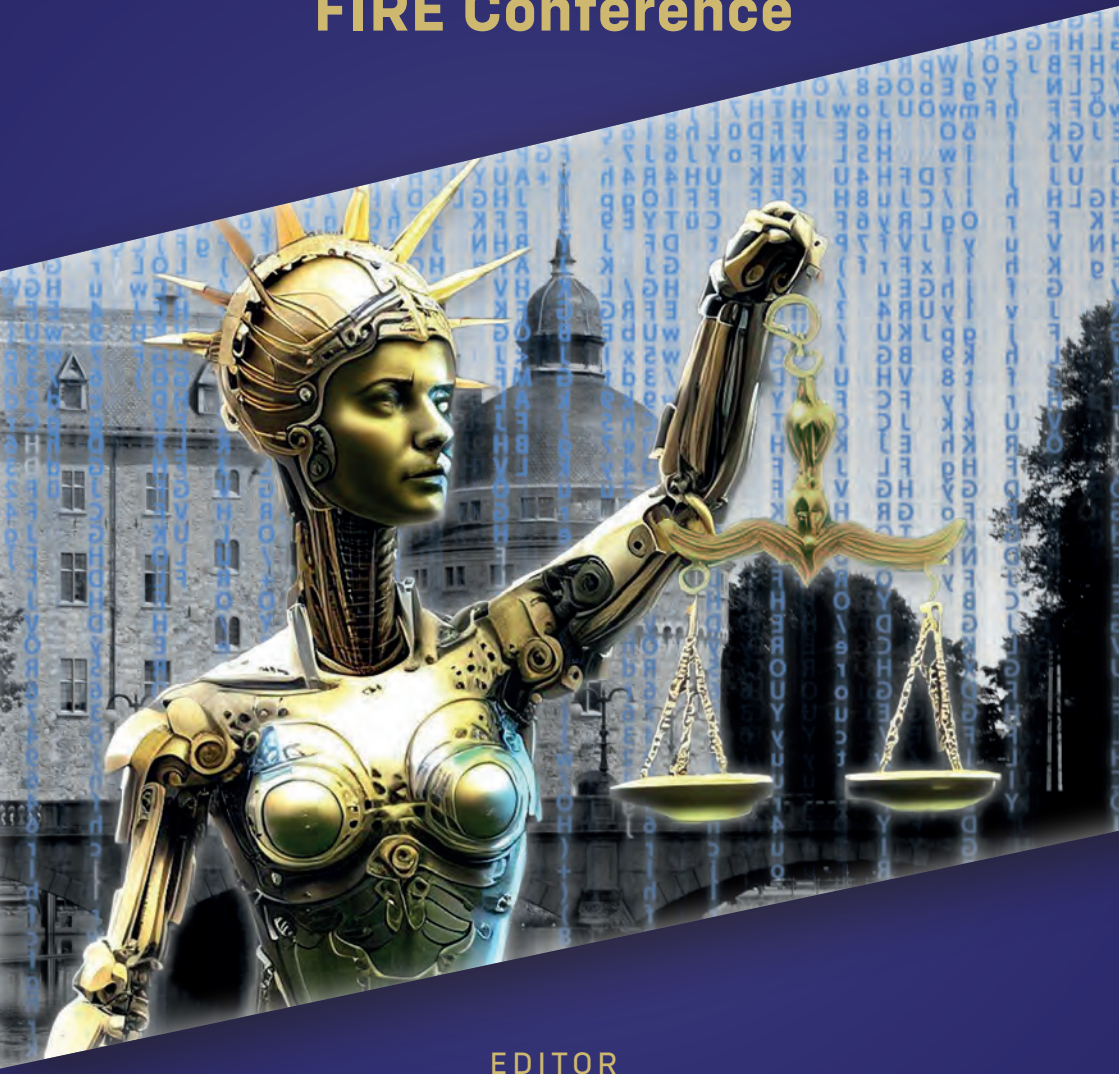
PROCEEDINGS FROM THE FIRST ANNUAL

FIRE Conference



EDITOR

Magnus Kristoffersson

iUSTUS

Proceedings from
the First Annual International

FIRE CONFERENCE

10th–11th of November 2022
Örebro University
Sweden

EDITOR
MAGNUS KRISTOFFERSSON

IUSTUS FÖRLAG

Table of Contents

Preface 7

The Authors 11

Magnus Kristoffersson
Chapter 1
An Overview of the FIRE Research Project 15

Rigmor Argren
Chapter 2
Using the European Convention on Human Rights to Shield Citizens from Harmful Datafication 43

Giovanni Botto
Chapter 3
Blockchain and European Administrative Integration: a Reflection on Public Governance and Technology, Starting from the European Competition Field 61

Clémence Garcia and Takeo Itabashi
Chapter 4
An Experiment on Double Entry Bookkeeping and Financial Reporting Using Blockchain 75

Hanna Grylin
Chapter 5
Income taxation of forestry, forest deduction and digitalization 93

