derecom

ISSN: 1988-2629. Nº. 27. Nueva Época. Septiembre 2019-Marzo 2020

Cómo citar este texto:
Giacomelli, L. (2019). Gender stereotypes and discrimination in the surveillance society. The challenges of new technologies in the protection of equality rights.
Derecom, 27, 45-74. http://www.derecom.com/derecom/

GENDER STEREOTYPES AND DISCRIMINATION IN THE SURVEILLANCE SOCIETY. THE CHALLENGES OF NEW TECHNOLOGIES IN THE PROTECTION OF EQUALITY RIGHTS.

ESTEREOTIPOS DE GÉNERO Y DISCRIMINACIÓN EN LA SOCIEDAD DE LA VIGILANCIA. LOS RETOS DE LAS NUEVAS TECNOLOGÍAS PARA LA PROTECCIÓN DEL DERECHO A LA IGUALDAD

© Luca Giacomelli
University of Florence (Italy)
luca.giacomelli@unifi.it

Resumen

Vivimos en una sociedad de vigilancia. Los cuerpos devienen datos. La información deriva del cuerpo pero es tratada separada de él, facilitando la creación de un "cuerpo-como-información" virtual separado. Aunque se hace abstracción de los contextos sociales, las discriminaciones se solidifican y copian. ¿Estamos realmente seguros de que este espacio virtual es neutro? Estrechamente ligada al control social y a la vigilancia está la clasificación de sexo y género. Lejos de ser una categoría unificada, la vigilancia deviene uno de esos mecanismos que generan exclusión, discriminación y modelos de género que son recogidos y circulan por el espacio virtual. Las tecnologías de la información no se han liberado de los discursos de género opresivos que acompañan a la corporeidad biológica.

La norma es incapaz de ir más allá del "dilema de la diferencia" y la vigilancia no es una excepción. La vigilancia es epistemología innatamente conservadora y la presión normativa recae sobre cuerpos y prácticas no normativas. Se puede retar la presunta neutralidad de las tecnologías de la información y de las técnicas de vigilancia: (i) La discriminación de cuerpos virtuales (reconoce que el *big data* incluye predisposiciones sobre a quién representan los data; (ii) La discriminación contextual y de uso (los contextos sociales ya están marcados por relaciones sexistas, luego las tecnologías de la vigilancia tienden a ampliar esas tensiones); (iii) La discriminación por abstracción (la vigilancia opera sobre la lógica masculina y paternalista).

Recibido: 30/07/2019 Revisado: 14/08/2019
Aceptado: 19/08/2019 Publicado:15/09/2019

Summary

We live in a surveillance society. Bodies become data. Information is plumbed from the body but treated as separate from it, facilitating the creation of a separate virtual 'body-as-information'. Although social contexts are abstracted away, discriminations are solidified and replicated. Are we really sure that this virtual space is neutral? Tied closely to the surveillance and social control is the classification of sex and gender. Far from being a unifying category, surveillance becomes one of those mechanisms generating exclusion, discrimination and gendered patterns that are collected and circulated in the virtual space. Information technologies haven't freed from the oppressive gendered discourses that accompany biological embodiment.

The law is unable to go beyond 'the dilemma of difference' and surveillance is no exception. Surveillance is innately conservative epistemology and puts normative pressure on non-normative bodies and practices. We can challenge the supposed neutrality of information technologies and surveillance techniques: (i) Virtual bodies discrimination (recognize that big data includes biases in who the data represents); (ii) Context/use discrimination (social contexts are already marked by sexist relations, then surveillance technologies tend to amplify those tensions); (iii) Discrimination by abstraction (surveillance operates upon masculine and paternalistic logic).

Palabras clave: Vigilancia. Discriminación por motivos de género. Igualdad. Vida privada. Tecnologías de Inteligencia Artificial. Control social.

Keywords: Surveillance. Gender Discrimination. Equality. Privacy. AI Technologies. Social Control.

1.Introduction.

