious manipulations, poses significant privacy risks. Both the training data[223] and data obtained and stored during downstream usage[224] risk leakage, particularly when data breaches are occasioned through malicious attacks.[225] Despite attempts to prevent these adversarial attacks, complete protection remains elusive.[226] This risk is exacerbated by GAI models' ability to memorise and generate precise data points, a stark

---

[217] ibid.

[218] Ghosheh et al, (n 105).

[219] Bo-Wei Tseng and Pei-Yuan Wu, 'Compressive Privacy Generative Adversarial Network, (2020) 15 IEEE Transactions on Information Forensics and Security 2499.

[220] Xu Guo and Yiquiang Chen, 'Generative LLMs for Synthetic Data Generation: Methods, Challenges and the Future' (2023) 29(1) International Journal of Information Technology 1, 5 <https://arxiv.org/abs/2403.04190> accessed 7 July 2024.

[221] See Md Abdur Rahman et al, 'A survey on security and privacy of large multimodal deep learning models: Teaching and learning perspective' (21st Learning and Technology Conference (L&T), Jeddah, Saudi Arabia, IEEE, 2024) 13, 15<https://ieeexplore.ieee.org/abstract/document/10469434>

[222] Cheong (n 104).

[223] Wang (n 7); Marco Antonio Beltran et al, 'Comparative Analysis of Generative AI Risks in the Public Sector' (Proceedings of the 25th Annual International Conference on Digital Government Research, June 2024) 610, 612 <https://dl.acm.org/doi/abs/10.1145/3657054.3657125> accessed 5 July 2024; Rahman et al (n 114); Morgan Briggs and Miranda Cross, Generative AI: Threatening Established Human Rights Instruments' (4th International Conference on Applied Artificial Intelligence (ICAPAI), Halden, April 2024) <https://ieeexplore.ieee.org/document/10541170> accessed 5 July 2024; see also OpenAI, 'Europe Privacy Policy' (OpenAI, 15 December 2023) <https://openai.com/policies/privacy-policy/> accessed 14 July 2024.

[224] Wang et al, (n 95) 289.

[225] Wang et al (96); Michele Bezzi, 'Large Language Models and Security' (2024) 22(2) IEEE Security & Privacy 60, 62-64 <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10413528> accessed 6 July 2024; Chuan Chen et al, 'Challenges and Remedies to Privacy and Security in AIGC: Exploring the Potential of Privacy Computing, Blockchain, and Beyond' (2023) 37(4) Journal of the Association of Computing Machinery 111, 114 <https://arxiv.org/abs/2306.00419> accessed 5 July 2024.

[226] See also Bezzi (n 117) 64.

contrast to conventional AI systems that merely produce responses based on 'prediction probabilities'.[227]

Research has shown that GAI models have the propensity to emit personal data from their training datasets. For instance, using a 'generate-and-filter pipeline' scheme, Nicholas Carlini et al.[228] demonstrated the ability to extract personal data including photographs of individuals with trademarked logos. In another study,[229] they also demonstrated the ability to use 'data extraction attack' to extract training data in GPT-2. Further studies highlight the concerning overlap between the features that enable data leakages in GAI models and those that optimise their performance. An empirical investigation conducted by Plant et al[230] revealed that there is a positive link between the volume of data used in training the model and the likelihood of data leakage. Additionally, the capacity of GAI models to accommodate large numbers of parameters and rapidly learn from input data further increases their susceptibility to data leakage.[231] This paradox poses significant threat to privacy rights and necessitates a careful evaluation of trade-offs between utility and privacy violations.

To circumvent these risks, several privacy-preserving mechanisms have been developed, including 'decoupling identity and attribute features',[232] 'memorisation rejection,[233] and privacy preservation technique, TrajGen,[234] which uses GAN and Seq2Seq to generate synthetic data.[235] However, as noted in 3.2.1. above, these counter mechanisms are not very efficient and synthetic data samples are still susceptible to data leakage.[236]

Additionally, inadvertent exposure of personal data can occur due to poor training data quality or interruptions within external training data sources.[237] For instance, a bug in an open-source

---

[227] Wang et al (n 96) 2.

[228] Carlini et al (n 90).

[229] Nicholas Carlini et al, 'Extracting Training Data from Large Language Models' (arXiv, 2021) <https://arxiv.org/abs/2012.07805> accessed 13 July 2024.

[230] Richard Plant et al, 'You Are What You Write: Preserving Privacy in the Era of Large Language Models' (arXiv, 2022) <https://arxiv.org/abs/2204.09391> accessed 13 July 2024.

[231] Chen et al, 'Challenges and Remedies (n 117) 123; see also Carlini et al (n 121).

[232] Maoguo Gong et al, 'Disentangled Representation Learning for Multiple Attributes Preserving Face Deidentification' (2022) 33(1) IEEE Transactions on Neural Networks and Learning Systems 244 <https://ieeexplore-ieee-org.libproxy.ncl.ac.uk/document/9229074> accessed 13 July 2024; Wang et al (n 7) 5.

[233] Andrew Bai, 'Reducing Training Sample Memorization in GANs by Training with Memorization Rejection' (arXiv, October 2022) <https://arxiv.org/abs/2210.12231> accessed 15 July 2024.

[234] See Chu Cao and Mo Li, 'Generating Mobility Trajectories with Retained Data Utility' (KDD '21: Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining, New York, August 2021) <https://dl-acm-org.libproxy.ncl.ac.uk/doi/abs/10.1145/3447548.3467158> accessed 13 July 2024.

[235] Wang et al, (n 7) 5 & 6.

[236] Ghosheh et al, (n 105).

[237] Chen and Esmaeilzadeh (n 114) 8.

library used by OpenAI's ChatGPT resulted in an inadvertent divulgence of users' chats, payment information and other personal data such as the names and email addresses of 1.2% of ChatGPT Plus subscribers.[238] Furthermore, Samsung's prohibition on the use of GAI tools by its employees due to concerns regarding potential leakage of sensitive internal source code by some of its employees[239] show that leakages may also result from users' reckless practices.

3.1.1.1 Memorisation

The memorisation capability of GAI models[240] poses significant privacy risks. It is influenced inter alia by the model's capacity, the size of the dataset and the number of occurrences or duplications of the training data.[241] This capability underpins other privacy risks such as data breaches and data leakages,[242] the amplification of biases and dissemination of misinformation present in training data, and challenges data subjects' rights to erasure[243] as personal data becomes muddled in training data.

A study conducted by Carlini et al[244] revealed that content memorised by GPT-2 included personal data as well as content removed from the internet but cached by Google search, revealing GAI models' potential to serve as unintended archives for removed data.[245] More so, an interaction with ChatGPT captured in a study conducted by Wu et al[246] revealed ChatGPT's ability to memorise downstream inputs, which include personal data, despite ChatGPT's assurance that it does not retain personal data.

---

[238] OpenAI, 'March 20 ChatGPT Outage: Here's What Happened' (OpenAI, 24 March 2023) <https://openai.com/index/march-20-chatgpt-outage/> accessed 13 July 2024.

[239] Arjun Kharpal, 'Samsung bans use of A.I. like ChatGPT for employees after misuse of the chatbot' (*CNBC*, 2 May 2023) <https://www.cnbc.com/2023/05/02/samsung-bans-use-of-ai-like-chatgpt-for-staff-after-misuse-of-chatbot.html> accessed 13 July 2024.

[240] See Wang et al (n 7); Wang et al (n 97) 3; Carlini et al (n 90); Carlini et al (n 121); See Kushal Tirumala et al, 'Memorization Without Overfitting: Analyzing the Training Dynamics of Large Language Models' (arXiv, November 2022) <https://arxiv.org/abs/2205.10770> accessed 15 July 2024.

[241] Seth Neel and Peter Chang, 'Privacy Issues in Large Language Models: A Survey' (arXiv, December 2023) <https://arxiv.org/abs/2312.06717> accessed 6 July 2024. [see this for more info and citation and cite in case study 2).

[242] See Wang et al (n 96), 2.

[243] General Data Protection Regulation (n 15), art 17.

[244] Carlini et al (n 121) 10.

[245] ibid.

[246] Xiaodong Wu et al, 'Unveiling Security, Privacy, and Ethical Concerns of ChatGPT' (arXiv, July 2023) <https://arxiv.org/abs/2307.14192> accessed 15 July 2024.

Notwithstanding a dissenting view, opining that memorisation is not found in GANs but in hybrid adversarial methods like CycleGAN,[247] numerous studies establish a divergent view,[248] with Park et al.[249] proposing a convolutional layer, perturbed convolution (PConv), to mitigate the memorisation problem in the discriminator angle in GANs. The memorisation function in GANs has also been established as essential for its optimisation,[250] and diffusion model is said to exhibit even stronger memorisation capabilities.[251]

Countermeasures to address the risk of memorisation are not entirely effective.[252] For instance, deduplication reduces but does not eliminate memorised data.[253] Anonymisation techniques such as named entity recognition (NER), which aims to detect personal information, can also create errors and may struggle with larger classifications of what amounts to personal information in complex situations.[254] This is particularly so given that the concept of personal data can be applied broadly, and every piece of information can be argued to be personal[255] as well as the broad interpretation of the concept of identifiability in Breyer's case.[256] Moreso, differential privacy has been noted to be ineffective when dealing with highly duplicated data.[257] These loopholes underscore the complexities of addressing memorisation as a data privacy risk.

---

[247] Ryan Webstar et al, 'Detecting Overfitting of Deep Generative Networks via Latent Recovery' (*arXiv*, January 2019) <https://arxiv.org/abs/1901.03396> accessed 15 July 2024.

[248] See Hongkang Yang and Weinan E, 'Generalization Error of GAN from the Discriminator's Perspective' (2022) 9 Research in the Mathematical Sciences 1, 8; Andrew Brock et al, 'Large Scale GAN Training for High Fidelity Natural Image Synthesis' (arXiv, February 2019) <https://arxiv.org/abs/1809.11096> accessed 15 July 2024; Shengyu Zhao, 'Differentiable Augmentation for Data-Efficient GAN Training' (arXiv, December 2020) <https://arxiv.org/abs/2006.10738> accessed 15 July 2024; Eyyup Yildiz, 'A single-image GAN model using self-attention mechanism and DenseNets' (2024) 596 Neurocomputing 127873; Abdallah Alshantti, 'CastGAN: Cascaded Generated Adversarial Network for Realistic Tabular Data Synthesis' (2024) 12 IEEE Access 13213, 13228 <https://ieeexplore.ieee.org/abstract/document/10410850> accessed 5 July 2024.

[249] Seung Park et al, 'PConv: Simple yet Effective Convolutional Layer for Generative Adversarial Network' (2022) 34 Neural Computing and Applications 7113 < https://link.springer.com/article/10.1007/s00521-021-06846-2> accessed 15 July 2024.

[250] Yang and E (n 140) 9.

[251] Carlini et al (n 90).

[252] Bezzi (n 117) 62-64.

[253] Katherine Lee, 'Deduplicating Training Data Makes Language Models Better' (arXiv, March 2023) <https://arxiv.org/abs/2107.06499> accessed 15 July 2024.

[254] Bezzi (n 117) 63.

[255] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) Law, Innovation, and Technology 40 <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> accessed 15 July 2024.

[256] See Case C-582/14 *Breyer v Federal Republic of Germany* EU:C:2016:779, [2017] 1 W L R 1569, para 57 – 78.

[257] Bezzi (n 117) 62-64.

3.1.1.2 Data Misuse

The inappropriate or unauthorised use of personal data for purposes other than its original intent can be occasioned during both the upstream development and the downstream usage of GAI models, posing significant threats to informational privacy. Informational privacy becomes threatened when there is a loss or apprehension of losing control over how and to what extent one's personal information is used or shared with others.[258]

Although the intrusive collection of data occurs both during the upstream development of GAI models and its downstream deployment and usage,[259] data misuse is particularly prevalent during upstream development, where extensive non-consensual scrapping of data, including personal and sensitive information, occurs from publicly accessible sources.[260] This re-purposing of personal data constitutes a misuse of data and is often justified by relying on 'legitimate interest' as the lawful basis for data collection/processing. Nevertheless, this justification is problematic, as will be seen in the case study analysis in Part 4. This intrusive collection also sets the stage for further privacy violations[261] and compromises data subjects' autonomy.

During downstream deployment, the generative capabilities of GAI models enable the creation of deepfakes which are capable of mimicking facial features and speech patterns and producing videos and imageries with astounding precision. This can result in identity theft, misrepresentation, and unauthorised access to personal information, as well as the generation of provocative and malicious content such as sexual deepfakes.[262] Although there are methods for detecting fake imagery and videos, they have several loopholes which could be exploited

---

[258]Black's Law Dictionary, 'Privacy' (12th edn, 2024) <https://www.westlaw.com/Document/I02fba78b808511e4b391a0bc737b01f9/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0> accessed 16 July 2024.

[259] Wang et al (n 95) 289.

[260] Alice Xiang, 'Fairness & Privacy in an Age of Generative AI' 25 The Columbia Science & Technology Law Review (2024) 288, 304 & 305; Chen et al (n 117) 112; Bridget Chimbga, Exploring the Ethical and Societal Concerns of Generative AI in Internet of Things (IoT) Environments in Anban Pillay, Edgar Jembere and Aurona Gerber (Eds), Artificial Intelligence Research (Springer, 2023) 44 <https://link-springer-com.libproxy.ncl.ac.uk/book/10.1007/978-3-031-49002-6> accessed 16 July 2024.

[261] Chen et al (118).

[262] Judy Lambert and Mark Stevens, 'ChatGPT and Generative AI Technology: A Mixed Bag of Concerns and New Opportunities' (2023) Computers in School 1, 8 <https://www.tandfonline.com/doi/full/10.1080/07380569.2023.2256710> accessed 7 July 2024; Cheong (n 54) 4.

as demonstrated by Hussain et al.[263] The misuse of personal data to create non-consensual sexual deepfakes will be analysed in Part 4. The said part will also be pivotal in understanding if and how the privacy rights of individuals are guarded against such misuse as well as the misuse occasioned by the intrusive collection of personal and sensitive data.

Misuse of personal data during downstream deployment can also manifest through social surveillance, profiling, and personalised advertising.[264] In the absence of informed consent by users, such activities will amount to a breach of privacy rights, and developers cannot rely on legitimate interest, particularly if personal data is used for services incompatible with the purposes for which they were initially collected.[265]

3.1.1.3 Inaccuracy

Generative AI models have the proclivity to hallucinate [266] and generate inaccurate information/narratives about individuals or individuals of a particular group. For instance, the algorithmic tool, COMPAS, adopted in the US to predict the probability of recidivism among ex-offenders, was found to be biased against black individuals, accurately predicting 'violent recidivism' only 20 per cent of the time.[267] In certain instances, while the source data may be accurate, particularly in terms of statistical data, it may result in the generation of inaccurate and biased inferences or reflect historical data, which often contain information that is undesirable to perpetuate.[268]

While there are several examples of GAI hallucinations,[269] some notable examples include ChatGPT's misinformation, accusing Mark Walters of embezzling funds from the Second

---

[263] Shehzeen Hussain et al, 'Adversarial Deepfakes: Evaluating Vulnerability of Deepfake Detectors to Adversarial Examples' (IEEE Workshop on Applications of Computer Vision (WACV), Waikoloa, HI, June 2021) <https://ieeexplore-ieee-org.libproxy.ncl.ac.uk/document/9423202> accessed 16 June 2024.

[264] Jochen Wirtz and Valentina Pitardi, 'How Intelligent Automation, Service Robots, and AI will Reshape Products and their Delivery' (2023) 2023 Italian Journal of Marketing 289, 295.

[265] See Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* EU:C:2023:537 [2023] 5 C M L R 22, para H23; see also General Data Protection Regulation (n 15), art 5(1)1(b).

[266] Templin et al (n 107) 7.

[267] Jeff Larson, Surya Mattu, Lauren Kirchner and Julia Angwin, 'How we Analysed the COMPAS Recidivism Algorithm' (ProPublica, 23 May 2016) <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> accessed 17 July 2024

[268] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why A 'Right to An Explanation' Is Probably Not the Remedy You Are Looking For' (2017) 16 (1) Duke Law and Technology Review 15, 28.

[269] See IBM, 'What are AI Hallucinations?' (*IBM*, 29 March 2023) <https://www.ibm.com/topics/ai-hallucinations> accessed 17 July 2024.

Amendment Foundation (SAF)[270] and the complaint filed against OpenAI by the Austrian NGO, NOYB, with the Austrian Data Protection Authority (DPA) for falsifying information concerning individuals.[271] The complaint also highlights a concerning issue: ChatGPT's inability to 'rectify' inaccurate information. This limitation may be indicative of a broader problem affecting other GAI models, particularly LLMs.

The generation of inaccurate information and GAI hallucinations is largely influenced by the quality and representativeness[272] of their pre-training[273] and training data.[274] GAI models generate content based on probabilistic predictions and learned patterns in training dataset.[275]

Consequently, inaccuracies and hallucinations in GAI models could have ripple effects on data subjects, including tarnished reputation, financial implications, dissemination of misinformation,[276] and wrongful medical recommendations in the healthcare sector.[277] In the healthcare sector, for example, Convolutional Generative Adversarial Networks (CorGAN) which centres on connections within medical records, are said to improve 'predictive accuracy',[278] however, caution is to be exercised, and adequate protection is required as GAI models/systems do not actually 'know' but rely on their training to generate outputs.[279]

The privacy risks associated with GAI models present a complex challenge for preserving data subjects' privacy rights. While GAI offers significant benefits across various domains its optimisation factors also contribute to privacy risks, potentially impacting data subjects adversely. This paradoxical relation between utility and privacy necessitates a balance between innovation and the protection of individuals' inherent right to privacy. The analysis

---

[270] Sabrina Ortiz, 'ChatGPT's Hallucination Just Got OpenAI Sued: Here's What Happened' (ZDNET, 9 June 2023) <https://www.zdnet.com/article/chatgpts-hallucination-just-got-openai-sued-heres-what-happened/> accessed 17 July 2024.

[271] NOYB, 'ChatGPT Provides False Information About People, and OpenAI Can't Correct It' (NOYB, 29 April 2024) <https://noyb.eu/en/chatgpt-provides-false-information-about-people-and-openai-cant-correct-it> accessed 17 July 2024.

[272] Global Privacy Assembly, '45th Closed Session of the Global Privacy Resolution on Generative Artificial Intelligence Systems' (EDPS, 20 October 2023) 1, 6 <https://www.edps.europa.eu/system/files/2023-10/edps-gpa-resolution-on-generative-ai-systems_en.pdf> accessed 22 July 2024.

[273] Guo and Chen (n 112) 5.

[274] Yusuke Kajiwara and Kouhei Kawabata, 'AI Literacy for Ethical use of Chatbot: Will Students accept AI Ethics?' (2024) 6 Computers and Education: Artificial Intelligence 100251 <https://doi.org/10.1016/j.caeai.2024.100251> accessed 6 July 2024; Davinder Kaur et al, 'Trustworthy Artificial Intelligence: A Review' (2022) 55(2) ACM Computing Survey 39, 40.

[275] Edwards and Veale (n 164).

[276] Information Commissioner Office, 'Generative AI Third Call for Evidence: Accuracy of Training Data and Model Outputs' (ICO, undated) < https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/generative-ai-third-call-for-evidence/ > accessed 17 July 2024.

[277] Templin et al (n 107) 7.

[278] Chen and Esmaeilzadeh (n 114) 2.

[279] Lambert (n 102) 6.

in this part highlights that privacy risks are interconnected, with one violation potentially leading to others.[280] Consequently, GAI models present unique privacy issues compared to conventional AI systems, underscoring the importance of examining how regulatory measures address these risks.

4. Case study analysis: intersection of generative AI models and data privacy

The structural design of GAI models, which requires reliance on vast amounts of data, including personal and sensitive data and anti-privacy practices such as memorisation,[281] creates unique challenges for the actualisation of individuals' fundamental right to privacy guaranteed under international,[282] regional[283] and national laws. Leveraging its internal market influence, the EU sets the pace at the regional level by providing unified laws to foster innovation and create certainty for digital actors while ensuring the preservation of privacy rights in this digitalised economy.

This part examines the multifaceted implications of generative AI (GAI) on data privacy based on two (2) real-life case scenarios.

The first is Meta's plan to collect users' (personal and sensitive) data dating back to 2007 to develop and improve its AI technology, highlighting privacy risks of data breaches and data misuse during GAI models' development stage. This case study represents a vital examination of the legality of development practices of GAI models amidst regulators' steps to challenge[284] and scrutinise[285] them. It takes a critical approach by examining the provisions for data

---

[280] Chen et al (n 117) 128.

[281] See 3.2.3. above for discussions on the memorisation capabilities and requirements for the functioning of GAI systems.

[282] International Covenant on Civil and Political Rights 1967, art 17

[283] See Charter of Fundamental Rights of the European Union [2012] OJ C326/391(CFR), Art 7; Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights as amended) (ECHR), art 8; see Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47, art 16 (1).

[284] See Irish Data Protection Commission (DPC), The DPC welcomes X's agreement to suspend its processing of personal data for the purpose of training AI tool 'Grok' (Irish DPC, 8 August 2024) <https://www.dataprotection.ie/en/news-media/press-releases/dpc-welcomes-xs-agreement-suspend-its-processing-personal-data-purpose-training-ai-tool-grok> access 23 August 2024; Aodhan O'Faolain, 'Irish watchdog takes court action against Twitter over AI user data concerns' (The Irish Times, 6 August 2024) <https://www.irishtimes.com/business/2024/08/06/dpc-takes-court-action-against-twitter-over-ai-user-data-concerns/> accessed 22 August 2024.

[285] Luca Bertuzzi, 'European Data Protection Authorities Launch Task Force on ChatGPT' (Euractiv, 13 April 2023) <https://www.euractiv.com/section/artificial-intelligence/news/european-data-protection-authorities-launch-task-force-on-chatgpt/> accessed 23 August 2024.

protection at the development stage and the adequacy of extant regulatory frameworks to address it.

The second case study explores the non-consensual creation and dissemination of a Taylor Swift deepfake, highlighting privacy risks such as data breach, memorisation, inaccuracy, and data misuse during the deployment stage. Research indicates that advancements in state-of-the-art GAI models have made it increasingly challenging to distinguish between authentic images and deepfakes,[286] demonstrating the potential of GAI technologies to generate and propagate inaccurate information about individuals, particularly as images are potent tools for captivating audiences and disseminating information.[287] This case study is a representation of privacy violations which could result in grievous harm,[288] what has been described as 'an emerging form of image-based sexual abuse',[289] underscoring a need for stringent prohibitory laws and penalties.

This part evaluates how EU regulatory frameworks address these issues and assesses the effectiveness of these frameworks in providing privacy protections in the context of generative AI. While both case studies focus on the GDPR,[290] the second case study further examines the recently enacted EU Artificial Intelligence Act (AIA).[291] It begins with a brief overview of the major laws under review: the GDPR and the AIA, and then delves into the analysis of the case studies.

4.1 Brief overview of examined regulatory frameworks

a. The GDPR regulates the processing of personal data relating to natural persons (data subjects) in the EU, irrespective of where the processing takes place and whether the

---

[286] Sophie J Nightingale and Hany Farid, 'AI-synthesized faces are indistinguishable from real faces and more trustworthy' (2022) 119 (8) Proceedings of the National Academy of Sciences of the United States of America <https://www.pnas.org/doi/full/10.1073/pnas.2120481119> accessed 24 August 2024; Sergi Bray, Shane Johnson and Bennett Kleinberg, 'Testing Human Ability to Detect 'Deepfake' Images of Human Faces' (2023) 9 (1) Journal of Cybersecurity 1.

[287] Eryn Newman and Norbert Schwarz, 'Misinformed by Images: How Images Influence Perceptions of Truth and What can be Done About It' (2023) 56 Current Opinion in Psychology 101778 <https://www.sciencedirect.com/science/article/pii/S2352250X23002233?ref=cra_js_challenge&fr=RR-1> accessed 26 August 2024.

[288] Regina Rini and Leah Cohen, 'Deepfakes, Deep Harms' (2022) 22(2) Journals of Ethics and Social Philosophy 143.

[289] Asher Flynn et al, 'Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse' (2022) 62 The British Journal of Criminology 1341.

[290] General Data Protection Regulation (n 15).

[291] Artificial Intelligence Act (n 27).

controller or processor is established in the EU.[292] It is rooted in the idea of informational self-determination, to the effect that natural persons should have autonomy over their data.[293] It defines personal data as "any information relating to an identified or identifiable natural person …"[294]

b. The AIA, which is complementary to the GDPR[295] regulates the placing on the EU market and the use of artificial intelligence (AI) systems and aims to *inter alia* ensure the adequate protection of fundamental rights,[296] including privacy rights. It takes on a risk-based approach to regulating AI systems by categorising risks as unacceptable, high, limited and minimal and imposing additional obligations on high-risk systems.[297]

4.2 Case study 1: allegations of pervasive collection of personal and sensitive data

4.2.1 Background

In May 2024, Meta notified its European users of its intention to change its privacy policy effective 26 June 2024. The major issue of contention in its new policy pertaining to privacy was Meta's intention to collect and use its users' personal (and sensitive) data, including public posts, comments, captions, and photographs on Facebook and Instagram dating back to 2007 for the development and improvement of its GAI technology, 'AI at Meta', relying on the legal basis of 'legitimate interest' and giving users an option to opt-out by filling out an objection form.[298] Meta also mentioned that this collection and use of European users' data would enable Meta to develop well-tailored AI products that reflect the diverse languages, cultures and geography of the European users.[299] Following several complaints and expressions of concern,

---

[292] General Data Protection Regulation (n 15), art 1 and 3
[293] ibid, recital 7.
[294] ibid, art 4(1).
[295] Artificial Intelligence Act (n 27), recital 9.
[296] Artificial Intelligence Act (n 27), art 1.
[297] Future Life Institute, 'High-Level Summary of the AI Act' (EU Artificial Intelligence Act, 27 February 2024) <https://artificialintelligenceact.eu/high-level-summary/> accessed 24 August 2024; Lilian Edwards, 'Expert explainer: The EU AI Act proposal' (*Ada Lovelace Institute*, 8 April 2022) <https://www.adalovelaceinstitute.org/resource/eu-ai-act-explainer/> accessed 12 August 2024.
[298] Stefano Fratta, 'Building AI Technology for Europeans in a Transparent and Responsible way' (*Meta*, 10 June 2024) <https://about.fb.com/news/2024/06/building-ai-technology-for-europeans-in-a-transparent-and-responsible-way/>accessed 5 August 2024; Ludovico Bossi, 'Meta's AI Arriving in Europe: Privacy Disputes Concealing Copyright Concerns' (*Kluwer Copyright Blog*, 20 June 2024) <https://copyrightblog.kluweriplaw.com/2024/06/20/metas-ai-arriving-in-europe-privacy-disputes-concealing-copyright-concerns/> accessed 5 August 2024.
[299] Ibid, Fratta (n 190).

including from the Norwegian Data Privacy Authority,[300] the Irish Data Protection Commission (DPC), Meta's lead regulator in the EU and on behalf of the European DPAs, requested Meta pause the implementation of its new policy, and Meta complied.[301]

The GDPR is the sole regulation examined in this case study, as provisions in the AIA on data governance and management practices are limited to high-risk systems[302] and these practices seem better spelt out in the GDPR.

4.2.1.1 Addressing privacy risks associated with the pervasive collection of personal and sensitive data under the EU GDPR

4.2.1.2 Collection of Personal Data Under the GDPR

The proposed extensive data collection by Meta for the development and improvement of 'AI at Meta', being purposes other than what they were initially processed for (mostly social interactions), amounts to a misuse of personal data. This practice challenges the notion of information self-determination[303] and risks further privacy violations.[304] To safeguard the privacy rights of data subjects and curb data misuse while ensuring a fair balance of trade-offs between utility and privacy, data controllers are required to adhere to principles for processing set out in Article 5 of the GDPR. However, the structural design and practices in GAI development challenge the adequacy of the GDPR in addressing data misuse through the pervasive collection of personal and sensitive data.[305] Building on the principle of lawfulness[306] and the decisions of European courts, this section explores the interconnectedness of data processing principles and data subjects' rights in protecting privacy rights, as well as the challenges of the GDPR in adequately protecting privacy rights.

---

[300] Datatilsynet, 'Meta Will Use the Users' Photo and Posts to Develop AI' (*Datatilsynet*, 4 June 2024) <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2024/meta-vil-bruke-brukernes-bilder-og-innlegg-til-a-utvikle-ki/> accessed 5 August 2024.
[301] Bossi (n 192); NOYB, 'NOYB Urges 11 DPAs to Immediately Stop Meta's Abuse of Personal Data for AI' (*NOYB*, 6 June 2024) <https://noyb.eu/en/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai> accessed 5 August 2024.
[302] See Artificial Intelligence Act (n 27), art 10.
[303] See General Data Protection Regulation (n 15), recital 7; Bruin (n 17).
[304] See also Office of the Australian Information Commissioner (OAIC), 'Global Expectations of Social Media Platforms and Other Sites to Safeguard Against Unlawful Data Scraping' (OAIC, 24 August 2023) <https://www.oaic.gov.au/newsroom/global-expectations-of-social-media-platforms-and-other-sites-to-safeguard-against-unlawful-data-scraping> accessed 5 August 2024; UK ICO (n 5).
[305] Paragraph 4.3.2.2. below would address sensitive data with more privacy risks.
[306] General Data Protection Regulation (n 15), art 5(1)(a)

The processing of any personal data must be done on one of the lawful grounds set out in the GDPR.[307] While the widespread practice of requiring consent creates a presumption that it is one of the most commonly used grounds,[308] and there has been the need to dispel the myth that all processing must be on the basis of consent,[309] consent remains one of the six grounds for which data may be processed. Of these grounds, Meta, like GAI developers/providers before it,[310] relies on 'legitimate interest' as a lawful ground for collecting personal data.[311] This is so because it allows for the balancing of diverse interests: those of the data subjects and the data controller or third parties.[312]

EU case laws[313] have consistently emphasised that reliance on legitimate interest must meet three cumulative conditions: the pursuit of a legitimate interest, necessity, and overriding interest of the data controller or a third party.[314]

4.2.1.3 The pursuit of a legitimate interest

The court[315] links the pursuit of legitimate interest with data subjects' right to be informed of the legitimate interest at the time of data collection.[316] This right to information is intrinsically linked to the principle of purpose limitation,[317] which is opposed to vague and generic expressions of purpose,[318] but requires data to be "collected for specified, explicit and

---

[307] General Data Protection Regulation (n 15), art 6.

[308] Shaira Thobani, 'Processing Personal Data and the Role of Consent' (2020) 2020 European Journal of Privacy Law and Technologies 93, 94

[309] UK Information Commissioner Office, 'Data Sharing Myths Busted' (*ICO*, undated) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-myths-busted/> accessed 25 August 2024.

[310] Bossi (n 190).