David Hadwick
Chapter 6
Breaking the Fiscal Omerta: The Roadmap to Transparency in EU Tax Algorithmic Governance 107

Jan Kellgren
Chapter 7
The Current Corporate Income Tax Rule Architecture & Automated, Real-Time Taxation – Would the Necessary Prerequisites of Today's Tax Rules Have to Be Changed? 127

Eleonor Kristoffersson
Chapter 8
ViDA – VAT in the Digital Age 143

Yurii Orzikh
Chapter 9
Accounting Regulation and Financial Reporting under Ukrainian Legislation 153

Mais Qandeel
Chapter 10
Blockchain Application in Information Ecosystems: The Right to Privacy in Cyberspace 177

Francesco Paolo Schiavone
Chapter 11
The Free Movement of Capital within The EU and Digitalisation: The Role of Cryptocurrencies 193

Vadym Tsymbal
Chapter 12
The Digitalization of Governance and Tax Administration in Ukraine 209

Sam van der Vlugt
Chapter 13
Ensuring an Inclusive Shift Towards a Technology-Driven Dialogue Between Taxpayer and Administration: How the Law Can Benefit from a Different Methodology 229

Anna Husman
Chapter 14
Automation in the Public Sector and the Principle of Non-Discrimination 249

Rigmor Argren

Chapter 2
Using the European Convention on Human Rights to Shield Citizens from Harmful Datafication

Abstract: Encoding and (re-)using data about or created by citizens to generate new value is a process referred to as datafication. Extracting data from and about citizens raises numerous human rights questions, particularly in the area of the right to private life. The European Court of Human Rights (ECtHR) has over the years developed and shaped the right to digital private life by outlining what type of collection, processing and retention of data about individuals is considered permissive – and what is not. Although the datafication process entails elements that currently lie outside the core ambit of the ECtHR, it has a longstanding and indeed heightened interest in defining and protecting what constitutes genuine human private life. In this regard, digital private life falls into a domain of matters which the ECtHR finds worthy of protection. By pointing out specific requirements in order to prevent the abuse of State power, the ECtHR is a mechanism that can be reckoned with when it comes to shielding European citizens from datafication.

2.1 Introduction

The ongoing digitalisation and automation of human existence means that human life is currently experiencing wide-reaching datafication. The encoding of data from and about citizens, the data subjects, can generate new value. This raises a number of human rights questions. It has been

pointed out that the mere knowledge about processes of datafication and encoding of human life can tacitly or explicitly influence human behaviour. What are, if any, the human rights implications when data snippets 'produced' by citizens in their daily lives, many online but also offline, are separated from the data subject and gathered by authorities and companies for (possible) value-generating purposes? What are citizens' reasonable expectations concerning the protection of their data? Is there a human right to *digital* private life?

This chapter begins by delineating the notion of datafication. Next, the right to private life is outlined thus unveiling the central original features of this classic right within the framework of the European Convention on Human Rights (ECHR), and the nature of State obligations it gives rise to. This is followed by an examination of how Article 8, which safeguards the right to private life, is used when datafication comes before the European Court of Human Rights (ECtHR). Although the right to private life is not the only right invoked in relation to datafication, Article 8 remains the most frequently used provision. The chapter ends by highlighting the key findings concerning how the ECtHR approaches datafication. Before we further explore the right to private life/privacy, an introduction to the concept of datafication is required.

2.2 The Notion of Datafication

Datafication now enables the "processing of personal information on an industrial scale" (Cohen, 2017:224). Commenting on these technological developments, Land & Aronson concluded that from a human rights perspective "the very same characteristics of technology that present the greatest opportunities also create the greatest risks." (Land & Aronson, 2018:126). Two decades have passed since the global community affirmed that the Universal Declaration of Human Rights (UDHR) should equally apply to cyberspace (Andrew & Bernard, 2021:1). The impact of new technology and digitalisation on human life and behaviour has been perceived to be fundamental enough to even potentially infringe on the freedom of thought (Alegre, 2022:132). Despite such alarmistic views, it is here submitted that human rights law is well-versed when it comes to 1) finding the balance between the interests of individuals on the one

hand and the State on the other, and 2) assessing whether the State has reached a fair balance between the competing interests of individuals.

The ECtHR relies on Article 2 of the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) when defining data processing as "… any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data" (Convention 108, Art 2). The net to capture what data processing entails is cast wide intentionally. Nevertheless, there is at times a presumption that data handling, in particular computerised analysis, data capturing and registration is done passively, while people do what they normally do anyway; this presumption may be false (Rothschild-Elyassi, 2022:56). In fact, datafication entails turning citizens' day-to-day actions, such as having a chat with a friend or waving down a cab into digital platforms and apps. In other words, common human habits that were previously done elsewhere have been turned into activities performed via digital media (Mejias & Couldry, 2019:5). It is this process of gathering, collecting and the storing of data that has led commentators to suggest that what has been taken away should not actually be called *data* (Latin: that which is given), but rather *capta* (that which is taken). (Mejias & Couldry, 2019:2). One may even argue that the taking of data can be understood as a colonial process, due to the same historical function of dispossession (Mejias & Couldry, 2019:6).

