frontiers
in Computer Science

ORIGINAL RESEARCH
published: 12 January 2022
doi: 10.3389/fcomp.2021.779957

AI Applications and Regulation: Mapping the Regulatory Strata

Mika Viljanen and Henni Parviainen*

Faculty of Law, University of Turku, Turku, Finland

Many accounts suggest that artificial intelligence (AI) law is still in its infancy with few statutes and other regulatory instruments regulating AI development and use. In this paper, we argue that such accounts are misguided. AI applications exist in a rich regulatory landscape, subject to multiple rules. To demonstrate our claim, we conduct two semi-fictional case studies under Finnish law. In the first case study, we chart the rules that currently would govern and impact AI tool use in recruitment. In the second case study, we map the legal framework for the Finnish COVID-19 contact tracing app. The article makes three contributions to the literature. First, the case studies provide ample evidence that the prevailing orthodoxy misstates the state of AI law. There is AI law on the books and existing laws have a profound impact on AI application design. Second, the mappings provide building material for developing a grounded theory framework for categorizing AI law and its types and modalities, allowing us to formulate a heuristic for understanding AI regulation. We argue that developers and AI application stakeholders should construe AI law as a complex stratigraphy consisting of five layers: data rules that regulate data use, application-specific AI rules that target specific AI applications or application domains, general AI rules that apply to a wide range of AI applications, application-specific non-AI rules that apply to specific activities but not to AI specifically and general non-AI rules that apply generically and across domains. Third, we provide guidance for practitioners for structuring AI compliance processes. We argue that practitioners should keep in mind that the rules and standards differ in their scopes, targets, certainty, and regulatory modalities. Consequently, understanding the AI regulatory landscape requires developing an understanding of multiple rule complexes, their dynamics, and regulatory modalities.

Keywords: artificial intelligence, regulation, regulatory landscape, AI development, AI use

OPEN ACCESS

Edited by:
Rebekah Ann Rousi,
University of Vaasa, Finland

Reviewed by:
Jenni Hakkarainen,
University of Helsinki, Finland
Adamantios Koumpis,
RWTH Aachen University, Germany
Suvi Sankari,
University of Helsinki, Finland

****Correspondence:***
Mika Viljanen
mivevi@utu.fi

Specialty section:
This article was submitted to
Human-Media Interaction,
a section of the journal
Frontiers in Computer Science

Received: *20 September 2021*
Accepted: *15 December 2021*
Published: *12 January 2022*

Citation:
Viljanen M and Parviainen H (2022) AI Applications and Regulation: Mapping the Regulatory Strata. Front. Comput. Sci. 3:779957. doi: 10.3389/fcomp.2021.779957

INTRODUCTION

Many accounts suggest that the artificial intelligence law is still in its infancy with few clear hard legal rules, statutes, and standards available to guide developers and users in implementing AI applications (see e.g., Scherer, 2016; Guihot et al., 2017). The infancy thesis gives AI law discussions a speculative, forward-looking character, with commentators often advocating for various potential future approaches to AI regulation. Some of the propositions call for aggressive measures, while others argue for lighter touch regulation to facilitate innovation and growth. The accounts often also stress the difficulties inherent in AI regulation (see e.g., Guihot et al., 2017; Butcher and Beridze, 2019; Erdélyi and Goldsmith, 2020), for example, arguing that AI regulation will constitute a challenge to regulators as the nature of AI applications will likely render attempts at traditional government regulation by national states ineffective and inadequate (see e.g., Guihot et al., 2017; Wallach and Marchant, 2019).

While law is diagnosed as either being absent or in its infancy, an ethics framing has emerged to dominate the AI discussions with countless government initiatives, NGOs, and academics exploring how to make sure that AI will be ethical. In some accounts, the regulation and ethics framings, however, interact (Larsson, 2020). The ethics framing is understandable: if hard regulation is absent, ethics constitute the only available frame for sustainable governance efforts. Simultaneously, insistence on ethics may also be a strategic move designed to pre-empt regulatory action (Hagendorff, 2020) and sustain the utopian projects of digital freedom (Cohen, 2019). Ethical AI, arguably, does not need regulation.

In this article, we argue that the AI law infancy thesis together with the dominance of the ethics framing, in fact, builds on a misguided understanding of the AI law landscape and may lead to misinformed design processes. As for example the EU High Level Expert Group Guidelines (AI HLEG, 2019) and the Commission White Paper (European Commission, 2020a) suggest, legal instruments already significantly constrains both AI development processes and use (see also European Commission et al., 2021). Academic research has, however, failed to account for the breadth and depth of existing law affecting AI application, make its composition and sources visible, and, consequently, mischaracterized its nature.

In this paper, we aim to address the research gap on real-life AI law by engaging in two fictional case studies that provide material for exploring what regulatory instruments already exist and govern AI applications. The first case study discusses AI application use in recruitment, while the other study focuses on a fictional COVID-19 contact tracing app, modeled after the Finnish Koronavilkku mobile application. We chose the cases to explore domains where AI law appeared dense and significant. Of course, the choices have their limitations. First, the case studies do not constitute a representative sample of all AI application domains. To mitigate the risk, we also draw on our knowledge of and engagements with other AI application contexts to build an overall understanding of the AI law landscape. Second, we conducted the case studies under Finnish law. The findings will, however, likely have relevance for the EU area as relevant legislative frameworks likely converge to a degree on the issues we discuss. The risks flowing from national deviations are further mitigated by the article design and objectives. If the details were to differ, discussion of Finnish serve as a substantive record on which to draw on in developing a grounded theory stratigraphy of AI law and also identifying practical implications and future research directions.

Building on the case study findings, we present a heuristic *stratigraphy* of AI law as a framework for understanding existing AI-related laws in Finland and, as an extension, in the EU. In geology, stratigraphy examines layered formations of lithic or biological material and their composition. We argue that the idea of stratigraphy offers an apt description of AI-related law we encountered in our case studies. In both cases, AI-related law comprised of multiple layers of rules with widely divergent scopes and regulatory modalities. However, layers of (1) data rules, (2) application-specific AI rules, (3) general AI rules, (4) application-specific non-AI rules, and (5) general non-AI rules were visible in both cases. The layers were of uneven composition, firmness, and relevance.

The article proceeds as follows. First, we will, in sections Case 1: Recruiting people and Case 2: Tracking COVID-19, report our case study findings. In section An AI law stratigraphy, we develop a heuristic AI law stratigraphy and, in section Implications, discuss the implications of our research.

CASE 1: RECRUITING PEOPLE

The first fictional case study focuses on AI use in recruitment. We assumed that an automotive assembly company based in Finland seeks to hire 400 new employees within a few weeks. To facilitate the process, the firm plans to use an AI-based tool to help in sourcing the applicants, screening applications, testing applicants, and analyzing video interviews. While AI tools may offer significant benefits such as cost savings, shorter processing times and better-quality recruitment decisions (see e.g., Guenole and Feinzig, 2018; Pillai and Sivathanu, 2020; Laurim et al., 2021), the techniques may also pose considerable risks among others on the applicants' rights to privacy and equal treatment (see e.g., Custers and Ursic, 2018; Kelly-Lyth, 2021). In the case study, a complicated picture of rules appears. AI recruitment tools are set in a complex regulatory landscape. In the following, we outline the landscape starting with applicable data protection rules.