[311] See Fratta (n 190); see also Meta, 'Privacy Policy' (*Meta*, updated 26 June 2024) <https://mbasic.facebook.com/privacy/policy/printable/version/25238980265745528/#> accessed 5 August 2024.

[312] Google Spain (n 26), para 81.

[313] Case C-13/16, *Valsts Policijas Rīgas Reģiona Pārvaldes Kārtības Policijas Pārvalde v Rīgas Pašvaldības SIA (Rīgas Satiksme)* EU:C:2017:336, [2017] 4 W L R 97, para 28; Case C-597/19, *Mircom International Content Management & Consulting (MICM) Ltd v Telenet BVBA* EU:C:2021:492, [2021] Bus. L.R. 1294, para 106.

[314] See also General Data Protection Regulation (n 15), art 6 (1) (f).

[315] Case C-252/21, Meta Platform (n 157), para 107.

[316] See General Data Protection Regulation (n 133), art 13.

[317] See Article 29 Data Protection Working Party (WP), 'Opinion 03/2013 on purpose limitation' (*European Commission*, adopted 2 April 2013), 15 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 24 July 2024; Liana Colonna, 'Data Mining and Its Paradoxical Relationship to the Purpose Limitation Principle' in Serge Gutwirth, Ronald Leenes and Paul De Hert (Eds), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (Springer, 2014) 299, 303.

[318] WP Opinion 03/2013 (n 121) 15 - 17.

legitimate purposes and not further processed in a manner that is incompatible with those purposes …"[319] [Emphasis mine].

Meta, in its privacy policy, stated its purpose for processing (collection) inter alia as:

> "To develop and improve artificial intelligence technology (also called AI at Meta) that we provide, on our products and to Third Parties."[320] [Emphasis mine]

Furthermore, the hyperlink on 'artificial intelligence technology' directs us to a page that does not specifically state the purpose of the collection but states, inter alia, that **"We're developing generative AI experiences …"**[321]

The lack of specificity in the information provided not only evidences a flagrant violation of the specificity requirement,[322] foundational to data protection,[323] but also highlights the incompatibility of developing GAI models with data processing principles.[324] GAI models, like the one Meta seeks to develop, are typical examples of general-purpose AI (GPAI) models that demonstrate broad generality and are capable of integration across various downstream applications.[325] This versatility likely drives the reluctance to provide explicit, specific and pre-determined purposes, allowing for future flexibility in applying the model. However, this practice undermines data subjects' informational control, as it prevents them from making informed decisions regarding the use of their data and from effectively challenging such use, thereby reinstating the informational power asymmetry the GDPR aims to address.[326]

An argument may be canvassed in relation to the tokenisation of training data, thereby converting personal data to anonymised/pseudonymised data in line with privacy-by-design (PbD) practices[327] and enabling the move of data as a model as opposed to explicit personal

---

[319] General Data Protection Regulation (n 15), art 5 (1)(b).
[320] Meta (n 273).
[321] Meta, 'How Meta Uses Information for Generative AI Models and Features' (*Meta*, undated) <https://www.facebook.com/privacy/genai> accessed 5 August 2024.
[322] NOYB (n 195); see also European Data Protection Supervisor (EDPS), 'EDPS Investigation into Use Of Microsoft 365 by the European Commission (Case 2021-0518)' (*EDPS*, 8 March 2024) <https://www.edps.europa.eu/data-protection/our-work/publications/investigations/2024-03-08-edps-investigation-european-commissions-use-microsoft-365_en> accessed 7 August 2024.
[323] WP Opinion 03/2013 (n 120).
[324] Ruschemeier (n 22), 9.
[325] See Artificial Intelligence Act (n 27), recital 99 and art 4 (63).
[326] Indra Spiecker and Genannt Dohmann, 'AI and Data Protection' in Larry DiMatteo, Cristina Poncibo and Michel Cannarsa (eds) *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (Cambridge University Press 2022) 132, 134.
[327] General Data Protection Regulation (n 15), art 25(1).

data, hence minimising privacy and regulatory concerns.[328] However, in the light of purpose specificity requirement, this practice represents an indirect way of processing personal data for purposes other than initially collected. While the purpose limitation principle is not averse to repurposing data provided it is compatible with the purpose for which it was initially processed,[329] the application of training data to diverse downstream applications means that personal data represented in those training data/models influences the functioning and output of these models. This undermines the purpose limitation principle, which is intended not only to bind processing to specific purposes but also to guide it[330] and amplifies concerns around data misuse as a privacy risk occasioned by the development and deployment of GAI models. While the principle of legitimate interest could protect privacy rights if rigorously applied,[331] particularly where the violation has not been occasioned, its effectiveness is compromised when violations stem from vague or unspecified data processing purposes.

4.2.1.4 The necessity requirement

This prong requires Meta to show that data collection is 'strictly necessary' for the purpose specified[332] and cannot reasonably be achieved in a less intrusive manner.[333] While there are hopes that future research will unveil techniques that can be developed from limited data,[334] several studies have established the need for vast amounts of data to train GAI models,[335]

---

[328] Michael Veale, Reuben Binns and Lilian Edwards, 'Algorithms that Remember: Model Inversion Attacks and Data Protection Law' (2018) 376 Philosophical Transactions of the Royal Society A 1, 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3212755> 25 August 2024.
[329] General Data Protection Regulation (n 15), art 5(1)(b).
[330] Spiecker and Dohmann (n 218) 136 & 137.
[331] Isabel Hahn, 'Purpose Limitation in the Time of Data Power: Is There a Way Forward?' (2021) 7 (1) European Data Protection Law Review 31.
[332] Meta Platforms (n 157), para 126; General Data Protection Regulation (n 15), art 6 (1)(f); European Data Protection Supervisor (EDPS), 'Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (EDPS, 11 April 2017) 7 < <https://www.edps.europa.eu/sites/default/files/publication/17-04-11_necessity_toolkit_en_0.pdf> accessed 6 August 2024.
[333] ibid, Meta Platform (n 157), para 108.
[334] Balagopal Ramdurai and Prasanna Adhithya, 'The Impact, Advancements and Applications of Generative AI' (*Researchgate*, undated) 1, 6 <https://www.researchgate.net/profile/Balagopal-Ramdurai/publication/371314493_The_Impact_Advancements_and_Applications_of_Generative_AI/links/647e ec9679a7223765138f73/The-Impact-Advancements-and-Applications-of-Generative-AI.pdf> accessed 28 August 2024.
[335] ibid; Ajay Bandi et al, 'The Power of Generative AI: A Review of Requirements, Models, Input–Output Formats, Evaluation Metrics, and Challenges' 15(8) Future Internet 260, 277 & 309 <https://www.mdpi.com/1999-5903/15/8/260> accessed 27 August 2024; Hacker et al (n 101) 1113.

linked to their 'increased scope of application',[336] seemingly satisfying the aspect of strict necessity.

However, the failure to explicitly specify the purpose for collection and reliance on the generic phrase "… to develop and improve Artificial Intelligence technologies …" means that Meta will collect any and every data, except private conversations; an intention captured in Meta's privacy policy.[337] This act makes obsolete the proportionality[338] and data minimisation[339] principles, requiring controllers to collect data that are "adequate, relevant and limited to what is necessary …"[340]

Indeed, all forms of data processing, irrespective of their justification, interfere with the privacy rights of individuals.[341] However, the data minimisation principle, which seeks to minimise the impact of privacy intrusions[342] is impeded by the structural design and nature of GAI models, obscuring the potency of the GDPR in protecting the personal data of data subjects from data misuse.

4.2.1.5 Overriding interest of the data controller or third party

The stringent requirement for an outweighed interest[343] serves as a critical safeguard against data misuse occasioned by the pervasive collection of personal data. The vast collection of personal data challenges the contextual nature of this determination, weighed on a case-by-case basis[344] and the individualistic nature of the GDPR fails to account for this.[345]

---

[336] Hacker et al (n 101) 1113.

[337] See also Meta (n 271).

[338] EDPS (n 214), 5.

[339] Meta Platforms (n 157), paras 109 and 121; see also Case C-708/18, *TK v Asociatia de Proprietari bloc M5A-ScaraA* EU:C:2019:1064, [2020] 2 C M L R 17, para 48.

[340] General Data Protection Regulation (n 15), art 5 (1)(b); European Data Protection Board (EDPB), ' Report of the Work Undertaken by the ChatGPT Taskforce' (EDPB, 23 May 2024) 1, 6 <https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf> accessed 16 August 2024.

[341] EDPS (n 216), 5.

[342] Md Abdul Malek, 'Bigger is Always not Better: Less is More, Sometimes: The Concept of Data Minimization in the Context of Big Data' (2021) 2021 European Journal of Privacy Law & technologies 212, 216.

[343] General Data Protection Regulation (n 15), art 6 (1)(f); Meta Platforms (n 158), para 126; see also Google Spain (n 26), para 74.

[344] Ibid, Meta Platforms (n 157), para 112.

[345] Ruschemeier (n 22), 8 & 9.

Moreso, the determination of an outweighed interest is initially based on self-evaluation by the data controller,[346] raising concerns about its objectivity, particularly in the context of the well-established principle of *nemo judex in causa sua* (no one should be a judge in their own case). However, while self-evaluation is a starting point, it may be subject to further evaluations, particularly when challenged by other stakeholders such as the data subjects or data protection authorities and eventually determined by the courts.[347]

The courts[348] and ChatGPT Taskforce have weighed in on the balancing act required under this prong. The Court of Justice of the European Union (CJEU), in Google Spain's case,[349] held that in balancing the diverse rights and interests, the *'potential seriousness of the interference'* on the privacy and data processing rights of the data subject is to be considered. While the facts in that case differ from the facts in this case study, in that, in the former, the interference resulted in overt and easy, structured accessibility of personal data to members of the public,[350] and the latter does not necessarily result in the same, salient applications can be drawn.

Research has shown that GAI models, built on personal data, though tokenised or converted into unintelligible representations during the training stage, can be reconstructed to reveal personal data.[351] Hence, if this susceptibility means that models are personal data,[352] then a case may be made in favour of the data subjects' interest as overriding. However, this seems unlikely, particularly considering the ChatGPT Taskforce position, which primarily reinstated Article 29 WP's position[353] that putting protective measures in place to subside excessive impact on data subjects can tilt the balancing requirement in the data controller's favour.[354]

Of interest and leaning towards the idea of information self-determination is the requirement of 'reasonable expectation' – encompassing foreseeability and acceptance[355] –, provided in

---

[346] Article 29 Data Protection Working Party (WP), 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (WP Opinion 06/2014) (European Commission, Adopted 9 April 2014) 14 <https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2014/wp217_en.pdf> accessed 7 August 2024.

[347] ibid.

[348] With a focus on Google Spain (n 26) and Meta Platform (n 157).

[349] Google Spain (n 26), para 81.

[350] ibid, para 37 & 80.

[351] See Carlini et al (n 90); Carlini et al (n 121).

[352] An interesting topic area that has emerged; see Veale, Binns and Edwards (n 220); please also note that this inference does not include re-identification of personal data obtained through illegal means (cyberattacks), which the court in Breyer (n 149), para 47 excludes from the categorisation of personal data.

[353] WP Opinion 06/2014 (n 237) 31& 42.

[354] EDPB ChatGPT Taskforce Report (n 5) 6 & 7.

[355] Irene Kamara and Paul De Hert, 'Understanding the Balancing Act behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach' in Evan Selinger, Jules Polonetsky and Omer Tene (Eds), *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press, 2018) 321, 335.

recital 47 of the GDPR and reinstated by the CJEU in the Meta Platforms case.[356] The stringent enforcement of this requirement would imply that the balancing scale will tilt in favour of Meta Platforms' users, who cannot be said to *reasonably expect* that their data will be processed indiscriminately at such scale without their consent.[357] This is particularly so given the extensivity of the data sought to be collected,[358] which, as in the Meta Platform' case, 'relates to potentially unlimited data' and could significantly impact users,[359] who will constantly feel apprehension that they are constantly being monitored.[360]

The strict application of both courts' interpretation of the balancing act would mean that Meta cannot rely on the ground of legitimate interest to mine users' data at the scale with which it seeks to mine them, and consequently, it may be said that the GDPR offers protection in this regard. However, this may not necessarily be the case as the legality or otherwise of processing is determined on a case-by-case basis. More so, in the Meta Platform case,[361] the court was asked to evaluate the legitimacy of using 'research and innovation for social good' as a basis for overriding data subjects' rights but refrained from doing so due to the lack of sufficient details before it. This missed opportunity to assess 'innovation for social good' as a legitimate ground for data collection, sufficient to override data subjects' rights, underscores the importance of being explicit when establishing an overriding interest, which is lacking.

4.2.1.6 Collection of Sensitive Data

Given the broad scope of user data Meta intends to collect—encompassing comments, chats with business and professional accounts, app usage, and activities carried out in them[362]—there is a high likelihood that sensitive data, which fall under special categories of personal data,[363] will be included. For instance, messages sent and received from professional accounts may contain information concerning a client's health or sexual orientation, political opinions, and sex life, which constitute sensitive data[364] and may have been shared based on trust.

---

[356] Meta Platform (n 157), para 112 & 116.
[357] See ibid, para 117.
[358] See also Article 29 Data Protection WP (n 185) 36 – 40.
[359] Google Spain (n 26), para 80 & 87.
[360] Meta Platform (n 157), para 118.
[361] Meta Platforms (n 157), para 114.
[362] Meta (n 202).
[363] See General Data Protection Regulation (n 15), art 9(1) and recital 51.
[364] General Data Protection Regulation (n 15), art 9 (1) & (2).

Additionally, sensitive data may be revealed by GAI models from ordinary data.[365] Processing of sensitive data, including those that cannot be separated from non-sensitive personal data,[366] is strictly regulated and generally prohibited under the GDPR, save in certain circumstances.[367] In the context of this case study, Meta may seek to rely on exceptions of consent and manifestly publicly available sensitive data to collect these data. However, the actions of Meta run afoul of these exceptions and show that while there are adequate protections for the processing of sensitive data in the context of this case, there is a flagrant disregard for its provisions, occasioning data breaches of users' sensitive data.

4.2.1.7 On consent

Explicit consent,[368] which must be 'freely given, specific, informed and an unambiguous indication' of the user's wishes either 'by a statement or a clear affirmative action'[369] is required to rely on this exception. The CJEU, in Planet 49's case[370] held that consent requires active rather than passive actions. Thus, the opt-out method adopted by Meta, requiring users who are opposed to the collection of their data to object to it, constitutes a passive act and cannot amount to consent required under Article 9(2), 6(1) and defined under Article 4(11) of the GDPR. Moreso, such an act will amount to a 'covert acquisition'[371] of sensitive data, particularly as the data sought to be collected ranges from users' data dating as far back as 2007, some of whom are either inactive users or unaware of the policy changes or may just accept generic privacy policy changes. For any such changes to be valid, requests for consent must also be obtained disparately for each processing operation required.[372] More so, while the court has held that a controller's dominant position does not necessarily hinder users from giving valid consent, it stresses that the controller must not make detrimental any refusal to give consent.[373]

---

[365] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2019(2) Columbia Business Law Review 494; case study 2 on the generation of sexual deepfakes exemplifies this and would be analysed below.
[366] Meta Platforms (n 157), para 89.
[367] ibid, art 9 (1) & (2).
[368] General Data Protection Regulation (n 15), art 9.
[369] ibid, art 4 (11)
[370] Case C-673/17 *Verbraucherzentrale Bundesverband eV v Planet49 GmbH* EU:C:2019:801, [2020] 1 W L R 2248, para 52.
[371] John Van de Pas and Geert-Jan Van Bussel, 'Privacy Lost – and Found?' The Information Value Chain as a Model to Meet Citizens' Concerns' (2015) 18(2) Electronic Journal Information Systems Evaluation 185, 191 <https://pure.hva.nl/ws/portalfiles/portal/140721/613113_ejise-volume18-issue2-article977.pdf> accessed 8 August 2024.
[372] Meta Platforms (n 157), paras 144 and 151.
[373] General Data Protection Regulation (n 15), recital 42 and 43; Ibid, para 143 and 147.

However, this does not stop Meta from charging a proportionate fee as an alternate option.[374] While Meta's opt-out option could play a pivotal role in safeguarding the rights of data subjects,[375] it cannot replace the role of consent or other limited exemptions for processing sensitive data.

4.2.1.8 On manifestly available sensitive data

To ensure the informational self-determination of data subjects, where Meta intends to rely on this exception, the GDPR requires Meta to ensure that the data is 'manifestly made public by the data subject'.[376] Hence, the collection of sensitive data relating to an individual but made public by another person/user amounts to a flagrant violation of the informational privacy of users. Meta can also not rely on mere visits and interactions with apps or websites and interactions such as likes and shares in satisfaction of this exemption, particularly where users are capable of adjusting their device settings to limit the access of the public to such interactions.[377] Meta's intention to rely on users' posts, which presumably include posts with limited access to the general public, blatantly violates the provision of the GDPR and amounts to data breaches. More so, Meta's reliance on grounds of legitimate interest to collect sensitive data is in clear violation of the GDPR and infringes on the privacy rights of data subjects.

Given the flagrant disregard of some robust provisions that ought to offer protections to data subjects and the practice of GAI model developers to bypass certain measures by virtue of the systemic nature of GAI models, it becomes imperative to consider the remedies put in place to protect the privacy and data processing rights of data subjects. While the Data subjects' rights as a remedy would be discussed next, the penalties would be discussed jointly after analysing case study 2.

4.2.1.9 Data Subjects' Rights Under the GDPR

The GDPR provides numerous rights aimed at protecting the informational self-determination and privacy rights of data subjects, offering remedies for data misuse and breaches arising from the collection of personal data. Meta, in compliance with its obligation to inform,[378] refers to

---

[374] Meta Platforms (n 157), para 150.
[375] Article 29 Data Protection WP (n 183), 45.
[376] General Data Protection Regulation (n 15), art 9(2)(e).
[377] Meta Platforms (n 157), paras 79 – 83.
[378] General Data Protection Regulation (n 15), art 13(2)(b) and 21(4).

some of these rights,[379] including the right to access,[380] data portability[381] and, particularly of focus under this heading due to space constraint, the right to object[382] and to erasure.[383]

While the right to object could provide an effective ex-ante remedy to prevent data misuse and breaches at the pre-training stage, it offers little or no protection as a post-ante remedy at the training and post-training stage. This is problematic as, in certain instances, data subjects only become aware of these violations after the act.

For instance, Meta provides that "If your objection is honoured, going forward we won't use your public information …"[384] [sic] and fails to address the possibility of an erasure regarding data collected for training its AI technology.

While the initial phrase 'if your objection is honoured' flows from the required balancing act,[385] the ambiguous phrase 'going forward' raises questions regarding how Meta will enforce DSR to object. The court has unequivocally held that where the controller honours the request, the controller 'must' end the processing of 'the data in question.'[386] Thus, failing to do so regardless of the processing stage, constitutes a violation of the GDPR.

However, the enforceability of this provision becomes challenging when the data collected is converted into training data, muddled with other data and difficult to distil. The remedy of resort may then fall on the right to an erasure or to restriction of processing, where the data subject opposes the erasure of personal data.[387] While the remedy of restriction of processing may be actualised through the use of filtering mechanisms, the black-box nature of AI models,[388] which pose difficulty in distilling specific personal data from training data, challenges the actualisation of the right to an erasure. Assuming this is possible, the circulation of these data points among several users[389] as well as the fact that learned patterns cannot be

---

[379] Meta, 'Privacy Policy' (*Facebook*, undated) <https://www.facebook.com/privacy/policy> accessed 27 August 2024.

[380] ibid, art 15.

[381] ibid, art 20.

[382] See Meta (n 204); General Data Protection Regulation (n 15), art 15; Article 29 Data Protection Working Party (WP) (n 183), 44.

[383] ibid, art 17.

[384] Meta, 'Object to Your Information Being Used for AI at Meta' (Facebook, Undated) <https://www.facebook.com/help/contact/6359191084165019?paipv=0&eav=AfaXL-dWUiC4vXTrB07l-9OqCdZhmPeeEL6HCOz1Lnreodsh_9zQPsiBbWzqmrVgWNM> accessed 27 August 2024.

[385] See General Data Protection Regulation (n 15), art 21(1).

[386] Google Spain (n 26), para 77.

[387] General Data Protection Regulation (n 15), art 18(1)(b).

[388] Melanie Fink and Michèle Finck, 'Reasoned A(I) Administration: Explanation Requirements in EU Law and the Automation of Public Administration' (2022) 47 European Law Review 376, 382.

[389] Claudio Novelli et al, 'Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity' (*arXiv*, 15 March 2024) 1, 12 < https://arxiv.org/abs/2401.07348> accessed 27 August 2024.

deleted,[390] challenges its effectiveness of both the right of an erasure and restriction of processing. This is particularly so where the model itself is considered personal data. This point is elaborated in section 4.4.2.2. below. Notwithstanding OpenAI's reference to the right to 'delete' personal data,[391] it remains uncertain how it can be actualised.[392] Particularly in the context of models as personal data, Veale et al[393] suggest that the right to erasure may be exercised by amending the model itself by 'machine unlearning' or by amending training dataset. While the practicality of these suggestions remains in doubt[394], they pose significant economic and environmental risks and do not guarantee an absolute remedy for data subjects, particularly when considering that the model has been widely applied and deployed across various systems[395] and the deletion of all these systems is not unrealistic but economically unsound.

4.3. Case study 2: non-consensual creation of Taylor Swift's sexual deepfake

4.3.1.1 Background

Sometime in January 2023, sexually explicit deepfake imagery of Taylor Swift, allegedly created using a diffusion model[396] and alleged by 404 media to have been generated through Microsoft Designer,[397] was circulated on social media platforms, including on X garnering over 45 million views.[398] This deepfake was allegedly created by exploiting loopholes in the GAI

---

[390] Veale, Binns and Edwards (n 221) 9; Cheng-chi Chang, 'When AI Remembers Too Much: Reinventing the Right to Be Forgotten for the Generative Age' (2024) 19(3) Washington Journal of Law, Technology and Arts 22, 37; Zeyu Zhao, 'The Application of the Right to Be Forgotten in the Machine Learning Context: From the Perspective of European Laws' (2022) 31(1) Catholic University Journal of Law and Technology 73, 94.

[391] See OpenAI, 'Privacy Policy' (updated 14 November 2023) <https://openai.com/policies/privacy-policy/> accessed 25 August 2024.

[392] Claudio Novelli et al, 'Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity' (*arXiv*, 15 March 2024) 1, 12 < https://arxiv.org/abs/2401.07348> accessed 27 August 2024.

[393] Veale, Binns and Edwards (n 221) 9 & 10.

[394] See Eduard Fosch Villaronga, Peter Kieseberg and Tiffany Li, 'Humans Forget, Machines Remember: Artificial intelligence and the Right to Be Forgotten' (2018) 34 Computer Law & Security Review 304, 310; Zhao (n 282).

[395] Novelli et al (n 283) 12.

[396] Kate Conger and John Yoon, 'Explicit Deepfake Images of Taylor Swift Elude Safeguards and Swamp Social Media' (The New York Times, 26 January 2024) <https://www.nytimes.com/2024/01/26/arts/music/taylor-swift-ai-fake-images.html> accessed 31 July 2024.

[397] See Emanuel Maiberg and Samantha Cole, 'Taylor Swift Porn Went Viral on Twitter: Here's How it Got There' (404 media, 25 January 2024) <https://www.404media.co/ai-generated-taylor-swift-porn-twitter/> accessed 29 July 2024; Kat Tenbarge, 'Microsoft CEO Responds to AI-Generated Taylor Swift Fake Nude Images' (NBC News, 26 January 2024) <https://www.nbcnews.com/tech/tech-news/taylor-swift-nude-deepfake-ai-photos-images-rcna135913> accessed 29 July 2024.

[398] Jess Weatherbed, 'Trolls Have Flooded X with Graphic Taylor Swift AI Fakes' (The Verge, 25 January 2024) <https://www.theverge.com/2024/1/25/24050334/x-twitter-taylor-swift-ai-fake-images-trending> 29 July 2024.

tool through name misspellings and the use of 'non-sexual descriptions'[399] suggesting a form of membership inference attack – not only to determine whether Swift's image, but to extract her image from training data to create her deepfake. This privacy violation, which occurred in the United States (U.S.) sparked outrage from fans and U.S. lawmakers.[400] X responded by temporarily banning searches for Taylor Swift, [401] while Microsoft, after an internal investigation, denied the allegations but stated that they had strengthened their 'text filtering prompts' to prevent misuse of their services.[402]

The creation and proliferation of non-consensual sexual deepfakes represent a severe and emergent form of image-based sexual abuse,[403] highlighting the grievous harms[404] linked to the use of personal data in training/developing GAI models. The memorisation function of these models poses inherent privacy risks leading to downstream violations such as data breaches, inaccuracy and data misuse during their deployment. The incident also raises critical questions about whether GAI models constitute personal data and underscores the need to evaluate current regulatory frameworks and their adequacy to protect data privacy and address privacy risks.

4.3.1.2 Addressing the non-consensual creation of sexual deepfakes in the EU

This section focuses on the GDPR and AIA and examines their effectiveness in mitigating and/or addressing privacy violations and risks, particularly data breaches, inaccuracies, and data misuse, emanating from the deployment of GAI models to create non-consensual sexual deepfakes. Before delving into the analysis, the preceding section examines who the data controllers are under the GDPR.

---

[399] Dylan Horetski, 'Microsoft Makes Major AI Change after Taylor Swift Deepfake Controversy' (*Dexerto*, 29 January 2024) <https://www.dexerto.com/tech/microsoft-makes-major-ai-change-after-taylor-swift-deepfake-controversy-2504555/> accessed 27 August 2024.

[400] Conger and Yoon (n 203).

[401] Nadine Yousif, 'X Blocks Searches for Taylor Swift After Explicit AI Images of her Go Viral' (BBC, 28 January 2024) < https://www.bbc.co.uk/news/world-us-canada-68123671?amp%3Bat_campaign=KARANGA > accessed 31 July 2024.

[402] Tenbarge (n 288); Weatherbed (n 287).

[403] Asher Flynn et al, 'Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse' (2022) 62 The British Journal of Criminology 1341.

[404] Regina Rini and Leah Cohen, 'Deepfakes, Deep Harms' (2022) 22(2) Journals of Ethics and Social Philosophy 143.

4.3.1.3 Who are the data controllers?

It is well established that any individual or entity that alone or jointly determines the purpose and means of processing personal data is a data controller.[405] In the context of the alleged membership inference, both the developers/providers of Microsoft Designer and the users creating and disseminating the deepfake are data controllers as they both determine the purpose and means of the processing, albeit in different capacities. However, complexities arise when/if the sexual deepfake was generated by users inputting Taylor Swift's personal data (face) into a GAI system and altering an existing video to create the deepfake.

The CJEU, in the Google Spain case, [406] expressed reservations about allocating the responsibilities of a controller to an intermediary that performs merely a formal function and lacks the factual knowledge required to fulfil the obligations in Articles 6, 7, and 8 of the defunct DPD, which corresponds with Articles 5, 6, and 9 of the GDPR with slight alterations.[407] If Microsoft Designer was merely a tool for processing personal data without actual knowledge of such processing and is unable to satisfy the conditions in Articles 5, 6, and 9, Microsoft could be exonerated from being deemed a controller and consequently from liability. However, the court's further and eventual holding puts this matter to rest.

The court clarified that a system capable of exerting control by determining its functionality and blocking certain activities – such as enforcing exclusion codes – would be considered a controller of personal data. [408] Consequently, in this scenario, developers of Microsoft Designers would also be regarded as controllers and thus responsible for safeguarding data subjects' rights. This is particularly relevant in the globalised technology landscape, where identifying users to enforce these rights can be challenging.[409]

Although two scenarios have been painted here, due to space constraints and flowing from the background in 4.4.1 above, the analysis in the subsequent sections will focus on the creation of non-consensual sexual deepfakes and associated privacy issues emanating from membership inference attacks and the effectiveness of the GDPR in addressing them.

---

[405] See General Data Protection Regulation (n 15), art 4 (7).
[406] Google Spain (n 26).
[407] ibid, para 82 – 90.
[408] ibid, para 91 – 93.
[409] See ibid, para 44.

4.3.1.4 Addressing the non-consensual creation of sexual deepfakes under the GDPR

The non-consensual creation of sexual deepfakes, which fall within the ambit of sensitive data, by revealing aspects of an individual's sex life[410] – albeit false – constitutes a clear violation of the GDPR, which prohibits such processing.[411] This act breaches the principle of lawful data processing and demonstrates how GAI systems can be weaponised to create/generate disinformation about individuals. This exemplifies the privacy risk of inaccuracy associated with GAI models/systems, extending beyond the conventional issues of poor/inaccurate training datasets[412] or AI hallucination,[413] and highlights the broader societal risks posed by AI-generated falsehoods.[414]

The extraction of training data, which constitutes a data breach and the misuse of extracted data for the unlawful generation of inaccurate information concerning a data subject not only evidences multiple violations and privacy risks but also the inadequacy of the GDPR to adequately address privacy issues/risks emanating from the development and deployment of GAI models.

For one, it exposes the inadequacy of privacy by design (PbD) mechanism,[110] such as encryption or tokenisation, in safeguarding the privacy rights and information self-determination of data subjects, which is a primary objective of this mechanism.[415] This is particularly concerning when systems containing 'anonymised/pseudonymised' data are used to perpetrate grievous harm. Microsoft's inability to find evidence that its GAI tool was bypassed[416] suggests either non-use or that these systems can be circumvented without detection, raising serious concerns about the enforcement of reporting obligation in Article 33 of the GDPR in the case of a breach, and the broader implications for monitoring privacy violations and protecting data privacy.

---

[410] See General Data Protection Regulation (n 15), art 9(1).
[411] ibid, art 9(1) & 2(a).
[412] Guo and Chen (n 122); Kajiwara and Kawabata (n 123)
[413] Templin et al (n 116).
[414] See Jiawei Zhou et al, 'Synthetic Lies: Understanding AI-Generated Misinformation and Evaluating Algorithmic and Human Solution' (CHI Conference on Human Factors in Computing Systems (CHI '23), 19 April 2023) 436, 437 <https://dl.acm.org/doi/full/10.1145/3544548.3581318> accessed 12 August 2024.
[415] Ann Cavoukian, 'Privacy By Design: The Seven Foundational Principles' (The Sedona Conference Institute, undated) 1, 2
<https://www.thesedonaconference.org/sites/default/files/conference_papers/Recommended%20%5B08b%5D%20Privacy%20By%20Design_Cavoukian.pdf> accessed 1 September 2024.
[416] Tenbarge (n 286).

The extraction of training data from GAI models, like Microsoft Designer (integrated with the DALL-E 2[417] and now DALL-E3)[418] could be attributed to their memorisation capabilities. Diffusion model,[419] a key generative modelling technique used in developing DALL-E 2,[420] is said to be 'trained to memorise and reconstruct their dataset'.[421] This capability raises pertinent considerations about whether (GAI) models can be considered personal data and how data subjects' rights will be protected and enforced if an infringement occurs.