When datafication amounts to surveillance, the ECtHR has held that it has a chilling effect, meaning that a person restrains him or herself from otherwise lawful speech or other acts, fearing legal consequences or privacy harm. (Penney 2022:1454). This impacts citizens in general, as well as the behaviour of those working in public authorities, be it with legal or non-legal tasks. Therefore, the term datafication "signals a historically new method of quantifying elements of life that until now were not quantified to this extent" (Mai, 2019:3).

Datafication is said to be a process that consists of the following three segments: First comes a transformative stage where something is encoded into data (Rothschild-Elyassi, 2022:56). Second, such data becomes the smallest building block from which knowledge and information is drawn (Kitchin, 2014:1). Third, this information constitutes a new value of

some sorts. The first segment, the encoding of human behaviour which also includes sentiments and attitudes (Mayer-Schönberger & Cukier, 2013:93), is a transformation that entails making what is encoded quantifiable (Mejias & Couldry, 2019:1). The sheer volume as well as the wide aspects of human life that are transferred into data in this manner, is unprecedented. The transformation is subtle and entails both cognitive and evaluative abstractions (Mejias & Couldry, 2019:3).

It is noteworthy that the encoding is not neutral to ideology. It is based on decisions regarding the selection of reality and how such quantification is done (Rothschild-Elyassi, 2022:61). As Mai has pointed out, "data has to be cleaned or conditioned to be usable, which involves deciding which attributes and variables to keep and which to ignore" (Mai, 2019:111). Other authors present the view that the values and views of those responsible for coding influence the datasets. (Goldkind *et al.*, 2018:175). Either way, there are indications that marginalised people remain the most vulnerable groups, also when it comes to having their data exploited (Goldkind *et al.*, 2018:176).

As for the second segment, it is important to remember that the tracking and analysing of data is increasingly done in real-time (Rothschild-Elyassi, 2022:61). Lastly, generating *new value* should not solely be understood in monetary terms, although profit can be generated through "data's sale as a commodity or data's incorporation as a factor of production" (Mejias & Couldry, 2019:5). *New value* could also be a "means of state control, cultural production, civic empowerment" (Mejias & Couldry, 2019:3); or aspects of social and healthcare benefits or, for example, improved customer experiences (Stănescu & Onufreiciuc, 2020:101).[1] Such value creation has been described as "a pattern of appropriation by some, with economic and political consequences for others" (Cohen, 2017:230). The infrastructure required for datafication is "owned or controlled mostly by corporations and states" (Mejias & Couldry, 2019:3). Thus, corporations are the main actors and beneficiaries of datafication, but many States also have strong stakes in this process (Mejias & Couldry, 2019:7). The next section begins with a brief look at the general features of the right to private life as protected by Article 8 of the ECHR. This is followed by

[1] For criticism regarding equating data with resources, see, *e.g.*, van Dijck, 2014 and Boyd & Crawford, 2012.

a short outline of how the right to digital private life has evolved in the light of contemporary technological developments.

2.3 The Expansion of the Protection of Private Life in the Age of Datafication

The ECHR is said to be "a living instrument anchored to the reality of the Member States in which it applies" (Andrew, 2021:2). Article 8 of the ECHR has been called "one of the most open-ended provisions of the Convention" (Ovey, C., & White, R., 2006:241). This provision has over the years become "one of the richest areas of legal development" (Schabas, 2015:366) in ECtHR case-law. Therefore, it is not surprising that this provision is at the forefront when it comes to tackling the "quantum leap in surveillance, interception of communications and data retention" (Data protection guide, 2022:7), faced by citizens.

2.3.1 Citizens' Right to Private Life

Article 8 belongs to those provisions in the ECHR which have inherent limitations.[2] It is important to point out that permissive limitations do not allow the authorities or companies to reduce the right to zero (*Barbulescu v Romania*, § 80). The right to private life is originally of the classical negative kind and the ECtHR holds that the essential object of the provision is to "protect the individual against arbitrary action by the public authorities" (*Kroon and Others v the Netherlands*, § 31), once referred to as "a right to be left alone" (Brandeis, cited in Schabas, 2015:358). This view has the underlying assumption "that we have a property right to our personal information" which immediately leads to the question: Who owns the information? (Mai 2019:96). However, this, Mai argues, misses the point, namely that what in fact is essential is what happens with personal data. What is foreseeably done with it?

[2] The other ECHR-rights with such limitations are Article 9, thought, conscience and religion, Article 10, freedom of expression, and Article 11, freedom of assembly and association. The inherent limitations are similar, but not identical. (Ovey & White, 2006:218).

Foreseeability is a special feature in the protection from arbitrariness: "Foreseeability is primarily dependent on the provision of an adequate indication as to the circumstances and conditions under which monitoring may be lawfully employed".