Data Protection Rules

Data protection rules constitute the first obvious hurdle the company and its software vendor will face in designing and deploying the AI-based recruitment tools. In recruiting people, the employer will inevitably collect vast amounts of personal data, potentially raising privacy and data protection concerns. Personal data processing is subject to intense regulation in the EU, in particular under the *General Data Protection Regulation* (2016/679/EU, GDPR), but fundamental rights to privacy and data protection are also recognized in several international conventions, such as the *EU Charter of Fundamental Rights* (2012/C 326/02), and in the *Constitution of Finland* (731/1999). In addition, privacy rules may also be relevant even if personal data is not processed, but AI-based decisions affect individuals.

The GDPR provides a starting point for charting the applicable data protection rules. The main rule in the GDPR is that personal data processing is forbidden unless the data controller may justify processing by appealing to a *lawful basis* for processing. The lawful bases include, for example, consent, legislative mandates, and controller legitimate interests. However, GDPR provisions are semantically contrived, remain contested in their details, and vary depending on the type of data processed (see e.g., Carey, 2018; Sartor et al., 2020).

The processing ban is relevant for both software developers and the AI application end users. Developers must have a lawful basis for processing the personal data they use to develop the AI application, while end users need a lawful basis for the deployment phase processing. In addition to lawful basis rules, the GDPR contains a number of other significant rulesets. The Regulation also imposes a set of requirements on what rights developers and end users must grant to the data subjects and what accountability and security measures they must implement.

Further, the qualified ban on automated decision-making contained in GDPR Article 22 is important in AI recruitment contexts. The ban sets limits on the recruiters' use of automated recruitment decision tools, but automated decision-making could be allowed, if some of the exceptions listed in Article 22 apply and appropriate safeguard measures are implemented. Consequently, when designing the recruitment processes, the employer and AI developer should ensure either that the AI recruitment system does not make automated decisions, or, if it makes such decisions, the decision framework must comply with all the requirements set in the GDPR. Similarly, the explainability requirements embedded in the GDPR may significantly affect AI application development and use.

The GDPR, although best known of data protection instruments, is by no means the sole source of data protection rules. Member State national rules often supplement the rules. The *Data Protection Act* (1050/2018) and the *Act on Services for Electronic Communications* (917/2014) lay out the general national framework for data protection in Finland. However, a wide range of recruitment-specific data protection rules also exist.

Unlike the general data protection rules, the recruitment-specific data protection rules typically target employers only. To comply with such requirements, developers must know their customers and the regulation applicable to their activities, as the rules may impose significant constraints on both data availability and AI application functionality. The *Act on Protection of Privacy in Working Life* (759/2004) constitutes the base layer of context specific data protection rules. The Act, first, constrains the sources from which the employer may lawfully obtain applicants' personal data. The primary rule is that employers may only collect data directly from the applicants. Other sources, including, for example, social media, can be used only with the applicants' consent. Second, the Act restricts how employers can use health data and personality and aptitude assessments. Third, the Act also constrains how background, credit history, and drug tests may be conducted. Further important limitations on background checks flow from the *Security Clearance Act* (726/2014) that allows the intelligence services to conduct security clearance processes, but only if the position the applicant is seeking makes it eligible for clearance. The *Act on Checking Criminal Background of Persons Working with Children* (504/2002) mandates that employers seek a criminal records extract if the applicant is to work with children. The *Occupational Health Care Act* (1383/2001) regulates how employers can use medical examinations.

In addition to imposing data availability limitations, legislative instruments also require that employers actively acquire information about the applicants. For example, the *Communicable Diseases Act* (1227/2016) mandates that employers under certain conditions process personal data on vaccinations and disease certificates, whereas the *Young Workers Act* (998/1993) requires the employer to obtain evidence of minor applicants' age and school attendance. The *Aliens Act* (301/2004) obliges employers to ensure that alien applicants have residence permits.

While data rules both constrain and mandate data processing, the *Act on Public Employment and Business Service* (916/2012) affects AI applications through another channel. The Act sets the legislative frame for state provided recruiting services and facilitates data connections to the Public Employment and Business Service registries, on the condition that the applicant has given consent to data transfers. The opportunity of using government data may affect AI application architecture designs.

Non-discrimination Rules

While data protection rules impose significant constraints, other non-data focused regulatory complexes such as non-discrimination and equal treatment rules are also highly relevant in recruitment context. For example, while employers enjoy a considerable freedom of choice in choosing whom to employ, the acceptable choices are constrained by the *non-discrimination rules*. The *EU Regulation on Freedom of Movement for Workers within the Union* (492/2011) explicitly prohibits the use of medical, vocational or other criteria that result in discrimination on the grounds of the applicant's nationality. National rules, which implement the EU non-discrimination directives, restrict the space further. The *Non-Discrimination Act* (1325/2014) and the *Act on Equality between Women and Men* (609/1986) further constrain employers' freedom of action, outlawing both direct and indirect discrimination. The structure of the rules entails that recruitment decisions may not subject individuals to differentiated treatment based on protected characteristics such as gender, religion, political opinions, or health, unless "the treatment is founded on a genuine and compelling reason related to the type of occupational tasks and their performance, and the treatment is proportionate to achieve a legitimate objective." While non-discrimination laws apply in recruitment contexts, the *Employment Contracts Act* (55/2001) imposes an equal treatment obligation that dwarfs their scope and intensity. The Act requires that employers treat all their current employees equally in all respects, unless deviating from equal treatment is justified in view of the duties and position of the employees. Importantly, the obligation does not hinge on specific protected characteristics and may be relevant, for example, when sourcing job applications from current employees.

Process Constraint Rules

In addition to data and non-discrimination rules, many rulesets affect what processes should be implemented. The *Employment Contracts Act*, for example, may have an impact on the design of the digitalized contract drafting processes possibly used in AI recruitment systems by establishing rules on what information should be included in the employment contract or otherwise provided to the employees. Further, labor laws may also impact system designs. Under the *Act on Co-operation within Undertakings* (334/2007), the employer, who employs at least 30 persons, must arrange co-operation negotiations before implementing or making amendments to the recruitment practices or to principles and practices governing the processing of applicant personal data. If the employer falls under the rules applicable to community-wide groups of undertakings it might have to inform and consult the employee representatives also at the group level before introducing new or modifying existing AI recruitment systems if the new operational models result in changes to the working methods of the HR personnel. Implementation schedules must include sufficient time for co-operation processes to play out.

Fundamental Rights, IPRs, Liability Rules, and Standards

While we have already identified several rule complexes, the AI law picture remains incomplete. Several human and fundamental rights rules, first, figure prominently in recruitment contexts. In addition to respecting the privacy and data protection related fundamental rights, AI application developers and end users must navigate the possible restrictions that emanate from rules on freedom of thought, conscience and religion, freedom of expression, freedom to choose an occupation and non-discrimination, just to mention a few. While fundamental rights rules are not binding on private employers or AI developers as such, they may trigger the emergence of unwritten rules and typically guide the interpretation of statutory rules.