An application of the CJEU's[422] interpretation of the expression 'any information' and 'relating to' in the definition of personal data[423] suggests that (GAI) models could be considered personal data.[424] The court, in line with the Article 29 Working Party's position,[425] further held that the information can relate to an individual by reason of its effect, content or purpose.[426]

In the context of this case study, the focus would be the effect element. The court in considering this element connects it to the 'consequence'[427] of the use of the data on the data subject's right or interest. Consequently, the use (extraction) of the training dataset (GAI model) to create Taylor Swift's sexual deepfake affects her [data] privacy rights and could breed several negative consequences/effects on her. An examination of various sexual deepfake stories has been shown to lead to both online and offline harassment, mental health issues and even death threats.[428]

---

[417] See Kyle Wiggers, 'Microsoft brings DALL-E 2 to the masses with Designer and Image Creator' (*Techcrunch*, 12 October 2022) <https://techcrunch.com/2022/10/12/microsoft-brings-dall-e-2-to-the-masses-with-designer-and-image-creator/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAAKMI-q09W4Eg8eHRzTxfwXUc0tLp1AGMymWSP9LiMYUhKro_t9o20hXf-uUkUh7uOFWk5r7m6QQIv-I6trA_qj1eMAdBS2HhWhfZo7OdIPbgr2g8utwBuGR35FYfLBdPx5HyNT4G9ItpvArOQBkhX7LAAWr1Hy6Y8ei4UXudB2FM> 31 July 2024.

[418] Microsoft, 'Designer improvements with DALL-E-3 (Bing Image Creator)' (Microsoft, 29 February 2024) <https://www.microsoft.com/en-us/bing/do-more-with-ai/image-creator-improvements-dall-e-3?form=MA13KP&msockid=268ec0d940a9681322f2d44a41ec690c> accessed 31 July 2024.

[419] See Github, 'DALL·E 2 Preview - Risks and Limitations' (*GitHub*, undated) <https://github.com/openai/dalle-2-preview/blob/main/system-card.md> accessed 1 September 2024.

[420] It is uncertain if the diffusion model is also a major modelling technique in DALL-E 3.

[421] Carlini et al (n 90) 12: Ryan O'Connor, 'How DALL-E 2 Actually Works' (Assembly AI, 29 September 2023) <https://www.assemblyai.com/blog/how-dall-e-2-actually-works/> accessed 31 July 2024.

[422] Case C-434/16 Nowak v Data Protection Commissioner EU:C:2017:582 [2018] 1 W.L.R. 3505, para 34.

[423] In article 2(a) of the defunct DPD, now contained in the General Data Protection Regulation (n 15), art 4(1) (a).

[424] See Veale et al (n 220) 6-8.

[425] Article 29 Data Protection Working Party (WP), 'Opinion 4/2007 on the Concept of Personal Data' (*European Commission*, adopted 20 June 2007) 1, 9 – 12 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 27 August 2024.

[426] Nowak (n 310), para 35.

[427] Nowak (n 312), para 39; Opinion 4/2007 (n 311) 11.

[428] Chidera Okolie, 'Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns' (2023) 25 (2) Journal of International Women Studies 1, 7&8.

In light of the above, it is safe to imply that GAI models/systems are personal data.[429] While there may be attempts[430] to broadly apply the CJEU's decision in Breyer's case[431] regarding the exclusion of illegally de-identified data from the definition of personal data, a closer examination of the court's dicta reveals limitations to this application.

Paraphrasing, the CJEU held that pseudonymised data provided by a service provider constitutes personal data 'in relation to that provider' where the provider has the legal means, that enable it to identify the data subject with additional data.[432]

This suggests that the restriction applies specifically to the provider of the pseudonymised data, in this case, the GAI model developers/providers and not broadly to all parties. Moreover, as rightly alluded to by Hacker,[433] the view that illegality excludes identifiability would contradict the 'protective regime' of the GDPR, which is designed to prevent illegal processing, and notes that Recital 26 of the GDPR which discusses identifiability does not mention the legality criteria.

However, while the expansive scope of personal data may be applied to models,[434] strictly applying provisions of the GDPR to these models as personal data may be extremely problematic and may create unrealistic expectations for data subjects and controllers.[435] For instance, users would be required to have lawful grounds for the deployment/use of GAI models/systems.[436] Hence, a more relaxed approach, applying provisions of the GDPR based on how the model affects data subjects, would be a better application of Nowak's case. This approach recognises individual data points as personal data, especially when de-identified, which seems to be the case in practice.

To address these issues, data subjects may invoke their right to object, to the restriction of processing, and/or to erasure. However, the enforcement of these rights, particularly against GAI providers, is limited, as discussed in case study 1 (section 4.3.2.3.) above. Hence, to maximise the space limit, the effectiveness of the enforcement of DSRs on individuals (both the direct deployers and persons who disseminate the deepfake) will be discussed.

---

[429] See Veale et al (n 220) 6-8.
[430] See Ruschemeier (n 22) 9; Purtova (n 148) 64 & 65.
[431] Breyer (n 148), para 49.
[432] Breyer (n 148), para 49.
[433] Philipp Hacker, 'A Legal Framework for AI Training Data—from First Principles to the Artificial Intelligence Act' 13(2) Law, Innovation and Technology 256, 267.
[434] See Veale et al (n 22) 8 – 12.
[435] See Veale et al (n 220) 10 & 11.
[436] Novelli et al (n 281) 12

In this case of an outright violation, the right to an erasure[437] will be triggered. However, the global reach of GAI system users, who are sometimes anonymous or reside outside the EU, complicates and deflects enforcement. This makes legal entities, especially multinational companies easy targets. However, even within the EU, the right to erasure may not offer adequate protection, as it would be nearly impossible to enforce against everyone who possesses the deepfake. While the Digital Services Act[438] provides some protection against the proliferation of illegal content online,[439] and some countries have legislation against revenge pornography, which in limited instances may cover the proliferation of sexual deepfakes offline, there seems to be no comprehensive regional framework addressing the proliferation of sexual deepfakes offline.

The inadequacies of the GDPR's principles and the limitation of DSRs in addressing issues of data breaches, misuse and inaccuracies resulting from the creation of sexual deepfakes necessitate an examination of the penalties provided under the GDPR and their effectiveness in addressing these issues. This will be explored in relation to case studies 1 and 2 in section 4.4.2.4. below.

4.3.1.5 Privacy protections under the EU AI Act

The EU AI Act[440] is vital to this case study in that it not only regulates large GAI models but also deepfakes. It provides that large GAI models such as DALL-E 2[441], which is integrated into Microsoft Designer are examples of General-Purpose AI (GPAI) models and define GPAI models as:

> "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market."[442]

---

[437] General Data Protection Regulation (n 15), art 17.
[438] 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), art 16.
[439] However, due to space constraint, this framework is not analysed.
[440] Artificial Intelligence Act (n 27).
[441] Or DALL-E 3 the updated version of the DALL-E series.
[442] ibid, art 3(63).

The AIA takes on a risk-based approach to regulating AI systems and imposes stringent rules on high risks[123] and systemic risks[124] with the objective of mitigating them.[125] However, the regulation of GAI models/systems used in generating deepfakes, does not fall into high-risk system[126] but falls under limited risks[443] with limited obligations on providers and deployers, which do not seem to offer any privacy protection in the context of this case study.

However, the AIA offers systemic protection against data breaches, stemming from GPAI models with systemic risk. This is so as providers of GPAI models that fall into this category are mandated to perform model evaluations – including 'conducting and documenting adversarial testing' with the aim of 'identifying and mitigating systemic risks.'[444] These evaluations seem akin to the ones conducted by Carlini et al[445] and would be instrumental in understanding how adversarial attacks are conducted and in observing loopholes within systems to address them and ensure safer deployment of GAI systems. To ensure uniformity of standards, the AI office is expected to roll out codes of conduct for the enforcement of the said provision by 2 May 2025.[446]

This systemic approach is in line with calls for structural measures beyond the GDPR,[447] and it can serve as an effective tool to protect training (personal) data. However, the limitation of this obligation to GAI models with systemic risks is a limitation to ensuring the safety of all GAI systems. Although it is uncertain whether DALL-E 2, integrated into Microsoft Designer meets the computational criteria to be classified as a GPAI model with systemic risk,[448] some other provisions are relevant for the regulation of deepfakes and provide some form of protection, albeit with certain limitations.

Article 50 (2) and (4) of the Act designates transparency obligations on providers and deployers of GPAI systems to ensure the labelling of outputs constituting deep fakes in a 'machine-

---

[443] ibid, Edwards (n 189).
[444] ibid, art 55 (1).
[445] Carlini et al (n 91); Carlini et al (n 121).
[446] Artificial Intelligence Act (n 27), art 56(9).
[447] European Data Protection Supervisor (EDPS) EDPS Ethics Advisory Group, 'Towards a Digital Ethics' (EDPS, 25 January 2018) <https://www.edps.europa.eu/sites/default/files/publication/18-01-25_eag_report_en.pdf> accessed 3 August 2024; Alessandro Mantelero, Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI, 36 International Technology and Law Series (Asser Press, 2022) 186; Daniel Solove, 'The Limitations of Privacy Rights' (2023) 98 Notre Dame Law Review 975.
[448] Artificial Intelligence Act (n 27), art 51.

readable format'.[449] Moreno[450] likens this labelling to C2PA's Content Credentials Icon which provides full disclosure of the tools (including the AI system) deployed.

While the provision is limited in that it seems to focus on protecting recipients of deep fake content from being misled[451] as opposed to protecting victims of data misuse, it could serve as a tool for easy identification of the GAI system deployed/used for the exercise of data subjects' rights to access, objection, erasure, etcetera, to the extent practicable. This requirement could also serve as a tool for monitoring the integrity of privacy by design mechanisms put in place by GAI providers.

4.3.1.6 Remedies based on penalties for the infringement of provisions of the GDPR

The current landscape of penalties under the GDPR reveals significant inadequacies in effectively protecting individuals' privacy rights and addressing privacy risks associated with GAI models/systems. While penalties under the GDPR should serve both symbolic and deterrent functions,[452] they fall short due to inconsistent imposition, uneven fine computations and varying national practices,[453] enabled by Articles 82 and 83 of the GDPR. Additionally, compensation for individuals whose rights have been violated is often insufficient or entirely lacking.[454]

Although member states are empowered to provide rules on other penalties which are not administrative fines, the penalties under the GDPR also fail to adequately account for the severity of the harm, particularly in cases where violations may have the semblance of a criminal dimension. Hence, there is a growing need to consider frameworks beyond the GDPR, particularly in cases where grievous harm is occasioned.

---

[449] See Artificial Intelligence Act (n 188), art 50 (2) and (4), recitals 133 and 134.

[450] Felipe Romero Moreno, 'Generative AI and Deepfakes: a Human Rights Approach to Tackling Harmful Content' (2024) International Review of Law, Computers & Technology, 5 <https://www.tandfonline.com/doi/full/10.1080/3600869.2024.2324540#> 3 August 2024.

[451] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) Computer Law Review International 97, 108 <https://www-degruyter-com.libproxy.ncl.ac.uk/document/doi/10.9785/cri-2021-220402/html> accessed 4 August 2024.

[452] W Gregory Voss & Hugues Bouthinon-Dumas, 'EU General Data Protection Regulation Sanctions in Theory and Practice' (2021) 37 Santa Clara High Technology Law Journal 1, 41 & 42.

[453] See also the enabling provision, General Data Protection Regulation (n 15), art 83 & 84; Ibid (n 339) 41.

[454] Mona Naomi Lintvedt, 'Putting a Price on Data Protection Infringement' (2022) 12(1) International Data Privacy Law 1

5. Conclusion

The development and deployment of GAI models significantly impact the data privacy rights of individuals and expose the limitations of the GDPR and AIA in providing adequate safeguards to protect privacy rights and address infringements.

The development of GAI models is marked by structural infringements, failing to *stricto senso*, satisfy any of the grounds for processing personal and sensitive data. This infringement exacerbates the power imbalance between data controllers and data subjects, leading to the realisation of privacy risks including data breaches, misuse, the generation of inaccurate information and data memorisation, resulting in further violation and the perpetration of grievous harm at the deployment stage.

The systemic nature of GAI privacy infringements, particularly the memorisation capabilities of GAI models and their ability to learn data patterns, contrasts with the individual-focused enforcement of privacy rights under the GDPR. This mismatch limits the regulation's effectiveness in addressing the broad and complex nature of privacy violations associated with GAI. Although the AIA offers some structural protection, such as requiring adversarial testing to mitigate risks, it applies to only large GAI models with systematic risks.

Furthermore, GDPR remedies do not account for the potential for privacy violations to result in grievous harm such as the creation and dissemination of sexual deepfakes. While the AIA regulates deepfakes, its focus is on preventing deception rather than protecting privacy. These limitations underscore the need for specific legal frameworks beyond the GDPR and AIA to address the complex and evolving privacy risks posed by GAI models/systems.

As generative AI continues to advance and advance society, it becomes imperative to understand its implications on society and the fundamental rights of humans. Using a case study approach, this research work aimed at understanding the privacy risks associated with generative AI (GAI) and analysing the effectiveness of the EU regulatory framework, particularly, the GDPR and the recently enacted AI Act in safeguarding the privacy rights of individuals and in addressing privacy risks associated with GAI models. To provide a wholesome view, the case studies explored infringements at the development (pre-training and training) stage and the deployment stage of GAI models.

The findings of this research reveal significant risks to the data privacy of individuals including data breaches, data misuse, inaccuracy and data memorisation and the potential for these risks to give rise to grievous harms against individuals such as the generation of non-consensual deepfakes which could have negative impacts on the affected data subject. It found that in cases of such grievous harm, the GDPR is ill-equipped to address grievous harm occasioned by users and thus, the inability of the law to serve as a deterrence against such violations, particularly where such violations are perpetrated by natural persons.

Generally, it finds that the GDPR while comprehensive in its scope, struggles to fully address the unique privacy risks associated with GAI models. Issues such as the memorisation capabilities of AI systems, the blatant violation of provisions of the GDPR and the generation of false and harmful content highlight gaps in the GDPR's ability to regulate the development and deployment of these models. Furthermore, the individualistic approach to data subjects' rights such as the right to object, to restrict processing and to erasure coupled with the memorisation capabilities of GAI models impair the ability of the GDPR to address privacy infringements which are structural and systemic in nature. Consequently, systemic/structural infringement may call for structural regulatory frameworks to address these violations.

The AIA offers a little structural framework for the protection of data privacy by mandating providers of GAI models to perform model evaluations including adversarial testing. This provision would go a long way in mitigating the risk of data breaches. However, this provision is limited to providers of GAI models with systemic risks limiting the scope of its applicability. Also, while the AIA regulates deepfakes, its focus on preventing deception rather than safeguarding privacy shows the limited scope of privacy protection it offers.

These limitations therefore call for more strategic ways of dealing with the impairments of the GDPR and AIA. While stricter enforcement of the GDPR, particularly at the development stage is encouraged, there may be the need for specific legislation outside of the GDPR that criminalise certain acts which would serve as a form of deterrence to users at the deployment stage to the extent possible. The European Data Protection Board (EDPB) could also offer guidelines and practical examples for compliance with the GDPR during the development and deployment stage.

Emerging Technology, Terrorism and Freedom of Speech in the context of the European Union
Thu Nguyen

1. Context of the emerging debate

The emergence of social media as a form of communication is associated with the rising of disinformation which causes many "regulatory concerns".[455] In the age of digital evolution, there is a contentious topic of criminalisation of disinformation among many scholars and this matter is still under the shadow of confusion.[456] In the context of the European Union, criminalisation of disinformation may be a good choice to build the deterrent model for someone may potentially be the spreaders of false news with bad intentions, but it leads to concerns about human rights and it actually cannot solve the root of the recent issues, therefore, policymakers should look for another alternative approach. My contribution in the form of a qualitative research comprises consideration of the context of social media and disinformation, the relevance of disinformation, radicalisation, and terrorism, the present concerns on criminalisation of disinformation which provides my observation on both sides using the combination of systemic review on documents and doctrinal method to analyse legal ground of EU on this matter. However, this article in general agrees with the idea of not criminalising disinformation.

2. The Concept of Disinformation on Social Media

Some researchers conceptualise the terms of disinformation as the deliberate act of creating, disseminating, deconceptualizing, manipulating, or fabricating information to intentionally misstate the fact to mislead and cause public harm.[457] This phenomenon should be considered

---

[455] Benjamin Farrand, '"Is This a Hate Speech?" the Difficulty in Combating Radicalisation in Coded Communications on Social Media Platforms' (2023) 29 European Journal on Criminal Policy and Research 477.

[456] Alexander Peukert, 'The Regulation of Disinformation in the EU – Overview and Open Questions' (Social Science Research Network30 June 2023); András Koltay, 'Freedom of Expression and the Regulation of Disinformation in the European Union', *Disinformation, Misinformation, and Democracy* (Cambridge University Press 2025) and Marie Robin, 'European Policies in the Fight to Counter Propaganda' (*Robert-schuman.eu*2023) <https://www.robert-schuman.eu/en/european-issues/0665-european-policies-in-the-fight-to-counter-propaganda>.

[457] Michael Hameleers, 'Disinformation as a Context-Bound Phenomenon: Toward a Conceptual Clarification Integrating Actors, Intentions and Techniques of Creation and Dissemination' (2022) 33 Communication Theory; American Psychological Association, 'Misinformation and Disinformation' (American Psychological AssociationJuly 2022) <https://www.apa.org/topics/journalism-facts/misinformation-disinformation> accessed 22 April 2024; W Lance Bennett and Steven Livingston, 'The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions' (2018) 33 European Journal of Communication 122; Viorela Dan and others, 'Visual Mis- and Disinformation, Social Media, and Democracy' (2021) 98

a multi-layered phenomenon with extremely high complexity.[458] Currently, there are many definitions closely related to disinformation such as misinformation or fake news, however, disinformation can be distinguished due to the "intentional" nature hidden within the cause of the act of spreading false information. One of the resulting problems of disinformation is radicalisation and terrorism. The former is defined as a process in which an "individual adopts an extremist belief system, including the willingness to use, support, or facilitate violence as a method to effect societal change".[459] When it comes to terrorism, this article works with the idea of the threatened or actual use of illegal force and violence to attain benefits in politics, economy, religion, etc through fear, coercion, or intimidation.[460] Therefore, terrorist content relevant to disinformation is defined as content which built intentionally radicalised implications with the intent to incite a target audience segment to engage in, respond to, or propagate content related to terrorist activities.

The policy regulating above terminologies can be divided into two categories: the legislation which can generally regulate both users and platform providers, and terms of use, code of conducts, or "terms and conditions"[461] that set out by platforms, in other words, "self-regulation".[462] Most of social media platforms utilise algorithms and AI to implement content moderation to identify radicalised and terrorist content.[463] In terms of self-regulation, there exists the fact that each platform has its owns definition and standards to define what should be classified as terrorist content.[464] Therefore, the mutual standard among these platforms is non-existent. With the current development of the Internet and the popularity of social

---

Journalism & Mass Communication Quarterly 641; Jeffrey T Hancock and Jeremy N Bailenson, 'The Social Impact of Deepfakes' (2021) 24 Cyberpsychology, Behavior, and Social Networking 149; Archita Pathak, Rohini K Srihari and Nihit Natu, 'Disinformation: Analysis and Identification' (2021) 27 Computational and Mathematical Organization Theory 357; European Commisson (2018), Action Plan against Disinformation, p.1.

[458] Clara Iglesias Keller, 'Don't Shoot the Message: Regulating Disinformation beyond Content' in Carlos Blanco de Morais, Gilmar Ferreira Mendes and Thomas Vesting (eds), The Rule of Law in Cyberspace (Springer Cham).

[459] Kate Gunton, 'The Impact of the Internet and Social Media Platforms on Radicalisation to Terrorism and Violent Extremism' [2022] Privacy, Security And Forensics in The Internet of Things (IoT) 167.

[460] Katarzyna Jasko and others, 'A Comparison of Political Violence by Left-Wing, Right-Wing, and Islamist Extremists in the United States and the World' (2022) 119 Proceedings of the National Academy of Sciences.

[461] Council Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277, article 3(u).

[462] Chris Marsden, Trisha Meyer and Ian Brown, 'Platform Values and Democratic Elections: How Can the Law Regulate Digital Disinformation?' (2019) 36 Computer Law & Security Review 105373. As can be seen, many scholars share common thoughts on the existence of two main pillars in the field: platforms and state actors, see 3 for more details.

[463] See Alexander Tsesis , 'Social Media Accountability for Terrorist Propaganda' (2017) 86 Fordham Law Review 605; and Thiago Dias Oliva, 'Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression' (2020) 20 Human Rights Law Review.

[464] Thiago Dias Oliva, 'Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression' (2020) 20 Human Rights Law Review.

networks, the boundaries of content leading to radicalisation and terrorism are no longer limited to a single country but have extended beyond national borders.[465] Incitement now comes from even outside of a state.[466]

When it comes to the legal background on disinformation, there is an interesting fact that every country in the world has its own different pathway. While Russia criminalise the dissemination of blatantly disrespectful fake news stated as both disinformation and misinformation in Ric Neo's article[467], the United States criminalises the conduct of conveying false or misleading information,[468] this topic is still left for debate in the EU. Recently, the approach of the EU Commission merely relies on the mechanism of social media platform providers to tackle disinformation rather than state explicitly punitive messages for false information spreaders. According to Regulation (EU) 2021/784 on addressing terrorist content online, it states the platform responsibility with the removal order rather than criminal punishment to the spreaders.[469] Additionally, the approach of the Digital Services Act (DSA) revolves around assigning platform responsibility around a range of issues, including disinformation and terrorist content, rather than specifying the responsibility of those who spreading it. The main focus of this Act on dealing terrorist content mainly concentrates on removing contents, even the request for preservation and storage data exists to be the ground for investigation and prosecution of terrorist offences. In general, current regulations related to disinformation and terrorist content are mainly aimed at binding platforms as the main subjects and also play a crucial role in assisting in mitigating the risk of.

Under the circumstances of the "digital competitive"[470] situation that appears in a wide range of fields, from politics to economy, the essence of social media platforms is increasingly larger[471] and disinformation, radicalised and terrorist content are emerging in social media

---

[465] European Council , 'Addressing the Dissemination of Terrorist Content Online'
<https://www.consilium.europa.eu/en/infographics/terrorist-content-online/> accessed 25 April 2024.
[466] See Alexander Tsesis , 'Social Media Accountability for Terrorist Propaganda' (2017) 86 Fordham Law Review 605, p.607.
[467] Ric Neo, 'The International Discourses and Governance of Fake News' (2021) 12 Global Policy 214.
[468] See 18 U.S. Code § 1038 - False information and hoaxes.
[469] Council Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L 172, article 3 and Council Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277, para 10.
[470] Michael Bossetta, 'Scandalous Design: How Social Media Platforms' Responses to Scandal Impacts Campaigns and Elections' (2020) 6 Social Media + Society.
[471] As of January 2024, Northern and Western Europe were the regions with the highest social network penetration rates globally (See We Are Social, DataReportal, Meltwater. (2024). Global social network penetration rate as of January 2024, by region. Statista. Statista Inc
<https://www.statista.com/statistics/269615/social-network-penetration-by-region/> accessed 25 April 2024);

more and more frequently.[472] In the wake of elections, concerns about disinformation are becoming more and more heated and heavily affected to democracy.[473] Another fact shows that the role of almost social media platform is recently ineffective. For instance, Facebook ignores the subsistence of images that glorify violence and even joins hands to disseminate terrorist posts and YouTube hosts terrorist videos and rarely accepts the requirements to delete them.[474] There are more and more forms of content that, at first glance, appear to be nothing but contain a lot of false information as well as provocative expressions intended to agitate marginalised groups. In addition, although content moderation has been promoted by the EU legal system, especially provisions in the DSA as well as in the operating policies of platforms, it still faces problems. This situation brings policymakers the concerns about preventing cyberspace from terrorist and radicalised content. Although there still exists a debate on the relationship between the Internet, social media, and radicalisation that causes terrorism and to the extent how they affect each other,[475] the relevance of these key terms would be mentioned in the second part of this contribution.

The intentional dissemination of false content can be the culprit of radicalisation[476] and terrorism. Firstly, disinformation is considered a catalyst of radicalisation. Disinformation in general cause severe impacts on the audience's belief and attitude.[477] With the features of misleading content that cause emotional attacks, false news can easily affect the recipient's mind, thereby spreading false ideas. It lies in the nature of using psychological tricks to make audiences believe that interests of an easily excitable group are being ignored or intruded. The unlimitedness of social media, specifically in terms of geography has led to the push of false

---

furthermore, see Vidya Prahassacitta and Harkristuti Harkrisnowo, 'Criminal Disinformation in Relation to the Freedom of Expression in Indonesia: A Critical Study' (2021) 27 Comparative Law Review 135.

[472] Alexander Tsesis , 'Social Media Accountability for Terrorist Propaganda' (2017) 86 Fordham Law Review 605 and also see Amy Watson , 'Frequency of Encountering Disinformation in EU Member States as of May 2022' (2024) <https://www.statista.com/statistics/1076568/fake-news-frequency-europe/> accessed 25 April 2024.

[473] Ricardo Ribeiro Ferreira, 'Liquid Disinformation Tactics: Overcoming Social Media Countermeasures through Misleading Content' [2021] Journalism Practice 1.

[474] See Alexander Tsesis , 'Social Media Accountability for Terrorist Propaganda' (2017) 86 Fordham Law Review 605.

[475] See 3; Daniel Koehler, 'The Radical Online: Individual Radicalization Processes and the Role of the Internet' (2014) 0 Journal for Deradicalization 116; Lila Ghosh, 'FOREIGN FIGHTERS - an Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq' (Policycommons.net8 December 2015).

[476] Becca Lewis and Alice E Marwick, 'Media Manipulation and Disinformation Online' (Data & Society15 May 2017).

[477] Andreas Jungherr and Ralph Schroeder, 'Disinformation and the Structural Transformations of the Public Arena: Addressing the Actual Challenges to Democracy' (2021) 7 Social Media + Society and Gregory Asmolov, 'The Effects of Participatory Propaganda: From Socialization to Internalization of Conflicts' (2019) 6 Issue 6: Unreal; and Donato Vese, 'Governing Fake News: The Regulation of Social Media and the Right to Freedom of Expression in the Era of Emergency' (2021) 13 European Journal of Risk Regulation 1.

information and led to the wider appearance of extremist groups and terrorist forces from local to global.[478]

Secondly, based on social media as a means of invaluable communication, disinformation facilitates terrorism from the system of radicalised content mentioned above. Moreover, the spread of disinformation creates the basis for the recruitment of new terrorist actors, through observing and selecting the most radicalised individuals from a pool of targets. The application of disinformation can be referred to as a type of "propaganda material"[479] to recruit new potential terrorists. Through that, it indirectly promotes the connection of "lone wolves".[480]

Generally, disinformation, especially political disinformation when social media platforms can be considered as a political actor[481] leads to many severe impacts on society. This radicalisation causes false beliefs and ideological legitimisation that violence and discrimination against a certain group are justified to achieve political goals. In addition, it also affects the purity and uniformity of some specific target groups.[482] Spreading false information to incite terrorism causes enormously negative impacts on national security.[483]

3. The Debate on the Criminalisation of Disinformation

Due to the aforementioned drastic effect that disinformation can have on our world, the issue of criminalisation of disinformation based on the background of the relevance between disinformation, radicalisation, and terrorism has been left for debate. Like many other contentious debates in the academic world, this topic is mainly divided into two main schools of thought, those who are against criminalisation and those who support it.

---

[478] See 3.

[479] Homeland Security Institute, 'Recruitment and Radicalisation of School-Aged Youth by International Terrorist Groups ' (2009) <https://www.edu-links.org/sites/default/files/media/file/2009-recruitment-and-radicalization.pdf> accessed 25 April 2024.

[480] 'House Committee on Homeland Security Subcommittee Hearing: Terrorism in Africa: The Imminent Threat to the United States - House Committee on Homeland Security' (perma.cc29 April 2015) <https://perma.cc/PSE2-H7LS> accessed 25 April 2024.

[481] Michael Bossetta, 'Scandalous Design: How Social Media Platforms' Responses to Scandal Impacts Campaigns and Elections' (2020) 6 Social Media + Society.

[482] Elena Dal Santo and Elena D'Angelo, 'Relationship of Online Hate, Radicalization, And Terrorism' in Edward W. Dunbar (ed), Indoctrination to Hate: Recruitment Techniques of Hate Groups and How to Stop Them (Bloomberg Publishing USA 2022).

[483] See 10, 11.

3.1 Advantages of criminalisation of disinformation

It is undeniable that criminalising disinformation will also have certain benefits. First, pursuant to the basis of criminology theory in legal research, it creates deterrent models for terrorists who intend to take advantage of the spread of false information to incite potential targets. From the psychological effects of deterrence, the effect on the above behaviors may partly help prevent those behaviors, but the actual effectiveness is difficult to determine. In addition, this can contribute to raising public awareness as the criminalisation of disinformation also joins hand to creating a warning announcement for anyone participating in the process of spreading disinformation as well as other types of user-generated content.

Another benefit of classifying disinformation as criminal offence should be recognised is its assurance to national security, especially cyber security. Bossetta have emphasised the importance of providing specific punishment to deter terrorist organisations from exploiting the media and the gullibility of less exposed groups in society. In addition, they have also spoken out clearly about the most important issue, the protection and improvement of national security and cyber security.[484] This can help create healthy environments for the public to enjoy freedom of expression and ensure the quality of information they are exposing to.

3.2 Disadvantages of criminalisation of disinformation

Although criminalisation of disinformation can bring some benefits, it deems to be ineffective and cannot solve the problem from its roots. This article is in agreement with the viewpoint that criminalisation of disinformation should not be passed. Whilst criminalisation of disinformation may partially tackle the issue of threats from terrorist organisations, it brings about an unintended side effect, which is the infringement on freedom of speech. In terms of criminalisation, it can be applied to two potential subjects: the platform and the disseminator. If we consider criminalising terrorist content disseminator, there will be certain challenges in prosecuting these individuals, due to issues related to politics and the actual situation of terrorism and the consequences it can cause. On the side of the platform, criminalisation might be too severe and make the situation of current human rights violation become more serious. To give a clearer picture, States under the authoritarian regime witness case that authorities take advantage of law to suppress dissent. Authoritarian regimes frequently ban public

---

[484] See 16.

gatherings and demonstrations, labeling them as threats to national security or public order. The Great Firewall of China blocks access to foreign news websites and social media platforms, significantly curbing online free expression.[485]

Firstly, considering the current situation, disinformation, radicalised and terrorist content appear in a subtle manner. Disinformation comprises engaging in false flag operations, disseminating wrong quotations or stories to unsuspecting intermediates, or deliberately boosting biassed or misleading material.[486] This subtle manner means that disinformation is reflected in many different forms. Terrorist actors will skillfully integrate false information into these forms, for example, recently, hate speech has been so sophisticated that it appears under the form of hilarious images like memes.[487] Although sometimes terrorist incitement and propaganda are not so obvious, false information when exposed for a long time can cause deviations in the beliefs of a certain target group, and from there, the It will be easier for this organization to deceive gullible people. It is this sophistication that has become the seed that causes platforms to become lost and confused in the job of classifying content. Even the very large platform like Facebook is confused about the basis of indentification of terrorist content.[488] When such hatred, incitement and various systems of false information are integrated, the difficulties will become more and more apparent.