The four interests for which Article 8(1) ensures *respect* are private life, family life, home and correspondence. Interestingly, *respect* does not appear in any other substantive provision in the ECHR (Schabas, 2015:367).[3] Although they are distinct interests, they occasionally overlap (Schabas, 2015:367). One may safely assume that the drafters had human beings in mind when seeking to protect private and family life (Emberland, 2006:115). This can be concluded from the reasoning in, for example (*X v Iceland*, 87), where the European Commission argued that private life should be understood in a broad sense, to include "the right to establish and develop relationships with other human beings, especially in the emotional field, for the development and fulfilment of one's own personality".[4]

Furthermore, the notion of 'private life' is so broad, that it neither can nor should be given an exhaustive definition (*Niemietz v Germany*, § 29). For instance, the ECtHR has held that private life includes someone's physical and psychological integrity, including at times aspects of an individual's physical and social identity (*Mikulić v Croatia*, § 53). In fact, the concept of private life is considered heterogenous and more far-reaching than an end in itself: "The specific contours of privacy can be clearly distinguished and perceived only when it is being defended against different kinds of encroachments. Moreover, privacy is an aspect of the person's general well-being, and not necessarily only an end in itself" (*Hatton and others v the United Kingdom*, 43: § 11) as the dissenting judges in this case argued. Furthermore, the ECtHR has elaborated on the protection of our consciousness, seeking to emphasise and appreciate less tangible aspects of human life by protecting every citizen's right to "freely pursue the development and fulfilment of his personality" (*Smirnova*

[3] 'Respect' does appear in the title of Article 1. The ECtHR has stated that the concept is not clear-cut, but emphasised that the 'rule of law' is one of its elements (Schabas, 2015:367).

[4] The Commission further held that such a right *did not* extend to relationships with dogs, and subsequently deemed the case inadmissible.

v Russia, § 95). This integrity of the self can be seen as the foundation for autonomy and human agency (Mejias & Couldry, 2019:6). But an autonomous personality does not exist in a vacuum. Rather, according to the ECtHR, it distinctively encompasses a social dimension, which extends beyond the family (*Biriuk v Lithuania*, § 38).

The social dimension directs attention towards professional activities, given that "professional life is often intricately linked to private life" (*Fernández Martínez v Spain*, § 110). Professional or business activities may under certain circumstances be given protection under Article 8. (*Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland*, § 130).[5] Most notably is this when the interference concerns "correspondence" or "home" and legal entities are seen to have the status of victim in the meaning of the ECHR.[6]

Although the right to private life originates from a desire to *restrain* State interference, it also clearly raises positive State obligations, in that a State must *actively* provide horizontal protection of the right to private life between private individuals themselves, or individuals and legal persons. The bulk of Article 8 case-law is in fact concerned with positive obligations that require an activity from the State (Schabas, 2015:366). In this case, the State has a wide margin of appreciation. If the principles laid out in ECtHR's case-law are followed by the domestic court, no violation is likely to occur (*Von Hannover v Germany*, §§ 125–126). As will be shown in the following section, the ECHR provides the State several legitimate purposes of interference with Article 8.

2.3.2 The Legitimate Interests of the State

The right to private life has to be respected both vertically and horizontally – giving rise to negative as well as positive State obligations. In practice, the positive and negative State obligations are similar. As for the former type of obligation, the ECtHR will assess whether a fair balance has been struck between the competing interests of an individual and the community as a whole. The requirements of Article 8(2) mean that the ECtHR will conduct a three-pronged test to establish whether the

[5] A comment to the case is available by McCully, J. (2018).

[6] See, *e.g., Bernh Larsen Holding AS and Others v Norway*; *Liberty and Others v the United Kingdom*.

interference was a) in accordance with the law, 2) pursued any of the permissible aims listed, and 3) was necessary in a democratic society. The listed permissible aims for limitations are a) national security, public safety b) the economic wellbeing of the country, c) the prevention of disorder or crime, d) the protection of health or morals, e) for the protection of the rights and freedoms of others. The ECtHR has explicitly held that the formulation of permissible limitations under Article 8(2) "leaves no room for the concept of implied limitations" (*Golder v United Kingdom*, § 44), a position that has been upheld.

The margin of appreciation enjoyed by the State will be wider, if the matter concerns balancing someone's right to private life against another fundamental right (Schabas, 2015:368) such as, for example, the freedom of expression. In contrast, a narrower margin of appreciation will be applied where "a particularly important facet of an individual's existence or identity is at stake" (*E.S. v Sweden*, § 58). This includes the most intimate aspects of private life (*ibid.*).

One may, as Deeks has done, argue that the existing international human rights framework is no longer fit for what is now technically possible in relation to human surveillance across national borders (Deeks, 2015:294). Nevertheless, the right to private life has been considerably extended by the ECtHR since the matter of (analogue) data protection first came before it in *Leander v Sweden*[7] almost 35 years ago. By now the right to private life also includes the right to digital private life. Mai has pointed out that the focus of the debate has "shifted from concerns about revealing information about oneself to others to concerns about the new insights that others can generate based on the already available data" (Mai 2016:199). The following section examines how the ECHR operates in view of this shift. Focus remains primarily on matters of legitimate State interests, such as national security, the well-being of the country and the prevention of disorder or crime.

