Regulation & Governance

Regulation & Governance **(2020)** doi:10.1111/rego.12331

Algorithmic state surveillance: Challenging the notion of agency in human rights

Eleni Kosta

Tilburg Institute for Law, Technology, and Society, Tilburg University, Tilburg, The Netherlands

Abstract

This paper explores the extent to which current interpretations of the notion of agency, as traditionally perceived under human rights law, pose challenges to human rights protection in light of algorithmic surveillance. After examining the notion of agency under the European Convention on Human Rights as a criterion for applications' admissibility, the paper looks into the safeguards of notification and of redress – crucial safeguards developed by the Court in secret surveillance cases – which are used as examples to illustrate their insufficiency in light of algorithmic surveillance. The use of algorithms creates new surveillance methods and challenges fundamental presuppositions on the notion of agency in human rights protection. Focusing on the victim status does not provide a viable solution to problems arising from the use of Artificial Intelligence in state surveillance. The paper thus raises questions for further research concluding that a new way of thinking about agency for the protection of human rights in the context of algorithmic surveillance is needed in order to offer effective protection to individuals.

Keywords: admissibility, agency, algorithm, human rights, state surveillance, victim.

1. Introduction

"Has a rampaging AI algorithm really killed thousands in Pakistan?" This was the headline of a 2016 article in The Guardian investigating a "killer machine-learning algorithm" guiding the US drone program (Robbins 2016). Numerous articles have been making headlines on the use of Artificial Intelligence (AI) in state snooping and surveillance (Vincent 2018). The Snowden disclosures that started in 2013 reveal surveillance operations in which the US National Security Agency and the UK Government Communications Headquarters were prominently involved. Such operations relied on metadata analysis and geolocation tracking (Gasson *et al.* 2011, p. 251) and led for instance to the identification of human targets and their elimination in Pakistan, Yemen, and beyond (Scahill & Greenwald 2014). Recently, facial recognition fostered by the use of AI has attracted a lot of attention on the challenges it raises for human rights protection. The UK Metropolitan Police Services (MPS) trialed live facial recognition technology during policing operations (Fussey & Murray 2019; Grierson 2019). Similar facial recognition trials were deployed by the Hamburg Police during the 2017 G20 summit (Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit 2018). The Berlin Police also carried out a live facial recognition trial at the Berlin Südkreuz railway station (Delcker 2019).

The development of Big Data analytics and AI offers new technological possibilities for modeling, processing, and exploiting large datasets in unique and unexplored ways. Machine learning algorithms make determinations and predictions about people and offer enhanced capabilities for state surveillance by both law enforcement authorities (LEAs) and security and intelligence agencies (SIAs). The use of AI in surveillance thus opens the doors to a new era of state surveillance, namely *algorithmic surveillance* (Murphy 2017, p. 225; Tannam 2018; Vincent 2018). Novel and crucial challenges for the individuals are raised, putting the protection of human rights at stake, as traditional human rights safeguards, such as notification and redress, are inadequate in dealing with the new challenges of algorithmic surveillance, while often biases (search bias, representation bias) are embedded in the machine learning algorithms, which affect the final outcome of the learning of the algorithm (Mitchell 2015).

Correspondence: Eleni Kosta, Tilburg Institute for Law, Technology, and Society, Tilburg University, PO Box 90153, 5000 LE, Tilburg, The Netherlands. Email: e.kosta@uvt.nl

Accepted for publication 30 May 2020.

Human rights play an important role within the European Union legal order (Cuyvers 2017, p. 382). The protection of human rights emerged in the 18th century as a movement for the "rights of man" (Marks 1981, p. 437). Traditional human rights, commonly known as first-generation human rights, aim at the protection of individuals against state interference to their freedoms (Marks 1981, p. 438). More than a century later a second generation of human rights evolved, relating to equality, which are economic, social, and cultural in nature and require institutional support from the state (Marks 1981, p. 435ff). Both these categories are rights that are recognized for individuals. The third generation of human rights emerged in the 1990s and these are rights of peoples and groups held against their respective states, which aligns with the final tenet of "fraternity." They constitute a broad class of rights that have gained acknowledgment in international agreements and treaties but are more contested than first- and second-generation ones (Twiss 2004; The Levin Institute 2017). AI creates a huge challenge relating to the protection of rights of individuals versus rights of groups subject to surveillance.

Algorithmic surveillance moves beyond the classic surveillance methods where the targets for surveillance are usually fairly specifically identified. Machine and deep learning algorithms have the potential to classify individuals in categories depending on specific parameters and lead to the creation of groups that share some common characteristics. Based on parameters fed by either LEAs or SIAs or as a result of autonomous algorithmic computations, algorithmic surveillance creates groups of people, often even seemingly completely unrelated to each other, whose rights need to be protected. These groups have common interests against state surveillance, but cannot enjoy collective protection as "groups" under the current human rights framework (Kosta 2017, p. 50). In addition, and as common in state surveillance cases, individuals may not know that they have actually been singled out as matching a particular "suspicious" profile or are actually profiled as falling under a specific group, following the application of an algorithm. Traditional European human rights law requires as a rule for offering human rights protection that the applicant is an agent bearing specific characteristics: being an identified natural or legal entity and a victim.

This paper explores the extent to which current interpretations of the notion of agency, as traditionally perceived under human rights law, pose challenges to human rights protection in light of algorithmic surveillance, thus restraining groups of individuals or potential subjects of surveillance from human rights protection. Primary aim of this paper is to identify the challenges relating to agency in the offering of efficient human rights protection, raising questions for further research rather than offering definitive answers. Section 2 provides a brief overview of state surveillance and the use of AI in this context. Section 3 examines the notion of agency under the European Convention on Human Right (ECHR) as a criterion for applications' admissibility. Section 4 illustrates some challenges that algorithmic surveillance brings on the notion of agency in human rights protection. Section 5 finally explores whether there is a need to rethink the notion of agency in the context of human rights protection in light of algorithmic surveillance.