Similar to any commercial activity, intellectual property rights, second, may have a significant impact on developer actions during AI application development. Thus, developers and end users should be mindful of the impact the *Copyright Act (404/1961)*, the *Patents Act (550/1967)* and the *Act on Utility Model Rights (800/1991)* may have. Similarly, the *Trade Secrets Act (585/2018)* could restrict the use of certain solutions, as well as affect the way the algorithms used are protected.

Developers and end users should not disregard criminal law rules, as some of their actions could trigger criminal liability under the *Finnish Criminal Code (39/1889)*. It is conceivable that a developer or end user commit crimes, such as, discrimination and discrimination in employment, data protection offense, secrecy offense, eavesdropping and illicit observation, while working on or using an AI recruitment system. In addition, several of the other statutes, such as the Act on Protection of Privacy in Working Life, also include penal provisions. Acknowledging and managing criminal liability risk is important for both the AI developers and the employers. Tort and other compensatory liability should also be taken into account. Many of the statutes discussed above have specific liability rules embedded in them, but the general tort liability rules may also be relevant. Administrative sanctions cannot be disregarded either. The GDPR's high maximum fines are a notorious example.

Finally, in addition to the multifaceted terrain of applicable "hard" law, relevant soft law instruments are also in place and numerous more are in the making. For instance, the IEEE P7005—Draft Standard for Employer Data Governance could be of assistance for both employers and developers working on AI recruitment systems.

CASE 2: TRACKING COVID-19

The Finnish COVID-19 tracking app Koronavilkku (Ministry of Social Affairs Health, 2020) provides the backdrop for the second case study. The case study is semi-fictional. This is unavoidable as artificial intelligence currently plays a limited role in the COVID-19 tracing apps. Consequently, to illustrate the problems, we discuss the Finnish Koronavilkku app and assume that the app, counterfactually, would be used to issue quarantine orders.

The legal backdrop for COVID-19 tracing apps is complex and involves questions ranging from privacy to administrative decision-making.

Data Protection Rules

Similarly to the recruitment case, data protection rules constitute the first hurdle to deploying a contact tracing app. This was clearly visible when the debates around COVID-19 tracking applications commenced during early spring of 2020. Privacy advocates feared that governments would spin the apps to serve law enforcement and other surveillance purposes. While the most invasive tracking schemes were discarded in Europe early, the debate over the role of privacy came to a head in late March 2020. At the time, multiple European governments came out in support of projects that built on maintaining central user databases and allowing authorities to identify who had been exposed to the virus (Abboud et al., 2020). Cyber security and other academic actors argued that the approaches, first, contained significant cyber security vulnerabilities (DP3T Consortium, 2020a,b,d) and, importantly, were irreconcilable with the GDPR data protection requirements (DP3T Consortium, 2020c). In the end, privacy actors won the day as the governments gave in. Most European countries adopted the decentralized approach where all contact data would be stored on individual devices, and only the fully anonymized contact keys of the people who were diagnosed were shared within the system. The same happened in Finland. The Finnish *Koronavilkku* app implements the decentralized pan-European DP-3T design. In the app, mobile device Bluetooth beacons exchange unique encrypted identifiers when the devices come into close proximity with each other. The app stores the identifiers locally. If a user tests positive for COVID-19, the user can opt to share their own identifiers by entering a key provided by a health care provider. The identifiers are, then, broadcast to all users. If the app finds a broadcasted identifier among the identifiers it has stored, an algorithm analyzes the contact properties and, if the conditions are met, informs the user of a possible exposure to COVID-19. The use of the app is voluntary and anonymous. Informing other users of testing positive is likewise voluntary and anonymous. Authorities gain no access to information on who is using the app and who has been exposed (Köykkä and Kaikkonen, 2020).

The privacy-emphasizing design choices were informed by a multitude of considerations. The Finnish government acknowledged that the public had to be confident that the app protected the privacy of its users else the adoption rate would likely be low. The data protection landscape that forced the decisions is convoluted. Further, the GDPR privacy rules required that the app developers implement robust privacy protections and minimize data collection. Consequently, doubts over the legality of non-DP-3T approaches lingered. Here the complexities kicked in. The GDPR rules did not outright outlaw an app that would implement invasive data collection and use. The Member States could, potentially, allow such collection and processing through legislative means to pursue important public health related objectives.

However, even if the GDPR would, on its face, allow for national discretion on public health grounds, its data protection principles would, nevertheless, apply. When governments allow for the processing of health data, controllers must comply with, for example, the data minimization principle contained in GDRP Article 5(1)(c). The data minimization principle forces controllers to limit processing to the minimum necessary for the objectives the processing pursues. In COVID tracing app contexts, the principle requires that the authorities analyze what benefits increased collection and processing are likely to confer. Importantly, additional collection is not allowed without significant benefits. In COVID tracking apps, the benefits of additional collection proved meager.

Fundamental Rights and Constitution

In addition to the GDPR, Member State discretion is constrained by other instruments, chief among them the EU Fundamental Rights Charter and the respective Member State constitutions. The Charter buttressed the GDPR data minimization principle. As the EU Commission pointed out in its Recommendations, "pursuant to the Charter of Fundamental Rights of the Union, restrictions on the exercise of the fundamental rights and freedoms laid down therein must be justified and proportionate. Any such restrictions should, in particular, be temporary, in that they remain strictly limited to what is necessary to combat the crisis and do not continue to exist, without an adequate justification, after the crisis has passed." (European Commission, 2020b) Consequently, the individuals' fundamental rights together with the need to prevent surveillance and stigmatization required that processing was strictly limited to what is necessary to manage contagion. In addition, sunset clauses were inserted. The Charter based rules also resulted in a requirement that regular reviews be conducted on whether a continuing need for processing still existed and that the collected data was destroyed once it is no longer useful for the public health purpose.

While the EU framework was already restrictive, the Finnish constitutional norms further narrowed the maneuvering room available to the government. The Constitutional Committee, the body presiding over the interpretation of the Finnish Constitution, had already previously ruled that the Government must, to comply with the Constitution, act within the ambit of the GDPR rules (The Finnish Constitutional Law Committee, 2016). Further, any restrictions to basic and fundamental freedoms must meet the "restriction conditions test," a staple of Finnish constitutional law analysis. Under the test, any restrictions to fundamental rights and freedoms must be precisely laid out in a statute, limited to what is absolute necessary, and designed to be proportional to the objectives of the legislative measures. Consequently, the state is barred from collecting and processing any data that is not necessary for serving a legitimate government function.

The app design was, thus, informed by the GDPR and a host of both EU and Finnish constitutional rules. However, it is important to note that the constitutional restrictions, in fact, targeted the legislative bodies and restricted the legislators' freedom of movement in adopting laws that would, then, give the government and the health authorities the authority to act. It is easy to miss the underlying rule. At least in Finland, public authorities need a legislative basis for all administrative actions they take. This constitutional rule is a significant constraint on AI to be used for public administration purposes. Barring new laws, AI use must fit existing authorizations.