[7] The claimant sought access to classified data about himself. The ECtHR found no violation, arguing that knowing what the secret service had on file on the applicant (which prevented him from getting a civil job in the marine base), did not constitute an interference with his private life.

2.4 Applying Article 8 of the ECHR to Shield Citizens from Datafication

The protection of citizens as data subjects is in human rights terms concerned with at least three aspects of data handling. The ECtHR pays attention to the collection, retention and disclosure actions of data, by State bodies as well as by private bodies. At the outset of this discussion, it is perhaps important to mention that scholars have already identified that international human rights law could make a useful contribution in relation to datafication and digitalisation, given its well versed system for approaching bias and discrimination (McGregor, Murray & Ng, 2019:326). This legal regime not only identifies and defines unlawful harm, it also provides a "means to determine harm through its interpretation of how rights may be interfered with, it also provides established tests to assess when and how rights may have been violated" (*ibid*.). The three-pronged test mentioned earlier will ensure that interferences with the right to digital private life is done for explicit purposes. In this discussion, the legitimate purposes of the State are national security, public safety, the prevention of disorder or crime, and the economic well-being of the country.

2.4.1 The Collection of Personal Data

The ECHR does not provide any autonomous right to *personal* data (digital or otherwise) (Data protection guide, 2022:7). Therefore, despite the increasing scope of what falls within the notion of 'private life', all contemporary automatic processing and handling of personal data will not categorically fall within the ambit of Article 8 or otherwise avail itself of protection by the ECHR (*ibid*.). Rather, it has to be anchored in the right to private life, as expressed in Article 8 of the ECHR. That being said, the ECtHR remains bound by numerous aspects of balancing the State's interests with the citizens right to digital private life. This includes data collected through covert surveillance by the authorities, the collection of data by employers at workplaces, data collection as evidence in courts, data in medical contexts, and citizens' compulsory communication of personal data. The ECtHR has consistently held that personal data is defined as "any information relating to an identified

or identifiable individual" (*S and Marper v UK*, § 41). Therefore, even "public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities" (*Rotaru v Romania*, § 43).

At the heart of the ECtHR's attention is the protection of the data subject – the citizen. In line with Article 6 of Convention 108, such data is termed as 'sensitive' by the ECtHR and merits a heightened degree of protection. Sensitive data pertains to data revealing racial or ethnic origin; political opinions, and religious or other beliefs, including philosophical beliefs; trade union membership; genetic and biometric data; health, sex life or sexual orientation and criminal offences and convictions (Convention 108, Article 6). Biometric data consists not only of biological characteristics such as fingerprints, the topography of face and fingers, or DNA, but also behavioural aspects such as voice and gait (Zwanenburg, 2021:1406).

The ECtHR assesses to what extent an individual is reasonably entitled to expect the protection of his/her private life as regards the processing of data by public authorities (*Perry v the United Kingdom*, § 37). This means that the ECtHR is concerned with the handling of personal data whether or not it has merely been collected or has been subjected to more sophisticated processing. ECtHR has referenced Article 3(2) of the Directive (EU) 2016/680 which states that processing is: "… any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Directive 2016/680).

The ECtHR is not only concerned with sensitive data, it also assesses the protection of 'other' data linked to citizens. This includes employment data, financial data, traffic data, voice samples, GPS location data and photography and the like. Although the assessment concerning these forms of data is carried out with the same three-pronged test set out in Article 8(2), the ECtHR is likely to provide a wider margin of appreciation to the State in these cases. For instance, in tax matters, where the State generally speaking has a wider margin of appreciation, the citizens will have their data protected should it be published in a manner or to

a degree beyond what the data subject could reasonably have foreseen (*M.N. and Others v San Marino*, § 72).

In its work with finding a fair balance between matters of security and the survival of the State, the ECtHR has carved out and follows clear lines. The ECtHR examines a) the proportionality of the measures taken b) if measures were subject to independent authorisation at the outset and c) the existance and nature of supervision and *ex post facto* review.

2.4.2 The Retention of the Smallest Data Block

Data collection may well increasingly be done in real-time, but the ECtHR is focussed on how any data (sensitive or otherwise) is retained. The ECtHR scrutinises what safeguarding measures a State has in place against abuse. If a State that resorts to using cutting-edge technology for mass surveillance for the legitimate aim of pre-empting incidences of serious crimes, then the ECtHR expects that the introduction of the use of new technology "…has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights" (*Szabó and Vissy v Hungary*, § 68). The safeguarding against abuse does not only require the State to have separate rules concerning sensitive and other data retention. Additionally, explicit rules concerning the destruction of both types of data are required.