2. State surveillance

2.1. State surveillance: LEAs and SIAs

Gary Marx defines surveillance of humans "as regard or attendance to a person or to factors presumed to be associated with a person" (Marx 2016, p. 15). It can be strategic and nonstrategic, involving the traditional and the new surveillance. The latter "is central to the emergence of a surveillance society with its extensive and intensive (and often remote, embedded) data collection, analysis, and networks" (Marx 2012, p. xxv). LEAs and SIAs have been systematically using algorithms for predictive policing, risk profiling, and pre-emptive surveillance (van Brakel 2016, p. 117; Leese 2014, p. 494; Bennett Moses & Chan 2016, p. 806; Ferguson 2017). Advancements in AI and in machine- and deep learning algorithms enhance the capabilities and potential for surveillance measures, creating a paradigm shift in surveillance, and in state surveillance in particular. Big Data and AI are the reasons and the essence of the shift toward what Marx calls the new surveillance, which offers "the ability to go beyond what is offered to the unaided senses and minds or what is voluntarily reported" (Marx 2012, p. xxv). In this context, private companies play an important role for the exercise of citizen surveillance. New, enhanced technical capabilities, developed by, and used in the private sector allow for novel surveillance methods

(Vincent 2018) that raise unprecedented challenges for individuals and profiled groups, particularly in relation to human rights protection (Fuchs (2012), p. 42; Zuboff 2015, p. 75; Zwick 2015, p. 484). As the shift from public to private surveillance has rightly attracted significant scholarship *already*, this paper focuses on state surveillance – both targeted and untargeted (mass/bulk) – which poses threats for human rights and requires a distinct set of safeguards to ensure their protection.

In the context of this paper algorithmic state surveillance is understood as surveillance carried out by both LEAs and SIAs. SIAs have a broader mandate in the exercise of their activities compared to LEAs (Born & Leigh 2005, p. 140). Although there are differences in the methods that are employed by these two categories of entities, as well as in the regulatory framework on their powers, the boundaries between them are disappearing (Završnik 2013, p. 181). Algorithmic surveillance is offering opportunities that are equally exploited and used by both of them. In addition, when it comes to human rights protection the European Court of Human Rights (ECtHR or Court) seems to be recently applying the same safeguards when surveillance takes place (Vogiatzoglou 2018, p. 566).

2.2. AI in surveillance

AI is "the field that studies *the synthesis and analysis of computational agents that act intelligently*" (Poole & Mackworth 2017, p. 3) based on data analysis and machine learning. This practice is not something new: targeted advertisements, credit rating systems, and airport security alerts all rely on machine learning; a term that was coined in 1959 covering "programming of a digital computer to behave in a way which, if done by human beings or animals, would be described as involving the process of learning" (Samuel 1959, p. 210). Machine learning is a system that relies on additional data or experience in order to improve at a task, according to some measure of performance (Mitchell 1997, p. 4–5); it relies thus on the feeding of initial parameters to a system that allows moving on to association rule mining. Association rule mining allows for the identification of patterns and correlations within the given datasets (Han *et al.* 2011, pp. 279–326). Deep learning is a "form of machine learning, the use of data to train a model to make predictions from new data" (Heaton *et al.* 2017, p. 3).

Mazurowski *et al.* provide a comprehensive overview of the major differences between deep learning and "traditional" machine learning: "In traditional machine learning, the first step is typically feature extraction. This means that to classify an object, one must decide which characteristics of an object will be important and implement algorithms that are able to capture these characteristics. A number of sophisticated algorithms in the field of computer vision have been proposed for this purpose and a variety of size, shape, texture, and other features have been extracted. This process is to a large extent arbitrary, since the machine learning researcher or practitioner often must guess which features will be of use for a particular task and runs the risk of including useless and redundant features and, more important, not including truly useful features. In deep learning, the process of feature extraction and decision making are merged and trainable, and therefore no choices need to be made regarding which features should be extracted; this is decided by the network in the training process. However, the cost of allowing the neural network to select its own features is a requirement for much larger training datasets" (Mazurowski *et al.* 2019, p. 944).

Deep learning algorithms differ from traditional machine learning ones in that they can *automatically* learn representations from data and are inspired by the structure and function of the brain, resembling neural networks. These artificial neural networks "provide a computer processing model that mimics networks of neurons in living biological systems" (Brookshear 2012, p. 489) and learn "the proper weight values via supervised training" (Brookshear 2012, p. 492). So, deep learning resembles a "black box" that reaches a specific decision, which cannot be fully explained. Researchers are however developing Explainable AI, whose functioning can be understood by humans. van Lent *et al.* coined the term "explainable artificial intelligence" to describe the ability of their system to summarize the events of the game/simulation, flag key events, and explain the behavior of computer controlled entities" (van Lent *et al.* 2004, p. 900; Core *et al.* 2006, p. 1766).

The use of AI and machine- and deep-learning in the field of surveillance are shaping the so-called new surveillance. Data are collected using different means and methods, they are processed, combined, and analyzed in new ways using AI (Lyon 2014, p. 4). David Lyon has successfully summarized the new potential offered to surveillance: "Now bulk data are obtained and data are aggregated from different sources before determining the full range of their actual and potential uses and mobilizing algorithms and analytics not only to understand a past sequence of events but also to predict and intervene before behaviors, events, and processes are set in train" (Lyon 2014, p. 4). Algorithmic surveillance increasingly targets persons as parts of a group rather than as individuals. Even when people may not be individually identified, they remain reachable. Algorithmic surveillance moves beyond the classic surveillance methods where the targets for surveillance are usually fairly specifically identified. Machine and deep learning algorithms have the potential to classify individuals in categories depending of specific parameters and lead to the creation of groups that share some common characteristics. Based on parameters either fed by LEAs and SIAs or as a result of autonomous algorithmic computations, algorithmic surveillance creates groups of people, often even seemingly completely unrelated to each other, whose rights need to be protected. These can for instance be groups of individuals that relate to a certain cultural or societal phenomenon, or groups that are targeting when they meet a specific criterion (for instance they are in touch with suspects x, y, z) or groups of individuals that have been singled out because they meet a number of criteria specified by a machine learning system.