The complexity and difficulty of identifying terrorist content coupled with the EU's current legal landscape has exacerbated human rights violations stemming from the abuse of algorithms that leads to "overblocking"[489] in the content moderation process. As mentioned above, the utilisation of algorithms and AI is considered the most dominant solution recently. Many large and very large platforms[490] invest in the betterment of these technologies[491] and even United States recommend further development of them.[492] This mechanism relies on some technical strategies to remove the majority of similar content whenever social media platforms

---

[485] Edmarverson A. Santos, 'The Struggle for Human Rights in Authoritarian Regimes' (*Diplomacyandlaw.com*) <https://www.diplomacyandlaw.com/post/the-struggle-for-human-rights-in-authoritarian-regimes>.
[486] See 17.
[487] See 1.
[488] Monika Bickert and Brian Fishman, 'Hard Questions: How We Counter Terrorism - about Facebook' (About Facebook15 June 2017) <https://about.fb.com/news/2017/06/how-we-counter-terrorism/> accessed 27 April 2024. This news article was written by the Director of Global Policy Management and Counterterrorism Policy Manager.
[489] See 9.
[490] Based on how the DSA Framework classify social media platforms.
[491] See 8; Daphne Keller, 'Internet Platforms: Observations on Speech, Danger, and Money' (papers.ssrn.com13 June 2018); and Drew Harwell, 'AI Will Solve Facebook's Most Vexing Problems, Mark Zuckerberg Says. Just Don't Ask When or How.' Washington Post (14 April 2018).
[492] See 16.

flag any of them as suspicion of terrorist content. An example of this can be shown in recent data that, as reported by the platforms, Facebook stated that its automated systems detect 99% of the terrorism-related content it removes.[493] While this example may demonstrate the effectiveness of artificial intelligence and algorithms in the quantity of terrorist content that it detects and then removes, it also raises doubt about effectiveness on the accuracy of these procedures. Mass deletion of content, based on algorithmic censorship and review, has been found needless.[494] As discussed in a 2018 study, platforms that operate notice and takedown systems often remove user-generated content unnecessarily because they interpret unclear laws too cautiously or take accusations of bad faith to be true on their face.[495] One potential risk that content moderation in general can pose to human rights is that content will be incorrectly labeled. Back to the legal basis that stated in the previous part of this essay, it is essential to emphasise that violations of the rights to freedom of expression as well as freedom of information are threatened in the current context of the European Union and its regulations on content censorship. Curent regulations have placed burden on platforms to deter them from not removing terrorist content, but also caused mass deletion in an unnecessary and unclear manner.

Treating disinformation as a criminal offence may also contribute to the misuse of law and punishment. As mentioned earlier, the popularity of disinformation, especially political disinformation, is associated with the emergence of elections. By leveraging the notion of terrorist content and content suppression, the platform presents a somewhat bleak outlook on the future of freedom of expression if disinformation is classified as a criminal act. Within the realm of underground confrontations in the political sphere, the influence of the platform, both as a mediator and a political force, will profoundly affect the ability of marginalised and opposing groups to freely express themselves. Furthermore, political authorities also gain advantages by employing the pretext that political adversary's specific content is disinformation intended to promote acts of terrorism. Based on that ground, these content will be deleted needlessly, which resulting in a significant violation of the opposing side's freedom of speech in spite of the fact that these contents may not mean what they. Considering disinformation as a criminal offence can be a highly advantageous strategy for the government

[493] Mark Zuckerberg, 'A Blueprint for Content Governance and Enforcement' (Facebook)
<https://www.facebook.com/notes/751449002072082/?hc_location=ufi> accessed 27 April 2024.
[494] Daphne Keller, 'Internet Platforms: Observations on Speech, Danger, and Money' (papers.ssrn.com13 June 2018).
[495] See 36.

to engage in domestically political battles. Governing party can make use of it to prevent the invasion of any opposing ideology or any perspective coming from the practices of the vulnerable group, especially in the context of elections.[496] Consequently, this issue has progressively escalated, posing a threat not just to people' freedom of speech but also to other fundamental human rights and democratic principles. For examples, Facebook has experienced accusations for disproportionately censoring content from minority groups, and has also been criticised for engaging in political campaigning. Several studies have examined the impact of both Facebook and other social networking companies on political transformations inside a wide range of States. Bossetta also stated that social media platforms should be regarded as a component of politics by virtue of its enormously complicated impact.[497] There have been opinions on Facebook contribution to the severity of human rights abuses around the world, stemming from a perception that the platform has a bias towards the government and is quietly removing content that has been created by marginalised groups.[498]

Based on the above analysis, the primary concern currently lies in establishing a definitive explanation of disinformation within the legal frameworks of the European Union and its member states. Specifically, there is a need to determine which content should be qualified as disinformation and how information that promotes terrorism through radicalisation can be identified as disinformation. It is evident that the act of criminalising misleading information would not effectively resolve this issue. The development of all forms of mass media is closely linked to the potential risks of terrorist organisation discreetly appearing in cyberspace. Identifying a piece of misinformation using an algorithm can be easy. But on the contrary, identifying false information with bad purposes, specifically inciting sensitive and easily excitable groups to commit terrorism, is not easy. From that reality, anxiety and confusion come from the platforms and moreover, the policy differences between major platforms are still loopholes that terrorist organizations can take advantage of to spread radicalised information. For example, Facebook and YouTube have completely different forms of storing information, in text or in images. Although these platforms have shared data about terrorism-related content,[499] the problem of cybersecurity will always exist. If there is no common

---

[496] See 12.

[497] See 14.

[498] See 12; Silvio Waisbord, 'Truth Is What Happens to News' (2018) 19 Journalism Studies 1866 and 'Facebook's Language Gaps Allow Terrorist Content and Hate Speech to Thrive' (PBS NewsHour25 October 2021) <https://www.pbs.org/newshour/world/facebooks-language-gaps-allow-terrorist-content-and-hate-speech-to-thrive> accessed 28 April 2024.

[499] See 9.

perspective on the definition of terrorist content, there will always be "hope" for terrorist organizations. Not only does criminalising disinformation fail to address the root of the problem, it also aggravates concerns about freedom of expression.

Comparing the two approaches mentioned above, it can be seen that opting not to criminalise the aforementioned behaviour and utilising alternative approaches would be a more reasonable choice. Firstly, the application of criminalisation will not be an effective solution to the problem, as if the level of radicalisation of terrorist groups becomes larger or sometimes, criminal penalties are not really deterrent enough for terrorists or not enough to prevent radical groups. Therefore, this contribution recommends the EU to collaborate with the platform providers in order to figure out the alternative approach for the situation after carefully discussing the mutual definitions and developing mutual and specific policies among very large online platforms. This, in essence, would be a direct solution to the problems facing the EU's legal system. In addition, it will also be an effective path in the long run, as it can solve the problem of disinformation at any time.

4. Conclusion

To sum up, policymakers in this field should dig deeper into alternative approaches rather than criminalising disinformation in order to both protect human rights and tackle the problem of disinformation, radicalisation and terrorism. Balancing human rights, specifically the public's right to freedom of expression, with the need to prevent provocative terrorist content and ensure national security is indeed a complex challenge. It requires significant efforts from policymakers to harmonise the interests of all stakeholders, including the public, social media intermediaries, and political considerations that must be taken into account.

Mediation on a Global Spectrum: Balancing Autonomy, Mandatory Frameworks, and Evolving Judicial Roles

Viktoriia Hamaiunova

1. Introduction and Methodology

Across Europe, court systems face mounting caseloads, delays, and resource constraints, motivating an increased interest in alternative dispute resolution (ADR). Mediation, in particular, has emerged as a means of relieving court congestion while embodying a more cooperative ethos. European governments and policymakers often view it as an instrumental mechanism for addressing broader concerns with efficiency and public trust in the legal system. Yet imposing mediation on unwilling parties can raise questions about autonomy, fair process, and the evolving role of legal institutions in shaping dispute resolution.

This article examines the varied ways in which legal systems integrate mediation, from fully voluntary approaches to entirely mandatory regimes backed by sanctions. It places special emphasis on the tension between protecting autonomy—a core value underlying mediation— and the state's broader objective of reducing litigation burdens. By weaving together comparative insights and theoretical frameworks from legal philosophy and institutional analysis, the article demonstrates how mediation's expansion is neither linear nor purely technical but deeply enmeshed in debates about freedom, power, and social justice.

The article proceeds in five parts. Part 2 explores the spectrum of mediation practices across European jurisdictions, from voluntary to fully mandatory models, highlighting the paradoxes of autonomy and compulsion. Part 3 turns to the role of courts and institutional actors, analysing varying degrees of judicial involvement and the implications for mediator independence. Part 4 offers a critical legal perspective on the structural and cultural integration of mediation into formal legal systems, assessing both the promises and risks of institutional design. Part 5 evaluates the significance of public awareness, education, and gradual institutional change in shaping the long-term viability of mediation. Finally, Part 6 concludes by arguing that mediation's success rests on maintaining a delicate balance between participation and choice, efficiency and fairness.

1.1 Methodology

This article adopts an integrated comparative framework that draws on diverse but complementary perspectives. First, it conducts a comparative doctrinal analysis of statutes, regulations, and official guidelines from select European jurisdictions (including Germany, Italy, France, Denmark, and others). This examination is then enriched by Critical Legal Engineering (CLE), which, in the sense outlined by Joanna Kusiak,[500] identifies how mediation "re-engineers" or is "layered onto" existing legal processes and questions whether reforms may reproduce or dismantle entrenched inequalities. Alongside these doctrinal and critical lenses, institutional theory—particularly James Mahoney and Kathleen Thelen's incremental "layering" model[501] and Patricia Thornton's emphasis on shifting "institutional logics"[502]—helps situate mediation's expansion within wider normative and cultural shifts in the legal system. Finally, the article employs a reflective approach informed by the autonomy theories of Stefano Bertea[503] and Thomas Khurana,[504] examining how mandatory mediation frameworks both shape and are shaped by the tension between freedom and legal constraints. Through this multi-dimensional analysis, the article seeks not only to outline and compare regulatory models of mediation but also to probe whether compulsion and judicial oversight can coexist with genuine collaborative ethos.

2. The Spectrum of Mandatory Mediation: Autonomy and Its Paradoxes

2.1 From Voluntary to Mandatory: A Gradual Transition

A frequent distinction in both academic literature and legislation is the one between "mandatory" and "voluntary" mediation. In reality, however, the shift between these categories tends to function more like a continuum than a strict dichotomy.[505] Constantin Mihalescu

---

[500] Joanna Kusiak, 'Trespassing on the Law: Critical Legal Engineering as a Strategy for Action Research' (2021) 53(4) *Area* 603, 603–10.

[501] James Mahoney and Kathleen Thelen, *A Theory of Gradual Institutional Change* (Cambridge University Press) 15–17.

[502] Patricia H Thornton, *Institutional Logics and Institutional Change in Organizations* (Oxford University Press) 125–28.

[503] Stefano Bertea, 'Is the Autonomy of the Will a Paradoxical Idea?' (2023) 201(1) *Synthese* 133, 134–39.

[504] Thomas Khurana, *Paradoxes of Autonomy: On the Dialectics of Freedom and Normativity* (Goethe University 2013) 4–8.

[505] Constantin Mihalescu, 'Arguments Regarding the Introduction of Mandatory Mediation in Certain Categories of Disputes' (2022) *Revista Științifică Internațională „Supremația Dreptului"* 110, 110.

underscores how "degrees of obligation" complicate efforts to categorically label a given system.[506]

This aligns with Stefano Bertea's observation that autonomy consists not in the complete absence of constraints but in the capacity to act rationally within a framework of legal structures.[507]

Reflectively, this suggests that as mediation becomes more compulsory, the tension between party choice and policy-driven objectives becomes more pronounced. While governments often mandate mediation to manage high case volumes in overburdened courts, success depends on persuading participants that they still retain meaningful control over the negotiation process.[508] Thomas Khurana's emphasis on the co-constitutive nature of freedom and law similarly highlights that autonomy can thrive within norms—provided those norms do not entirely subsume individual agency.[509]

2.2 Voluntary Mediation

Fully voluntary mediation places the decision to mediate solely in the hands of the parties, requiring neither judicial encouragement nor legal obligation.[510] For instance, Germany's Mediation Act of 2012 endorses this approach in civil disputes, enabling participants to initiate mediation independently of the courts.[511] Denmark similarly adopts a voluntary framework, where mediation proceeds only if both sides agree.[512]

From a methodological standpoint—particularly when viewed through CLE—fully voluntary systems can reflect liberal ideals of self-determination. Yet as multiple empirical studies suggest, purely voluntary models may remain underutilised, leaving courts as the default forum

---

[506] ibid 110.
[507] Bertea (n 4) 133–35.
[508] ibid 135–36.
[509] Khurana (n 5) 4–5.
[510] Mikheil Bichia, 'Advantages of Mediation in Civil Disputes' (2023) 9(3) *Law and World* 5.
[511] C.H. van Rhee, *Mediation in German Civil Procedure* (Springer 2021) 166; European e-Justice Portal, 'Mediation in EU Countries – Germany' https://e-justice.europa.eu/64/EN/mediation_in_eu_countries?GERMANY&member=1 accessed 10 February 2025.
[512] Helle Isager, *Mediation in Denmark* (DJØF Publishing 2018) 94.

for most disputes.[513] Bertea's lens reveals a paradox: by maximising party freedom, the system risks low uptake, thereby limiting mediation's potential societal impact.[514]

2.3 Soft Mandatory Approaches

In judicial encouragement or "soft mandatory" models, courts recommend or nudge parties toward mediation without imposing an outright compulsion.[515] Belgium, for example, mandates that courts in family law cases inform parties about mediation,[516] while Finland strongly encourages it in family disputes.[517] From a reflective perspective, such soft nudges exemplify Khurana's point that autonomy can coexist with normative structures intended to guide party behaviour.[518]

Yet the question arises whether "recommendations" from a judge carry implicit pressure that compromises free will. Reflecting critically, one might argue that even gentle judicial suggestions disproportionately influence disputants who may fear alienating the court by refusing mediation. This scenario exemplifies the nuanced interplay of autonomy, subtle compulsion, and institutional authority.

2.4 Increased Compulsion: Mandatory Sessions and Condition Precedent

Legal systems with mandatory information sessions or mandatory initial mediation sessions occupy a middle ground on the spectrum.[519] In these contexts, parties must at least explore or attend mediation-related sessions before returning to (or commencing) litigation.[520] Lithuania requires attendance at information sessions prior to filing suit,[521] while Italy obliges an initial mediation session for civil disputes before parties can opt out.[522]

---

[513] Bichia (n 11) 51–53.

[514] Bertea (n 4) 134.

[515] Boularbah Hakim, *Droit du procès civil* (Presses Universitaires de Liège 2019) 15.

[516] Hakim (n 16) 15.

[517] K Ervasti, 'Past, Present and Future of Mediation in Nordic Countries' in *Nordic Mediation Research* (Springer 2018) 98; European e-Justice Portal, 'Mediation in EU Countries – Belgium' https://e-justice.europa.eu/64/EN/mediation_in_eu_countries?BELGIUM&member=1 accessed 10 February 2025.

[518] Khurana (n 5) 6.

[519] Stefano Bertea, 'Is the Autonomy of the Will a Paradoxical Idea?' (2023) 201(1) *Synthese* 134.

[520] A Tyulkanov and O Gevorkova, *Legislative Foundations for Mediation in the CIS* (Statut 2015) 149.

[521] European e-Justice Portal, 'Mediation in EU Countries – Lithuania' https://e-justice.europa.eu/64/EN/mediation_in_eu_countries?LITHUANIA&member=1 accessed 10 February 2025.

[522] Giuseppe De Palo, 'Mediating Mediation Itself: The Easy Opt-Out Model' (2021) *ADR Publishing* 564.

Critically, these approaches serve as a "gateway" to litigation, exposing disputants to the potential benefits of collaboration. From an institutional change perspective, such mandatory steps represent layering, where a new procedure is added onto existing structures. Yet the genuine impact on disputant behaviour is varied: if perceived merely as a formality, the sessions may not foster any real change in conflict resolution culture.[523]

Where condition precedent mediation is required—such that litigation cannot even begin without an attempt to mediate—the compulsion becomes more pronounced.[524] France's Code of Civil Procedure Article 127, for instance, demands good-faith mediation in certain matters before a lawsuit may be filed.[525] Here, the state harnesses litigation as leverage, further showcasing the paradox of autonomy under strong normative frameworks.

2.5 Fully Mandatory Mediation and Sanctions

At the far end of the continuum lies fully mandatory mediation, often backed by sanctions for non-compliance.[526] Croatia, for example, requires family law disputants to complete mediation before litigation,[527] while Ireland's Mediation Act 2017 imposes similar requirements in specific contexts.[528] Although these regimes can help reduce court congestion, one must reflect on whether coerced participation undermines the inherently collaborative nature of mediation.

Sanction-based models—such as those in Italy and Portugal—reinforce compliance by penalising parties that refuse to mediate, sometimes through fines or case dismissal.[529] Critical Legal Engineering suggests that while this ensures high participation rates, it can perpetuate power imbalances if one party views mediation as a strategic delay or if mandatory attendance masks genuine reluctance to negotiate.[530] As Bertea cautions, an overload of legal compulsion can overshadow the autonomy that is supposed to define mediation.[531]

---

[523] Khurana (n 5) 6–7.
[524] De Palo (n 23) 564.
[525] Antonello Miranda, 'The Origins of Mediation and ADR Tools' in *Mediation in Europe at the Cross-Road of Different Legal Cultures* (Springer 2014) 65.
[526] N Sandzhieva, *Models of Mediation in Developed Countries of the World* (Routledge 2020) 15.
[527] ibid.
[528] O'Grady and Browne, *Family Mediation: Law and Practice in Ireland* (Round Hall 2019) 45.
[529] Sandzhieva (n 27) 15; Joao Teixeira, 'Mediation and Consumer Law in Portugal' (2019) 82.
[530] Kusiak (n 1) 605–06; Panu Minkkinen, 'Critical Legal "Method" as Attitude' in Dawn Watkins and Mandy Burton (eds), *Research Methods in Law* (2nd edn, Routledge 2017) 150–51.
[531] Bertea (n 4) 137.

3. Mediation's Organisational and Control Frameworks: Court Involvement and Mediator Independence

3.1 Levels of Court Oversight

Parallel to the degree of mandatory participation are frameworks defined by how closely the courts themselves oversee or administer mediation.[532] Kant's concept of heteronomy—where external authority dictates rules—offers a theoretical lens for understanding how substantial court control might limit mediator autonomy or shape disputant expectations.[533]

Under court-provided mediation, judges or court staff act as mediators, fully integrating the process into judicial proceedings.[534] Parts of France and Germany employ this model, especially in civil or family disputes.[535] From a reflective standpoint, judicially provided mediation can benefit from institutional legitimacy but risks blending adversarial norms with a process meant to be collaborative, thus diluting the role of neutral facilitation.[536]

3.2 Judicial Referrals and Independent Services

Court-annexed mediation programmes mark a transition away from full judicial control. Mediators—though appointed or approved by the court—may be external professionals. Italy's preliminary mediation requirement in certain civil and commercial disputes typifies this hybrid approach,[537] as does Spain's integration of mediation in family and labour matters.[538] Although mediators operate under judicial endorsement, they retain some autonomy, consistent with the idea of "conditional autonomy" in Kantian and Bertean terms.[539]

Judicial appointment and referrals grant judges discretion to direct disputants to a mediator from an accredited list, as seen in England and Wales or in the Netherlands.[540] Here, the court

---

[532] See section 3.4.2 of the source material (internal references).
[533] Pauline Kleingeld and Marcus Willaschek, 'Autonomy Without Paradox: Kant, Self-Legislation, and the Moral Law' (2019) 19(6) *Philosophers' Imprint* 1, 6.
[534] *Code de procédure civile* (France) art 131–1.
[535] European e-Justice Portal, 'Mediation in EU Countries – Germany' (n 12).
[536] Kleingeld and Willaschek (n 34) 6–7.
[537] European e-Justice Portal, 'Mediation in EU Countries – Italy' https://e-justice.europa.eu/64/EN/mediation_in_eu_countries?ITALY&member=1 accessed 10 February 2025.
[538] Consejo General del Poder Judicial (Spain), 'Mediación' https://www.poderjudicial.es/cgpj/es/Temas/Mediacion accessed 10 February 2025.
[539] Kleingeld and Willaschek (n 34) 7.
[540] 'Civil Mediation' (UK Ministry of Justice) https://www.civilmediation.justice.gov.uk/ accessed 10 February 2025; https://www.rechtspraak.nl/English/Mediation accessed 10 February 2025.

maintains a facilitative role, yet the mediator is not a court employee. Reflectively, this approach underscores Khurana's insight that autonomy can coexist with normative oversight when the parties retain an opt-out option or the freedom to manage the mediation's content.[541]

3.3 Mandatory Mediation Bodies vs. Fully Independent Practice

Mandatory mediation bodies established by law reflect limited but significant court involvement. Parties must engage with these bodies before pursuing litigation, although the bodies themselves operate independently from the judiciary. Norway's Conciliation Boards and Denmark's specialised mediation agencies demonstrate how the state can delegate dispute resolution to quasi-independent institutions.[542]

In sharp contrast, fully independent mediation unfolds entirely outside the court system, as in Switzerland and Austria.[543] Mediators in these settings function with near-total autonomy, subject only to overarching legal standards that ensure professionalism.[544] Reflecting critically, one sees how this model embodies Kant's notion of "self-legislation,"[545] but can also raise access-to-justice concerns: a process free from court structures may be poorly understood or inaccessible to certain demographics lacking the resources to locate and pay for independent mediators.

4. Integration of Mediation into Legal Systems: A Critical Legal Perspective

4.1 Typology by Integration Level

A separate but related typology categorises how deeply mediation is integrated into formal legal proceedings.[546] Mandatory mediation requirements, such as pre-trial obligations, fundamentally reshape litigation, emphasising consensus-building over adversarial confrontation.[547] Italy's Legislative Decree No. 28/2010 offers a key example, covering real property, banking, and other civil disputes.[548] From a CLE viewpoint, these reforms are

---

[541] Khurana (n 5) 7–8.
[542] 'Forliksråd – Conciliation Boards' (Norway) https://www.sivilrett.no/forliksraadet.260661.no.html accessed 10 February 2025; https://www.kfst.dk/consumer/mediation-and-complaints/ accessed 10 February 2025.
[543] https://www.mediation-ch.org/en accessed 10 February 2025; https://www.mediatorenliste.justiz.gv.at/mediatoren/ accessed 10 February 2025.
[544] ibid.
[545] Kleingeld and Willaschek (n 34) 10.
[546] Minkkinen (n 31) 146–69.
[547] Kusiak (n 1) 603–10.
[548] Legislative Decree No 28 of 4 March 2010 (Italy).

"infrastructural innovations," re-engineering caseflow to prioritise alternative resolutions.[549] However, Minkkinen warns that if insufficient attention is paid to equity, such reforms risk perpetuating existing power asymmetries.[550]

4.2 Integration into Specific Court Processes

In some jurisdictions, mediation is embedded into certain procedural niches, such as small claims or family disputes, without imposing an absolute mandate across the board.[551] England and Wales exemplify this through the Small Claims Mediation Service,[552] while Finland integrates mediation into family courts.[553] These limited scopes of integration can facilitate incremental acceptance among litigants, though a critical view suggests that such partial reforms may not be transformative enough to alter adversarial legal cultures.[554]

4.3 Publicly Funded Mediation and Hybrid Med-Arb Models

Publicly funded or subsidised mediation aims to expand access beyond those with ample financial resources. Ireland's Family Mediation Service and Norway's mandatory family counselling reflect state-led efforts to ensure that cost does not impede ADR uptake.[555] Yet, from a reflective standpoint, one questions whether such programmes truly alter power dynamics or merely replicate them if staff are overworked or if parties lack understanding of their rights.[556]

Hybrid mediation-arbitration (Med-Arb) is another innovation, enabling a mediator to transition into an arbitrator role if initial efforts fail.[557] Institutions like the Swiss Chambers' Arbitration Institution and the Vienna International Arbitral Centre provide frameworks for

---

[549] ibid; Kusiak (n 1) 608–09.

[550] Minkkinen (n 31) 160–62.

[551] Family Procedure Rules 2010 (SI 2010/2955) (England and Wales), part 3.

[552] 'Small Claims Mediation Service' (HM Courts & Tribunals Service) https://www.gov.uk/guidance/small-claims-mediation-service accessed 10 February 2025.

[553] European e-Justice Portal, 'Mediation in EU Countries – Finland' https://e-justice.europa.eu/64/EN/mediation_in_eu_countries?FINLAND&member=1 accessed 10 February 2025.

[554] Minkkinen (n 31) 160–61.

[555] Legal Aid Board, 'Family Mediation' (Ireland) https://www.legalaidboard.ie/en/our-services/family-mediation/ accessed 10 February 2025; 'Family Counselling Service' (Norway) https://www.bufdir.no/en/Family_counselling/Family_mediation/ accessed 10 February 2025.

[556] Minkkinen (n 31) 161–62.

[557] Swiss Chambers' Arbitration Institution, 'Mediation' https://www.swissarbitration.org/mediation accessed 10 February 2025.

such hybrid proceedings.[558] This duality can expedite final decisions but raises ethical and practical concerns, such as the potential erosion of neutrality once the mediator wields binding adjudicative power.[559] In Minkkinen's critical perspective, such reforms can inadvertently blur boundaries between consensus-driven and adjudicative processes, necessitating vigilant oversight to prevent coercion.[560]

5. Informational and Educational Support: Transformation or Token Gesture?

5.1 Gradual Institutional Change and Institutional Logics

Mediation's emergence within formal legal orders often occurs through layering, whereby a new procedure overlays existing litigation without displacing it.[561] Mahoney and Thelen note that these incremental modifications can accumulate into substantial institutional transformation.[562] Thornton's concept of institutional logics adds another layer, explaining how cultural shifts—like a growing preference for collaboration—redefine what constitutes legitimate dispute resolution.[563]

Methodologically, this reflects a dual emphasis: a structural analysis of how legal systems adopt mediation (layering) and a cultural-normative assessment of changing attitudes (institutional logics). A reflective lens suggests that while layering can foster gradual reform, it may also result in patchwork implementation if courts, lawyers, or the public remain sceptical of non-adversarial norms.

5.2 Court-Linked Education and Public Awareness

Public awareness campaigns, mandatory information sessions, and mediator training represent key avenues for entrenching mediation in mainstream dispute resolution.[564] In England and Wales, for instance, parties in certain family cases must attend a Mediation Information and

---

[558] German Arbitration Institute, 'DIS Mediation Rules 2010' https://www.disarb.org/en/51/rules/dis-mediation-rules-01-july-2010-id7 accessed 10 February 2025; Vienna International Arbitral Centre https://www.viac.eu/en/mediation accessed 10 February 2025.

[559] Minkkinen (n 31) 162.

[560] ibid.

[561] Mahoney and Thelen (n 2) 12–18.

[562] ibid.

[563] Thornton (n 3) 125–28.

[564] Pablo Cortés, 'Embedding Alternative Dispute Resolution in the Civil Justice System: A Taxonomy for ADR Referrals and a Digital Pathway to Increase the Uptake of ADR' (2018) 37(2) *Legal Studies* 286, 314–15.

Assessment Meeting (MIAM).[565] Germany and Austria similarly ensure litigants learn about mediation before proceeding with specific civil claims.[566]

These initiatives can be viewed as conscious attempts to shift the "logic" of dispute resolution toward a collaborative ethos.

Critically, however, mere provision of information does not guarantee transformative change. Many parties continue to choose litigation for strategic or familiar reasons.[567] CLE thus prompts further questioning of whether education and training can dismantle entrenched hierarchies or whether they serve as a surface-level fix that fails to alter deeper power relations.

Collaborations with law schools and educational bodies likewise aim to reorient future legal professionals.[568] As mediation training becomes standardised, new lawyers may internalise more cooperative values, influencing courtroom dynamics over time. This shift resonates with Khurana's and Bertea's insights on autonomy within structured frameworks—when upcoming generations of practitioners see value in mediation, normative constraints can become opportunities for consensual resolution rather than mere obligations.

6. Conclusion

Mediation has emerged as a leading strategy in Europe to confront the twin challenges of overloaded courts and waning faith in purely adversarial justice. Yet its incorporation into formal legal systems reveals a complex spectrum: from purely voluntary models that champion autonomy but risk low uptake, to highly mandated schemes that can erode the consensual ethos at mediation's core.

Reflectively, drawing on the works of Bertea, Khurana, Minkkinen, and others, one sees that autonomy is neither an absolute nor a mere absence of constraints. Instead, it is shaped and potentially bolstered by carefully designed normative frameworks. Mandatory features can indeed foster broad participation and reduce litigation backlog, but if they devolve into box-

---

[565] Family Procedure Rules 2010 (SI 2010/2955) (England and Wales).
[566] European e-Justice Portal, 'Mediation in EU Countries – Germany' (n 12); 'Mediation in EU Countries – Austria' https://e-justice.europa.eu/64/EN/mediation_in_eu_countries?AUSTRIA&member=1 accessed 10 February 2025.
[567] Minkkinen (n 31) 161–62.
[568] Philippe Charrier, 'La médiation judiciaire en France. Innovation institutionnelle et pratiques professionnelles des magistrats' (2019) *Revue des sciences sociales* 83; European e-Justice Portal, 'Mediation in EU Countries – Spain/Czech Republic' https://e-justice.europa.eu accessed 10 February 2025.

ticking exercises or heavily penalise non-participation, they risk deepening resentment and power imbalances.

From an institutional perspective, the layering of new mediation requirements onto traditional litigation—combined with public education and professional training—can gradually reorient legal cultures toward cooperative dispute resolution. However, the success of these incremental reforms depends on maintaining genuine opportunities for party self-determination and ensuring that mediation procedures do not become "cheap justice" lacking safeguards for vulnerable participants.

Ultimately, embedding mediation within existing legal architectures calls for a delicate balance: harnessing the efficiencies of compulsory frameworks while fostering true collaboration. Doing so demands ongoing dialogue among legislators, courts, mediators, and the public. Only by sustaining such reflective engagement can mediation evolve into a robust, equitable mechanism that fulfils its promise of aligning efficiency with fairness—meeting the modern demands of justice without sacrificing the very autonomy that defines its fundamental ethos.