2.4.3 The Duration of Data Retention

The ECtHR acknowledges that personal data may have to be retained for the purpose of crime prevention. This can be seen in the case of *B.B. v France*, where the applicant, a convicted sex offender, complained about the inclusion of his address in a sex offender database, with the obligation to update his address once a year. The ECtHR found that the aim sought, to prevent criminal activities, was a legitimate one. On assessing the safeguarding measures against abuse, the ECtHR held that they were satisfactory. First, such gathered data can only be consulted by the courts, police or administrative authorities subject to a duty of confidentiality. Second, the duration of the data retention was pre-determined, albeit amounting to the maximum of 30 years (§ 68). Thus, the ECtHR was satisfied that independent reviews were available to the applicant (*ibid.*) and found no violation of Article 8.

Furthermore, a State seeking to retain the data of convicts must distinguish between serious offences (such as terrorism, sexual offences and crimes against humanity) and non-serious offences such as striking a gendarme with an umbrella in connection with turmoil at a political rally (*Aycaguer v France*, § 44).[8]

As mentioned above, data retention if determined precisely, even for a maximum of 30 years, may be deemed not to violate the right to private life of a convicted sex offender. Although the ECtHR requires the precise determination of the duration of data retention, there is an outer limit: the ECtHR has held that a definite period of forty years may be equal to an indefinite period in practice, as it is likely to extend beyond the reasonable life expectancy of the applicant (*ibid.,* § 42).

But the length of retention can also be lawfully organised without an explicit duration period. Such was the case where sensitive data such as blood samples had been taken for the purpose of an exhumation programme to identify deceased relatives. ECtHR held that no violation was found, because the destruction of the samples was determined to take place when the consent form expired (*Cakicisoy and Others v Cyprus*, § 52).

The ECtHR has found violations of the right to digital private life when: 1) the data retention was indefinite; 2) the seriousness of the offence had not been taken into consideration, and 3) no real possibility of review was provided (*Gaughran v the United Kingdom*, § 94). These criteria are not cumulative since every one of them has to be satisfied independently of the other. In the view of the ECtHR, measures against abuse can be achieved through end-to-end protection.

2.4.4 End-to-End Protection

The practice of bulk surveillance although not automatically prohibited requires specific safeguarding measures. Notably, fundamental safeguards against abuse in the form of end-to-end safeguards are required. First,

[8] Similarly, pertaining to private companies, the ECtHR has held that the tax authorities did not overstep their margin of appreciation when a backup file was taken from a mixed server jointly used by three companies for the purpose of tax auditing (*Bernh Larsen Holding AS and Others v Norway*, § 173). The majority of five votes to two argued that the situation was less serious than a search and seizure under criminal law.

an assessment of the necessity and proportionality has to be made at the domestic level, at each stage of the measures taken. Second, from the outset, any bulk interception should be subject to independent authorisation. Third, the operation should be subject to supervision and *ex post facto* review (*Big Brother Watch and Others v the United Kingdom*, § 350). Additionally, should journalistic material and the professional protection of sources' anonymity be at risk due to bulk interception, Article 10 will also be used (*ibid.*, § 448). The end-to-end requirement of safeguarding bulk inceptions can also be invoked by a non-governmental organisation. The requirement includes clear rules on the destruction of incepted data even if it does not include personal data (*Centrum för rättvisa v Sweden*, § 369).[9] The ECtHR has also held that when incepted data is transmitted to foreign partners, the privacy interests of citizens should be given consideration by the law (*ibid.*).

2.4.5 Disclosure Actions

The ECtHR has distinguished between the disclosure of personal data by one authority to another and public disclosure by media. The disclosure of personal data is safeguarded by clear requirements: 1) domestic law must regulate the measures taken by the data processor; 2) their responsibility in the case of non-compliance must be in place; and 3) the data receiving authority must have corresponding rules and guarantees, notably, the duty of confidentiality should be in place (*M.S. v Sweden*, § 43). When it comes to sensitive personal data, the prior consent of the data subject is one element to consider, albeit not a decisive one (*ibid.*, § 35). Furthermore, even when citizens do not actively hide data that make them identifiable, there is a reasonable expectation of privacy that should be protected (*Benedik v Slovenia*, § 116). Should, however, a person actively seek publicity, such a legitimate expectation of privacy becomes limited (*Axel Springer AG v Germany*, § 101).

The ECtHR has held that, in principle, the public's interest to know, as protected under Article 10, should be given equal weight with the

[9] A separate discussion exists concerning to what extent examining cases pertaining to general matters of mass surveillance, rather than the handling of petitions of individual victims of violations, can be said to alter the ECtHR's nature, turning it into a constitutional court. See, *e.g.*, van der Sloot, (2020).

individual's right to privacy (*Satakunnan v Finland*, § 163). In that case, the ECtHR held that no violation of Article 10 had occurred when the news outlet was held liable for making extracted data pertaining to taxation publicly available. In passing, the ECtHR notes that even if regulating the manner in which data is disclosed by a media outlet may render the business less profitable, this is not a sanction in the eyes of the ECtHR. (*ibid.*, § 197).