The distinction introduced by Yeung between *reactive* and *pre-emptive* algorithmic systems is interesting for the discussion of algorithmic state surveillance. Such surveillance may rely on information gathering and monitoring and the machine learning systems may operate "on a *reactive* basis, configured automatically to mine historic performance data in real-time to detect violation" or "may be configured to detect violations on a *pre-emptive* basis, applying machine-learning algorithms to historic data to infer and thereby predict *future* behavior" (Yeung 2018, p. 508). The use of reactive algorithmic systems for state surveillance, which "trigger and automated response based on algorithmic analysis of historic data" (Yeung 2018, p. 509) in principle would lead to targeted surveillance measures. However, the use of pre-emptive algorithmic systems for state surveillance can be understood "as a form of systematic surveillance-driven social sorting" may lead to profiling the sorting of individuals into groups (Yeung 2018, pp. 511–512) and subject individuals to state surveillance without real suspicion. Individuals are usually oblivious of the profiling and they cannot understand how decisions about them are made (Yeung 2018, p. 515).

Algorithmic groups are in principle dynamic, which has impact on the protection of human rights. In particular in relation to privacy protection "group privacy may be infringed even in cases in which the members of the group are not aware of this: a group that has been silently profiled and that is being targeted as a group does not need to know any of this to have a right to see its privacy restored and respected" (Taylor *et al.* 2017, p. 7). The concept of group privacy attempts to supplement individual privacy and the question whether a group would have the right to invoke the right to privacy is definitely an open one at the moment, with scholars like van der Sloot arguing that groups should be "allowed to invoke a right to privacy to protect their group interest" (van der Sloot 2017, p. 216).

Explicit or implicit biases in machine learning algorithms can also lead to discrimination (Barocas & Selbst 2016), which cannot be protected under the current framework. Individuals may not know they have been singled out as matching a "suspicious" profile or fall under a dynamic algorithmic group (Taylor *et al.* 2017, p. 7; Kosta 2017, p. 50). The right to individual petition for human rights protection is "the keystone of the supervision process" (Reid 2015, p. 57-003) of the ECtHR. In order to explore the rights of groups in relation to algorithmic state surveillance in human right protection, we first need to study the notion of agency in European human rights: *who* is the victim of a violation, a question that is based on a fundamental presupposition that it is assumed that the "victim" of a violation is or can be known. I argue that algorithmic state surveillance challenges this presupposition and questions the notion of agency *ratione personae* in its core. Before exploring whether algorithmic surveillance challenges this presupposition, this paper will examine the notion of agency in the European Convention on Human Rights, as a fundamental element of the admissibility requirements, set out in Article 34 ECHR.

3. Agency under the ECHR

3.1. Article 34 ECHR

Article 34 ECHR states that "[t]he Court may receive applications from any person, nongovernmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right". The importance of Article 34 has been repeatedly highlighted by the Court. It has been characterized as "one of the keystones in the machinery for the enforcement of the rights and freedoms set forth in the Convention" (*Klass and Others v. Germany* 1978, para. 34) and as "one of the fundamental guarantees of the effectiveness of the Convention system of human rights protection. In interpreting such a key provision, the Court must have regard to the special character of the Convention as a treaty for the collective enforcement of human rights and fundamental freedoms. Unlike international treaties of the classic kind, the Convention comprises more than mere reciprocal engagements between Contracting States. It creates, over and above a network of mutual, bilateral undertakings, objective obligations which, in the words of the Preamble, benefit from a 'collective enforcement'" (Schabas 2015, p. 734; citing *Mamatkulov and Askarov v. Turkey* 2005, para. 100; *Loizidou v. Turkey* 1995, para. 70). Following this Article individual applications need to fulfill two requirements in order to be admissible: the applicant "must fall into one of the categories of petitioners mentioned in Article 34 and must be able to make out a case that he or she is the victim of a violation of the Convention." (Schabas 2015, p. 736, citing *Vallianatos and Others v. Greece* 2013. para. 47).

3.2. Entities

Any person, nongovernmental organization or group of individuals may be applicant. The Convention does not set out any rules, requirements or limitations in this regard. Any person, irrespective or their legal capacity, nationality or age are allowed to file an application to the ECtHR. It is interesting to note that any person can be applicant, even when in accordance with national legislation they would be deprived of legal capacity (Schabas 2015, p. 736). The Court has accepted applications by minor applicants, that is, applicants under the age of 18, as well. The term nongovernmental organizations is equally very broad. There are no requirements in order to qualify an organization as such: there is no obligation for it to be subject to formalities of registration, nor to have an official corporate status (Schabas 2015, p. 736). However, governmental bodies or public corporations, under the control of the State cannot be applicants (Rainey *et al.* 2017, p. 29). Notwithstanding the broadness of this Article, as confirmed by the case law of the ECtHR, the applicant needs to be an identified natural or legal entity, in order for the Court to then examine the second criterion, that is, the victim status.

3.3. Victim status

The second requirement is that the entity that files an application shall claim to be a "victim" of a violation of the rights protected by the Convention and its Protocols. Traditionally the Court has held that the victim status is recognized to the applicants when they are "directly affected by the impugned measure" (Schabas 2015, p. 736). The notion of victim is not to be interpreted in line with the relevant national legislation; it has "an autonomous and independent meaning" (Schabas 2015, p. 738) and is examined by the Court on a case by case basis. Dead persons are not recognized as applicants; however, the Court has recognized in several cases next-of-kin applications (Schabas 2015, p. 736).

As a rule, applicants cannot undertake an *in abstracto* claim, that is, a claim against a law or a policy without any personal effect on the applicants or an *actio popularis*, that is, an act "to initiate abstract review regardless of their specific legal interest in the case in question" (Sadurski 2005, p. 6) to protect the rights of others or of the society. This is in line with the argumentation of the ECtHR that is role is "to determine whether the manner in which they were applied to, or affected the applicant gave rise to a violation of the Convention" (Roman *Zakharov v. Russia* 2015, para. 164). However, occasionally the Court has allowed the submission of cases where the applicants suspect interference of their rights that are protected under the Convention, even when they cannot prove it, especially in relation to secret surveillance (van der Sloot 2016, pp. 419–422, 426–429).