Constitutional Rules on AI Decision-Making

To explore the AI design constraints further, we must move over to the realm of the fictional. The Finnish government made a decision not to connect the Koronavilkku app to quarantine decision-making. The Koronavilkku amendment to the Communicable Diseases Act explicitly forbade the use of app exposure data as the sole basis for assigning a person to quarantine.

The decision flowed from existing law rules. While the GDPR Article 22 could have in theory allowed for AI based quarantine decisions if a statutory authorization existed, Finnish law rules rendered the approach unfeasible. Again, the backdrop was complex. The Government had in 2018 introduced a bill that would have allowed the Finnish Immigration Service to build automated decision-making systems. The Constitutional Law Committee, however, ruled that automated decision-making was not allowed if decision-making contained a discretionary element (The Finnish Constitutional Law Committee, 2019a) as such decision-making was incompatible with the Finnish Constitution. Furthermore, the Committee imposed a freeze on further automated decision-making initiatives until a general statute on automated decision-making was passed (The Finnish Constitutional Law Committee, 2019b) and, for example, criminal and civil liability issues resolved. Consequently, automated quarantine decisions would not have been possible.

AN AI LAW STRATIGRAPHY

Stratigraphy?

The two case studies suggest that AI applications are, in fact, already subject to intense regulation. There is, thus, AI law on the books. The existing AI law, however, makes up a complex stratified geology. The existing AI rules drastically differ in their character, makeup, and targets, have varied pedigrees, and emanate from a wide variety of institutional actors.

To facilitate mapping exercises by AI developers and users in the various application contexts, the article offers a *stratigraphy* of AI law. The idea of stratigraphy is taken from geology, where stratigraphy studies layered formations of lithic and biological material (On another use of stratigraphy metaphor in AI contexts, see Wood, 2021). We find stratigraphy an apt framework for understanding AI-related law. As lithic layers and sediments, rules that affect AI development and deployment constitute multiple strata with varying density, firmness. At times, regulation may be extremely dense with multiple overlapping instruments applicable in a specific use case, while in other use cases the normative material may be extremely porous or even non-existent. Similarly, the firmness of the normative material varies. Some rules impose clear cut "hard law" obligations backed up with credible threats of crippling sanctions, while others remain amorphous and speculative in their purchase and scope. Further, the depth dimension of the stratigraphy also offers a useful heuristic. In the stratigraphy we offer, uncertainty over the rules' potential impact on AI design processes and use grows the deeper we move in the stratigraphy. Developers and end users will be likely able to identify relevant data and application-specific AI rules relatively easily, but, for example, the exact contents and impact of general non-AI rules will likely remain uncertain until an analogous case is resolved by a court.

The stratigraphy we offer consists of five layers. The uppermost layer is made up of *data rules*. Data rules determine what data developers and users have access to and can use in AI applications. We segregate and place data rules on the top of our stratigraphy as they condition access to the raw material AI applications use, have unique features, and constitute the first feasibility hurdle in AI application development. Without legal data access for both development and deployment phases, development risks will likely be prohibitive. The second layer in our stratigraphy is made up of *application-specific AI rules*. Such rules explicitly target a specific AI application or application domain. While rare at the moment, the rules, such as the future EU AI Act, will constitute the primary future AI design constraints. The third layer contains *general AI rules* targeting specifically activities characteristic of AI use but not confined to particular AI applications or application domains. While the two categories inevitably bleed into each other, we argue that they should be kept conceptually separate as application-specific AI rules should constitute the primary area of interest for most developers. The fourth and fifth layers contain *non-AI rules*. These rules may, as well as AI rules, be application-specific or general. The different layers of our stratigraphy are depicted in **Figure 1**. In the following, we will examine each category of rules in more detail.

Data Rules

The first layer of the stratigraphy consists of data rules. The case studies showed that rules on how data can be collected, processed, and transferred play a crucial role in AI development and use. While crucial, the data rules layer is highly complex. As was seen in particular in the COVID-19 tracking case, the data rules layer is geographically fragmented. Data rules derived from multiple sources, even within the EU. While the EU GDPR was the primary source of data rules in both case studies, the ruleset was in both cases augmented by national data protection rules. Outside the EU, the picture is complicated. While data protection rules are typically less stringent outside the EU than inside, their variety and potential extraterritorial reach complicates the legal mapping processes.

Both cases, second, demonstrated that the data rules layer is highly uneven and granular. On the one hand, personal data may be subject to extremely intense regulation. While the GDPR applies to most personal data processing within the EU and imposes stringent restrictions on data use, the framework is augmented by numerous sectoral data rulesets, further increasing regulatory intensity. Data rules may at times combine with other rulesets to further constrain data availability. For example, Finnish public authorities are constrained in their data use by, first, the GDPR Article 6 rules that bar them from relying on the legitimate interest and consent grounds to justify data processing, second, the applicable sectoral data rules, and, third, the Finnish constitutional and administrative law rules that limit the scope of admissible administrative action. On the other hand, regulatory intensity might also be extremely light. For example, data use in industrial AI applications with no personal data implications is primarily governed only by database rights, trade secrecy rules and the background competition law norms.

The cases also suggested that the regulatory modalities, third, vary greatly in the data rules layer. GDPR is a prime example of the differences in regulatory modalities. The Regulation, first, imposes an apparent blanket ban on personal data processing, only to provide a number of lawful grounds for processing. The lawful grounds in turn, vary greatly in their character, ranging from data subject consent, contracts and data controller legitimate interests to explicit legislative authorizations, national security concerns, and data subject vital interests. These fairly traditional command-and-control rules are augmented by avantgarde privacy-by-default and privacy-by-design regimes that put in place complex institutional constraints on how data processing should be planned and implemented (Binns, 2017).

In sum, while data rules are important constraints in AI development, their heterogeneous nature will complicate developers' efforts as no one-size-fits-all solutions exist. Mapping the data rules layer relevant to a particular AI application requires developing a comprehensive, in-depth understanding of the data rules landscape and the fit of the application with the rules. The particular features of each use case such as the application context, end-user features, and system architectures affect what rules are applicable. As the rules are detailed and intricate compliance will require an integrated design approach where legal expertise is brought to bear on system architecture and system implementation decisions. The rule complexity, however, cuts both ways. While rules may constrain and inhibit certain activities, creative system architecture solutions may facilitate AI applications that, in their first iteration, were legally unfeasible.

Application-Specific AI Rules

The second layer in the AI law stratigraphy consists of application-specific AI rules. The rules target explicitly specific AI applications or application domains. These rules remain rare.