2.5 Concluding Discussion

The first segment of datafication which concerns the encoding of human life does not currently draw much direct attention from the ECtHR, if it is considered primarily from a technological perspective. However, if considered from the inverted perspective, that is seeking to establish what genuine private life *is* and what truly human aspects of being or existence are, an emerging stance from the ECtHR can be discerned. First, the ECtHR recognises that humans do not and cannot thrive and develop in isolation or on their own, being requires and happens in context: the ECtHR seeks to capture nuances of humanness, with aspects of social life and the fulfilment of one's personality. Second, arguably, the ECtHR protects the humanness of digital private life by distinguishing between sensitive data and other data, clearly providing the first category more attention and scrutiny. Third, the ECtHR explicitly requires the State to develop separate sets of rules for both data categories.

The second segment of datafication, dealing with when and how data is gathered and processed, gives rise to an abundant amount of case-law. The ECtHR has a strong focus on what is done with personal data in terms of its capturing, collection, retention and disclosure. The actual type or kind of data is not that much on the ECtHR's radar. What matters, and rightly so, is what is done with it.

Finally, the third segment of datafication leading to the creation of new value which is not limited to monetary aspects, but that also could consist of public values such as security gains, or improvements in health care systems, occasionally draws attention from the ECtHR. This will be the case when the appropriation of new value has consequences for the human rights of citizens. The ECtHR clearly is of the view that States

that strive to be at the forefront and aim to lead technical developments and the quest for datafication, through such a commitment have an automatic obligation to develop satisfactory safeguards against abuse. One such mechanism against abuse that the ECtHR has repeatedly asked for, is so called end-to-end protection, with legal rules pertaining to the duration of retention, and the explicit regulation of data destruction. This end-to-end requirement also applies to sensitive and other data.

Although legal persons such as associations and companies may avail themselves of Article 8 protection from time to time, it is clear that what the ECtHR provides human rights protection for are aspects of human private life and the enterprises, function in relation thereto. The ECtHR's approach to business interests such as profit making, may at best be described as indifferent.

In conclusion, it can be argued that the ECtHR is capable of shielding citizens from several aspects of datafication. This is done primarily by requiring regulation against abuse in matters pertaining to digital private life and what is considered sensitive data. Given the ECtHR's capacity to define and identify harm, it is possible to conclude that the human rights framework is a mechanism to be reckoned with when it comes to shielding citizens from harmful datafication.

References

1948 Universal Declaration of Human Rights, G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948).

1950 Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by the protocols) [ECHR] adopted 3 September 1953, 213 UNTS 222.

1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, [Convention 108] (ETS No. 108, 28.01.1981).

Alegre, S. (2022). *Freedom to Think: The Long Struggle to Liberate our Mind*. Atlantic Books.

Andrew, J. (2021). Introduction. In J. Andrew & F. Bernard (eds), *Human rights responsibilities in the digital age: states, companies and individuals*. Hart Publishing.

Boyd, D. & Crawford, K. (2012). Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information,*

Communication & Society, *15*(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878.
Cohen, J. E. (2017). The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy. *Philosophy & Technology 31*, 213–33.
Deeks, A. S. (2015). An international legal framework for surveillance. *Virginia Journal of International Law*, *55*(2), 291–368.
ECtHR, *Axel Springer AG v Germany* (Application no. 39954/08) Judgment [GC] 7 February 2012.
ECtHR, *Aycaguer v France* (Application no. 8806/12) Judgment Final 22 September 2017.
ECtHR, *Barbulescu v Romania* (Application no. 61496/08) Judgment [GC] 5 September 2017.
ECtHR, *B.B. v France* (Application no. 5335/06) Judgment Final 17 March 2010.
ECtHR, *Benedik v Slovenia* (Application no. 62357/14) Judgment Final 24 July 2018.
ECtHR, *Bernh Larsen Holding AS and Others v Norway* (Application no. 24117/08) Judgment 27 November 2009.
ECtHR, *Big Brother Watch and Others v the United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15) Judgment [GC] 25 May 2021.
ECtHR, *Biriuk v Lithuania* (Application no. 23373/03) Judgment Final 25 February 2009.
ECtHR, *Cakicisoy and Others v Cyprus* (Application no. 6523/12) Judgment 23 September 2014.
ECtHR, *Centrum för rättvisa v Sweden* (Application no. 35252/08) Judgment 25 May 2021.
ECtHR, *E.S. v Sweden* (Application no. 5786/08) Judgment 21 June 2012.
ECtHR, *Fernández Martínez v Spain* (Application no. 56030/07) Judgment [GC] of 12 June 2014.
ECtHR, *Gaughran v the United Kingdom* (Application no. 45245/15) Judgment Final 13 June 2020.
ECtHR, *Golder v the United Kingdom* (Application no. 4451/70) Judgment of 21 February 1975, Series A, No 18. (1979–80) 1 EHRR 524.
ECtHR, Guide to the Case-law of the European Court of Human Rights: Data protection [Data protection guide], updated 31 August 2022. Available for downloading at www.echr.coe.int.
ECtHR, *Hatton and others v the United Kingdom* (Application no. 36022/97) Judgment [GC] 8 July 2003.
ECtHR, *Kroon and Others v the Netherlands* (Application no. 18535/91) Judgment 27 October 1994.