3.4. Toward acceptance of *in abstracto* claims in surveillance cases

State surveillance typically does not affect one specific individual, but rather large parts of society. The legal question with respect to laws that grant powers of bulk interception to intelligence agencies is not so much whether concrete harm has been done to a person in a concrete instance, and whether such interference would be legitimate. Rather, what is at stake is whether the law itself conforms to the principles of legality, legitimacy and incorporates sufficient checks and balances to mitigate the risk of abuse of power.[1] In *Zakharov v. Russia* and *Szabó and Vissy v. Hungary*, the Court made concrete reflections on admissibility in surveillance cases. The Court accepted that "the secret nature of surveillance measures would deprive individuals of access to effective review [seeing] the mere existence of surveillance laws as a threat" (Cole & Vandendriessche 2016, p. 129) and explicitly stated that it accepts *in abstracto* claims (*Roman Zakharov v. Russia* 2015, para. 178). The Court elaborated on *κennedy v. UK* and established in *Roman Zakharov v. Russia* a harmonized approach, laying down concrete conditions for admissibility in cases of secret surveillance, bringing an end to the ambiguity regarding *in abstracto* considerations by the Court:

> *(…) the Court accepts that an applicant can claim to be the victim of a violation occasioned by the* mere existence *of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the* scope of the legislation *permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the* availability of remedies *at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies. (emphasis added) (*Roman Zakharov v. Russia *2015, para. 171)*

Judge Dedov in his concurring opinion in *Zakharov v. Russia* questioned the Court's competence to examine the domestic law *in abstracto* (*Roman Zakharov v. Russia* 2015, Concurring opinion of Judge Dedov). He referred to *Klass and Others v. Germany* (1978) and *Kennedy v. UK* (2010) where the Court examined *in abstracto* the national law is Germany and the United Kingdom, respectively. He recognized though that both countries[2] were involved directly or indirectly in the mass surveillance scandals revealed by Edward Snowden, claiming that "[t]his indicates that something was wrong with the Court's approach from the very outset" (*Roman Zakharov v. Russia* 2015, Concurring opinion of Judge Dedov). Nevertheless, the Grand Chamber in *Zakharov v. Russia* implicitly acknowledged that the technological developments that facilitate secret surveillance allow for and actually dictate a change in the position of the Court in order for it to accept *in abstracto* examination of domestic laws in cases of secret surveillance, something that was clearly stated in *Szabó and Vissy v. Hungary*.

Following *Zakharov v. Russia* and *Szabó and Vissy v. Hungary*, the Court established in cases of secret surveillance, two conditions – the scope of legislation and the availability of remedies – that shall be fulfilled in order to recognize the applicants as victims. In this way it brought the two main admissibility issues under one umbrella: the discussion on general challenges and the effectiveness of national remedies. In the recent *Big Brother Watch and Others v. UK* the Court repeated the two criteria under which such *in abstracto* claims would be accepted, established in *Roman Zakharov v. Russia* (*Big Brother Watch and Others v. UK* 2018, para. 392).

4. Challenges posed by algorithmic surveillance on the admissibility criteria

The ECHR introduces minimum safeguards for the protection of human rights (European Commission for Democracy through Law 2015, p. 24) and has been used as a tool for the protection of individuals against state surveillance for almost half a century. The FRA considers ECHR standards a benchmark when assessing surveillance legislation or a surveillance practice (European Union Agency for Fundamental Rights 2015, p. 10). However, the safeguards developed by the ECtHR are woefully insufficient when addressing the needs for human rights protection in view of modern algorithmic state surveillance, which challenges human rights protection at its core and raises new questions that require rethinking of the traditional approaches. Algorithmic regulation has triggered a number of concerns "about accountability, fairness, bias, autonomy, and due process-exacerbated by the widely bemoaned opacity and inscrutability of computational systems" (Ziewitz 2016, p. 4). Relevant to these concerns are two cornerstone safeguards in human right protection in relation to state surveillance: notification and redress. Both these safeguards rely on the assumption that the applicant can be identified: an applicant shall be known in order for notification to be served and a person shall be known in order for him or her to exercise their rights to redress.

4.1. Notification

Notification requires that the persons concerned should be informed "[a]s soon as notification can be carried out without jeopardizing the purpose of the restriction after the termination of the surveillance measure" (*Roman Zakharov v. Russia* 2015, para. 287). It has been thus established case law of the ECtHR that the notification of interception of communications is "inextricably linked to the effectiveness of remedies before the courts" (*Roman Zakharov v. Russia* 2015, para. 234) and that the persons concerned should be informed "[a]s soon as notification can be carried out without jeopardizing the purpose of the restriction after the termination of the surveillance measure" (*Roman Zakharov v. Russia* 2015, para. 287). The issue of notification of the affected individuals (Boehm & De Hert 2012) was also crucial in *Tele2/Watson*, where the Court of Justice of the European Union (CJEU) stated that "the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardize the investigations being undertaken by those authorities" (*Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* 2016, para. 121). However, the UK Investigatory Powers Tribunal (UK IPT) found the notification requirements to "be very damaging to national security."[3] The UK IPT recognized that the notification requirements would be difficult to enforce in relation to bulk data and wondered on its practical implantation.[4] The UK IPT sent a request for a preliminary ruling to the CJEU, which will have to clarify its position on the limits, if any, of the notification requirement in the first place, something that is especially to be expected if decisions are based on algorithmic computations (case pending at the time of writing).[5] False negatives and false positives in AI systems are still a reality and technology is far from finding the perfect algorithms that will always make a correct decision. Ex post notification is definitely not ensuring that wrongful surveillance measures will not be taken. How can the notification requirement be implemented when the surveillance measure is not addressed to named individuals but to any person matching a (potentially dynamic) profile? And even if the individuals affected can be identified, does it still make sense to contact hundreds, thousands or potentially even millions of people?

4.2. Redress

Notification, discussed earlier, is "inextricably linked to the effectiveness of remedies before the courts" (*Klass and Others v. Germany* 1978, para. 57; *Weber and Saravia v. Germany* 2006, para. 135; *Roman Zakharov v. Russia* 2015, para. 286) and omission of such notification after surveillance measures has been found as violation of the right to an effective remedy -among others (Boehm & De Hert 2012). The right to an effective remedy is essential component of access to justice, and empowers individuals to seek redress against infringements to their rights (European Union Agency for Fundamental Rights 2015, p. 61). Criticizing the rise of algorithmic power, Yeung notes that "the profiled individual is typically oblivious to how she is being profiled (or indeed that she is being profiled at all), and has no opportunity to understand the basis upon which assessments about her are made. Hence, it is practically impossible for any individual to assert a claim of right, to protest that she is "not like that," or that while she might have been like that in the past, she does not propose to be "like that" in the future. In other words, concerns about the profiling process may not lend themselves easily to the claiming of individual rights, given the nature and structure of fundamental rights within contemporary western jurisprudence" (Yeung 2018, p. 515). Especially in cases of secret surveillance, there may be complete lack of awareness that such surveillance takes place, so the affected subjects cannot seek for redress. This difficulty is increased, both in terms of scale and in terms of nature. Linked to the discussion above under notification, who can exercise their right to effective remedies? How can the affected individuals seek for redress if they do not know that they are subject of surveillance? Or even more challenging, how can the affected individuals seek for redress if the system itself does not know exactly who has been subject of surveillance? How can the effectiveness of remedies be measured in relation to the harm caused? These are questions that future research will have to focus on.