One specimen of such rules, however, stood out in the cases. In the COVID-19 case, unwritten rules of Finnish constitutional law ruled out many forms of automated decision-making in public administration. This ruleset has a complex pedigree. While

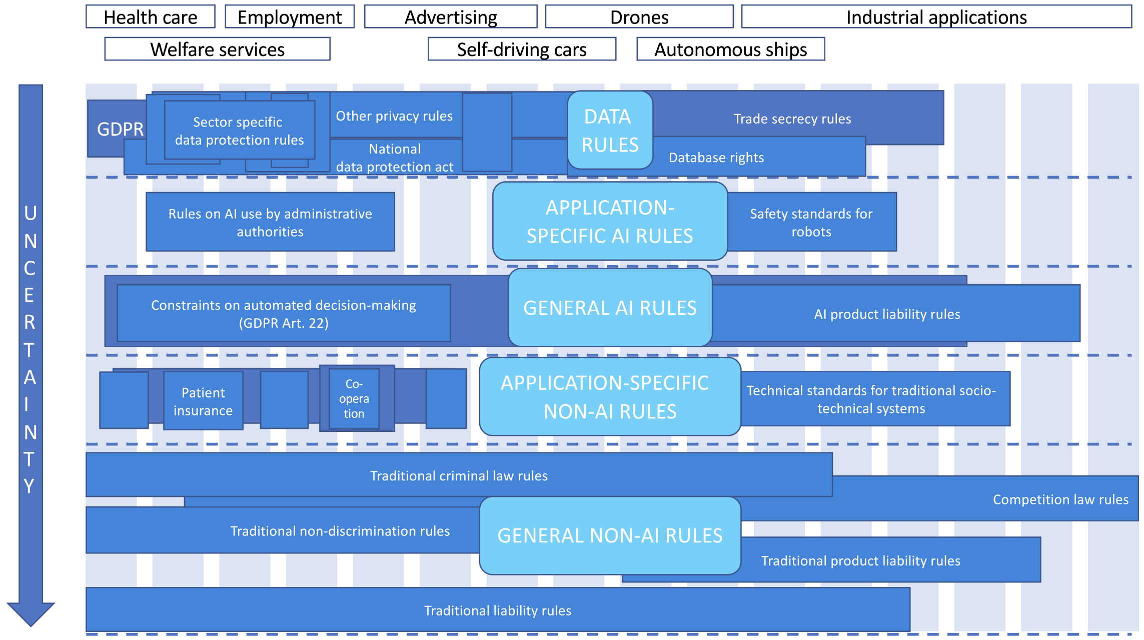
Health care
Employment
Advertising
Drones
Industrial applications
Welfare services
Self-driving cars
Autonomous ships
UNCERTAINTY
GDPR
Sector specific data protection rules
Other privacy rules
National data protection act
DATA RULES
Trade secrecy rules
Database rights
Rules on AI use by administrative authorities
APPLICATION-SPECIFIC AI RULES
Safety standards for robots
Constraints on automated decision-making (GDPR Art. 22)
GENERAL AI RULES
AI product liability rules
Patient insurance
Co-opera tion
APPLICATION-SPECIFIC NON-AI RULES
Technical standards for traditional socio-technical systems
Traditional criminal law rules
Competition law rules
Traditional non-discrimination rules
GENERAL NON-AI RULES
Traditional product liability rules
Traditional liability rules

FIGURE 1 | The AI Law Stratigraphy.

the Constitution remains silent on automated decision-making, the Constitutional Law Committee, the parliamentary body that presides over the interpretation of the Finnish Constitution, added detail through interpretation. The Committee held that rule of law, principles of good administration, individuals' due process rights, and the constitutional requirement that all exercise of public power should have its basis in Acts of Parliament constrain when automatic decision-making can be used. First, all automated decision-making by public authorities must be based on specific legislation, which unambiguously defines the scope of such decision-making. Decision-making should, second, be limited to situations where no discretion is used, and where decisions may be made by machines based on the legislation and known unequivocal facts. Third, the public sector automated decision-making must strictly comply with both substantive and procedural legislation.

While application-specific AI rules are currently few, they will likely increase in the future. In particular, the number and scope of technical product standards may explode. In such a case, the rules will probably differ significantly in their regulatory modalities, scopes, targets, objectives, and pedigrees. For instance, the regulatory modalities of application-specific AI rules could range from outright bans of specific AI technologies to detailed technical standards which regulate the makeup of AI systems, various explainability standards, development process standards, and liability rules. The EU AI Act proposal reflects this tendency. The proposal targets a limited roster high-risk AI application and puts forward a highly variegated regulatory template that combines prohibitions, management-based regulation, binding technology rules with complicate ex ante and ex post-conformity monitoring and hefty sanctions (Viljanen, 2021). The institutional pedigree of the rules may similarly be diverse, affecting the weight and purchase the rules will have. Bans, disclosure, and explainability standards will likely emanate from the traditional legislative actors and even constitutional rules and be backed by sanctions. The technical standards, on the other hand, are likely to emanate, instead, from more amorphous, non-governmental actors such as standardization organizations, yet the rules may, nevertheless, be *de facto* and *de jure* binding despite their origins.

General AI Rules

General AI rules make up the third layer in the stratigraphy. These rules are not specific to particular AI applications or domains and cover a wider area of potential applications. Although still rare, two such rules figured prominently in the case studies. First, the GDPR Article 22 semi-ban on automated decision-making was relevant in both cases. The article establishes significant restrictions on *decision-making solely based on automated processing of personal data*. If such automated processing produces legal effects or similar significant effects on individuals it may be only performed if the decision is necessary for entering into or performing a contract, authorized by law, or the data subject has given an explicit consent for processing. In addition, the data controller must put in place suitable safeguards to protect the data subject's rights, freedoms and legitimate interests. Thus, AI applications facing natural persons already encounter significant restrictions in Europe. Although at first glance extensive, the ban is, however, far from comprehensive (Brkan, 2019). The article is ambiguously worded and contains several uncertain elements. It is, for example, uncertain what kind of activities the notion of "automated decision-making" covers and how free of human intervention decision-making must be in order to fall under the ban. Systems where AI provides support to human decision-makers or where humans review the decisions are often on the borderline.

The requirement that automated decisions be explainable is established, again in vague terms, in GDPR Articles 13(2)(f), 14(2)(g), and 15(1)(h). Together with Article 12, they mandate controllers to provide data subjects meaningful information about the logic of automated decision-making in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Like the ban on automated decision-making, the explainability requirement remains ambiguous with scholars arguing over what actually is meant by meaningful information about the logics involved (see e.g., Goodman and Flaxman, 2017; Mendoza and Bygrave, 2017; Selbst and Powles, 2017; Wachter et al., 2017; Adadi and Berrada, 2018; Brkan, 2019; Casey et al., 2019; Miller, 2019; Brkan and Bonnet, 2020; Sartor et al., 2020). And authorities contributed guidelines (see e.g., ICO and The Alan Turing Institute, 2020). Nevertheless, the scope and contents of the requirement can only be ultimately clarified in future case law. Further, the complexity of AI systems may make it technically difficult to provide explanations of the logics that are meaningful to the individuals concerned (see e.g., Mittelstadt et al., 2016; Vedder and Naudts, 2017). This is likely the case, especially, if the explicability requirement has not been adequately addressed in the development phase. Trade secrets and intellectual property rights may also complicate the processes (see e.g., Burrell, 2016; Vedder and Naudts, 2017; cf. e.g., Tene and Polonetsky, 2013; Diakopoulos, 2016).