ECtHR, *Leander v Sweden* (Application no. 9248/81) Judgment 26 March 1987.
ECtHR, *Liberty and Others v the United Kingdom* (Application no. 58243/00) Judgment Final 1 October 2008.
ECtHR, *Mikulić v Croatia* (Application no. 53176/99) Judgment Final 4 September 2002.
ECtHR, *M.N. and Others v San Marino* (Application no. 28005/12) Judgment Final 7 October 2015.
ECtHR, *M.S. v Sweden* (Application no. 74/1996/693/885) Judgment 27 August 1997.
ECtHR, *Niemietz v Germany* (Application no. 13710/88) Judgment 16 December 1992.
ECtHR, *Perry v the United Kingdom* (Application no. 63737/00) Judgment Final 17 October 2003.
ECtHR, *Rotaru v Romania* (Application no. 28341/95) Judgment 4 May 2000.
ECtHR, *S and Marper v UK* (Application nos 30562/04 and 30566/04) Judgment [GC] 4 December 2008.
ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy [Satakunnan] v Finland* (Application no. 931/13) Judgment [GC] 27 June 2017.
ECtHR, *Smirnova v Russia* (Applications nos. 46133/99 and 48183/99) Judgment Final 24 October 2003.
ECtHR, *Szabó and Vissy v Hungary* (Application no. 37138/14) Judgment Final 6 June 2016.
ECtHR, *von Hannover v Germany* (No. 2) (Applications nos. 40660/08 and 60641/08) Judgment [GC] 7 February 2012.
Emberland, M. (2006). *The Human Rights of Companies: Exploring the Structure of ECHR Protection*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199289837.001.0001.
European Commission, *X v Iceland* (Application no. 6825/74). Decision of 18 May 1976. 5 DR 86.
European Parliament, *Directive (EU) 2016/680 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* [Directive 2016/680].
Goldkind, L., Thinyane, M. & Choi, M. (2018). Small Data Big Justice: The Intersection of Data Science Social Good and Social Services. *Journal of Technology in Human Services*, *36*(4), 175–178. https://doi.org/10.1080/15228835.2018.1539369.
Kitchin, R. (2014). *The data revolution: big data, open data, data infrastructures and their consequences*. Sage.
Land, M. K. & Aronson, J. D. (2018). Technology and Human Rights Enforcement. In M. K. Land & J. D. Aronson (eds) *New Technologies for Human*

Rights Law and Practice, 125–128. Cambridge University Press. https://doi.org/https://doi.org/10.1017/9781316838952.

Mai, J. E. (2016). Big Data Privacy: The Datafication of Personal Information. *The Information Society 32*, 192–199.

Mai, J. E. (2019). Situating Personal Information: Privacy in the Algorithmic Age. In R. F. Jørgensen (ed.), *Human Rights in the Age of Platforms*, 95–116. The MIT Press.

Mayer-Schönberger, V. & Cukier, K. (2013). *Big Data. A Revolution That Will Transform How We Live, Work and Think*. Harper Collins.

McCully, J. (2018). Satakunnan Markkinapörssi Oy and Satamedia Oy V. Finland (Eur. Ct. H.R.) *International Legal Materials 57*, 437–489.

McGregor, L., Murray, D. & Ng, V. (2019). International Human Rights Law as a Framework for Alghorithmic Accountability. *The International and Comparative Law Quarterly 68*, 309–343.

Mejias, U. A. & Couldry, N. (2019). Datafication. *Internet Policy Review*, *8*(4), 1–10. https://doi.org/10.14763/2019.4.1428.

Penney, J. W. (2022). Understanding Chilling Effects. *Minnesota Law Review 106*, 1451–1529.

Ovey, C. & White, R. (2006). *Jacobs and White: The European Convention on Human Rights* (Oxford, Trans.; 4th edn). Oxford University Press.

Rothschild-Elyassi, G. (2022). The Datafication of Law: How Technology Encodes Carceral Power and Affects Judicial Practice in the United States. *Law & Social Inquiry*, *47*(1), 55–94. https://doi.org/10.1017/lsi.2021.10.

Schabas, W. A. (2015) *The European Convention on Human Rights: A Commentary*, Oxford University Press.

Stănescu, L. E. & Onufreiciuc, R. (2020). Some reflections on 'datafication': Data governance and legal challenges. *European Journal of Law and Public Administration*, *7*(1), 100–115. https://doi.org/10.1186/s 13065-015-0118-z.

State of Wisconsin v Eric L. Loomis 2016 WI 68, 881 N.W.2d 749.

van der Sloot, B. (2020). The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 11*, 160–85.

van Dijck, J. (2014). Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society*, *12*(2), 197–208.

Zwanenburg, M. (2021). Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law. *International Law Studies 97*, 1404–1431.