Should the law in England and Wales be reformed to better protect cohabiting couples' property rights when their relationship breaks down?

Leah Charlton

1. Introduction

Picture this: after years of building a life together, caring for each other, and nurturing a family, you suddenly find yourself facing the heart-wrenching reality of a relationship breakdown. Despite the emotional investment, financial contributions to everyday living costs, and contributions to childcare and/or homemaking, individuals may discover that they lack legal recognition and protection. Consequently, they can be left without property shares in a home built together. Such a scenario represents a possible reality for cohabitants under the current property law in England and Wales (E&W). The lack of automatic legal rights can leave many vulnerable to significant injustices if no voluntary legal agreements are in place. This differs significantly from spouses/partners who have mechanisms such as legal recognition and court discretion to assist in fair property division upon divorce/dissolution proceedings.

It is disheartening that despite efforts advocating for policy reform to increase cohabitation rights, the outcomes have fallen short. For example, in 2020, the Cohabitation Rights Bill[569] attempted to add a statutory framework for cohabitants' property rights when their relationship breaks down for reasons other than death. Again, in 2022, the Government rejected the Women and Equalities Committee's recommendations to reconsider policy reform. Instead, the Government has continuously prioritised marriage and divorce law.[570] However, recent statistics show a rise of almost 18% in cohabiting couples between 2011 and 2021.[571] Now, cohabiting couples account for roughly 1 in 5 families in the UK, showcasing the importance of attaining policymakers' attention. These statistics show the changing dynamics of modern

---

[569] HL Bill (2019-2020) 97.

[570] Abigail Pearse, 'Will the Wheel turn for cohabitants in England and Wales anytime soon?' (2021) 6 Private Client Business 254, 257; Women and Equalities Committee, *The Rights of Cohabiting Partners: Government Response to the Committee's Second Report* (HC 776 2022-23) iii.

[571] Kate Whiting, 'Cohabitation in England & Wales and Scotland: The Case for Granting Equal Rights to Marital and Non-marital cohabitants' (2020) 4(1) Edinburgh Student Law Review 52, 53; Office for National Statistics, 'People's Living Arrangements in England and Wales: Census 2021' (*Office for National Statistics*, February 2023) <https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/articles/livingarrangementsofpeopleinenglandandwales/census2021> accessed 4th April 2024.

relationships, highlighting the necessity of reforming legal frameworks to increase protection for cohabiting couples.[572]

There have been notable changes to the law regarding cohabiting couples, specifically regarding parental responsibility (PR). Spouses/partners automatically receive PR when their child is born.[573] However, for cohabitants, only the mother is automatically granted PR. The father is not. Instead, the father can acquire PR by registering on the birth certificate,[574] entering into a parental responsibility agreement with the mother, [575] or obtaining a parental responsibility order from the court.[576] Before reforms, unmarried fathers could only establish PR through the latter two options. Similarly, if same-sex couples have a child through fertility treatment and are spouses/partners, both will have automatic PR.[577] However, if they are cohabitants, the gestational parent automatically has PR, and the second parent can acquire PR akin to unmarried fathers.[578] Many argue that these groups are still not treated equally in law,[579] and I agree that there is still room for improvement. However, I focus on cohabitants' property rights. I use PR to highlight an area of law that indicates a step towards better recognition for cohabiting couples. However, despite these advancements, the legal framework in E&W has failed to adequately adapt to address injustices within property law.

Burns[580] is a clear example of injustice. Although it is an old case and not a legal precedent, similar injustices could still occur today without declarations of beneficial interests or formal cohabitation agreements. The couple lived together for 19 years as cohabitants, with only one partner being the legal property owner. The non-legal owner contributed by paying bills, childcare and domestic duties, and redecorating the property. Unfortunately, after the

---

[572] Office for National Statistics, 'Families and households in the UK: 2022' (*Office for National Statistics,* May 2023) <https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/families/bulletins/familiesandhouseholds/2022> accessed 4th April 2024.

[573] Children Act 1989, s.2(1).

[574] ibid, s.4(1)(a).

[575] ibid, s.4(1)(b).

[576] ibid, s.4(1)(c).

[577] ibid, s.2(1).

[578] ibid, s.2A.

[579] Sally Sheldon, 'Unmarried Fathers and Parental Responsibility: A Case for Reform?' (2001) 9(2) Feminist Legal Studies 93, 104-5; Stephen Gilmore, 'Parental responsibility and the unmarried father – a new dimension to the debate' (2003) 15(1) Child and Family Law Quarterly 21, 22; Andrew Bainham, 'What is the point of birth registration' (2008) 20(4) Child and Family Law Quarterly 449, 472; Emma Hitchings and Leanne Smith, 'Re G (Children) (Residence: Same-sex Partner [2006] UKHL 43, [2006] 1 WLR 2305' (2007) 29(3-4) Journal of Social Welfare and Family Law 307, 315; Richard Collier, *Men, Law and Gender: Essays on the 'man' of the law* (Routledge 2010) 220-221.

[580] *Burns* v *Burns* [1984] Ch 317 (CA Civ Div).

relationship broke down, the non-legal owner was not awarded any beneficial shares in the property. This highlights the unfair consequences of the current property law, which fails to recognise the value of non-financial contributions to a relationship, typically undertaken by women.[581] While a more holistic approach is desirable, recent cases show similar unjust outcomes where the courts have not fully appreciated the value of non-financial contributions.[582] This highlights a gender dimension of duties women typically carry out,[583] which is an integral part of the problem I aim to address. Otherwise, failure to reform cohabitation property laws could perpetuate these existing gender inequalities when the relationship breaks down.[584]

In Part 1, I explore societal paradigms that shape the perceptions of family ideology. I acknowledge that, although marriage may be a prevalent family formation, the rise in cohabitating couples should not go unnoticed. I confront the enduring Common Law Marriage (CLM) myth that exacerbates the misconception that cohabiting couples gain the same legal rights and protections as spouses/partners. By delving into statistics and studies, I reveal the widespread misconception surrounding CLM, highlighting the need for policy interventions to safeguard vulnerable individuals and ensure social justice.

In Part 2, I aim to dispel CLM misconceptions by highlighting the legal disparities between spouses/partners and cohabitants. By outlining the divorce/dissolution proceedings, I demonstrate the formal legal process for separating spouses/partners in contrast to the less formal process for cohabitants. Then, I focus on property law, specifically the Common Intention Constructive Trust (CICT), to expose the uncertainty and unfairness when determining cohabitants' property interests. I examine insufficient statements to express a common intention to share the property and circumstances where the courts have been reluctant to infer a common intention. This includes when non-legal owners give up their jobs and contribute towards property improvements.

---

[581] Anne Bottomley, 'From Mrs Burns to Mrs Oxley: Do Cohabiting Women (Still) Need Marriage Law?' (2006) 14 Feminist Legal Studies 181, 182; Simone Wong, 'Cohabitation Reform in England and Wales: Equality or Equity' (2015) 27 Canadian Journal of Women and the Law 112, 114.

[582] *James* v *Thomas* [2007] EWCA Civ 1212, [2007] 11 WLUK 610; *Thomson* v *Humphrey* [2009] EWHC 3576 (Ch), [2010] Family Law 351.

[583] Helen Reece, 'The Autonomy Myth: A Theory of Dependency' (2008) 20(1) Child and Family Law Quarterly 109, 111-112.

[584] Marilyn Friedman, 'Autonomy, Social Disruption, and Women' in Catriona Mackenzie and Natalie Stoljar (eds), *Relational Autonomy* (Oxford University Press 2000) 24.

In Part 3, I address the urgency of extending cohabitation property rights in an ever-evolving societal landscape. I engage with alternative perspectives on law reform to encompass concepts of undermining marriage, individual autonomy and legal complexities. I suggest an opt-out scheme could help bridge the gap between neglecting vulnerable individuals by automatically opting them into the scheme, with the choice to opt-out to preserve individual autonomy. I also explore establishing a legal definition for cohabitation without running analogies with marriage. I acknowledge that extending cohabitation rights is not a simple framework, but I maintain that reform is essential to rectify the current injustices in property law.

In Part 4, I look further afield to analyse Scotland and New Zealand, two countries that provide greater protection for cohabiting couples' property interests when their relationship breaks down. I draw insight into how these jurisdictions legally define cohabitants and commend utilising non-exhaustive factors that reflect modern relationships instead of marriage analogies. These factors recognise the value of non-financial contributions, elements which E&W formally lack, possibly perpetuating gender injustices.[585] I recommend introducing a minimum duration period, similar to New Zealand, to encourage equitable, fair and consistent case outcomes. I also consider implementing an extended timeframe to bring claims, addressing current issues in Scotland, and attempting not to inadvertently overwhelm the E&W justice system. Although I explore these jurisdictions, I recognise that E&W operate under a distinct legal system and social realities. Therefore, policymakers must adapt future reforms to the context accordingly.

By exploring avenues for law reform, I envision a future where all individuals have equitable legal protection for their property rights, regardless of marital status, in the event of a relationship breakdown.

2. Cohabitation

This part delves into the socio-legal context of cohabitation, examining the interplay of evolving societal norms and family ideologies. I navigate the complexities of defining cohabitants, explicitly focusing on couples in relationships who share a residence. Furthermore, I explore various reasons for relationship breakdown but focus on reasons other than the death

---

[585] Bottomley (n 13)182; Wong (n 13)114.

of a partner. Then, I examine the implications of the CLM myth, which erroneously suggests that cohabitants enjoy legal protection akin to spouses/partners. By elucidating the persuasiveness of this myth within society, I highlight its potential to distort individuals' perceptions of their legal rights. This distortion can lead to injustices and unfair outcomes, emphasising the importance of clarifying and reforming legal realities surrounding cohabiting couples' property rights.

2.1 Family Ideology

Marriage remains the most common family formation in E&W.[586] However, a noticeable increase has occurred in couples choosing to cohabit without marriage.[587] Nevertheless, the law prioritises and promotes certain family formations over cohabitation.[588] For example, it prioritises marriage/partnerships, particularly since the introduction of the Civil Partnership Act 2004 and the Marriage (Same-Sex Couples) Act 2013. Though a step in the right direction to recognise more family realities, not legally recognising a cohabitant's status implies that spouses/partners are the superior family ideology.[589] Despite cohabitation reforms being in discussions over the years, marriage laws have consistently taken precedence on the policy agendas.[590] For example, in 2022, the Women and Equalities Committee recommended that the Government reform many aspects of family law to better protect cohabitants from financial hardship in case of a relationship breakdown.[591] This call for reform echoes a similar attempt by the Law Commission in 2007.[592] However, despite these repeated recommendations, the proposals were declined both times. This recurring pushback highlights a significant gap in the Government's policies to ensure equitable legal protection for cohabiting couples who may be left vulnerable in the event of a relationship breakdown.[593]

---

[586] People's Living Arrangements in England and Wales: Census 2021 (n 3)

[587] Carol Smart, 'Stories of Family Life: Cohabitation, Marriage and Social Change' (2000) 17(1) Canadian Journal of Family Law 20, 31; Jonathan Herring, Rebecca Probert and Stephen Gilmore, *Great Debates in Family Law Statistics* (2nd edn, Palgrave 2015) 176.

[588] Michael Freeman, *Understanding Family Law* (Sweet & Maxwell 2007) 46; Alison Diduck and Felicity Kaganas, *Family Law, Gender and The State* (3rd edn, Hart Publishing 2012) 31.

[589] Anne Barlow and Grace James, 'Regulating Marriage and Cohabitation in the 21st Century' (2004) 67(2) The Modern Law Review 143, 145; Freeman (n 20).

[590] Smart (n 19); *The Rights of Cohabiting Partner* (n 2) iii.

[591] *The Rights of Cohabiting Partners* (n 2) iv.

[592] Law Commission, *Cohabitation: The Financial Consequences of Relationship Breakdown* (Law Com No.307, 2007).

[593] Bottomley (n 13)182.

Societal norms historically favour nuclear families, with mum, dad, and two children as the ideal family formation.[594] These suggest that this structure is crucial for societal welfare, implying that cohabiting couples living together are less stable than spouses/partners.[595] Nevertheless, despite the absence of a statutory definition of a family, social shifts highlight the importance of functions performed within the family unit, such as protection from emotional, physical and economic hardship and supportive welfare.[596] Spouses/partners typically carry out these functions.[597] However, despite the rise in people choosing to cohabit and the lack of legal recognition, studies show that many cohabitants also take on functions similar to those of spouses/partners.[598] By recognising similar functions between spouses/partners and cohabiting couples, policymakers can better understand the needs and dynamics of diverse family structures in accordance with social reality.[599]

2.2 Defining Cohabitants and Relationship Breakdown

In this section, I aim to elucidate the different groups that can be categorised as cohabitants, although not explicitly defined by statute. This clarification will help delineate the groups which I focus on. Then, I consider the phrase 'breakdown of a relationship' to delimit the scope of the legal area of interest.

It is fascinating that the number of cohabiting couples in the UK has steadily increased in recent years.[600] However, the term cohabitant can be quite ambiguous, referring to various living arrangements.[601] For example, it can refer to groups of students living together during their time at university, a couple contemplating marriage, or a couple living together without legal

---

[594] John Eekelaar, *Family Law and Society* (Fletcher & Son Ltd 1978) 4; David Archard, 'The Future of the Family' (2000) 6 Ethics and Social Welfare 132, 137; Freeman (n 20)53.
[595] Freeman (n 20)53.
[596] Eekelaar (n 26)7-8; Simone Wong, 'Cohabitation and the Law Commissions Project' (2006) 14 Feminist Legal Studies 145, 153.
[597] Eekelaar (n 26) 7-8; Barlow and James (n 21).
[598] Martha Minow, 'All in the Family & in All Families: Membership, Loving, and Owing' (1992) 95(2) 5 West Virginia Law Review 275, 285; Anne Barlow, Simon Duncan, Grace James and Alison Park, 'Just a Piece of Paper? Marriage and Cohabitation' in Alison Park, John Curtice, Katarina Thompson, Lindsey Jarvis and Catherine Bromley (eds), *British Social Attitudes: The 18th Report: Public Policy, Social Ties* (SAGE Publications 2001) 20; Barlow and James (n 21) 153; Anne Barlow, 'Cohabitation Law Reform – Messages from Research' (2006) 14 Feminist Legal studies 167, 172; Brienna Perelli-Harris, Stefanie Hoherz, Trude Lappegard and Ann Evans, 'Mind the "happiness' gap: the relationship between cohabitation, marriage, and subjective well-being in Australia, the UK, Germany and Norway' (2018) 56(4) Demography 1219, 1221.
[599] Penny Booth and Cathy Kennedy, 'The Traditional Family and The Law' (2005) 35 Family Law 482, 485; Freeman (n 20) 53; Pearse (n 2) 255.
[600] People's Living Arrangements in England and Wales: Census 2021 (n 3)
[601] Rebecca Probert, *The Changing Legal Regulation of Cohabitation: From Fornicators to Family Law* (Cambridge University Press 2012) 4; Pearse (n 2) 255.

intervention, such as marriage/partnership. Hereafter, cohabitants refer to unmarried couples who live together in a romantic relationship.

As I explore in the next part, the legal process of ending a marriage/partnership differs from ending a cohabiting relationship. These relationships may break down due to similar causes, including changes in personal needs, infidelity, or unreasonable behaviour.[602] However, since the enactment of the Divorce, Dissolution and Separation Act 2020, couples seeking divorce no longer need to provide a reason for their separation. Therefore, data on relationship breakdowns may only reflect separations under previous legal frameworks where a reason for separation was necessary. [603] I will focus on the breakdown of cohabiting couples' relationships, excluding scenarios involving the death of one partner. Consequently, I will not consider bereavement and succession laws. Nevertheless, further research into these areas is pivotal for a comprehensive evaluation to ensure cohabiting couples' property rights are safeguarded in all relationship ending situations.

2.3 Common Law Marriage Myth

Before I delve into the legal frameworks in the next part, it is essential to recognise that cohabitants do not enjoy the same legal property protections as spouses/partners, regardless of the duration of their relationship.[604] Despite this, there has been considerable uncertainty around automatic property rights stemming from the CLM.[605] Exploring this myth is crucial to help understand the legal protection individuals believe they have as cohabitants, emphasising the importance of education and reform.

Despite an increasing social acceptance of cohabiting couples, a significant concern persists regarding CLM.[606] The myth wrongly implies that couples who cohabit for a particular

---

[602] Alan Hawkins, Brian Willoughby and William Doherty, 'Reasons for Divorce and Openness to Marital Reconciliation' (2012) 53(6) Journal of Divorce and Remarriage 453, 454.
[603] Office for National Statistics, 'Divorces in England and Wales: 2022' (*Office for National Statistics,* February 2024) <https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/divorce/bulletins/divorcesi nenglandandwales/2022#marriages-ending-in-divorce> accessed 4th April 2024.
[604] Harriet Meyer, 'Cohabiting Couples: your rights on money, property, tax and more' *The Guardian* (London, 13th November 2023).
[605] Claire Chisnall, 'Under My Roof: Cohabitation and Couples' Rights' (2022) 165 Solicitors Journal 16.
[606] Anne Barlow, Carole Burgoyne, Elizabeth Clery and Janet Smithson, 'Cohabitation and the Law: Myths, Money and the Media' in Alison Park, John Curtice, Katarina Thomson, Miranda Phillips, Mark Johnson and Elizabeth Clery (eds), *British Social Attitudes: The 24th Report* (24th edn, SAGE Publication Ltd 2008) 29; Whiting (n 3)53.

duration attain a legal status akin to marriage/partnership, conferring legal protection in a relationship breakdown.[607] Although people often approach myths with scepticism, CLM remains prevalent among society's beliefs.[608] In 2019, 46% of people in E&W incorrectly believed cohabiting couples were in a CLM with a legal status similar to spouses/partners.[609] Chisnall aptly acknowledges this issue by emphasising the lack of legal status, and instead, the CLM proposes a definition of cohabiting couples' living arrangements.[610] Still, believing the myth can have significant repercussions for couples. Cohabitants may not seek legal advice about property allocation by assuming automatic legal protection akin to spouses/partners. This may leave parties with a significant financial disadvantage if their relationship ends.[611] This highlights a vital policy concern: protecting vulnerable cohabitants' property rights to uphold social justice.[612] Therefore, the Government should not continuously overlook this issue, implying that cohabitants are inferior in society.[613]

Barlow launched the Living Together Campaign to examine individual perceptions of legally aware cohabitants.[614] Specifically, it sought to assess how participants' perceptions of their legal rights were affected after engagement with educational resources. Despite the findings dating back to 2007, cohabitation legal rights remain relevant today despite changes to other areas of family law. The participants did not believe in the CLM myth. Additionally, they had some prior knowledge of their position either through independent research or by accessing the informative website created by the campaign. The study revealed that despite participants' legal awareness, less than 10% sought legal advice before the breakdown of their relationship.[615]

---

[607] Catherine Fairbairn, 'Common Law Marriage' and Cohabitation (House of Commons Library, Briefing Paper No 03372, 2022) 5.

[608] Whiting (n 3)53.

[609] John Curtice, Elizabeth Clery, Jane Perry, Miranda Phillips and Nilufer Rahim, 'British Social Attitudes 36' (British Social Attitudes 36th Report, 2019) <https://bsa.natcen.ac.uk/media/39363/bsa_36.pdf> accessed 17th November 2023, 12; Graham Fraser, Cohabitation reform in England and Wales – Comparative perspectives; and how to reset the reform campaign?' [2023] Family Law Review 341, 342-3.

[610] Chisnall (n 37).

[611] John Curtice, Elizabeth Clery, Jane Perry, Miranda Phillips and Nilufer Rahim, 'British Social Attitudes 36' (British Social Attitudes 36th Report, 2019) <https://bsa.natcen.ac.uk/media/39363/bsa_36.pdf> Accessed 17th November 2023, 12; Women and Equalities Committee, *The Rights of Cohabiting Partners* (HC 92 2022-23) [17].

[612] Jane Scoular, *Family Dynamics: Contemporary Issues in Family Law* (Butterworths 2001) 141; Jens Scherpe, 'Written evidence submitted by Professor Jens Scherpe' (HAB0385, 2022) <https://committees.parliament.uk/writtenevidence/43563/pdf/?> accessed 19th March 2024.

[613] Women and Equalities Committee (n 2) iv.

[614] Anne Barlow, Carole Burgoyne and Janet Smithson, 'The Living Together Campaign – An investigation of its impact on legally aware cohabitants' (Ministry of Justice Research Series 5/07 July 2007) <https://ore.exeter.ac.uk/repository/bitstream/handle/10036/15235/living-together-research-report.pdf?sequence=1&isAllowed=y> accessed 20th November 2023, 5.

[615] ibid.

The findings indicate optimism bias, believing that relationships would not follow the same trajectory as others, leading to a reluctance to seek legal advice.[616] Furthermore, some experienced practical barriers, including high legal fees associated with establishing agreements and property interest allocation.[617] In addition, some also highlighted their partners' unwillingness to make legal arrangements.[618]

Despite being aware of their legal status, cohabitants hesitate to pursue additional protection. These elements often derive from practical barriers, mainly where an individual experiences unequal power dynamics in their relationship.[619] Studies suggest that women are more likely to perform household and childcare duties or be restricted to part-time work.[620] In these contexts, solely allocating funds to attain legal advice may not be possible, particularly since the cuts made to legal aid.[621] Moreover, the observed gender disparities significantly hinder cohabitants who aspire to safeguard their property rights through legal means. Although cohabitants may be aware of their legal status limitations, they can still find themselves in a precarious situation when their relationship ends, resulting in inequitable and unjust outcomes.[622]

To summarise, considering the socio-legal perceptions surrounding cohabitation, I advocate that the existing laws in E&W require reform to better protect cohabiting couples' property rights in the event of a relationship breakdown. In the following part, I explore the legal provisions pertaining to spouses/partners seeking a divorce/dissolution, highlighting the disparities between the relatively uncomplicated nature of divorce law and the intricacies of cohabitation case law.

3. Legal Framework For Spouses/Partners and Cohabitants

---

[616] ibid, 11.

[617] ibid, 5.

[618] ibid, 21.

[619] Sharon Thompson, 'Written Evidence from Dr Sharon Thompson, Cardiff University' (HAB0342, 2021) <https://committees.parliament.uk/writtenevidence/37669/pdf//> accessed 19th March 2024 [15].

[620] Freeman (n 20)51; Marsha Garrison, *Family Life, Family Law, and Family Justice: Tying the Knot* (Routledge 2022) 38; Fairbairn (n 39) 32.

[621] Legal Aid, Sentencing and Punishment of Offenders Act 2012; Alison Diduck, 'Dividing the Family Assets' in Shelley Sclater and Christine Piper, *Undercurrents of Divorce* (Dartmouth Publishing Company Ltd 1999) 224.

[622] Freeman (n 20)51; Samantha Singer, 'What provision for unmarried couples should the law make when their relationships break down?' [2009] Family Law 234, 234-5.

In the previous part, I explored the prevalent social misconception that cohabiting couples have similar legal rights and privileges as spouses/partners when their relationship ends. In this part, I examine the legal framework for the divorce/dissolution process before focusing on the CICT. I aim to elucidate the disparities in legal proceedings and highlight how the case law for cohabitating couples can leave those who contribute non-financially in a vulnerable and unfair position regarding their property rights.[623]

3.1 Legal Framework Divorce/Dissolution Proceedings

Recently, the legislation governing divorces underwent reform to introduce a 'no fault' divorce. Instead of requiring proof of a 'fact' and allocating blame,[624] both parties can now pursue a divorce on the premise that their marriage has irretrievably broken down.[625] Similarly, civil partners can apply for a dissolution.[626] Both routes adhere to comparable legal protocols despite using different terminology, including dissolution and divorce.

As a prerequisite, parties must have been spouses/partners for at least one year.[627] These applications, whether individual or joint with their former partner, can now be completed conveniently online due to technological advances. However, both parties should still seek legal advice.[628] Nevertheless, it is essential to note that obtaining legal advice may also be subject to similar constraints due to legal aid cuts. Before filing for divorce/dissolution, parties should try to agree on dividing their assets, including property. However, Diduck recognises that encouraging parties to reach agreements independently can sometimes lead to neglecting the perception of fairness regarding the income provider.[629] This can make the wife feel accomplished even when receiving something minimal from her husband. A filing can proceed without these agreements but may prolong the proceedings. The court will make a conditional order 20 weeks after the initial application,[630] confirming the parties' intention to continue.[631] The timeframe aims to address initial worries about divorce reform, believing that the process

[623] Bottomley (n 13)182.
[624] cf *Owens* v *Owens* [2018] UKSC 41, [2018] AC 899; Herring, Probert and Gilmore (n 19) 200.
[625] Divorce, Dissolution and Separation Act 2020, s.1(1).
[626] ibid, s.3(1)-(3).
[627] Matrimonial and Family Proceedings Act 1984, s.1(1).
[628] Amelia Hill, 'Women Losing out as Couples Try to Divorce on the Cheap' *The Guardian* (London, 3rd November 2023).
[629] Alison Diduck, 'Dividing the Family Assets' in Shelley Sclater and Christine Piper, *Undercurrents of Divorce* (Dartmouth Publishing Company Ltd 1999) 215.
[630] Divorce, Dissolution and Separation Act 2020, s.4(a).
[631] ibid, s.5.

may result in quicker and easier divorces instead of working on reconciliation.[632] Following the conditional order, the parties have 6 weeks and 1 day to request the final order, which will legally terminate the marriage/partnership.[633]

3.1.1 Property Division

As I mentioned, separating spouses/partners are encouraged to strive towards a mutual agreement upon property division. However, this can be challenging, especially when dealing with the family home - a significant shared asset.[634] In some cases, separating spouses/partners choose to establish a fair division of their property and formalise the agreement in court through a legally binding consent order.[635] Alternatively, some separating spouses/partners may seek the assistance of a mediator to reach a mutually agreeable solution.[636] Although mediators cannot offer legal advice, they facilitate productive conversations, encouraging the parties to take practical steps towards a fair resolution.[637] During mediation, if the parties reach an agreement, the mediator will draft a memorandum of understanding. After review, a solicitor can convert the document into a consent order. This is crucial as it enables the parties to seek legal recourse if their former partner fails to comply with the terms of the agreement.[638]

The inability to reach a consensus on property matters during separation can have significant and long-lasting effects on everyone involved.[639] Not only can it result in costly and drawn-out legal proceedings, but it could also result in lasting emotional damage.[640] Therefore, it is imperative for separating spouses/partners to prioritise reaching a mutually agreeable and fair resolution, regardless of the perceived value of assets.[641] By doing so, they can mitigate the potential negative consequences of separation and build a foundation for a more stable and

---

[632] Jonathan Herring, Rebecca Probert and Stephen Gilmore, *Great Debates in Family Law* (2nd edn, Palgrave 2015) 197-8.
[633] Divorce, Dissolution and Separation Act 2020, s.4(b).
[634] Polly Morgan, 'Property Division on Divorce' in Ruth Lamont (ed), *Family Law* (2nd edn, Oxford University Press 2022) 136.
[635] Matrimonial Causes Act 1973, s.33A; *Vince* v *Wyatt* [2015] UKSC 15, [2015] 1 WLR 1228; Emily Dugan, 'Divorces delayed by cost of living crisis, research finds' *The Guardian* (London, 1st January 2024).
[636] Diduck (n 53) 216-7.
[637] ibid.
[638] *Vince* v *Wyatt* [2015] UKSC 15, [2015] 1 WLR 1228; Dugan (n 67).
[639] ibid.
[640] Jornt Mandemakers, Christiaan Monden and Matthijs Kalmijn, 'Are the Effects of Divorce on Psychological Distress Modified by Family Background?' (2010) 15 Advances in Life Course Research 27.
[641] Brian Sloan, 'A Hippy-Hippy Clean Break?' (2015) 74 The Cambridge Law Journal 218.

fulfilling future. This process ensures that both parties are fully informed and actively engaged in decision-making.[642]

Consulting a mediator is essential before resorting to court proceedings. However, if the parties cannot reach an agreement, the court can issue a financial order to divide the assets of the separating couple. The court considers various factors, such as the length of the marriage/partnership, the value of the property, and the contributions of each party, including financial support and childcare responsibilities.[643] This aims to achieve a fair outcome that addresses the needs of both parties and any children involved. [644] Due to the unique circumstances of each case, there is no one-size-fits-all approach, allowing for court discretion.[645] Despite the legal framework, predicting the outcome of a divorce/dissolution case can still be challenging.

When determining financial orders, courts consider multiple factors beyond mere legal ownership.[646] While the resulting property shares may not be equal, the non-legal owning spouse/partner is still entitled to a share as part of the marital assets.[647] *White*[648] was pivotal in establishing equality as the court's fundamental position in property division, aided by statutory discretion.[649] In the initial judgment, the judge made an error by unfairly favouring the husband in asset allocation.[650] This highlights the importance of discretionary powers,[651] questioning the patriarchal idea that the husband, as the primary breadwinner, should be entitled to a bigger portion in divorce settlements.[652] Moreover, it emphasises the courts' responsibility to evaluate all factors in a case without gender bias.[653] Additionally, it accentuates the significant role of childcare responsibilities, household duties or lesser financial contributions due to part-time employment. [654] *White*[655] emphasises that when spouses/partners contribute equally to the

---

[642] ibid.
[643] Matrimonial Causes Act 1973, s.25(2).
[644] ibid, s.25(1); *White* v *White* [2001] 1 AC 596 (HL) 605.
[645] *Hammond* v *Mitchell* [1991] 1 WLR 1127 (Fam Div) 1129.
[646] Matrimonial Causes Act 1973, s.25(2).
[647] *White* v *White* [2001] 1 AC 596 (HL); *Charman* v *Charman* (No. 4) [2007] EWCA Civ 503, [2007] 4 WLUK 616.
[648] *White* v *White* [2001] 1 AC 596 (HL).
[649] ibid, 597.
[650] ibid.
[651] Matrimonial Causes Act 1973, s.25(2).
[652] Diduck (n 53) 213-4.
[653] *White* v *White* [2001] 1 AC 596 (HL) 605; Sclater and Piper (n 53) 19.
[654] *White* v *White* [2001] 1 AC 596 (HL) 603.
[655] ibid.

family, financial contributions should not be preferred over non-financial ones.[656] This signals a shift towards acknowledging the value of non-financial contributions,[657] enabling courts to accommodate diverse family dynamics during divorce/dissolution proceedings. [658] Furthermore, *McFarlane*[659] exemplifies the equitable and just approach towards economically disadvantaged individuals who forego their careers to raise children[660] despite not being restricted to property-related matters.