Both examples of general AI rules fail to provide closure, leading to the conclusion that many of the current general AI rules may still be emergent by their nature. Importantly, the emergent general AI rules may have surprising pedigrees and provenances in existing rules, further complicating the regulatory mapping processes. For example, had the COVID-19 pandemic begun before the Constitutional Committee had weighed in, anticipating the detailed constitutional constraints would have been challenging. Consequently, the AI law landscape will remain unsettled until future use cases trigger legal processes that force the law to encounter and internalize AI technologies. Of course, general AI rules may also be introduced in legislation. In the future, for example AI-specific liability rules could constitute an important part of the third layer (Bertolini and Episcopo, 2021).

Application-Specific Non-AI Rules

The fourth layer of the stratigraphy comprises application-specific non-AI rules. These rules target specific applications or application domains and apply whether AI is used or not. The stratum contains a diverse group of rules with highly varying regulatory modalities, scope, targets, objectives, and pedigrees.

For example, in the recruitment case, the legislative landscape was dominated by a plethora of EU directives that aim among others to protect the employees and job seekers. The directives have been implemented in the Member States in differing ways and are often supplemented by a complex set of national employment law rules, case law and, in Finland, collective bargaining agreements. The co-operation obligations discussed in relation to the recruitment case are an example of such EU based legislation with a national, Finland-specific twist. In the COVID-19 case, application specific non-AI rules were mostly invisible, yet provided the backbone for the legislative framework of Koronavilkku.

Here, one must bear in mind that application specific sectoral rules often impose significant constraints on regulated applications. AI use does not suspend the rules and action mediated by AI technologies falls under the scope of existing sectoral regulation if no specific exceptions exist.

Many of the sectoral rules relevant in AI contexts target entities with human presence. This is often reflected in the structure of the rules. Ships, for example, must have a master and a crew that serve particular rule-specified human functions. The human-oriented application-specific AI rules may serve as effective barriers to AI deployment. At least, the requirements the rules impose on action must be translated to the AI domain. These processes will infuse uncertainty into regulatory outcomes.

General Non-AI Rules

The fifth and last layer of the stratigraphy consists of general non-AI rules. The layer consists of a heterogeneous set of rules. These rules typically apply across action and sectoral domains and provide the general legal framework for behavior control. The rules do not target AI activities specifically, but non-AI rules may, nevertheless, have a significant impact in AI development and use contexts.

Antidiscrimination rules encountered in the recruitment case study are a case in point. The rules have an extensive scope and cover, under Finnish law, all private and public action but family and other private life and religious activities. Importantly, antidiscrimination rules are highly relevant in AI applications that face individuals. The rules, potentially, directly impinge on algorithm design, establishing constraints on what kind of data can be used, what decision-making parameters algorithms can incorporate, and what substantive decisions can be made. Unfortunately, the antidiscrimination rules are semantically and normatively open and remain emergent in their content.

For example, the Finnish Non-discrimination Act Section 11 prohibits all differential and unfavorable treatment of individuals on the basis of age, origin, nationality, language, religion, belief, opinion, political activity, trade union activity, family relationships, state of health, disability, sexual orientation or other personal characteristics. This much is relatively clear. However, the act also provides that differential treatment does not constitute discrimination in all cases. This is true, first, if the treatment based on a legislative mandate, has an acceptable objective, and the measures to attain the objective are proportionate. Second, where no legislative mandate exists, differential treatment is, nevertheless, not discrimination if the treatment has an acceptable aim in terms of basic and human rights, and the measures to attain the aim are proportionate. In the Act, the boundary between what is legal and illegal becomes *ex ante* blurred, requires forward-looking expert analysis, and remains highly dependent on the facts of each case.

Similar open-ended and ambiguity repeat in many other general non-AI rule contexts. Developers and users may find themselves facing a potentially applicable existing rule but little guidance as to how the rule is likely to be interpreted by enforcement bodies or by courts in the future disputes. This is particularly true for constitutional and basic and human rights rules. The rules often play a crucial role in AI contexts, but the detailed contents of law are notoriously difficult to predict. While guidance may be available from, for example, previous case law, only lawyers with expertise in human and basic rights jurisprudence are capable of retracing and assessing the likely argumentation patterns.

Tort law and criminal law offer a slightly different challenge. The rulesets contribute to providing a last resort background layer of behavioral controls in modern societies. Tort law imposes a strict liability for damage caused by particular activities and a general liability for damage caused by *negligent* action. AI developers should take the risk of both tort and criminal liability into account. However, both liability types build on anthropocentric conceptual foundations and are best equipped to deal with action taken by humans immediately. Consequently, how the rulesets can be applied in AI contexts is uncertain.

Non-discrimination, constitutional, tort liability and criminal liability rules only serve as examples of general non-AI rules. Other relevant rulesets, such as competition law and IPR rules, however, exist and may have an impact on AI development and deployments.

IMPLICATIONS

Above, we outlined a heuristic stratigraphy of existing AI-related law. Seen through the lens of the stratigraphy, AI law presents as a fragmented, highly convoluted patchwork of rules with diverse scopes, regulatory targets, and regulatory modalities.

While we are convinced that the five-layered stratigraphy offers a useful heuristic for classifying the existing AI regulation measures, we want to highlight five themes that are crucial to understanding what kind of material the regulatory strata consist of and how law, ultimately, affects AI development and deployments.

First, the case studies demonstrated that the detailed individual legal rules constitute the appropriate unit of analysis when analyzing the contents of AI-related law. Focusing on legislative instruments as the objects of inquiry is insufficient and will likely lead the analysts miss important regulatory inputs. Similarly, superficial scannings are likely inadequate. For example, the constitutional law dimensions of the COVID-19 tracing app demonstrated that while some instruments may at first sight appear completely irrelevant to AI development and use, they may, nevertheless, impose important constraints on development processes or AI application deployments. Consequently, practitioners should conduct wide-ranging surveys of legislation when advising clients developing or using AI applications in domains unfamiliar to the practitioner.

Second, it is important to bear in mind that the regulatory layers in the stratigraphy are internally uneven. This will cause the regulatory intensity varying significantly across application domains. Some application domains are subject to intense regulation. Health care AI, for example, is already subject to intensive data regulation, application-specific AI regulation initiatives are underway, and the sector is generally intensely regulated. Other domains may simultaneously remain sparsely regulated or completely unregulated. Some industrial AI applications face no regulation apart from the general tort and criminal liability rules, IPR rules and competition law rules. Even these general non-AI rules might be barely relevant in some AI applications. The unevenness advocates for caution in regulatory mappings. Relying on insights and experiences from a bordering domain could provide inadequate guidance.

Third, the scopes of the rules vary significantly, as is evident for example in the data rules layer. While the GDPR has a wide scope, other data rules often affect only a specific sector, such as health care, education, or employment. Significant differences exist also between the regulation of personal data and non-personal data as well as public and private actors. The variations in the scope create a regulatory mapping challenge, necessitating case-by-case assessments, which could complicate compliance processes and raise compliance costs. Further, AI developers must not only be aware of the context-specific regulation that affects the developers but also be cognizant of the law that affect their customers and other AI end users. As demonstrated by the tracing app case, the public authority decision-making context imposed significant constraints on AI use, forcing prospective vendors to carefully consider what regulations their clients face.