4.3. Interim thoughts

The brief examination of the aforementioned existing safeguards has illustrated their insufficiency to address the challenges incurred by algorithmic surveillance because they assume knowledge of the entity that has been victim of a violation. State algorithmic surveillance questions the notion of *ratione personae* in its very core. The safeguards discussed above illustrate that the question whether an applicant has "individually and substantially" (van der Sloot 2016, p. 416) suffered from a human rights violation cannot be answered in a definite way.

5. Need to rethink agency in human rights in light of algorithmic state surveillance?

5.1. *In abstracto* claims

As elucidated in Section 3, the ECHR admissibility system relies on two crucial assumptions: that the applicant can be identified, be it a natural person, a nongovernmental organization or a group of (identified) individuals and that the applicant is a victim of a violation. In relation to admissibility of applications in surveillance cases, the Court has followed until now three different approaches: (i) it focuses on "reasonable likelihood" of a hypothetical harm; (ii) it accepts a "chilling effect" in relation to a future harm; and finally (iii) it accepts *in abstracto* claims (van der Sloot 2016, p. 411). As discussed in Section 3, the Court has accepted *in abstracto* claims in cases of state surveillance in order to tackle challenges that are raised by state surveillance. Would this position of the Court be suitable to resolve the challenges on the notion of agency, as exemplified in Section 4?

The Court accepted *in abstracto* claims even before *Roman Zakharov v. Russia*. Already in *Klass v. Germany* the Court recognized that the mere existence of secret surveillance regulation or of secret surveillance measures could suffice for an applicant to be recognized as victim of the alleged violation, even when they could not prove that the measures had been applied to them (*Klass and Others v. Germany* 1978, para. 34). In a series of cases, the Court followed the line of *Klass v. Germany* and accepted the status of victim to applicants based on the mere existence of such secrete surveillance measures or legislation (*Malone v. United Kingdom* 1984, para. 64; *Weber and Saravia v. Germany* 2006, para. 78; Association for European Integration and Human Rights and Ekimdzhiev 2008, paras. 58, 59, 69; *Liberty and Others v. United Kingdom* 2008, paras. 56–57). In some other cases, the ECtHR tried to limit the broad interpretation of the notion of a victim requiring "a reasonable likelihood that the security services had compiled and retained information concerning his private life" (*Roman Zakharov v. Russia* 2015, para. 167). Given these two different interpretations of the notion of a victim, in *Roman Zakharov v. Russia* the Court tried to develop a harmonized approach for the interpretation of Article 34 in cases of secret surveillance.

In *Roman Zakharov v. Russia* the Court recognizes that "an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures" (*Roman Zakharov v. Russia* 2015, para. 171). However this can be accepted when two criteria are met: The Court will take "into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies." (*Roman Zakharov v. Russia* 2015, para. 171). This criterion clearly makes reference to legislation permitting secret surveillance measures in the context of which the Court will examine whether the applicant can *possibly* be affected by it.

The Court repeated these criteria in *Big Brother Watch v. UK* where the Court summarized these two criteria in a slightly simpler way: "Where the domestic system did not afford an effective remedy, there would be a greater need for scrutiny by the Court and the individual would not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures *only if* he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures" (Big *Brother Watch and Others v. UK* 2018, para. 392). The formulation of the two criteria in *Big Brother Watch v. UK* seems to clarify the *Zakharov* criteria in a stricter way: if the national legislation provides for effective remedies, then the individual may claim to be a victim of a violation *only if* they are able to show that they are at potential risk of being subjected to such measures, an issue that will be judged based on the personal situation of the applicant.

In *Roman Zakharov v. Russia* the Court found that the Russian legislation does not provide for effective remedies (*Roman Zakharov v. Russia* 2015, para. 176) and therefore "the applicant does not need to demonstrate that, due to his personal situation, he is at risk of being subjected to secret surveillance" (*Roman Zakharov v. Russia* 2015, para. 177). The Court came to a similar conclusion in *Szabó and Vissy v. Hungary*: the applicants in that case were staff members of a watchdog organization and argued that their position as members of a civil rights organization "were at particular risk of having their communications intercepted as a result of their employment with civil-society organisations criticising the Government" (*Szabó and Vissy v. Hungary* 2016, para. 37). However the Court found that due to the lack of effective remedies there was no particular reason to examine whether they were at risk of being subjects of the surveillance measures and did not examine this issue.

In *Big Brother Watch v. UK* the Court examined the admissibility criteria in the three joined cases and with regard to various alleged violations. With regard to the regime for the bulk interception of communications under section 8(4) of RIPA the applicants in all three cases were recognized as victims. In relation to the complaints about intelligence sharing, the Court recognized that the UK legislation offered effective remedies. However, the Court accepted that "the applicants were potentially at risk of having their communications requested from a foreign intelligence service [and that] they were also potentially at risk of having their communications obtained by a foreign intelligence service" (*Big Brother Watch and Others v. UK* 2018, para. 395) and therefore found they that be victims of the alleged violation relating to the intelligence sharing regime. With regard to the Bureau of Investigative Journalism and Alice Ross, the Court recognized them as victims on the basis of the argument that although the UK legislation had effective remedies in place in relation to the request of specific communications data under Chapter II of RIPA they were potentially at risk: "Given that the applicants in the second of the joined cases are investigative journalists who have reported on issues such as central intelligence agency torture, counter-terrorism, drone warfare, and the Iraq war logs, the Court would accept that they were potentially at risk of having their communications obtained by the UK authorities either directly, through a request to a communications service provider (CSP) for their communications data, or indirectly, through a request to a CSP for the communications data of a person or organisation they had been in contact with" (*Big Brother Watch and Others v. UK* 2018, para. 454).