3.1.2 Matrimonial Home Rights

Spouses/partners who co-own property are subject to legal ownership rights rather than relying on matrimonial home rights. If one spouse/partner moves into a property solely owned by the other, they do not have legal ownership rights to the property by default. However, marriage and civil partnerships offer advantages, such as automatic home rights.[661] Therefore, neither spouse/partner can be compelled to vacate the marital home during separation until a final order ending the marriage/partnership is obtained.[662] This may differ in circumstances involving domestic violence.[663] Home rights provide temporary protection until a final financial order is issued, preventing the legal owner from selling the marital home without the other spouse/partner's consent.[664] However, non-legal cohabitants do not have automatic home rights, making establishing property rights more difficult. For cohabitants, the focus is on property ownership rather than equitable distribution, despite *White's*[665] emphasis on impartiality in divorce proceedings.[666]

3.2 Legal Framework for Cohabitants

To explore property ownership rights, I outline the procedure for cohabitants who have legally expressed their property intentions in the event of a relationship ending for reasons other than death. Additionally, I delve into the property law that applies to cohabitants who do not hold joint legal ownership and explore the possibility of a CICT arising through their actions. I focus

---

[656] ibid, 605.
[657] ibid, 605-6; Wong (n 28) 145-6.
[658] *Porter* v *Porter* [1969] 1 WLR 1155 (CA Civ Div) 1159.
[659] *McFarlane* v *McFarlane* [2006] UKHL 24, [2006] 2 AC 618.
[660] ibid, 626.
[661] Family Law Act 1996, s.30.
[662] ibid, s.30(2)(a), s.30(8)(a); Divorce, Dissolution and Separation Act 2020, s.4(b).
[663] Family Law Act 1996, s.33(7).
[664] ibid, s.30(2).
[665] *White* v *White* [2001] 1 AC 596 (HL) 605.
[666] Martin Parry, *The Law Relating to Cohabitation* (3rd edn, Sweet & Maxwell 1993) 11.

on this group because they are particularly vulnerable in the event of a relationship breakdown and warrant attention.

3.2.1 Legal Ownership of Property

In contemporary society, determining the legal owner of a property is typically straightforward, as most land ownership is available on the HM Land Registry. When a couple purchases a property together, and both names are registered, they become joint legal owners of the property on the registry.[667] However, if only one person's name is on the legal register, they are the sole legal owner of the property.[668] This can occur if one party buys the property before the relationship begins. Accordingly, the sole legal owner is also the sole beneficial owner.[669] However, if parties can provide evidence of an equitable interest through an express or implied trust, they may challenge this presumption in court.

3.2.2 Express Trust

A formal, written declaration of trust is required to establish an express trust.[670] This means that transferring property necessitates a legal document, such as a deed, and an oral statement will not suffice. Implementing this aspect of property law is relatively straightforward. If a cohabiting relationship were to end with an express agreement in place, the law would simply use the express arrangements that the couple signed and agreed. The challenges and intricacies emerge when couples have not made an express agreement, which seems to be common among cohabiting couples.[671] Consequently, the party not listed on the legal title must demonstrate a beneficial interest in the property through a CICT to acquire property rights.

---

[667] *Stack* v *Dowden* [2007] UKHL 17, [2007] 2 AC 432; *Jones* v *Kernott* [2011] UKSC 53, [2010] 1 AC 776.
[668] *Lloyds Bank Plc* v *Rosset* [1991] 1 AC 107 (HL).
[669] *Stack* v *Dowden* [2007] UKHL 17, [2007] 2 AC 432, 453.
[670] Law of Property Act 1925, s.53(1)(b).
[671] Charlotte Coyle and Fiona Wilson, 'The law needs to support cohabiting couples' *Financial Times* (London 5th December 2022).

3.2.3 Common Intention Constructive Trust

Unlike the potential ease of an express trust, the current legal framework for cohabiting couples without an express trust reveals gaps and issues. When there is no express agreement, the assumption is that the sole legal owner is also the sole beneficial owner.[672] The burden then falls on the party claiming a financial interest to establish their interest through a CICT.[673] The Trusts of Land and Appointment of Trustees Act[674] allows courts to impose a CICT to determine property ownership and beneficial shares. However, the guidance is limited, and the process can be complex, resulting in unjust outcomes.

The starting point for establishing a CICT trust is *Stack* v *Dowden*.[675] In this case, a couple who jointly owned property sought to rebut the presumption that equity follows the law. Although a joint legal owner case, these principles also apply to sole legal owner cases, which is my focus. To determine if a CICT exists, two key questions must be established: (1) is there a CICT between the parties? and (2) if so, what are the beneficial shares owed to each party?[676] In the following section, I break down the second part of the test to examine how the courts identify a common intention and explore financial disadvantages that certain groups may experience following a relationship breakdown.

3.2.4 Does a CICT Exist?

In order to determine the existence of a CICT, two criteria must be met: (a) there must be a common intention to share the property, and (b) the party making a claim must have relied on that common intention to their detriment.[677] If both elements are present, the presumption that sole legal ownership implies sole beneficial ownership will be rebutted, resulting in recognition of the non-legal owner's beneficial interest.

(1a) Establishing a Common Intention
Express

---

[672] *Stack* v *Dowden* [2007] UKHL 17, [2007] 2 AC 432.
[673] ibid.
[674] 1996, s.14(1).
[675] *Stack* v *Dowden* [2007] UKHL 17, [2007] 2 AC 432.
[676] ibid, 432-3.
[677] ibid.

One way to establish a common intention to share property is through express agreements. When establishing a CICT, oral statements may suffice, differing from an express trust. However, this still depends on the statement's content, requiring an agreement to share property ownership instead of an agreement to share residence. For example, in *Hammond*,[678] 'half is yours' and in *Clough*,[679] the words '50/50' were both deemed sufficient express agreements to demonstrate a common intention to share property ownership. Conversely, statements such as 'family home' in *Rosset*[680] and a promise that 'you will be looked after' in *Thomson*[681] were inadequate in evidencing a common intention ownership. However, without express agreements, the courts may infer a common intention to share property ownership.

Inferred

If there is no explicit agreement, the court may infer a common intention based on the conduct of the non-legal owner. This could include contributing financially to the mortgage or purchase price of the property. In *Stack*,[682] Lady Hale recommended a holistic approach to inferring common intention and a list of non-exhaustive factors to consider, such as non-financial contributions like household duties and childcare.[683] Recognising these contributions reflects a shift from relying solely on financial contributions to determining common intention.[684]

Although Lady Hale appears to widen the scope for non-financial factors, the comments were made in obiter and, therefore, do not constitute a binding precedent. As a result, subsequent cases have generally adopted a more restrictive approach. For instance, in *James*,[685] a cohabiting partner made significant property improvements and even quit her job to work for her partner's business, which did not constitute a common intention. This highlights the uncertainty surrounding the extent to which substantial improvements can establish a common intention.[686] Similarly, in *Thomson*,[687] the court was hesitant to infer a common intention between cohabiting partners where the woman had given up her job and left her home to move

---

[678] *Hammond* v *Mitchell* [1991] 1 WLR 1127 (Fam Div) 1131.
[679] *Clough* v *Killey* [1996] 3 WLUK 61 (CA Civ Div) 61-62.
[680] *Lloyds Bank Plc* v *Rosset* [1991] 1 AC 107 (HL) 109.
[681] *Thomson* v *Humphrey* [2009] EWHC 3576 (Ch), [2010] Family Law 351.
[682] *Stack* v *Dowden* [2007] UKHL 17, [2007] 2 AC 432.
[683] ibid, 456.
[684] ibid, 432-3.
[685] *James* v *Thomas* [2007] EWCA Civ 1212, [2007] 11 WLUK 610.
[686] *Stack* v *Dowden* [2007] UKHL 17, [2007] 2 AC 432.
[687] *Thomson* v *Humphrey* [2009] EWHC 3576 (Ch), [2010] Family Law 351.

in with her partner. The court held that her conduct was insufficient as it did not entail detrimental reliance, the second element of the criteria to determine the existence of a CICT.

(1b) Detrimental Reliance

To establish a CICT, even if a common intention could be inferred, the non-legal owner must also show that she or he detrimentally relied on their conduct to gain an interest in the property.[688] For instance, in *Eves*,[689] the court found that the woman's manual labour on the property was sufficient to establish detrimental reliance since such manual work was not expected of a woman.[690] Conversely, in *Rosset*,[691] supervising building work did not meet the threshold for detrimental reliance, as it was considered a typical role for a wife. [692] Unfortunately, property law lacks clarity for individuals seeking to establish a CICT and avoid costly legal proceedings, but it also perpetuates gender stereotypes.[693] Therefore, reforming the law to better protect cohabiting couples not only ensures fairness and clarity but also mitigates and reinforces existing gender inequalities.[694]

(2) Beneficial Shares

After establishing a CICT between the parties, the courts will look to share the financial proportions. However, quantifying interests can prove challenging since the parties likely did not express their desired financial shares. Nevertheless, the court must infer a percentage of each party's beneficial shares. While Lady Hale suggests that factors beyond financial contributions should be considered, it can be difficult for the court to quantify non-financial factors.[695] Therefore, cohabitants who are non-legal owners and need to establish a CICT may be left financially disadvantaged if their relationship breaks down due to the current law's lack of clarity and complexity, as seen in *Rosset*[696] and *Thomson*.[697]

In summary, I explored the divorce/dissolution process for spouses/partners in this part. I shed light on the significant disparities between these proceedings and the legal framework

---

[688] *Grant* v *Edwards* [1986] Ch 638 (CA Civ Div).
[689] *Eves* v *Eves* [1975] 1 WLR 1338 (CA Civ Div).
[690] ibid, 1345.
[691] *Lloyds Bank Plc* v *Rosset* [1991] 1 AC 107 (HL).
[692] ibid, 109.
[693] Friedman (n 16).
[694] ibid.
[695] *Stack* v *Dowden* [2007] UKHL 17, [2007] 2 AC 432, 436.
[696] *Lloyds Bank Plc* v *Rosset* [1991] 1 AC 107 (HL).
[697] *Thomson* v *Humphrey* [2009] EWHC 3576 (Ch), [2010] Family Law 351.

governing cohabitation property rights when their relationship breaks down. Contrary to prevalent social misconceptions, cohabiting couples do not enjoy the same legal rights and privileges as spouses/partners. Instead, they adhere to a complex and sometimes unfair process, particularly for those who are not the main financial contributors. I suggest that implementing greater regulation for cohabiting couples in E&W would be desirable.[698] However, I recognise it is not a simple solution given the challenges surrounding individual autonomy, undermining marriage and legal complexities. I engage with these challenges further in the subsequent part.

4. Exploring Discussions on Extending Property Rights

In the previous part, I argued that the current laws regarding property rights for cohabiting couples who separate leave many vulnerable to injustices. In this part, I explore the evolving landscape of family relationship structures by examining existing empirical research suggesting a rise in cohabitation and a decline in marriage rates. I propose that laws in E&W should reflect these societal shifts. Next, I engage with alternative perspectives that challenge extending property rights to cohabiting couples, including concerns that it could undermine the institution of marriage, infringe on individual autonomy, and create legal complexities. Finally, I synthesise the research and recommend a legislative reform that values essential principles such as care and commitment. The proposed legal framework recognises the value of non-financial contributions and seeks to address past injustices where individuals received inadequate property interests through CICT. While implementing reforms to extend property rights may be challenging, I maintain that greater protection is necessary.

4.1 Evolving Family Relationships

In the UK, approximately 1 in 5 families (19%) are cohabiting couples[699] due to societal changes that sociologists call the 'second demographic transition'.[700] The increase in the divorce rate and the rising prevalence of cohabitation may contribute to this shift.[701] While I do not address the reason for the decline in marriages,[702] increasing cohabitation may reflect a

---

[698] Scoular (n 44) 141.
[699] Families and households in the UK: 2022 (n 4)
[700] Garrison (n 52) 37.
[701] ibid.
[702] Living Arrangements in England and Wales: Census 2021 (n 3).

movement toward Scandinavian cultural norms.[703] In contemporary times, marriage is seen as a conscious decision made by individuals rather than something they are obligated to do due to societal, religious, or financial pressures.[704] Consequently, it is vital to reform the law to safeguard the property rights of cohabiting couples as they become a more popular family structure.[705]

4.1.1 Exploring Society Through Existing Empirical Research

According to the British Social Attitudes Survey (2000), more than 80% of individuals under the age of 35 considered cohabitation an acceptable family formation, with one-third of respondents living together as cohabitants.[706] These findings mark a noticeable deviation from traditional family norms.[707] While the survey insights were significant, I acknowledge that the study is from 2000, and cultural and legislative changes may have impacted more recent attitudes towards cohabitation. Nonetheless, the scale of the study has served as a foundation for subsequent research, albeit on a smaller scale.

Moving forward to 2021, Resolution, a group of family justice professionals, undertook a smaller-scale investigation into contemporary perspectives on family formation. Their results were similar to those of previous studies, with 83% of respondents expressing support for cohabitation and its future growth.[708] Resolution compromises professionals who deal with the complexities of family dynamics, working directly with individuals and families during difficult situations.[709] Therefore, their research provides a unique perspective based on first-hand experiences and interactions, which enhances their understanding of contemporary family relationships. This reaffirmation of attitudes demonstrates the ongoing acceptance of cohabitation and emphasises the resilience and adaptability of evolving relationship norms.[710]

---

[703] Simon Duncan, Anne Barlow and Grace James, 'Why Don't They Marry? Cohabitation, Commitment and DIY Marriage' [2005] Child and Family Law Quarterly 383, 384; The Centre for Social Justice (n 135); Garrison (n 52) 40.

[704] Duncan et al (n 135) 396; Steven Berenson, 'Should Cohabitation Matter in Family Law?' (2011) 13 Journal of Law and Family Studies 289, 315.

[705] Graeme Fraser, 'Cohabitation Policy: Where Are We Now?' [2021] Family Law Journal 1407, 1408.

[706] Barlow et al (n 30) 4; Duncan et al (n 135) 383-4.

[707] ibid.

[708] Resolution, 'Resolution Calls for More Rights for Unmarried Couples' (*Resolution*, 2023) <https://resolution.org.uk/news/resolution-calls-for-more-rights-for-unmarried-couples/> accessed 16th March 2024.

[709] Resolution, 'Vision for Family Justice' (Resolution, 2023) <https://resolution.org.uk/wp-content/uploads/2023/11/Resolution-Vision-for-Family-Justice-full-221123.pdf> accessed 22nd March 2024.

[710] Anne Barlow, Simon Duncan, Grace James and Alison Park, 'Just a Piece of Paper? Marriage and Cohabitation' in Alison Park, John Curtice, Katarina Thompson, Lindsey Jarvis and Catherine Bromley (eds),

Furthermore, by challenging controversial narratives, such as the idea that marriage is the superior family formation, Resolution's research recognises the diverse attitudes and values present in society rather than adhering to rigid paradigms.[711]

The evolving landscape of relationship formations in E&W reveals a shift in generational attitudes towards cohabitation, particularly among younger generations, who are increasingly embracing more liberal views.[712] However, this trend is not limited to younger age groups, as older demographics also recognise the value of cohabiting family units despite historical social norms favouring marriage.[713] This growing acceptance indicates broader societal changes and highlights the need for reform in legal and social frameworks governing modern family dynamics.[714] The prevailing sentiment is that the law should not 'turn its back on social facts.'[715] As relationships evolve, legal policies, particularly regarding property law for cohabiting couples, must adapt accordingly.

As discussed earlier, the legal landscape surrounding the property rights of cohabiting couples is intricate and uncertain, often leading to perceived injustices, as illustrated in *Burns*.[716] Despite the increasing prevalence of cohabitation, policymakers and scholars remain wary of its potential impact on traditional marriage values.[717] This concern is evident in the prioritisation of divorce law reforms over the rights of cohabiting partners.[718] Such actions may implicitly favour conventional marital norms over advocating for fairness for cohabiting couples, possibly driven by fears of destabilising societal structures.[719] As a result, there is a palpable apprehension about the potential consequences for the stability of marriage and cohabitation in society. Addressing these challenges requires not just legal reforms or policy adjustments but also acknowledging broader cultural shifts and economic realities.

British Social Attitudes: The 18th Report: Public Policy, Social Ties (SAGE Publications 2001) 5; Duncan et al (n 135).

[711] Baroness Brenda Hale, 'Unmarried Couples in Family Law' [2004] Family Law Journal 419, 420-1; Anne Barlow, Simon Duncan, Grace James and Alison Park, *Cohabitation, Marriage and the Law: Social Change and Legal Reform in the 21st Century* (Hart Publishing 2005) 23-5.

[712] ibid.

[713] Duncan et al (n 135) 383-4.

[714] Barlow et al (n 143) 19.

[715] Rebecca Bailey-Harris, 'Law and the Unmarried Couples – Oppression or Liberation?' [1996] Child and Family Law Quarterly 137, 137-8.

[716] *Burns* v *Burns* [1984] Ch 317 (CA Civ Div).

[717] Jane Lewis, 'Marriage and Cohabitation and the Nature of Commitment' [1999] Child and Family Law Quarterly 355.

[718] *Rights of Cohabiting Partners* (n 2)5.

[719] Lewis (n 149)

4.2 Engaging with Alternative Perspectives

4.2.1 Undermining Marriage

The issue of extending property rights to cohabiting couples is often linked to concerns about undermining the institution of marriage.[720] This viewpoint is commonly associated with conservative, political, and religious beliefs prioritising traditional values such as commitment and stability.[721] For example, Marriage Resource, a Christian charitable organisation, acknowledges that the legal system can lead to unfair outcomes but believes that introducing reforms would weaken the institution of marriage.[722] Similarly, the Coalition for Marriage advocates for marriage as the 'gold standard' of society, elevating it superior to other family dynamics.[723] However, these positions reveal a bias against recognising diverse family arrangements. These arguments may overlook important broader issues and lack nuance because they fail to acknowledge the changing nature of societal relationships. While it is valuable to consider alternative perspectives, it is crucial to critically examine these arguments and acknowledge the various social factors that shape family dynamics.

While spouses/partners demonstrate a high level of commitment due to their legal rights and responsibilities, cohabitation has become increasingly common and can display similar levels of functionality and commitment.[724] However, the Coalition for Marriage argues that acknowledging these trends could diminish the public perception of marriage, weakening 'the bedrock of family life.'[725] Knight also draws on contentious perspectives, suggesting that recognising new family formations would transform family units entirely.[726] Nonetheless, research indicates that instability in non-marital relationships can influence various societal issues, including burdening the Government with rising crime rates, poor public health and economic instability.[727] However, this perspective fails to consider significant shifts in gender

---

[720]Whiting (n 3)55; Women and Equalities Committee (n 43)17.

[721] Barlow (n 30).

[722] Law Commission (n 24) [2.38].

[723] Coalition for Marriage, 'Written Evidence from Coalition for Marriage' (HAB0289, 2021) <https://committees.parliament.uk/writtenevidence/37604/html/> accessed 19th March 2024.

[724] Barlow andJames (n 21) ; Wong (n 13)120.

[725] Coalition for Marriage (n 155).

[726] Robert Knight 'How Domestic Partnerships and Gay Marriage Threaten the Family' in Robert Baird and S.P Rosenbaum (eds) *Same-sex Marriage: The Moral and Legal Debate* (Prometheus Books 2004) 110.

[727] Coalition for Marriage (n 155).

and social realities.[728] Stychin provides a more favourable and nuanced view, suggesting that conferring legal status to cohabitants could help address some of the challenges commonly associated with family stability.[729] For example, a legal framework could provide couples with greater security in their commitments and responsibilities to each other, ultimately reducing the likelihood of relationship breakdowns. This, in turn, could positively impact those involved in physical and mental well-being.[730]

Enabling legal recognition for cohabitation is not about undermining marriage but acknowledging and protecting the diversity of relationships in modern society.[731] While this is the primary stance, Graff suggests that recognising new relationships will, in fact, reshape marriage by instigating changes within the institution.[732] Hunter builds upon this idea, suggesting that transforming the current patriarchal structure of marriage into an egalitarian system could significantly alter the fundamental concepts of marriage, potentially undermining its role as a social hierarchy.[733] While the primary argument is that extending rights should not undermine marriage, alternative perspectives suggest that we should not prioritise the traditional nuclear family form[734] and instead reconsider marriage's hierarchical structure to prevent the perpetuation of inequalities.[735]

Parry questions whether it would be appropriate to treat cohabitants who have chosen not to marry as if they were married.[736] Coalition for Marriage goes a step further to argue that this would be 'illogical.'[737] However, these positions fail to consider the injustices cohabitants face,

---

[728] Kate Nash, 'A Movement Moves…Is There a Women's Movement in England Today?' (2002) 9(3) European Journal of Women's Studies 311, 324; Nicola Barker, *Not the Marrying Kind: A Feminist Critique of Same-Sex Marriage* (Palgrave Macmillian 2013) 130.

[729] Carl Stychin 'Family Friendly? Rights, Responsibilities and Relationship Recognition' in Alison Diduck and Katherine O'Donovan (eds), *Feminist Perspectives on Family Law* (Routledge-Cavendish 2006) 29.

[730] ibid.

[731] Celia Kitzinger and Sue Wilkinson, 'The Re-branding of Marriage: Why we Got Married Instead of Registering a Civil Partnership' (2004) 14(1) Feminism and Psychology 127, 139; Ibid 31; ; Law Commission (n 24) [2.44].

[732] EJ Graff, 'Retying the Knot' in Andrew Sullivan (ed), *Same-Sex Marriage Pro and Con: A Reader* (Vintage Books 2004) 135.

[733] Gerda Lerner, *The Creation of Patriarchy* (Oxford University Press 1986) 239; Nan Hunter, 'Marriage, Law and Gender: A Feminist Inquiry' in Nan Hunter and Lisa Duggan (eds), *Sex Wars: Sexual Dissent and Political Culture* (Routledge 2014) 112.

[734] Martha Fineman, *The Neutered Mother, the Sexual Family, and Other Twentyish Century Tragedies* (Routledge 1995) 27.

[735] Robert Wintemute, 'Sexual Orientation and the Charter: The Achievement of Formal Legal Equality (1985-2005) and its Limits' (2004) 49 McGill Law Journal 1143, 1174; Chai Feldblum, 'Gay is Good: The Moral Case for Marriage and Equality and More' (2005) 17 Yale Journal of Law and Feminism 139, 182; Hunter (n 165).

[736] Parry (n 98) 5.

[737] Coalition for Marriage (n 155).

who are not automatically granted legal protections. This raises concerns about fairness in denying marital-like protections to couples who function similarly but have chosen not to formalise their relationship through marriage.[738] By extending property rights, the aim is not to devalue marriage but rather provide safeguards for those who have chosen not to marry for various reasons yet still share their lives and resources like spouses/partners. Therefore, it is crucial to recognise that cohabiting couples may differ from spouses/partners and appreciate that these differences do not imply inferiority but signify the importance of celebrating diverse relationships.[739]

Moreover, providing legal recognition for cohabiting relationships could help promote their stability. This recognition not only benefits cohabitants by offering greater property protection, but it also encourages long-term commitment and investment in the relationship, which positively affects dependents who rely on their care and support.[740] On an economic level, recognising cohabitants can relieve state burdens, as the expenses incurred from lengthy disputes during family breakdowns annually amount to roughly £50bn.[741] Manifesting a diminished reliance on state assistance will emphasise the parties' shared resources.[742] Accordingly, by acknowledging the broader implications, I demonstrate the multi-layered advantage of reforming cohabitation property rights while mitigating undermining marriage.

As indicated, arguments against extending property rights to cohabitants often fail to consider the broader implications and societal context. A study examining the relationship between law reform for cohabitation and marriage rates in Australia found that the decline in marriage rates was not solely linked to the legal recognition of cohabiting couples.[743] Instead, societal trends, such as a shift towards conscious decision-making regarding marriage, were significant factors.[744] Similarly, European jurisdictions have shown no direct correlation between declining marriage rates and legal recognition of new family units through partnership registration.[745] While the study provides valuable insights into law reform, it is important to exercise caution when applying these findings. The socio-cultural landscape and legal

---

[738] Fraser (n 137).

[739] Bruce MacDougall, 'The Celebration of Same-Sex Marriage' (2000) 32(2) Ottawa Law Review 235, 256.

[740] Fineman (n 166) 26; Stychin (n 161).

[741] The Centre for Social Justice (n 135) 5.

[742] Stychin (n 161)

[743] Kathleen Kiernan, Anne Barlow and Rosangela Merlo, 'Cohabitation Law Reform and its Impact on Marriage' [2006] Family Law Journal 1074, 1074-6.

[744] Duncan et al (n 135) 396; Kiernan et al (n 175); Berenson (n 136).

[745] Kiernan (n 175).

framework in E&W may not directly align with those in Australia or continental Europe. Nevertheless, policymakers in E&W can use this study to develop a tailored and effective strategy to address these concerns more accurately.

4.2.2 Preservation of Individual Autonomy

The focus of the discussion now shifts towards exploring the concept of individualism advocated by Baroness Deech and the Marriage Foundation. Their shared belief in extending marital-like rights to cohabiting couples highlights a foundational principle: preserving individual and couple autonomy within family dynamics.[746] Baroness Deech emphasises the need for legal structures to respect personal autonomy and refrain from imposing marital rights upon couples who consciously choose not to marry.[747] For instance, couples who may have gone through a difficult divorce should not face penalties for their previous failed marriage.[748] The law should leave a 'corner of freedom' to exercise their autonomy as a family without state intervention.[749] Similarly, the Marriage Foundation criticises the automatic assignment of rights and responsibilities as an invasive state interference that goes against liberal principles.[750] Both advocate for a greater emphasis on cohabitants voluntarily making legal agreements as a more desirable approach to establishing legal obligations within their relationship.

Although Baroness Deech and the Marriage Foundation's emphasis on individual autonomy is admirable, their approach overlooks potential vulnerabilities within cohabiting relationships. Relying solely on voluntary agreements to establish legal boundaries could risk creating gaps that leave cohabiting couples unprotected.[751] This lack of automatic legal safeguards could result in unequal power dynamics or bargaining power imbalances during relationship breakdowns, leading to property inequality and injustices.[752] Privileging individual autonomy often promotes the norm of the 'unattached, unencumbered person,' [753] which tends to

---

[746] Baroness Ruth Deech, 'Written Evidence from Baroness Ruth Deech' (HAB0002, 2021) <https://committees.parliament.uk/writtenevidence/36132/pdf/> accessed 19th March 2024; Paul Coleridge and Harry Benson, 'Written evidence from Sir Paul Coleridge and Harry Benson of Marriage Foundation' (HAB0007, 2021) <https://committees.parliament.uk/writtenevidence/36943/pdf/> accessed 19th March 2024.
[747] Deech (n 178).
[748] Baroness Ruth Deech, 'Cohabitation' [2010] Family Law Journal 39, 42-3.
[749] ibid, 42-3.
[750] Coleridge and Benson (n 178).
[751] Thompson (n 51) [14].
[752] ibid, [15].
[753] Friedman (n 16)

downplay the significance of childcare and domestic work, traditionally carried out by women.[754] This leaves the non-legal property owner, who typically carries these functions, more vulnerable.[755] It is important to note that revaluing non-financial contributions should not imply that women are obligated to fulfil these roles.[756] Instead, society's interest is acknowledging the importance of such work, transcending traditional gender stereotypes, and ensuring adequate value and compensation.[757] Therefore, failing to reform existing property laws could perpetuate and reinforce existing inequalities.[758]

The concept of liberal individual autonomy suggests that individuals should be free to make their own choices.[759] However, feminist critiques highlight the limitations of frameworks that prioritise individual choice without adequately accounting for the social relations that shape individual lives.[760] Instead, relational autonomy provides a more comprehensive perspective by recognising the impact of relationships and societal structures on decision-making.[761] Nedelsky proposes that individual identities are built through relationships,[762] revealing a deep connection between individuals and their social contexts.[763] While individualism acknowledges the value of relationships, relational autonomy further asserts that these connections influence individuals and their choices.[764] In contrast, liberalism tends to overlook mutual obligations and resource sharing inherent within family relationships.[765] Furthermore, relational autonomy emphasises the importance of these responsibilities and obligations and

---

[754] Reece (n 15)111-112.

[755] Bottomley (n 13)182; Wong (n 13)114.

[756] Fineman (n 166) 26.

[757] Pamela Laufer-Ukeles, 'Selective Recognition of Gender Difference in the Law: Revaluing the Caretaker Role' (2007) 31 Harvard Journal of Law and Gender 1, 3; Carol Smart, *The Ties that Bind: Law Marriage, and the Reproduction of Patriarchal Relations* (Routledge 2013) 222.

[758] Friedman (n 16)..

[759] Joseph Raz, *The Morality of Freedom* (Oxford University Press 1988) 204; Helen Reece, *Divorcing Responsibly* (Hart Publishing 2003) 13.

[760] Jennifer Nedelsky, 'Reconceiving Autonomy: Sources, Thoughts and Possibilities' (1989) 1(7) Yale Journal of Law and Feminism 7, 10; Catriona Mackenzie and Natalie Stoljar, *Relational Autonomy: Feminist Perspectives on Autonomy, Agency, and the Social Self* (Oxford University Press 2000) 4; Mara Marin, 'Care, Oppression, and Marriage' (2014) 29(2) Hypatia 337.

[761] Nedelsky (n 192)10.

[762] Jennifer Nedelsky, *Law's Relations: A Relational Theory of Self, Autonomy, and Law* (Oxford University Press 2013) 3-5.

[763] Jonathan Herring, 'The Human Rights Act and the Welfare Principle – Conflicting or Complimentary?' (1999) 11(3) Child and Family Law Quarterly 223.

[764] Linda Barclay, 'Autonomy and the Social Self', in Catriona Mackenzie and Natalie Stoljar (eds), *Relational Autonomy: Feminist Perspectives on Autonomy, Agency, and the Social Self* (Oxford University Press 2000); Reece (n 15) 111; Jonathan Herring, *Relational Autonomy and Family Law* (Springer 2014) 11.

[765] Marian Verkerk, 'The Care Perspectives and Autonomy' (2001) 4(3) Medicine, Health Care and Philosophy 289, 291.

challenges the idea that freedom should be the default position.[766] Doing so aims to safeguard individuals from exploitation or disadvantage within their relationship.[767]

Furthermore, the lack of legal recognition for those cohabiting may lead to unfair disadvantages when compared to spouses/partners, ultimately undermining the principle of equality before the law. While the value of autonomy is important, it is crucial to acknowledge the intricate nature of the issue and the potential for injustices to arise from the absence of adequate legal protection. Therefore, it is vital to establish an inclusive legal framework that balances preserving individual autonomy with providing equitable legal protections for cohabiting relationships. This framework would address vulnerabilities and disparities while upholding fairness, justice, and autonomy principles.