Fourth, the regulatory instrument types and regulatory modalities vary significantly across and within the layers. In addition, regulation often originates from multiple institutional sources. Some of the rules are statutory and easily identifiable, as many of the data rules are. Other rules may have less clear-cut pedigrees and sources. The constitutional rule banning most automated decision-making in Finnish public authorities is a good example of the latter type of rules. The rule was unwritten and emerged once the Constitutional Law Committee reconstructed the foundational principles of Finnish constitutional and administrative law. Tracking down these unwritten rules can be an arduous task requiring specific legal expertise.

The four themes highlighted above suggest that understanding AI law, thus, seems to require a particular type of regulatory expertise. This expertise must cut across multiple established legal domains. An expert in AI law must be well-versed in data regulation, the sectoral rules that may be relevant to both the developer organization, its customers, and other end users, and also have an understanding of the general legal framework. This expertise is likely to remain rare for some time as it differs from established profiles of legal expertise.

Fifth, AI law still remains largely an emergent entity and its details unclear. One important problem is that AI technologies, in common with other digital technologies, trigger a transformation toward non-anthropocentric settings. In these settings, traditional rules designed to target and affect human behavior presume immediate human action to be present but none is. This transformation is bound to disrupt established interpretative frames for existing legislation (Cohen, 2019). Traffic, for example, is governed by criminal law rules that create humans an incentive to drive carefully. These rules, however, provide little guidance to metalevel actors such as autonomous mobility developers. Thus, AI technologies will likely force participants to retrofit the existing rules to function in environments where human presence is scarce. The retrofit together with the emergence of new legislative rules will likely entail that the exact contents of rules in the new application contexts remain unsettled and uncertain for at least some time. The GDPR Article 22 ban on automated decision-making is an example of the trouble with the new rules. At best, the present contents of the rule can be represented as probability distribution of future enforcement process outcomes and case law, but the rule details will remain uncertain until comprehensive case law emerges.

This *unsettled nature of AI law* will likely be the characteristic condition of using law in AI contexts in near future. The uncertain state of law will force developers and users to constantly keep up with the twists and turns of legal developments. Further, many decisions on the development and deployment of AI must be made without firm knowledge of the precise contents of the applicable law. Consequently, providing an understanding of the uncertainties and risks associated with them is an essential task for the legal function in AI development and user organizations.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author/s.

AUTHOR CONTRIBUTIONS

MV and HP contributed to the design and implementation of the research, to the analysis of the results, and to the writing of the manuscript. Both authors contributed to the article and approved the submitted version.

FUNDING

This research was conducted under AALAW (Academy of Finland project number 315007), ETAIROS (AoF pn 327357) and AIGA (Business Finland) projects. The research was partly funded by the Eino Jutikkala Fund of the Finnish Academy of Science and Letters.

ACKNOWLEDGMENTS

The authors would like to thank the Academy of Finland, Business Finland and the Eino Jutikkala Fund of the Finnish Academy of Science and Letters for funding this research. The authors also thank the colleagues working in the AALAW, ETAIROS and AIGA projects, who have kindly commented on the earlier versions of this article.

REFERENCES

Abboud, L., Miller, J., and Espinoza, J. (2020). *How Europe Splintered Over Contact Tracing Apps*. Financial Times. Available online at: https://www.ft.com/content/7416269b-0477-4a29-815d-7e4ee8100c10 (accessed June 17, 2021).

Adadi, A., and Berrada, M. (2018). Peeking inside the black-box: a survey on explainable artificial intelligence (XAI). *IEEE Access* 6, 52138–52160. doi: 10.1109/ACCESS.2018.2870052

AI HLEG. (2019). *Ethics Guidelines for Trustworthy AI. High-Level Expert Group on Artificial Intelligence*. Available online at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (accessed June 10, 2021).

Bertolini, A., and Episcopo, F. (2021). The expert group's report on liability for artificial intelligence and other emerging digital technologies: a critical assessment. *Eur. J. Risk Regul.* 12, 644–659. doi: 10.1017/err.2021.30

Binns, R. (2017). Data protection impact assessments: a meta-regulatory approach. *Int. Data Privacy Law* 7, 22–23. doi: 10.1093/idpl/ipw027

Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *Int. J. Law Inform. Technol.* 27, 91–121. doi: 10.1093/ijlit/eay017

Brkan, M., and Bonnet, G. (2020). Legal and technical feasibility of the GDPR's quest for explanation of algorithmic decisions: of black boxes, white boxes and fata morganas. *Eur. J. Risk Regul.* 11, 18–50. doi: 10.1017/err.2020.10

Burrell, J. (2016). How the machine 'thinks': understanding opacity in machine learning algorithms. *Big Data Soc.* 3:205395171562251. doi: 10.1177/2053951715622512

Butcher, J., and Beridze, I. (2019). What is the state of artificial intelligence governance globally? *RUSI J.* 164, 88–96. doi: 10.1080/03071847.2019.1694260

Carey, P. (2018). *Data Protection: A Practical Guide to UK and EU Law, 5th Edn*. Oxford: Oxford University Press.

Casey, B., Farhangi, A., and Vogl, R. (2019). Rethingking expainable machines: the GDPR's 'Right to Explanation' debate and the rise of algorithmic audits in enterprise. *Berkeley Technol. Law J.* 34, 145–189. doi: 10.15779/Z38M32N986

Cohen, J. E. (2019). *Law for the Platform Economy*, Vol. 51. Davis, CA: University of California, 133.

Custers, B., and Ursic, H. (2018). Worker privacy in a digitalized world under european law. *Comp. Labor Law Policy J.* 39, 323–344.

Diakopoulos, N. (2016). Accountability in algorithmic decision making. *Commun. ACM* 59, 56–62. doi: 10.1145/2844110

DP3T Consortium. (2020a). *Security and Privacy Analysis of the Document 'PEPP-PT: Data Protection Architechture and Information Security Architecture'*. Available online at: https://github.com/DP-3T/documents/blob/master/Security%20analysis/PEPP-PT_%20Data%20Protection%20Architechture%20-%20Security%20and%20privacy%20analysis.pdf (accessed August 30, 2021).

DP3T Consortium. (2020b). *ROBERT - Security and Privacy analysis.pdf*. Available online at: https://github.com/DP-3T/documents/blob/master/Security%20analysis/ROBERT%20-%20Security%20and%20privacy%20analysis.pdf (accessed August 30, 2021).

DP3T Consortium. (2020c). *DP-3T Model DPIA.pdf*. Available online at: https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf (accessed August 30, 2021).

DP3T Consortium. (2020d). *DESIRE - A Practical Assessment.pdf*. Avaialble online at: https://github.com/DP-3T/documents/blob/master/Security%20analysis/DESIRE%20-%20A%20Practical%20Assessment.pdf (accessed August 30, 2021).

Erdélyi, O. J., and Goldsmith, J. (2020). *Regulating Artificial Intelligence: Proposal for a Global Solution*. ArXiv:2005.11072 [Cs]. Available online at: http://arxiv.org/abs/2005.11072 (accessed October 6, 2020).

European Commission, Directorate General for Communications Networks, Content and Technology, CEPS., ICF., and Wavestone. (2021). *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe: Final Report (D5)*. Publications Office. Available online at: https://data.europa.eu/doi/10.2759/523404 (accessed June 10, 2021).