5.2. The insufficiency of relying on *in abstracto* claims

Undoubtedly the adoption of a clear harmonized approach on the interpretation of the notion of a victim in the context of secret surveillance is very valuable and is bound to offer legal security to the applicants in such cases. The applicants in *Roman Zakharov v. Russia*, in *Szabó and Vissy v. Hungary* and in *Big Brother Watch v. UK* could not prove that they have been affected by secret surveillance measures. The Court following the criteria established in *Roman Zakharov v. Russia* examined in all these cases first whether there were effective remedies in place. If the national legislation provided for effective remedies, then the Court required the applicants to show that they were potentially at risk; if no effective remedies were foreseen, then any applicant could be considered as potential victim of the alleged violation. However, all these applicants were either journalists or member of civil rights of organizations or in any case entities that had a special interest in the protection of human rights. Eijkman argues that "the admissibility of groups, who may for no apparent reason be singled out by algorithms, should be considered" (Eijkman 2017, p. 132) by the ECtHR.

The question however remains, whether the harmonized approach can be the tool to solve the issues relating to agency in view of the challenges raised by the use of AI in state surveillance, as discussed above. Even if effective remedies exist for a secret surveillance measure that is taken on the basis of algorithmic computations, is it really meaningful for the average citizen? The discussion about remedies is extremely important, but it comes into play only when somebody has at least a vague suspicion that they may be subjects of secret state surveillance. AI can be used to scan entire populations or parts of a population and create profiles in order to place individuals in groups that are then placed under secret surveillance; it can also be used to feed the algorithm with criteria based on which individuals are placed under secret surveillance in order to find potential suspects that are then placed under secret surveillance. Leaving aside the fact that the criteria that feed the algorithms as well as the decisions made can be dynamic, raising ethical and legal issues relating to nondiscrimination, equality of arms, etc., one fundamental concern is how can the individual even suspect that they may be subject of such secret surveillance measures. The simple answer is that they cannot. National legislation on secret surveillance cannot be too detailed or too concrete, because exactly the whole power of such surveillance relies on the use of algorithms and AI technologies that are not static or predefined. When the national legislation provides for effective remedies, then it will be very impossible for applicants to prove that they are potentially at risk. Even in cases when, following the *Zakharov* criteria, the national legislation on secret surveillance does not provide effective remedies, the way that such legislation is drafted will make it too difficult for individuals to guess that perhaps they are affected by the secret surveillance measure.

Focusing on the victim status has proven extremely problematic in light of algorithmic state surveillance. However, algorithmic surveillance challenges a very central element in human rights protection, the notion of agency: *who* is the victim of a violation, a question that is based on a fundamental presupposition that it is assumed that the "victim" of a violation is or can be known. The assumption that the first admissibility criterion of Article 34 ECHR that the applicant can be any (identified) person, nongovernmental organization or group of individuals is met should not be taken for granted. In cases of group profiling for instance it is not always possible to identify the individuals that are subject to the secret surveillance measures, as often in pre-emptive algorithmic systems predictions on future behavior of individuals are made, relying on algorithmic assessment of historic data (see Section 2.2). In other cases, the targets of secret surveillance are dynamic and the entity affected cannot be spotted. And more importantly, individuals are unaware of the fact that they are subjects of surveillance.

The adoption of a harmonized approached on the victim status in secret surveillance cases and the acceptance by the ECtHR of *in abstracto* claims in relation to secret surveillance measures is of high importance for the protection of human rights. However, this new approach does not solve problems on the notion of agency raised by the use of AI in state surveillance, secret or not, as the latter questions a fundamental presupposition in human rights protection, that the victim of the alleged violation is or can become known.

6. Conclusions

This paper explored the extent to which current interpretations of the notion of agency, as traditionally perceived under human rights law, pose challenges to human rights protection in light of algorithmic surveillance. It examined the notion of agency under the European Convention on Human Rights as a criterion for applications' admissibility. It elucidated on the two admissibility criteria: the entities that can file an application and the victim status. The interpretation of the victim status in secret surveillance cases has been expanded in the case law of the ECtHRs in order to accept *in abstracto* claims under specific criteria.

The safeguards of notification and of redress – crucial safeguards developed by the Court in the context of protection of human rights, and in particular the right to privacy, in secret surveillance cases – were used as examples to illustrate their insufficiency in light of algorithmic surveillance. The use of algorithms for state surveillance creates new surveillance methods and challenges fundamental presuppositions on the notion of agency in human rights protection. A close analysis of the Court's approach to the admissibility criteria of Article 34 ECHR in recent ECtHR case law on secret surveillance showed that the focus of the Court's analysis lies on the victim status. The existence of effective remedies is crucial in order to acknowledge the victim status to applicants with or without the need to demonstrate that they are potentially at risk.

This approach however is not providing a viable solution to problems arising from the use of AI in state surveillance, as it assumes that the individuals can suspect that they are potentially at risk and argue that in front of the Court. Even when applicants do not need to show that they are potentially at risk, there would need to be some indication that the secret surveillance measure resulting from the use of AI can be relevant for them. Problems relating to group profiles or dynamic groups discussed in the paper show that in some cases it is impossible to actually know *who* is or could be victim of the surveillance measure. Therefore, further research is needed in order to find a completely new way of thinking about agency for the protection of human rights in the context of algorithmic surveillance in order to offer effective protection to individuals.

Endnotes

[1] *Szabó and Vissy v. Hungary* 2016, para. 32: "in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has accepted that, under certain circumstances, an individual may claim to be a victim on account of the mere existence of legislation permitting secret surveillance, even if he cannot point to any concrete measures specifically affecting him."

[2] In this context Judge Dedov recalled that "the mobile telephone conversations of the Federal Chancellor of Germany were unlawfully intercepted by the national secret service; and secondly, the UK authorities provided a US secret service with access to and information about the former State's entire communication database" (Roman Zakharov v Russia 2015, Concurring opinion of Judge Dedov).

[3] Judgment of 8 September 2017 [2017] UKIPTrib IPT_15_110_CH, para. 63.