Opt-In v Opt-Out Framework

Baroness Deech advocates for a voluntary legal opt-in system that allows couples to choose whether or not they want legal intervention in their relationship, prioritising individual autonomy.[768] However, this approach fails to consider a critical factor: the vulnerability of those who may not opt-in to the regime. As demonstrated by CICT, some couples are left financially disadvantaged and without property rights when automatic protection is absent. This highlights the limitations of the voluntary opt-in proposal in safeguarding all individuals in cohabiting relationships. Howard Kennedy LLP builds upon Baroness Deech's proposal by recommending a two-fold approach that allows couples to register their relationship and voluntarily opt-in.[769] Nevertheless, this approach centres on obtaining mutual consent from both parties, which may prove difficult in relationships with imbalanced power dynamics.[770]

An alternative approach that is more favourable is an opt-out model. Unlike the voluntary opt-in model that may leave unprotected cohabitants, the opt-out approach automatically opts couples in for protection to couples unless they actively choose to opt-out.[771] This helps to mitigate the risk of leaving vulnerable individuals unprotected while still upholding the principle of autonomy by allowing couples to make their own decisions. Extending legal

---

[766] Nedelsky (n 192).
[767] Herring (n 196) 16.
[768] Deech (n 178).
[769] Howard Kennedy, 'Written Evidence from Howard Kennedy LLP' (HAB0299, 2021) <https://committees.parliament.uk/writtenevidence/36132/pdf/> accessed 19th March 2024.
[770] ibid.
[771] Thompson (n 51) [11].

protection to cohabitants primarily aims to promote equality and safeguard vulnerable parties. The opt-out scheme addresses concerns about unequal power dynamics by providing a mechanism for the financially weaker party to benefit from legal protection, even if they are not the legal property owner.[772] While some may suggest that the opt-out scheme still infringes on autonomy,[773] it ultimately prioritises the critical policy objective of protecting vulnerable individuals and upholding social justice.[774]

4.2.3 Legal Complexities

Advocating for greater protection for cohabitants involves navigating many legal complexities, all intertwined with social and ethical considerations. These concepts raise critical questions about the extent to which rights should be extended.[775] Although an opt-out scheme provides a promising avenue, establishing the legal criteria for coverage remains a significant challenge. In E&W, cohabitation lacks a legal definition, making statutory guidance an attractive option for recognising the evolving dynamics of family life.[776] However, defining cohabitation presents hurdles, as it must be comprehensive enough to encompass diverse relationships while still ensuring legal clarity and equity.[777]

The Cohabitation Rights Bill[778] aimed to provide legal rights to cohabitants. The proposed definition included any two people living together as a couple, irrespective of gender, under specific conditions such as having children or cohabiting for a minimum of 3 years.[779] Barlow acknowledges that the three-year period is consistent with research showing that this is often when claims for CLM arise.[780] However, it is worth noting that women, not men, commonly hold this presumption.[781] Recognising and comprehending these gender disparities is essential to developing legal and social structures that address biases and meet the requirements of contemporary relationships.

---

[772] Thompson (n 51) [14], [16].
[773] Deech (n 178).
[774] Scherpe (n 44).
[775] John Eekelaar and Mavis Macclean, 'Marriage and the Moral Bases of Personal Relationships' (2004) 31(4) Journal of Law and Society 500, 514.
[776] Anne Barlow and Craig Lind, 'A Matter of Trust: The Allocation of Rights in the Family Home' (1999) 19(4) Legal Studies 468, 474.
[777] Law Commission (n 24) [3.8]; Fraser (n 137)
[778] HL Bill (n 1).
[779] Cohabitation Rights Bill (2019-2020) 97, s.1-3.
[780] Barlow and Lind (n 208) 478.
[781] ibid.

The Law Commission conducted interviews with various consultees who expressed a strong desire for legal recognition.[782] While it remains unclear which specific demographics were included in the research, most interviewees favoured legal recognition provided that it did not undermine marriage through analogies.[783] Furthermore, utilising the term 'as a couple' helps prevent analogies to spouses/partners, which could burden the state with further litigation challenges. Instead, this term could be suitably applied to couples who may reject traditional marriage but still require legal protections.[784] Therefore, addressing the current issues faced by cohabitants could alleviate concerns about undermining the institution of marriage,[785] which seems to be a significant factor in the lack of enthusiasm for extending property rights.[786]

Eligibility

A qualifying checklist could serve as a functional test to determine whether a relationship meets eligibility requirements for legal recognition. For instance, appreciating caring dependants, where one partner may have incurred financial detriment. This would not only provide greater clarity for the couple and thir parties but also offer more comprehensive protection than a one-size-fits-all solution.[787] Research indicates that in heterosexual relationships, men tend to contribute significantly less to domestic work compared to women, who perform unpaid childcare in addition to other household duties.[788] Even women who earn more than their partners financially may take on more domestic work to counteract gender deviations.[789] While this data provides insight into gender disparities, it primarily applies to heterosexual couples and does not account for same-sex relationships. As such, it may not provide a complete picture of domestic work dynamics in modern relationships. Smart advocates for a more holistic approach that goes beyond improving existing conditions to make patriarchal structures more tolerable and long-lasting.[790] This goal is to recognise the value of domestic work, which not only serves the state's interests but also benefits individual men.[791] For example, less reliance

---

[782] Law Commission (n 24) [3.5].
[783] ibid.
[784] ibid, [3.6], [3.7].
[785] Hale (n 143) 423-5.
[786] Gillian Douglas, Julia Pearce and Hilary Woodward, 'Cohabitants Property and the Law: A Study of Injustice' (2009) 72(1) Modern Law Review 24, 27.
[787] Hale (n 143) 424.
[788] Garrison (n 52).
[789] ibid.
[790] Lerner (n 165); Smart (n 189).
[791] Hale (n 143) 422; Smart (n 189).

on state support and benefits allows resources to be redirected to other policies and agendas.[792] Additionally[793] Therefore, it is necessary to provide property compensation for women who have sacrificed material benefits.

Although I briefly touch upon the subject of a checklist in this part, I delve deeper into it in Section 5.2 as I examine the comparable strategy employed by New Zealand. By drawing comparisons to their approach, I aim to explore the feasible implementation of a checklist within the framework of cohabitation property reform.

4.3 Reform Proposals

So far, I have delved into CICT and explored different viewpoints on extending the rights of cohabiting couples. I suggest that legislative reform would be beneficial in safeguarding and determining the property interests of family homes. This proposal aims to address the complexity and lack of clarity in CICT, making property disputes less intricate through the adoption of uniform principles. Moreover, it introduces automatic protection, which is currently absent, while still allowing couples to regulate their arrangements outside of statutory presumptions. Giving courts discretion would also help redistribute interests in exceptional circumstances, mitigating potential injustices.

Barlow recommends a 'sliding scale' for property ownership, in which a non-legal owner could potentially acquire a 20% interest after two years and 50% after five years.[794] This encourages stability and commitment in the relationship while also recognising the value of non-financial contributions. Smart advocates for a 25% presumption of property ownership in relationships where one partner is the primary caregiver.[795] These measures can be assessed against previous cases, such as *Burns*[796] and *Defoe*,[797] where CICT led to inequitable outcomes by unjust enrichment for one party.[798] For example, in *Burns*,[799] the couple cohabited for over twenty years, during which the woman was the primary caregiver. Under the revised sliding scale reform, she could rightfully claim a 50% share of the property accrued during their relationship,

---

[792] Stychin (n 161) 2; Smart (n 189) 223.
[793] Hale (n 143) 422.
[794] Barlow and Lind (n 208) 478.
[795] ibid, 479; Smart (n 189).
[796] *Burns* v *Burns* [1984] Ch 317 (CA Civ Div).
[797] *Springette* v *Defoe* [1992] 2 FLR 388 (CA Civ Div).
[798] Douglas et al (n 218).
[799] *Burns* v *Burns* [1984] Ch 317 (CA Civ Div).

with up to 25% compensation for the financial struggles endured while raising their children.[800] This would have been a more just outcome than receiving nothing under CICT. Similarly, in *Defoe,*[801] a presumption of 50% property interest could have been entitled after six years of cohabitation instead of the 25% awarded.[802] These proposed changes are a significant step towards addressing the injustices cohabiting couples face due to complex property laws that do not recognise the value of domestic work in light of societal shifts.

In this part, I advocate for greater protection of the property rights of cohabiting couples. Exploring existing empirical research, I recognise that societal norms are evolving, and the law must adapt accordingly. By engaging with alternative perspectives, I acknowledge that extending cohabitation rights can be a complex issue that involves balancing concerns about undermining marriage and individual autonomy. To address these challenges, I propose an opt-out scheme that would help bridge the gap by enabling vulnerable individuals to receive legal protections while still giving couples the freedom to make their own decisions. Additionally, I examined the more intricate details of this proposal, including defining cohabitants and determining eligibility. I emphasise the importance of uniform principles and inclusivity and avoiding analogies with marriage that could be seen as undermining the institution. Ultimately, reforming these measures could lead to more fair and equitable outcomes for cohabiting couples' property rights than the current system, which falls short of providing adequate protection.

In the next part, I examine the implementation of property protection rights for cohabiting couples in New Zealand and Scotland, drawing insights that could potentially influence the legal framework in E&W.

5. Exploring Scotland and New Zealand's Approach

In the previous part, I propose legal reform that aligns with societal shifts by addressing opposing viewpoints against extending property rights for cohabiting couples. In this part, I analyse cohabitation rights offered in Scotland and New Zealand to establish a preferred system for E&W. I commend both approaches for their automatic opt-in element, which balances

---

[800] Barlow and Lind (n 208) 484.
[801] *Springette* v *Defoe* [1992] 2 FLR 388 (CA Civ Div).
[802] Barlow and Lind (n 208) 484.

safeguarding vulnerable individuals with maintaining autonomy. I suggest adopting a definition of cohabitants similar to New Zealand and Scotland's reform proposals, which incorporate non-exhaustive factors to recognise contemporary relationships rather than relying on marriage analogies. To ensure clarity and consistency in case outcomes, I propose a minimum duration akin to New Zealand's model. Furthermore, I suggest incorporating an extended timeframe to bring claims, similar to New Zealand's 3-year period, instead of Scotland's 1-year period, to prevent overburdening the justice system. While I draw inspiration from these jurisdictions, I acknowledge that E&W has a unique legal system, and adjusting reforms to suit political and social contextual differences is essential.

5.1 Cohabitation Law in Scotland

The Family Law (Scotland) Act 2006 was strongly influenced by the need for greater safeguarding mechanisms amid the rise of cohabiting couples. It aims to address the economic disparities arising from a relationship breakdown by introducing a financial provision scheme.[803] The scheme enables cohabiting couples to make financial claims in the event of a separation, establishing a framework that encourages fairness and helps to mitigate economic disparities. While cohabitants do not possess the same rights as spouses/partners, the scheme acknowledges the contributions made by each party to the relationship.[804] To begin, I will explore the current statutory definition of a cohabitant, which is insufficient, before delving into more favourable reform proposals. Scotland lacks the resources to transfer property interests, making it distinct from E&W.[805] Therefore, I will focus on the administrative aspects rather than providing an in-depth analysis of the financial provision framework.

5.1.1 Breakdown and Analysis of the Legislation

Definition

The current legislation being reviewed defines a cohabitant as a couple, man or woman, living together like husband and wife[806] or two people of the same sex living together like civil partners.[807] Although this definition aims to cover a range of relationships, it comes with

---

[803] Whiting (n 3)59.

[804] Lucy Metcalf, 'Scotland's Cohabitation Law – Ahead of the Time' (UK Legal News Analysis, 2019).

[805] Scottish Law Commission, *Aspects of Family Law: A Discussion Paper on Cohabitation* (Scots Law Com No 170, 2020) [5.76].

[806] Family Law (Scotland) Act 2006 (asp 2), s.25(1)(a).

[807] ibid, s.25(1)(b).

various challenges and shortcomings.[808] Recent proposals for legal reform in Scotland (2020) serve as a reminder of how complex it can be to define cohabitation within a legal framework.[809] However, one admirable aspect of the definition is that it does not require a registration process. [810] This benefits vulnerable individuals who cannot register their cohabitation due to financial or personal circumstances.[811] All the elements I explore are automatic unless the couple opts-out through a cohabitation agreement.[812] This approach strikes a good balance between safeguarding autonomy and reducing the risk of exploitation for the weaker party,[813] an approach that E&W should implement.

The 2011 Wasoff, Miles, and Mordaunt Report initially found no significant issues in practice regarding the identification of cohabiting couples.[814] However, upon closer examination, substantial criticism is directed at the statutory definition for its constrained and antiquated scope that fails to capture contemporary relationships' complex and varied landscape. [815] Although the report was relevant at the time of its publication, the findings are even more pertinent today due to the increasing recognition of diverse relationship structures. Consequently, these limitations highlight the urgent need for reformed frameworks that better reflect the realities of modern relationships. The analogy initially drawn between spouses/partners suggested a minimum age requirement and excluded relationships with criminal elements.[816] However, due to mounting public pressure, reform proposals advocate for recognising that cohabitants are not synonymous with spouses/partners and that the law should not equate them.[817] This shift in perspective reflects a growing awareness of the distinct dynamics and nuances in cohabiting arrangements, which E&W should embrace to accurately reflect the diverse nature of interpersonal relationships rather than utilising analogies.

---

[808] Jamie Foulis, 'Scottish Law Commission Report on Cohabitation' (2023) 181 Family Law Bulletin 1, 1-2.
[809] Scottish Law Commission (n 237).
[810] Family Law (Scotland) Act 2006 (asp 2), s.25.
[811] Scottish Law Commission, *Report on Cohabitation* (Scots Law Com No 261, 2022) [3.65].
[812] Family Law (Scotland) Act 2006 (asp 2), s.27(2); Scottish Law Commission (n 243) [1.13]; Scottish Law Commission (n 237) [2.63]; Graeme Fraser, 'Cohabitation reform in England and Wales – Comparative perspectives and how to reset the reform campaign' [2023] Family Law 341.
[813] Fraser (n 137).
[814] Fran Wasoff, Jo Miles and Enid Mordaunt, 'Legal Practitioners' Perspectives on the Cohabitation Provisions of the Family Law (Scotland) Act 2006' (2010) University of Cambridge Faculty of Law Research Paper No.11/03 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1736612> accessed 1st April 2024, 124-5.
[815] Scottish Law Commission (n 237) [3.21]; Foulis (n 240).
[816] Sexual Offences (Scotland) Act 2009 (asp 9); Scottish Law Commission (n 243) [3.35].
[817] Scottish Law Commission (n 243) [3.10]; Foulis (n 240) 2-3.

Litigation regarding couples who fit the cohabitant definition has been infrequent.[818] However, in *Harley*,[819] the relationship's stability was initially compared unfavourably to a traditional husband and wife dynamic. Conversely, in *E.M*,[820] while one partner acknowledged the familial nature of the relationship, they rejected the characterisation of it being akin to marriage. Nevertheless, the court considered various aspects of the relationship, such as emotional support and interdependence, and concluded that it resembled a marital bond.[821] The Scottish Law Commission 2023 has recommended a departure from the spouse/partner analogy.[822] Instead, they propose a broader definition that includes 'two people who live together enduring a family relationship; over the age of 16; are not spouses/partners; and are not closely related to each other.'[823] This approach offers several advantages, including flexibility in accommodating family structures and functions. Additionally, it addresses concerns raised in *Harley*,[824] as couples under this definition could be represented without extensive legal deliberation. Overall, this proposal demonstrates a step towards a more inclusive and adaptable framework, an element I advocate introducing in E&W.

Court Discretion

In legal proceedings regarding cohabitation, courts can evaluate eligibility based on various factors, such as the length and nature of the relationship and financial agreements.[825] Although this approach offers a tailored evaluation for each case, the lack of clear guidelines can lead to ambiguity.[826] Without established criteria or benchmarks, individuals may find it difficult to understand how their situation will be assessed, resulting in uncertainty and difficulty in making informed decisions. Addressing these concerns can provide more precise guidance to promote consistency, transparency, and fairness in cohabitation legal proceedings in E&W.

---

[818] University of Glasgow, 'Women and Equalities Committee Inquiry: The Rights of Cohabiting Partners - Response' (n 2).
[819] *Harley* v *Robertson* [2011] ScotSC 194.
[820] *E.M* v *A.I* [2012] ScotSC 24 [16].
[821] ibid, [23].
[822] Alan Brown, 'The Legal Regulation of Cohabitation in Scotland: A Failed Attempt at Compromise' (2022) 44(2) Houston Journal of International Law 221, 232; Scottish Law Commission (n 243) [3.29].
[823] Scottish Law Commission (n243) [3.72].
[824] *Harley* v *Robertson* [2011] ScotSC 194.
[825] Family Law (Scotland) Act 2006 (asp 2), s.25(2).
[826] Tom Guthrie and Hilary Hiram, 'Property and Cohabitation: Understanding the Family Law (Scotland) Act 2006' (2007) 11(2) Edinburgh Law Review 208, 213.

Minimum Duration

The proposals suggest a minimum duration to clarify and alleviate judicial system burdens.[827] However, public surveys revealed that attitudes varied on how long this duration should be,[828] with suggestions ranging from 6 months to 25 years.[829] In practice, the lack of clarity around the duration requirement may cause confusion. For instance, in *Harley*,[830] the couple lived together for less than 7 months and asserted they satisfied the definition of cohabitation.[831] However, without this assertion, the court admitted they would have likely ruled that they did not meet the criteria.[832] This uncertainty highlights the value of introducing a minimum duration to provide clear guidance for individuals and legal professionals.[833]

Despite concerns about the potential impact of cohabitation claims on the judicial system for short-term relationships,[834] an analysis of court data reveals that only a small percentage (6%) of disputes arise from relationships lasting 0-2 years.[835] This suggests that short-term relationships may not significantly impact the judicial system regarding cohabitation claims. While this data may be outdated, further research could provide valuable insights into the effectiveness of implementing a minimum duration requirement. However, unlike Scotland, introducing a minimum duration would be the most effective approach for the E&W framework. Nevertheless, this difference in approach highlights the importance of policymakers adopting a tailored approach to legal reform that balances public perceptions with the need for fair and consistent outcomes for cohabitants.[836]

Non-Exhaustive Factors

The Scottish Law Commission propose enhancing the definition of cohabitation by introducing determinative characteristics.[837] This is intended to offer more distinct direction for legal professionals and the general public concerning their entitlements in the event of a relationship

---

[827] Scottish Law Commission (n 243) [3.40].
[828] ibid, [3.45].
[829] *Harley* v *Robertson* [2011] ScotSC 194; Scottish Law Commission (n 243) [3.46].
[830] *Harley* v *Robertson* [2011] ScotSC 194.
[831] ibid, [4].
[832] ibid, [56].
[833] Brown (n 254) 233, 242.
[834] Scottish Law Commission (n 243) [3.40].
[835] Jo Miles, Fran Wasoff and Enid Mordaunt, 'Reforming Family Law – the case of cohabitation: things may not work out as you expect' (2012) 34(2) Journal of Social Welfare and Family Law 167, 176.
[836] University of Glasgow (n 250).
[837] Scottish Law Commission (n 243) [3.50].

dissolution.[838] Nevertheless, it is important to note that an overly rigid application of criteria may discount certain societal intricacies, given that cohabitation is often viewed as 'more easily recognised than defined.'[839]

Barlow and MacQueen advocate for a more nuanced approach that considers various non-exhaustive factors, such as financial independence, domestic and economic roles, and shared commitment.[840] These factors challenge traditional family norms and acknowledge alternative forms of family or kinship relations. While courts appear to take a more liberal family approach, it becomes crucial to challenge judges' assumptions about expected behaviour within relationships, as this influences how the law is applied.[841] By focusing on social aspects rather than financial values, non-exhaustive factors aim to address outdated family structures and gender biases.[842] Moreover, this emphasises the significance of considering how people share their lives and are committed to each other, rather than just their residence, to recognise structures beyond traditional norms.[843] These proposals offer a potential framework for E&W to acknowledge diverse relationships and prevent prioritising certain factors over others. The approach permits a subjective, case-by-case assessment, allowing for a more holistic understanding of contemporary relationships.[844] This mitigates the risk of strict reliance on determinative criteria that may not fully capture the complexities of cohabiting arrangements.

Financial Provisions

A cohabiting couple attains legal recognition if they live together like spouses/partners, are not in a legal relationship, are not closely related, and have lived together for at least 2 years.[845] Once this criterion is met, they are automatically eligible to apply for financial provisions in the event of a separation other than death.[846] The legal landscape for financial provisions differs

---

[838] ibid, [3.52].
[839] *M.B* v *J.B* [2014] ScotSC 89, [27].
[840] Scottish Law Commission (n 243) [3.52]; Jamie (n 240) 3.
[841] Rebecca Probert, 'Equality in the Family Home?: Stack v Dowden' (2007) 15(3) Feminist Legal Studies 341; Simone Wong, 'Shared Commitment, Interdependency and Property Relations: A Socio-Legal Project for Cohabitation' (2012) 24(1) Child and Family Law Quarterly 60.
[842] Helen Carr and Simone Wong, 'Feminist Approaches to Property Law Research' (2016) 3(3) Property Law Review 247.
[843] Kathrine O'Donovan, *Sexual Divisions in Law* (Weidenfeld and Nicolson 1985); Carole Smart, 'Law's Power, the Sexed Body, Feminist Discourse' (1990) 17 Journal of Law and Society 194; Stevi Jackson, 'Interchanges: Gender, Sexuality and Heterosexuality: The complexity (and limits) of heteronormativity' (2006) 7(1) Feminist Theory 105, 105-6.
[844] Brown (n 254) 233-35.
[845] Family Law (Scotland) Act 2006 (asp 2), s.25.
[846] ibid, s.28.

significantly between Scotland and E&W. Despite no remedies to transfer property shares, cohabitants can apply for monetary compensation for their financial and non-financial contributions to the home.[847] This includes situations where one cohabitant experiences an economic disadvantage that benefits the other or a child.[848] In contrast, in E&W, financial provisions are not awarded on relationship breakdown, except regarding child welfare.[849] This aspect of Scottish legislation is commendable for acknowledging the economic sacrifices often associated with homemaking and childcare responsibilities.[850] This was demonstrated in *Gow*,[851] where the applicant received a capital sum after demonstrating an economic disadvantage by selling her former home and giving up work to move in with her partner. Similarly, in *Shilliday*,[852] the applicant funded home improvements, leading to increased property value, while the other parties' economic advancement resulted from not bearing the cost of these contributions.

There are notable differences in the property rights landscape between E&W and Scotland. Scotland places more emphasis on financial provisions than on transferring beneficial shares. Therefore, I avoid detailed discussions on financial provisions as implementing this in E&W could put cohabitants in a better position than spouses/partners. Financial provision schemes often provide greater flexibility and less restrictive criteria than property rights regimes. This means cohabiting couples might have easier access to financial support upon separation without legal requirements. However, I highlight criticism regarding the timeframe to bring a claim, which E&W could address in their reform. In Scotland, claims must be made within 1 year of separation.[853] While this is intended to reflect the limited scope of cohabitation claims, it has resulted in unintended consequences.[854] For instance, individuals may feel pressured to make rushed applications and court actions despite potential success through alternative dispute

---

[847] Anne Barlow, 'Cohabitation and Marriage in Scotland: Attitudes, Myths and the Law' in John Curtice, David McCrone, Alison Park and Lindsay Paterson (eds), *New Scotland, New Society? Are Social and Political Ties Fragmenting?* (Edinburgh University Press 2001) 78.
[848] Family Law (Scotland) Act 2006 (asp 2), s.28(5).
[849] Children Act 1989, s.1; Whiting (n 3)58.
[850] Barlow (n 279) 87.
[851] *Gow* v *Grant* [2012] UKSC 29, [2012] SLT 828.
[852] *Shilliday* v *Smith* [1998] SLT 976.
[853] Family Law (Scotland) Act 2006 (asp 2), s.28(8).
[854] Hector MacQueen, 'Cohabitants in the Scottish Law of Unjustified Enrichment' (2019) 1 Acta Juridica 419, 436; Fraser (n 244) 342.

procedures.[855] This can burden the family justice system's resources.[856] To address this, E&W could consider extending the timeframe to encourage alternative resolutions rather than court proceedings.[857]

5.2 Cohabitation Law in New Zealand

In New Zealand, two distinct statutory definitions of a '*de facto* relationship' apply in various legal contexts. I focus on the definition relevant to the Property (Relationship) Act 1976. The New Zealand regime is automatic after a minimum of 3 years,[858] with an option to contract out.[859] Once a *de facto* relationship is established, it receives the same criteria for property division as spouses/partners.[860]

5.2.1 Breakdown and Analysis of the Legislation

Definition

A *de facto* relationship is two people over 18 years old who live together as a couple, are not spouses/partners, and regardless of sex, sexual orientation, or gender identity. [861] All circumstances must be considered when determining whether two people live together as a couple.[862] The legislation gives the court broad discretion to consider various factors, such as property ownership, childcare and support, household duties, and more. [863] This approach, similar to Scotland's reform proposals, allows for a flexible, case-by-case determination of *de facto* status.[864] Additionally, by recognising both heterosexual and homosexual relationships, New Zealand demonstrates a commitment to equality before the law, which is also crucial for E&W.

---

[855] Fran Wasoff, Jo Miles and Enid Mordaunt, 'No longer living together: how does Scots cohabitation law work in practice' (CRFR 51, 2010) <https://www.nuffieldfoundation.org/sites/default/files/files/Briefing%2051.pdf> accessed 28th March 2024; Fraser (n 244) 342.

[856] Wasoff et al (n 287).

[857] Fae Garland, 'Gender Imbalances, Economic Vulnerability and Cohabitation: Evaluating the Gendered Impact of Section 28 of the Family Law (Scotland) Act 2006' 19(3) Edinburgh Law Review 311, 316.

[858] Property (Relationships) Act 1976 (NZ), s.1(C)(2).

[859] ibid, s.21D.

[860] Bill Atkin, 'The Legal World of Unmarried Couples: Reflections on De Facto Relationship in Recent New Zealand Legislation' (2009) 39 Victoria University of Wellington Law Review 793, 795; Margaret Briggs, 'Re: Supplementary evidence on the status of de facto relationships in New Zealand' (HAB00383, 2021) <https://committees.parliament.uk/writtenevidence/43558/html/> accessed 31st March 2024; Fraser (n 244).

[861] Property (Relationships) Act 1976 (NZ), s.2(D)(1).

[862] ibid, s.2(D)(2).

[863] ibid.

[864] ibid, s.2(D)(3).

The definition's flexibility was considered suitable for acknowledging the diverse realities of relationships.[865] However, there have been challenges in interpreting and applying the legislation. For instance, in *B*,[866] the lower court's emphasis on residential occupancy led to an erroneous determination of *de facto* status.[867] This serves as a reminder of the potential uncertainty and inconsistency when assessing the factors that define a *de facto* relationship.[868] Nevertheless, results from a 2018 public survey conducted in New Zealand indicate widespread support for the definition's flexibility,[869] notwithstanding *B*.[870] Concerns were only raised regarding the exclusion of relationships under a more rigid approach.[871] Notably, this survey represents the first nationwide research of its kind, providing reliable and current insights into societal attitudes.[872] In order to alleviate any uncertainties and improve comprehension, E&W could initiate public awareness initiatives and resources that could aid individuals in comprehending how the law relates to their specific situation.[873]

Property Division

When a *de facto* relationship ends, property division is governed by the principle of equal sharing.[874] This is typically applied after a minimum duration of 3 years,[875] and couples have three years to make a claim once their relationship has ended.[876] This presumption aims to recognise the equal contributions made by both partners during the relationship,[877] including financial and non-financial contributions, like caregiving, household duties and support for each other's business endeavours. For example, in *Nash*,[878] one partner's claim was based mainly on their housekeeping and childcare contributions, which resulted in being awarded a share of the family home.[879]

---

[865] New Zealand Law Commission, *Review of the Property (Relationships) Act 1976: Preferred Approach* (Issue Paper 44, 2018) 81.
[866] *B* v *F* [2010] NZFLR 67 (NZ).
[867] ibid, [50].
[868] Nicola Peart, 'The Property (Relationships) Amendment Act 2001: A Conceptual Change' (2008) 39(4) Victoria University of Wellington Law Review 813, 823; Zhixiong Liao, 'Finding Certainty in Determining Whether a De Facto Relationship Exists: An Impossible Task?' (2015) 21 *Canterbury Law Review* 112, 115.
[869] New Zealand Law Commission (n 297) 84.
[870] *B* v *F* [2010] NZFLR 67 (NZ).
[871] New Zealand Law Commission (n 297) 89.
[872] ibid, 17.
[873] ibid, 89.
[874] Property (Relationships) Act 1976 (NZ), s.1C(3).
[875] ibid, s.11.
[876] ibid, s.24.
[877] Liao (n 300).
[878] *Nash* v *Nash* [1994] NZFLR 921 (NZ).
[879] ibid, 925.

In New Zealand, all couples are granted equal treatment in terms of property division, regardless of their relationship status. This aligns with the country's unified commitment to equality and fairness.[880] However, couples can choose to opt-out of this system if they wish to determine their own property division in the event of a separation.[881] For this to happen, the couple must create a written agreement specifying how their property will be divided upon separation and register it with the Family Court.[882] Despite relatively high public awareness of equal sharing, with 79% of respondents indicating general awareness and 68% knowing that equal sharing applies to married and unmarried couples, only 7% of respondents had contracted out of the regime.[883] However, less than half knew the key criteria – living together for 3 years or longer.[884] This suggests that there may be a gap in public knowledge regarding the legal criteria. E&W should introduce a minimum duration, like New Zealand, alongside implementing education and awareness campaigns for additional clarity. Ultimately, context-specific research will be crucial in determining the most appropriate approach for ensuring fairness and equality in property division.

In short-duration relationships, there may be exceptions to the presumption of equal property sharing.[885] Legislation safeguards spouses/partners in relationships lasting less than 3 years.[886] However, *de facto* relationships lack similar statutory protection unless there are extraordinary circumstances, such as child involvement or significant contributions by one party.[887] Property rights in short-duration *de facto* relationships adhere to standard ownership rules, with each party retaining what they brought in unless the non-legal property owner can demonstrate the existence of a constructive trust.[888] While New Zealand's constructive trust is more generous than E&W, it still presents challenges regarding predictability and protection for *de facto*

---

[880] William Atkin, 'De Facto Relationships in New Zealand – A Largely Unified Law' (2016) 50(2) Family Law Quarterly 393, 321

[881] Property (Relationships) Act 1976 (NZ), s.21.

[882] ibid, s.21D.

[883] Binnie I, Taylor N, Gollop M, Henaghan, M, Simmonds S and Robertson J, *Research Summary – Relationship property division in New Zealand: Public attitudes and values. A general population survey* (Michael and Suzanne Borrin Foundation 2018) 3, 7.

[884] ibid; New Zealand Law Commission (n 297) 23.

[885] Property (Relationships) Act 1976 (NZ), s.14A, s.2E.

[886] ibid, s.14, s.14AA.

[887] ibid s.14AA (2); Virginia Grainer, 'What's yours is mine: Reform of the Property Division Regime for Unmarried Couples in New Zealand' (2002) 11(2) Washington International Law Journal 285, 305; Atkin (n 292) 796.