European Commission. (2020a). *White Paper—On Artificial Intelligence—A European Approach to Excellence and Trust. COM(2020) 65 Final*. European Commission. Available online at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed June 5, 2021).

European Commission. (2020b). *Commission Recommendation (EU) 2020/518 of 8 April 2020 on a Common Union Toolbox for the Use of Technology and Data to Combat and Exit the COVID-19 Crisis, in Particular Concerning Mobile Applications and the Use of Anonymised Mobility Data*. Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020H0518andfrom=EN (accessed August 30, 2021).

Goodman, B., and Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a 'right to explanation'. *AI Magazine* 38, 50–57. doi: 10.1609/aimag.v38i3.2741

Guenole, N., and Feinzig, S. (2018). *The Business Case for AI in HR*. IBM Smarter Workforce Institute, 1–36. Available online at: https://www.ibm.com/downloads/cas/AGKXJX6M (accessed May 6, 2021).

Guihot, M., Matthew, A. F., and Suzor, N. P. (2017). Nudging robots: innovative solutions to regulate artificial intelligence. *Vand. J. Entertain. Technol. Law*, 20, 385–456. doi: 10.31228/osf.io/5at2f

Hagendorff, T. (2020). The ethics of ai ethics: an evaluation of guidelines. *Minds Mach.* 30, 99–120. doi: 10.1007/s11023-020-09517-8

ICO, and The Alan Turing Institute. (2020). *Explaining Decisions Made With AI*. Information Commissioner's Office, 136. Avaialble online at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-artificial-intelligence-1-0.pdf (accessed May 6, 2021).

Kelly-Lyth, A. (2021). Challenging biased hiring algorithms. *Oxford J. Legal Stud.* 41, 899–928. doi: 10.1093/ojls/gqab006

Köykkä, S., and Kaikkonen, R. (2020). *Näin toimii koronavirusaltistuksia jäljittävä mobiilisovellus*. Solita. Available online at: https://www.solita.fi/blogit/nain-toimii-suomen-koronavirusaltistuksia-jaljittava-mobiilisovellus/ (accessed June 17, 2021).

Larsson, S. (2020). On the governance of artificial intelligence through ethics guidelines. *Asian J. Law Soc.* 7, 1–15. doi: 10.1017/als.2020.19

Laurim, V., Arpaci, S., Prommegger, B., and Krcmar, H. (2021). "Computer, whom should i hire? – acceptance criteria for artificial intelligence in the recruitment process," in *Proceedings of the 54th Hawaii International Conference on System Sciences* (New York, NY), 5495–5504. doi: 10.24251/HICSS.2021.668

Mendoza, I., and Bygrave, L. A. (2017). "The right not to be subject to automated decisions based on profiling," in *EU Internet Law: Regulation and Enforcement*, eds T.-E. Synodinou, P. Jougleux, C. Markou, and T. Prastitou (Cham: Springer), 77–98.

Miller, T. (2019). Explanation in artificial intelligence: insights from the social sciences. *Artif. Intell.* 267, 1–38. doi: 10.1016/j.artint.2018.07.007

Ministry of Social Affairs and Health. (2020). *Koronavilkku Has Now Been Published – Download the App to Your Phone!* Finnish Government. Available online at: https://valtioneuvosto.fi/en/-/1271139/koronavilkku-has-now-been-published-download-the-app-to-your-phone- (accessed May 6, 2021).

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., and Floridi, L. (2016). The ethics of algorithms: mapping the debate. *Big Data Soc.* 3, 1–21. doi: 10.1177/2053951716679679

Pillai, R., and Sivathanu, B. (2020). Adoption of artificial intelligence (AI) for talent acquisition in IT/ITeS organizations. *Benchmarking Int. J.* 27, 2599–2629. doi: 10.1108/BIJ-04-2020-0186

Sartor, G., European Parliament, European Parliamentary Research Service, Scientific Foresight Unit, and Lagioia, F. (2020). *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Study*. EPRS European Parliamentary Research Service. Available online at: http://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (accessed May 6, 2021).

Scherer, M. U. (2016). Regulating artificial intelligence systems: risks, challenges, competencies, and strategies. *Harvard J. Law Technol.* 29, 353–400. doi: 10.2139/ssrn.2609777

Selbst, A. D., and Powles, J. (2017). Meaningful information and the right to explanation. *Int. Data Privacy Law* 7, 233–242. doi: 10.1093/idpl/ipx022

Tene, O., and Polonetsky, J. (2013). Judged by the tin man: individual rights in the age of big data. *J. Telecommun. High Technol. Law* 11, 351–368.

The Finnish Constitutional Law Committee. (2016). *Perustuslakivaliokunnan lausunto PeVL 42/2016 vp—HE 111/2016 vp Hallituksen esitys eduskunnalle nuorisolaiksi (Opinion of the Constitutional Law Committee on Government Proposal to Parliament for a Youth Act)*. Available online at: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/PeVL_42$+$2016.pdf (accessed August 30, 2021).

The Finnish Constitutional Law Committee. (2019a). *Perustuslakivaliokunnan lausunto PeVL 62/2018 vp—HE 224/2018 vp Hallituksen esitys eduskunnalle laiksi henkilötietojen käsittelystä maahanmuuttohallinnossa ja eräiksi siihen liittyviksi laeiksi (Opinion of the Constitutional Law Committee on Government Proposal to Parliament for a law on the processing of personal data in the Immigration Administration and some related laws)*. Available online at: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/PeVL_62$+$2018.pdf (accessed May 6, 2021).

The Finnish Constitutional Law Committee. (2019b). *Perustuslakivaliokunnan lausunto PeVL 7/2019 vp—HE 18/2019 vp Hallituksen esitys eduskunnalle laiksi henkilötietojen käsittelystä maahanmuuttohallinnossa ja eräiksi siihen liittyviksi laeiksi (Opinion of the Constitutional Law Committee on Government Proposal to Parliament for a law on the processing of personal data in the Immigration Administration and some related laws)*. Available online at: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/PeVL_7$+$2019.pdf (accessed May 6, 2021).

Vedder, A., and Naudts, L. (2017). Accountability for the use of algorithms in a big data environment. *Int. Rev. Law Comput. Technol.* 31, 206–224. doi: 10.1080/13600869.2017.1298547

Viljanen, M. (2021). *EU Published an AI Regulation Proposal. Should We Worry?* Artificial Intelligence Governance And Auditing. Avaialble online at: https://ai-governance.eu/eu-published-an-ai-regulation-proposal/ (accessed June 17, 2021).

Wachter, S., Mittelstadt, B., and Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *Int. Data Privacy Law* 7, 76–99. doi: 10.1093/idpl/ipx005

Wallach, W., and Marchant, G. (2019). Toward the agile and comprehensive international governance of AI and robotics [point of view]. *Proc. IEEE* 107, 505–508. doi: 10.1109/JPROC.2019.2899422

Wood, M. A. (2021). Rethinking how technologies harm. *Br. J. Criminol.* 61, 627–647. doi: 10.1093/bjc/azaa074

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.