[4] Judgment of 8 September 2017 [2017] UKIPTrib IPT_15_110_CH, para. 64.

[5] Order for reference to the Court of Justice of the European Union issued in case [2017] UKIPTrib_IPT_15_110_CH. Available at: http://www.ipt-uk.com/docs/IPT%20BULK%20DATA%20ORDER%20FOR%20REFERENCE%20TO%20CJEU.pdf (Accessed 13 July 2019).

References

Barocas S, Selbst A (2016) Big Data's Disparate Impact. *California Law Review* 104, 671–732.

Bennett Moses L, Chan J (2016) Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability. *Policing and Society* 28(7), 806–822.

Boehm F, De Hert P (2012) Notification, an Important Safeguard against the Improper Use of Surveillance – Finally Recognized in Case Law and EU Law. *European Journal of Law and Technology* 3(3). [Last accessed 13 Jul 2019.] Available from URL: http://ejlt.org/article/view/155/264.

Born H, Leigh I (2005) *Making Intelligence Accountable – Legal Standards and Best Practice for Oversight of Intelligence Agencies*. Publishing House of the Parliament of Norway, Oslo.

Brookshear JB (2012) *Computer Science*, 11th edn. Reading, MA: Pearson (Addison-Wesley).

Cole M, Vandendriessche A (2016) From *Digital Rights Ireland* and *Schrems* in Luxembourg to *Zakharov* and *Szabó/Vissy* in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance. *European Data Protection Law Review* 2(1), 121–129.

Core M, Lane HC, van Lent M, Gomboc D, Solomon S, Rosenberg M (2006) Building Explainable Artificial Intelligence Systems. *Proceedings of the 18th Innovative Applications of Artificial Intelligence Conference*, pp. 1766–1773. Boston, Massachusetts: AAAI Press. [Last accessed 13 Jul 2019.] Available from URL: https://pdfs.semanticscholar.org/5bff/e555e2a9d1976f8180ab2aed4f738ffa2f34.pdf.

Cuyvers (2017) Judicial Protection under EU Law: Direct Actions. In: Ugirashebuja E, Eudes Ruhangisa J, Ottervanger T, Cuyvers A (eds) *East African Community Law: Institutional, Substantive and Comparative EU Aspects*, pp. 254–264. Leiden Boston: Brill Nijhoff.

Delcker J (2019) Big Brother in Berlin – As Germany Dabbles in State Surveillance, Facial-Recognition Technology Raises Privacy Concerns, *Politico*, 19 Apr. [Last accessed 30 Sep 2019.] Available from URL: https://www.politico.eu/article/berlin-big-brother-statesurveillance-facial-recognition-technology/

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit. *Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg*.(2018). [Last accessed 21 Jan 2020.] Available from URL: https://datenschutzhamburg.de/assets/pdf/Pruefbericht_Gesichtserkennungssoftware.pdf

Eijkman Q (2017) Indiscriminate Bulk Data Interception and Group Privacy: Do Human Rights Organisations Retaliate through Strategic Litigation? In: Taylor L, Floridi L, van der Sloot B (eds) *Group Privacy – New Challenges of Data Technologies*, pp. 123–138. Switzerland: Springer.

European Commission for Democracy through Law (Venice Commission) (2015) *Update of the 2007 Report on the Democratic Oversight of the Security Services*. Study No. 719/2013, Doc. CDL-AD(2015)006.

European Union Agency for Fundamental Rights (FRA) (2015) *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Mapping Member States' Legal Frameworks*. Vienna, Austria: Publications Office of the European Union.

Ferguson A (2017) *The Rise of Big Data Policing: Surveillance, Race and the Future of Law Enforcement*. New York University Press, New York.

Fuchs C (2012) Google Capitalism. *tripleC: Communication, Capitalism and Critique* 10(1), 42–48.

Fussey P, Murray D (2019) *Independent Report on London Metropolitan Police's Services Trials of Live Facial Recognition Technology*. Project Report. [Last accessed 21 Jan 2020.] Available from URL: http://repository.essex.ac.uk/24946/

Gasson M, Kosta E, Royer D, Meints M, Warwick K (2011) Normality Mining: Privacy Implications of Behavioral Profiles Drawn from GPS Enabled Mobile Phones. *IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews* 41(2), 251–261.

Grierson J (2019) *Police Trials of Facial Recognition Backed by Home Secretary*. *The Guardian*, 12 July. [Last accessed 21 Jan 2020.] Available from URL: https://www.theguardian.com/uk-news/2019/jul/12/police-trials-facial-recognition-home-secretary-sajidjavid-technology-human-rights

Han J, Kamber M, Pei J (2011) *Data Mining: Concepts and Techniques*, 3rd edn. Waltham, MA: Morgan Kaufmann Publishers.

Heaton JB, Polson N, Witte J (2017) Deep Learning for Finance: Deep Portfolios. *Applied Stochastic Models in Business and Industry* 33(1), 3–12.

Kosta E (2017) *Surveilling Masses and Unveiling Human Rights – Uneasy Choices for the Strasbourg Court*. Inaugural Address (Tilburg Law School Research Paper. [Last accessed 12 Jul 2019.] Available from URL: https://ssrn.com/abstract=3167723

Leese M (2014) The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-Discriminatory Safeguards in the European Union. *Security Dialogue* 45(5), 494–511.

Lyon D (2014) Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society*. 1(2), 1–13.

Marks S (1981) Emerging Human Rights: A New Generation for the 1980s. *Rutgers Law Review* 33, 435–452.

Marx GT (2012) "Your Papers Please": Personal and Professional Encounters with Surveillance, Preface. In: Ball K, Haggerty K, Lyon D (eds) *Routledge Handbook of Surveillance Studies*, pp. xx–xxxi. Abington Oxon: Routledge.

Marx GT (2016) *Windows into the Soul: Surveillance and Society in an Age of High Technology*. The University of Chicago Press, Chicago.

Mazurowski M, Mateusz B, Ashirbani S, Mustafa B (2019) Deep Learning in Radiology: An Overview of the Concepts and a Survey of the State of the Art with Focus on MRI. *Journal of Magnetic Resonance Imaging* 49(4), 939–954.

Mitchell T (1997) *Machine Learning*, 1st edn. New York: McGraw Hill.