[888] Atkin (n 292) 797.

partners.[889] Research indicates general satisfaction with the minimum 3-year duration before equal sharing applies in *de facto* relationships.[890] However, the legislation implies that equal division of short-duration relationships may not be fair, upholding the concept of justice. This highlights the importance of nationwide research to understand social, political and legal attitudes toward establishing a minimum duration, as the contrast of spouses/partners treated equally to cohabitants after 3 years highlights jurisdiction disparities.

5.3 Suggestions for E&W

After examining cohabitation property rights in Scotland and New Zealand, I have identified promising approaches to establishing a desired regime in E&W. One aspect I highly recommend is the automatic opt-in for couples, which protects vulnerable individuals while still allowing individuals to opt-out to maintain their autonomy. Additionally, I suggest adopting a definition of cohabitants similar to New Zealand's and Scotland's reform proposals, which use non-exhaustive factors to reflect modern relationships rather than relying on marriage analogies. This approach would help E&W avoid the problematic definition currently used in Scotland and better represent diverse arrangements. Moreover, I propose incorporating a minimum duration similar to New Zealand to ensure fair and consistent outcomes for cohabitants. While a 3-year minimum duration works in New Zealand, policymakers in E&W must conduct research to determine an appropriate duration that reflects public attitudes. I also identified a potential gap in awareness of minimum duration criteria in New Zealand, highlighting the need for public awareness schemes to ensure clarity in E&W. Furthermore, incorporating a timeframe to bring claims similar to New Zealand (3 years) rather than Scotland (1 year) could help E&W mitigate overburdening the justice system. While I acknowledge each jurisdiction's unique societal and legal systems, further research is necessary to develop an appropriate and context-specific cohabitation scheme for E&W.

6. Conclusion and further thoughts

Through my exploration of law reform and its potential to enhance protection for cohabiting couples in E&W, I have envisioned a future where all individuals are granted equitable legal protection, regardless of their marital/partnership status. Currently, cohabiting couples in E&W are not granted the same legal rights and protections as spouses/partners. This disparity has led

---

[889] *Lankow* v *Rose* [1995] 1 NZLR 277 (NZ); Atkin (n 292) 797.

[890] New Zealand Law Commission (n 297) 86.

to significant unfairness, particularly regarding property rights, in the event of a relationship breakdown. These disparities have disproportionately affected women, highlighting the social injustices surrounding the undervaluation of unpaid childcare and domestic labour. [891]

After exploring the legal frameworks for cohabiting couples in Scotland and New Zealand, I commend both jurisdictions for their efforts to reflect social changes in their laws. I draw attention to the automatic opt-in element for couples in both jurisdictions, which provides much-needed protection for vulnerable individuals while still preserving their autonomy. E&W should adopt a definition similar to New Zealand's while also considering reform proposals from Scotland. These include using non-exhaustive factors for eligibility to reflect diverse modern relationships rather than relying on marriage analogies. Moreover, to further promote fairness, incorporating non-financial contributions into property law would assist in recognising the value of childcare and household duties. This would help address gender injustices perpetuated by the current system.[892] I propose introducing a minimum relationship duration similar to New Zealand to ensure equitable and consistent outcomes for cohabitants. Furthermore, policymakers must conduct further research to determine the most appropriate duration. While I recognise each jurisdiction's unique contexts and legal systems, developing a context-specific scheme suitable for E&W is crucial.

Proposing a legal framework without marital/partnership analogies could alleviate concerns expressed by critics who worry that such analogies may undermine the institution of marriage. Instead, the framework could recognise cohabitants as their own distinct group, providing support for families during difficult times and avoiding situations that leave them vulnerable and disadvantaged. Introducing statutory regulation can be challenging, as discovered while researching Scotland and New Zealand's frameworks. Nevertheless, I maintain that additional measures are necessary to correct the injustices faced by cohabitants due to the complexity and ambiguity of the current legal system. By acknowledging the value of caregiving and domestic duties, E&W could take a significant step toward ensuring that non-legal property owners who have made significant non-financial contributions are no longer subject to unjust outcomes.

---

[891] Scoular (n 44) 141; Reece (n 15)-112; Scherpe (n 44).
[892] Bottomley (n 13)182; Wong (n 13)114.

In addition to addressing property law injustices, it is crucial to dispel the widespread misunderstanding of CLM, especially considering the growing number of cohabiting couples. Reforms would provide much-needed protection for couples who erroneously assume they are afforded the same legal rights and safeguards as spouses/partners. Data analysis yielded valuable insights into CLM misconceptions. Nevertheless, further research may be worthwhile. I relied heavily on previous studies because I could not conduct primary research. However, I note possible limitations as some studies were conducted prior to changes in the law, such as civil partnerships being available to opposite-sex couples and the introduction of same-sex marriage. In light of these legal developments, more up-to-date research may provide a better understanding of contemporary societal views on cohabitation.

Furthermore, enacting cohabitation legislation alone may not suffice. Creating public education and awareness campaigns could also help cohabitants understand their legal position by clarifying how and when their property rights can be protected. Further research into this may assist in implementing a successful legal reform scheme in E&W despite the Government's previous rejections.

Therefore, after years of cohabitants building a life together and nurturing a family, there could be more significant support from the law during relationship breakdowns to help establish beneficial shares in a home built together.

The Task of Reining in Technological Advancement

Athina Savva

1. Introduction

The many technological advances that have been evident after the Industrial Revolution and are currently evolving, unquestionably provide important means which make life on earth less complicated. Nonetheless, the same cannot be said for the role of the law in regulating these new advancements. It can be noticed though, that these development signpost a more 'effortless' day to day life than simply assisting in tasks that the humankind may find challengeable to overcome. The ensuing discourse under various sub-headings have been product of sociolegal debates which evidently the role of politics cannot be disregarded within these discussions.

2. Artificial Intelligence

It is comprehensible that the induction of new artificial intelligence technologies has been a product of controversiality the last couple of years. This induction to the human society has resulted in decreased agricultural and urban centre employment. [893] Apart from this, misinformation and fraud mostly noticed in developed areas is a huge concern for people who do not radically support such improvements.[894] There is no doubt that artificial intelligence has been a matter of radical development and a matter of ongoing discussion during the last decade. Gunther argues that its ability to produce 'independent situation-based decisions'[895] provides humankind with many benefits.[896] However, the different and rather controversial benefits that this technological development could produce is the reason why experts strongly support it or disregard it. In relevance to autonomous systems, their ability to produce outcomes that do not stem from a 'set of predetermined instructions'[897] is a unique opportunity for the future of human evolution. For the first time, it would not be restrained by the limits of the human mind but would reach answers that no human could ever possibly generate.

---

[893] Department of Economic& Sociala Affairs, *The impact of the technological revolution on labour markets and income distribution* (31 July 2017).

[894] James Clayton, ''Overwhelming consensus' on AI Regulation-Mask', (14 September 2023) <https://www.bbc.co.uk/news/technology-66804996 >

[895] Georg borges, Christoph sorge, *Law and Technology in a Global Digital Society Autonomous Systems*, *Big Data, IT Security and Legal Tech* (Springer, 2022)

[896] Gunther, *Roboter und rechtliche Verantwortung* (2016).

[897] Committee on Legal Affairs draft report of 27 April 200 with recommendations to the Commission on a civil liability regime for Artificial Intelligence, 2020/ 2014 (INL) (JURI AI draft report), Article 3(b).

Undoubtedly, the European Commission accepts that AI produces important solutions for us to overcome some of the major global challenges long in existence. Moreover, suggesting 'countless more examples' of how AI could be found to be beneficially used in the future. From that they conclude that the way in which AI is handled by humans will frame the future world.

3. Controlling the development of AI systems

As AI appears in human lives more commonly, than people think, it is logical to conclude that legally regulating such activity should be implemented at the very least. Many platforms that people use are being driven by artificial intelligence. The controversy around embedding AI in everyday use technologies leads to the question of what these 'new technologies are,' since they could be understood simultaneously as a learning platform and as a robot or an agent.[898] This is the premise upon which the most common arguments against AI is founded. For instance, economists project the inherent risk of embedding AI in the work place leading to largescale layoffs.[899] Moreover, the European Commission argues that AI generates risks for fundamental human rights which are not sufficiently protected by legal frameworks.[900] Consequently, this saw to the proposal and enactment of Artificial Intelligence Act, albeit not sufficiently covering core areas in need of further regulation.[901]

Borges argues that this frustrates the goal towards comprehensive regulation since an 'agenda of international organisations' is needed for the AI technology's ethical implementation in the technology.[902] This is evidenced in a 2017 study which not only pointed out the loss of employment risk by constant innovative technologies, but further concluded that a 'right policy mix and institutional arrangements' could ensure a more equal transition of the technological advancements to the society majorly known by its labour market.[903] Similarly, the UN was not involved in many actions consisting of a framework for AI, particularly relating to human rights concerns.

---

[898] Georg borges, Christoph sorge, Law and Technology in a Global Digital Society Autonomous Systems, Big Data, IT Security and Legal Tech (springer, 2022)

[899] Department of Economic& Sociala Affairs, *The impact of the technological revolution on labour markets and income distribution* (31 July 2017).

[900] European Commission (2021) 205 final on Fostering a European approach to Artificial Intelligence.

[901] Georg borges, Christoph sorge, Law and Technology in a Global Digital Society Autonomous Systems, Big Data, IT Security and Legal Tech (Springer, 2022).

[902] Ibid.

[903] Department of Economic& Sociala Affairs, *The impact of the technological revolution on labour markets and income distribution* (31 July 2017).

Importantly, as society desires to evolve constantly, technological advancements cannot be just 'stopped.' This is where the Governments, the UN and other international organisations must take a legal position within this debate.[904] The law should control these developments to make sure that AI's abilities do not extend beyond of what humans desired them to do. Most importantly, if AI is left unconstrained, the outcome could majorly impact society along different spheres of life. This outcome could be credited to the difference in risk levels arising dependent on the action the AI is instructed to act upon. This notion drove the European Commission's proposals when suggesting specific examples of what 'high risk AI systems' could be.[905] Some actions have been pinpointed throughout the years, that tried to evolve a set of rules to regulate AI advancement. As Borges observes, the European Union has made some 'advanced' discussions on this issue.[906] Moreover, The European Commission has been active in supporting a future satisfactory framework of rules that reflect the innovative technologies. Particularly in regulating AI, they ensured to support the creation of an 'ethical and legal framework for AI,'[907] stressing for a 'human centric approach' to be employed.[908] The EU's approach to AI regulation conceptualises frameworks that should ensure a benefit to the 'people and society as a whole.'[909] However, creating such a framework has not been proven an easy task as evidenced in the case of US Congress's difficulties not reaching a consensus on AI regulation.[910]

4. Framing a legal framework: liability for AI machines

The contribution that the law can give to this debate is fundamental but extremely complicated. AI's autonomy is the main concern that the proposed legal frameworks are trying to regulate. When confronted with the question on whether the autonomy will go beyond the restraints set by a human. The answer may depend on whether 'external inputs'[911] are needed for the proper

---

[904] Department of Economic& Sociala Affairs, *The impact of the technological revolution on labour markets and income distribution* (31 July 2017).
[905] European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence COM(2021)206 final (AI Act), Annex III.
[906] Stefan Wrbka and Mark Fenwick, *The Cambridge Handbook of AI and Consumer Law.*
[907] Georg borges, Christoph sorge, Law and Technology in a Global Digital Society Autonomous Systems, Big Data, IT Security and Legal Tech (Springer, 2022).
[908] Nikos Th. Nikolinakos, EU Policy and Legal Framework for Artifi cial Intelligence, Robotics and Related Technologies- The AI Act Volume 53 (Law, Governace and Technology Series 53, Springer)
[909] European Commission (2018)/237 on Artificial Intelligence for Europe.
[910] James Clayton, ''Overwhelming consensus' on AI Regulation-Mask', (14 September 2023) <https://www.bbc.co.uk/news/technology-66804996 >
[911] Sebastian Scholtysek, 'ÔWann ist ein Roboter ein Roboter?', <http://www.roboterwelt.de/magazin/wann-ist-ein-roboter-ein-roboter >asessed on 01 November 2017).

operation of the machine. Additionally, how can an 'inventive step by a machine' be credited to a human being?[912] That is where the law should actively take a position in this debate. Where should AI stop and be responsible for its actions? And where, the human also being included, should be partially or fully responsible? The law should and can produce an innovative framework to either reflect the changing nature of 'autonomous systems like AI[913] or to disrupt those advancements. The need is urgent since if legislators slow down such process, it could be taken as granted that law reacts only under 'existing technological developments.'[914]

4.1 The task of attaching liability to an AI machine

Imposing liability to a machine has been the subject of ongoing debates in the last couple of years. Strict liability for providers and users of high risk is desired under many worldwide proposals and thus 'rank high on the list of possibly applicable tools' of regulating the AI.[915] But in the context of strict liability, AI can hardly satisfy the requirements that tort law has set. As a result of AI's 'technical particularities,' the law's massive gaps become apparent, since it has not regulated anything like machines before.[916] The determination of a machine's 'behaviour' is obviously a hard task to accomplish. This is evidenced in the European Commission's Regulation Proposal 2021, not including direct provisions for the civil liability of AI schemes.[917] Furthermore, the challenge that this could bring globally demonstrates the legal uncertainty in this context. One important contribution was the JURI's (European Parliament's Committee on Legal Affairs) recommendations.[918]

Logically, adapting a framework which establishes liability for such systems, would involve compensation schemes given to successful claimants, under civil law. But establishing compensations under these uncertain and unregulated circumstances is obviously a complicated task, as argued by the JURI.[919] This is attributed to cybersecurity and protection of data being not strongly based systems. Introducing two limps to this debate including strict

---

[912] Georg borges, Christoph sorge, Law and Technology in a Global Digital Society Autonomous Systems, Big Data, IT Security and Legal Tech (Springer, 2022)
[913] Ibid.
[914] MONIKA SIMMLER and NORA MARKWALDER, 'GUILTY ROBOTS? – RETHINKING THE NATURE OF CULPABILITY AND LEGAL PERSONHOOD IN AN AGE OF ARTIFICIAL INTELLIGENCE' (2019) 30 Crim Law Forum 1.
[915] Stefan Wrbka and Mark Fenwick, *The Cambridge Handbook of AI and Consumer Law.*
[916] Ibid.
[917] Ibid.
[918] Committee on Legal Affairs draft report of 27 April 200 with recommendations to the Commission on a civil liability regime for Artificial Intelligence, 2020/ 2014 (INL) (JURI AI draft report).
[919] ibid 25.

liability for risk AI systems and fault-based liability of other AI types, had a logical rationale behind. However, unsurprisingly many disagreed to some specifics in this proposal. It may be logical to find liable the implementer of the AI system under both limps.[920] Even if this sounds fair, despite the fact that the deployer may have not in fact created that risk, in practical legal terms it is challenging. As Borges and Sorge claim, the absence of relevant case law does not help the proposed definition of the 'deployer'.[921] If the deployer is 'exercising control over the associated risk', that may be the boundary in which they will be liable, although a presumption towards them is evident after a quick read of the recommendations.[922] And controversially, the 'existing non-fault keeper liability rules' continue to be adopted in the European Union countries.[923] Nonetheless, the differentiation between the different types of harm, is a useful addition to this debate. The later AI Regulation Draft which adopted some of the JURI's initiatives, cleared this uncertainty of the 'deployer' and included the word 'operator of the AI system' with broader interpretative meaning. [924] But once again, the definition finds controversies in practise. One could question why only a person who 'on continuous basis' is included in running such technology.[925] The suggestion in the Bertolini Report which included the influence on the AI's decision-making procedure as a possible step to find the extend of liability, is an interesting one. But again, it determined that a variety of factors should be taken into account when producing a framework for AI systems, to avoid uncertainty and thus injustice under the law.

4.2 A working consensus

Evidently, the countries are free to adapt their own national laws regulating such issues. But as the Explanatory Memorandum indicates, these adoptions could result in 'legal fragmentation' in different legal areas and thus affect as a result the 'internal market'.[926] Even though, there are 'always some overlaps among rules and institutions,' because policy concerns vary within different countries, a 'baseline' could be argued to exist.[927] The security net and restrictions that people should adopt to protect them from possible drawbacks is evident. This is because

---

[920] Ibid.
[921] Stefan Wrbka and Mark Fenwick, *The Cambridge Handbook of AI and Consumer Law.*
[922] Ibid.
[923] Ibid.
[924] Ibid.
[925] Committee on Legal Affairs draft report of 27 April 200 with recommendations to the Commission on a civil liability regime for Artificial Intelligence, 2020/ 2014 (INL) (JURI AI draft report), Article 3.
[926] Stefan Wrbka and Mark Fenwick, *The Cambridge Handbook of AI and Consumer Law.*
[927] Jacod Katz Cogan, 'The idea of fragmentation' (2011) Harmony and Dissonance in International Law 123.

as any new addition to the society, AI needs its own legal regulation to operate properly. In relevance to this, the different legal personality of the machine that has been mentioned by the European Parliament is under a numerous critique.[928] A possible view will support that in the future 'machines and humans' may be treated equally under the eyes of the law.[929] Many agree that innovation could be reenforced by AI, but do not disregard the important of security within this process. As such, in relevance to robotics, a future legal framework should ensure that it covers sociopsychological implications as well as the ethical implication that may arise within it.[930] While practically this will sound extremely complicated, legislators should keep in mind the 'overvaluation of the actual capabilities of even the most advanced robots' when establishing its separate legal personality.[931] Afterall, the intention behind the Convention for the Protection of Human rights and Fundamental Freedoms was not to protect the rights of a dry machine. Rather, as many people signed under an open letter to the EU, it is the protection of human beings and innocent third parties that should be the main goal of the European Union.[932]

5. Ascribing Legal personhood

Due to the rather challenging ability to attribute liability in relevance to harm caused by AI systems, Wrbka and Fenwick argued that legal personhood could be added 'as a supplementary option, if made in appropriate terms, to enhance access to justice'.[933] This would mean that if there is a possibility that some AI machine is included in a civil wrong, it could hold legal personhood. In other words, it could be seen as a person in the eyes of the law.

In the civil field, this would make sense. In the context of combined complicated worldwide licences and agreements involving hardware integration of software, as physical persons would not need to be identified. This could minimise costs effectively.[934] Although this would not make sense in a morally constituted discussion, and go against the protection discussed above, it could practically ensure solutions to the compensation schemes issues. If the European

---

[928] European Parliament resolution of 16 February 2017 on possible evolutions of and adjustments to the current institutional set-up of the European Union (2014/2248(INI)) (2018/C 252/22)

[929] Georg borges, Christoph sorge, Law and Technology in a Global Digital Society Autonomous Systems, Big Data, IT Security and Legal Tech (Springer, 2022)

[930] Open Letter to the European Commission Artificial Intelligence and Robotics, <http://robotics-openletter.eu >

[931] Ibid.

[932] Ibid.

[933] Stefan Wrbka and Mark Fenwick, *The Cambridge Handbook of AI and Consumer Law.*

[934] Ibid.

Union's adoption of insurances for AI models is made, then it may provide faster compensation schemes and move the liability imposing to the insurers of such systems.[935] In terms of fairness, this is a sound approach since the insurer accepts responsibility and risks being liable for any AI issues that may arise in the future. The AI, the machine without any sign of ownership of property, can become a legal person with the condition that such insurance is implemented. The European Parliament in 2017 suggested a strict liability and supported the idea that obligatory insurance for autonomous systems would be a good addition to stabilise some of those issues.[936] But considering that this would be mandatory, the persons who operate the system would be responsible for such adoption.[937]

5.1 Implications to criminal Liability

Additionally, the higher risk is involved in the field of robotics where criminal liability is argued to be relevant. Whereby, a robot is a 'suitable agent of responsibility'[938] depending on practical factors as well as social ones. Of course, this does not concern the robot that were purposely programmed to act in such a prohibited way as under current criminal law legislation they would be liable.[939] Rather, it could involve mistakes under programming, insufficient risk management and due diligence. But the idea that the adoption of such a legal personality would 'keep moral philosophy busy' stands. This is because, under a moral consideration it can be argued that robots cannot be the ones fundamentally responsible 'agents' and neither they can understand the idea and purpose of punishment.[940] It could be supported that it is more sensible to hold responsible the 'manufacturer or the programmer' of such robot.[941] This is practically more convenient since proving the *mens rea* of the robot is a challenge. Furthermore, the determination of the terms under which the machine could be culpable to criminal liability is

---

[935] G Borges,'New Liability Concepts: The Potential of Insurances and Compensation Funds' Liability for Artificial Intelligence and the Internet of Things, 145

[936] Georg borges, Christoph sorge, Law and Technology in a Global Digital Society Autonomous Systems, Big Data, IT Security and Legal Tech (Springer, 2022)

[937] Stefan Wrbka and Mark Fenwick, *The Cambridge Handbook of AI and Consumer Law.*

[938] MONIKA SIMMLER and NORA MARKWALDER, 'GUILTY ROBOTS? – RETHINKING THE NATURE OF CULPABILITY AND LEGAL PERSONHOOD IN AN AGE OF ARTIFICIAL INTELLIGENCE' (2019) 30 Crim Law Forum 1.

[939] Gless, Silverman and Weigend, 'ÔIf Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability', New Criminal Law Review 19(3) (2016), 415.

[940] Ibid.

[941] MONIKA SIMMLER and NORA MARKWALDER, 'GUILTY ROBOTS? – RETHINKING THE NATURE OF CULPABILITY AND LEGAL PERSONHOOD IN AN AGE OF ARTIFICIAL INTELLIGENCE' (2019) 30 Crim Law Forum 1.

elusive.[942] Importantly, this idea would go against the inherent notion of the criminal legal theory.[943] If someone is found to be at 'fault,' it is prominently because that person intended such action and 'have had the opportunity to behave in different manner.'[944] Some believe that free will is only part of the society and not part of the criminal justice system.[945] Monika and Nora argue that humans in the future are more likely to 'experience this autonomy' of robots, powered with 'capacities' to act freely.[946] However, it is questionable how a robot can actually be included in a society or norms which made humans understand their rights and responsibilities. Although as Monika and Nora argue, 'the attribution of capacities is a normative process,' it cannot be easily and wholly understood the way in which robots could be introduced in the society. Societal norms at the time, are the basis on which the definition of a 'person' will develop.[947] Even if 'social interaction is not biophysical in character,'[948] recent studies only show some 'personable, expressive robots'.[949] Those do not demonstrate their ability to be wholly introduced in the society and its legal frameworks. Only if the future technological advancements are made to consider such 'ePersons' 'equal' to humans, 'in the sense that they are constituted as addresses of normative expectations'[950], then that idea may be more comprehensible. Even if experts are positive about the possible decision-making abilities of robots in the future,[951] the 'instability' caused by technological advancements does genuinely not support such argument.[952]

---

[942] Ibid.

[943] Calo,ÔRobotics and the Lessons of Cyberlaw', (2015) 103 California Law Review.

[944] MONIKA SIMMLER and NORA MARKWALDER, 'GUILTY ROBOTS? – RETHINKING THE NATURE OF CULPABILITY AND LEGAL PERSONHOOD IN AN AGE OF ARTIFICIAL INTELLIGENCE' (2019) 30 Crim Law Forum 1 , Wohlers,Ôindividualverkehr, 'Jahrhundert: das Strafrecht vor neuen Herausforderungen', (2016) 3 Basler Juristische Mitteilungen 114.

[945] Ibid.

[946] Ibid.

[947] Ben Chester Cheong, 'Granting legal personhood to artificial intelligence systems and traditional veil-piercing concepts to impose liability' (2021) 1 SN Soc Sci 231 <https://doi.org/10.1007/s43545-021-00236-0 >

[948] MONIKA SIMMLER and NORA MARKWALDER, 'GUILTY ROBOTS? – RETHINKING THE NATURE OF CULPABILITY AND LEGAL PERSONHOOD IN AN AGE OF ARTIFICIAL INTELLIGENCE' (2019) 30 Crim Law Forum 1 , Wohlers,Ôindividualverkehr, 'Jahrhundert: das Strafrecht vor neuen Herausforderungen', (2016) 3 Basler Juristische Mitteilungen 114.

[949] Adriana Hamachera, Nadia Bianchi-Berthouzeb, Anthony G. Pipec and Kerstin Ederd, 'Believing in BERT: Using expressive communication to enhance trust and counteract operational error in physical Human-Robot Interaction' <https://arxiv.org/pdf/1605.08817 > .

[950] MONIKA SIMMLER and NORA MARKWALDER, 'GUILTY ROBOTS? – RETHINKING THE NATURE OF CULPABILITY AND LEGAL PERSONHOOD IN AN AGE OF ARTIFICIAL INTELLIGENCE' (2019) 30 Crim Law Forum 1 , Wohlers,Ôindividualverkehr, 'Jahrhundert: das Strafrecht vor neuen Herausforderungen', (2016) 3 Basler Juristische Mitteilungen 114.

[951] Beck, 'ÔGrundlegende Fragen zum rechtlichen Umgang mit der Robotik', (2009) 6 Juristische Rundschau 230.

[952] MONIKA SIMMLER and NORA MARKWALDER, 'GUILTY ROBOTS? – RETHINKING THE NATURE OF CULPABILITY AND LEGAL PERSONHOOD IN AN AGE OF ARTIFICIAL

5.2 Exercising property rights

Implications arise also in the field of property ownership. This is exceptionally important since, as Rafael posits, it 'relies on the most valuable property today: data.'[953] Even if now the AI is only deemed as a tool, agency law is not far away in adopting robots within their definition of agents.[954] This may be logical since under the Deiser's definition personality is only recognised where there is some property owned.[955] Of course in human history there have been many debates about who can hold property and who was in fact property, which were given an end by the 'changing of social values affecting a change in legal constructs.'[956] This 'transition' shows that AI holds possibilities in the legal personhood debate.

In agency law, the introduction of AI has complicated its rather 'easily satisfied' definition of personhood.[957] Nonetheless, such systems may improve 'corporate decision making' making the agency law keener to recognise their personhood.[958] As AI's autonomy grows, more unexpected results will come forward. This is relevant where, even under current circumstances AI operating under human assistance, to the future where it is likely that it will be included in 'possessing and controlling' properties which may be unfamiliar from humans.[959] This could result in the impression that AI 'manipulates, controls, and possesses data and digital property.'[960] However, agency law can 'prerequisite for the exercise of property rights for nonhumans.'[961] This is practically adopted in the corporate context where corporations legally own property. The problem is to what extent this right to property should be granted. Under the general rules of property law, taking 'actual possession', control or dominion over a property' is a requirement to exercise those rights.[962] 'Constructive possession' from a machine

---

INTELLIGENCE' (2019) 30 Crim Law Forum 1 , Wohlers,Ôindividualverkehr, 'Jahrhundert: das Strafrecht vor neuen Herausforderungen', (2016) 3 Basler Juristische Mitteilungen 114.

[953] Rafael Dean Brown, 'Property ownership and the legal personhood of artificial intelligence' (2021) 30 Information & Communications Technology Law 2.

[954] Ibid.

[955] G Deiser,'The Juristic Person' [1908] 48 U Pennsylvania L Rev 131.

[956] Rafael Dean Brown, 'Property ownership and the legal personhood of artificial intelligence' (2021) 30 Information & Communications Technology Law 2.

[957] DALTON POWELL, 'AUTONOMOUS SYSTEMS AS LEGAL AGENTS: DIRECTLY BY THE RECOGNITION OF PERSONHOOD OR INDIRECTLY BY THE ALCHEMY OF ALGORITHMIC ENTITIES'.

[958] Ibid.

[959] Rafael Dean Brown, 'Property ownership and the legal personhood of artificial intelligence' (2021) 30 Information & Communications Technology Law 2.

[960] Ibid.

[961] Ibid.

[962] C Rose,'Possession as the Origin of Property' [1985] 52 U Chicago L Rev 73, R Nimmer,'Revised Article 9 and Intellectual Property Asset Financing' [2001] 53 Maine L Rev 287, 292.

can happen in a more obvious way[963] from a machine rather than a company or any other nonhuman could, [964] but human assistance will be needed in some circumstances. This specifically true in the current 21st century where some AIs are 'weak' and 'even unsupervised AI requires limited human assistance.'[965] This intervention of humans in the exercise of property rights from an AI robot could be more easily accepted. However, as Rafael believes, the issue would be with stronger AI where they could theoretically take independently actual possession of property. AI robots could 'exercise beyond the control of laws and human beings.'[966] This could possibly happen due to the robots' belief that 'they think they know more than they do, and they think they are smarter than they actually are.'[967] And again this is where the law should and could intervene, since if the courts do not provide machines with legal personhood, they 'would not be able to fully exercise its property rights despite its autonomy.'[968] Of course, the 'inability' to exercise property in the ordinary way may not be a strong argument to deny legal personhood, but the previous discussion of 'enforcing punishment or liability' may be more arguable and consistent.[969] The problem still remains even if people hold their own beliefs under the labour principle of property rights and in the idea that property rights are necessary part of the exchange of goods in an economically based society:[970] AI is a threat if it is not regulated properly.

6. Conclusion

As showcased, there are many difficulties in adopting a consistent legal framework to regulate the downsides of the AI's operation. Legal regulation requires 'cross disciplinary research.'[971]

---

[963] Rafael Dean Brown (2021) Property ownership and the legal personhood of artificial intelligence, Information & Communications Technology Law, 30:2, 208-234, DOI:10.1080/13600834.2020.1861714

[964] S Solaiman,'Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy' [2016] 25 Arti cial Intelligence L 245.

[965] Raf Rafael Dean Brown, 'Property ownership and the legal personhood of artificial intelligence' (2021) 30 Information & Communications Technology Law 2.

[966] Ibid.

[967] Elon Musk famously gave an apocalyptic prediction about the existential risk AI poses to humans. C Cli ord,'Elon Musk:"Mark My Words— A.I. is Far More Dangerous than Nukes"' CNBC (13 May 2018) <https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html > accessed 27 November 2020, C Domonoske,'Elon Musk Warns Governors: Arti cial Intelligence Poses"Existential Risk" National Public Radio (2017) <http://www.npr.org/2017/07/17/537686649/elon-musk-warns-governors-arti cial-intelligence-poses-existential-risk >accessed 27 November 2020.

[968] Rafael Dean Brown, 'Property ownership and the legal personhood of artificial intelligence' (2021) 30 Information & Communications Technology Law 2.

[969] Rafael Dean Brown, 'Property ownership and the legal personhood of artificial intelligence' (2021) 30 Information & Communications Technology Law 2.

[970] Ibid.

[971] Georg borges, Christoph sorge, Law and Technology in a Global Digital Society Autonomous Systems, Big Data, IT Security and Legal Tech (Springer, 2022).

It has been highlighted that this is not a simple task since many complications may arise in trying to attribute liability to AI machines. Furthermore, the paper has argued that the possibility of recognising separate legal personhood for machines depends on the constant changes in societal norms. Nonetheless, this is shown to be complicated as many orthodox notions as possible areas of various legal fields may be affected, particularly in the criminal law and property law systems.