Mitchell T (2015) Generative and Discriminative Classifiers: Naïve Bayes and Logistic Regression. In: Mitchell TM (ed) *Machine Learning*, 2nd edn. New York: McGraw Hill. [Last accessed 22 Jan 2020.] Available from URL: http://www.cs.cmu.edu/%7Etom/mlbook/NBayesLogReg.pdf.

Murphy MH (2017) Algorithmic Surveillance: The Collection Conundrum. *International Review of Law, Computers & Technology* 31(2), 225–242.

Poole D, Mackworth A (2017) *Artificial Intelligence – Foundations of Computational Agents*, 2nd edn. Cambridge: Cambridge University Press.

Rainey B, Wicks E, Ovey C (2017) *Jacobs, White, and Ovey, the European Convention on Human Rights*, 7th edn. Oxford University Press, Oxford.

Reid K (2015) *A Practitioner's Guide to the European Convention of Human Right*, 5th edn. London: Sweet & Maxwell.

Robbins M (2016) Has a Rampaging AI Algorithm Really Killed Thousands in Pakistan? *The Guardian*, 18 Feb. [Last accessed 12 Jul 2019.] Available from URL: https://www.theguardian.com/science/the-lay-scientist/2016/feb/18/has-a-rampaging-ai-algorithm-really-killed-thousands-in-pakistan

Sadurski W (2005) *Rights before Courts: A Study of Constitutional Courts in Postcommunist States of Central and Eastern Europe*. Dordrecht, The Netherlands: Springer.

Samuel AL (1959) Some Studies in Machine Learning Using the Game of Checkers. *IBM Journal of Research and Development* 3(3), 210–229.

Scahill J, Greenwald G (2014). The NSA's Secret Role in the U.S. Assassination Program. *The Intercept*, 10 Feb. [Last accessed 12 Jul 2019.] Available from URL: https://theintercept.com/2014/02/10/the-nsas-secret-role/

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

Tannam E (2018). State Surveillance and Automated Warfare: Experts Call for AI Regulation, *Siliconrepublic*, 21 Feb. [Last accessed 12 Jul 2019.] Available from URL: https://www.siliconrepublic.com/enterprise/ai-cyberattacks-artificial-intelligence

Taylor L, Floridi L, van der Sloot B (2017) Introduction: A New Perspective on Privacy. In: Taylor L, Floridi L, van der Sloot B (eds) *Group Privacy – New Challenges of Data Technologies*, pp. 1–7. Cham, Switzerland: Springer.

The Levin Institute (2017). *Three Generations of Human Rights*. [Last accessed 8 Oct 2018.] Available from URL: http://www.globalization101.org/three-generations-of-rights/

Twiss S (2004) History, Human Rights, and Globalization. *Journal of Religious Ethics* 32(1), 39–70.

van Brakel R (2016) Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing. In: van der Sloot B, Broeders D, Schrijvers E (eds) *Exploring the Boundaries of Big Data*, pp. 117–141. The Hague, The Netherlands: Amsterdam University Press.

van Lent M, Fisher W, Mancuso M (2004) An Explainable Artificial Intelligence System for Small-Unit Tactical Behaviour. *Proceedings of the 16th Innovative Applications of Artificial Intelligence Conference*, pp. 900–907. San Jose, California: AAAI Press. [Last accessed 8 Oct 2018.] Available from URL: https://www.aaai.org/Papers/IAAI/2004/IAAI04-019.pdf.

van der Sloot B (2016) Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities. In: Gutwirth S, Leenes R, de Hert P (eds) *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, pp. 411–436. Dordrecht, The Netherlands: Springer.

Van der Sloot B (2017) Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected under Article 8 ECHR. In: Taylor L, Floridi L, van der Sloot B (eds) *Group Privacy – New Challenges of Data Technologies*, pp. 197–224. Cham, Switzerland: Springer.

Vincent J (2018). Drones Taught to Spot Violent Behavior in Crowds Using AI. *The Verge*, 6 Jun. [Accessed: 12 July 2019.] Available from URL: https://www.theverge.com/2018/6/6/17433482/ai-automated-surveillance-drones-spot-violent-behavior-crowds

Vogiatzoglou P (2018) Centrum för Rättvisa v. Sweden: Bulk Interception of Communications by Intelligence Services in Sweden Does Not Violate the Right to Privacy. *European Data Protection Law Review* 4(4), 563–567.

Yeung K (2018) Algorithmic Regulation: A Critical Interrogation. *Regulation and Governance* 12(4), 505–523.

Završnik A (2013) Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance? *Journal of Contemporary European Research* 9(1), 181–202.

Ziewitz M (2016) Governing Algorithms: Myth, Mess, and Methods. *Science, Technology, & Human Values* 41(1), 3–16.

Zuboff S (2015) Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30, 75–89.

Zwick D (2015) Defending the Right Lines of Division: Ritzer's Prosumer Capitalism in the Age of Commercial Customer Surveillance and Big Data. *The Sociological Quarterly* 56, 484–498.

Cases cited

European Court of Human Rights

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (2008) Application no. 62540/00.
Big Brother Watch and *Others v. United Kingdom* (2018) Applications nos. 58170/13, 62322/14 and 24960/15.
Kennedy v. United Kingdom (2010) Application no. 26839/05.
Klass and Others v. Germany (1978) Series A no. 28. Application no. 5029/71.
Liberty and Others v. United Kingdom (2008) Application no 58243/00.
Loizidou v. Turkey (preliminary objections), judgment of 23 March 1995, Series A no. 310.
Malone v. United Kingdom (1984) Series A no. 82. Application no. 8691/79.
Mamatkulov and Askarov v. Turkey (2005) Applications nos. 46827/99 and 46951/99, ECHR 2005-I.
Roman Zakharov v. Russia (2015) Application no. 47143/06.
Szabó and Vissy v. Hungary (2016) Application no. 37138/14.
Vallianatos and Others v. Greece (2013) Applications nos. 29381/09 and 32684/09, ECHR, 7 November.
Weber and Saravia v. Germany (2006-XI) Application no. 54934/00.

Court of Justice of the European Union

Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others (2016) Judgment of 21 December 2016. (C-203/15 and C-698/15). ECLI:EU:C:2016:970.

National Courts

Judgment of 8 September 2017 (2017) UKIPTrib IPT_15_110_CH.