During the past twenty years, Western society has seen incredible development in information technology that has changed our lives and our minds. However, while we easily understand the positive side of information technology – mobile phones, computers, Internet-, it also has a darker side. The darker side includes the use of sophisticated and rapidly advancing technology to collect our personal data for surveillance purposes. We live in a Surveillance Society:[1] Both State and private sectors engage in widespread surveillance based on modern information technology. The need for security has resulted in an increase in monitoring and control systems. Every day, we are followed by invisible eyes, scanned by metal detectors in public buildings, constantly rendered traceable and intercepted by the trail of information that we leave behind. We are not aware of this happening. Security operations have increasingly driven towards the privatisation of monitoring systems and a lowering of guarantees provided by the law. In the so-called "War on terror"[2] we relinquished part of our freedom and privacy in favour of the promise of safety, but the point is that new information technology monitors us even when there is no need.

The trail of information we generate – text messages, e-mails, social networks, credit cards, etc. – leaves us exposed and visible (to whom? For what purposes?) everywhere and contributes to the composition of our virtual identity. Like pieces of a mosaic, bodies become data. This information can then be used for many purposes: scientific research, social control, advertising and marketing. Surveillance is quickly coming to a point where it threatens the

democratic fibre of our society.[3] In the face of this phenomenon, the law is inadequate to protect the rights and freedoms of individuals. Privacy as a defence of a sort of private citadel, *my house, my castle*,[4] no longer exists.[5] Today the protection of privacy is still paramount only if understood as *a necessary tool to protect society of freedoms and to oppose the push towards the construction of a society of surveillance, classification, social control*.[6] Legislation for the protection of personal data does not always ensure effective protection and is unable to guarantee against violations of the individual's most intimate sphere.[7] Virtual space is an area at risk, not just because personal information can be stolen and used without our permission (identity theft or credit card cloning, for example), but also because we can be classified and monitored through this information. Any form of control classifies people and the classification of gender is closely tied to surveillance and social control. Surveillance becomes one of those mechanisms that generate social exclusion, discrimination and gendered patterns that are collected and circulated in virtual space. Information technology hasn't freed us from the oppressive gendered issues that accompany biological embodiment.[8]

In this sense, we can say that surveillance techniques are normative, because they exercise a standardizing pressure on non-normative bodies and practices, such as those of queer and gender-queer subjects.[9] In recent years, surveillance studies have put more and more emphasis on the techniques of classification and social control. One of the most important things to note about the categorisation practices usually discussed in studies of surveillance is that categories are statistically generated. Central to the operation of a category is its norm, or average: the ascription of any case – human or otherwise – to a category implies some kind of proximity to the norm expressed by the category. Categories thus have a normalising tendency. So, the point is not only to protect the privacy of the individual, the castle in which everyone is "free to be oneself" or to regulate the flow of personal data in and out of computer systems, but to become aware of a virtual, parallel world in which there are the same stereotypes and prejudices that are present in the real one. These classifications are discriminatory and have real and negative effects on people's lives, especially for those that do not fit into predetermined social patterns.

The law is unable to fix Martha Minow's *Dilemma of Difference*[10] and surveillance provides us with another proof of this. The potentially normative effect of this type of classification is perhaps clearest in the case of the transsexual who has changed from one gender to another. The body data, in the case of a transgender or intersexual person, appears contradictory, confusing; in fact, surveillance is based upon an innately conservative epistemology and puts normative pressure on non-normative bodies.[11] Information technology, used for surveillance and social control purposes, seems to operate according to a masculine and paternalistic logic and tends to reproduce the typical heterosexist and discriminatory relations that exist on the real plane. We can challenge the supposed neutrality of surveillance techniques and virtual spaces. According to Monahan's study, *We understand technologies to betray their gendered dimensions through (a) body discrimination, (b) context or use discrimination, and (c) discrimination by abstraction*.[12] In particular, this last dimension is the most original and interesting: Even virtual bodies suffer the same discriminatory treatment as real bodies.[13] Instead of everyone being subjected equally to the disciplinary gaze, we are now observing advanced "social sorting" made possible by technology surveillance in all its forms.[14] This paper turns our attention to three particularly problematic phenomena that surround surveillance practices. The first is the oft-cited and fallacious public response to surveillance as being "if I have nothing to hide then I have nothing to fear". The second concerns the outcomes of categorisation for gendered and sexualised subjects. The third highlights how the anti-

discrimination law is inadequate to protect the fundamental rights and freedoms of individuals because it is the first to suffer from a classificatory, individualistic and non-intersectional logic.[15]

2. From the *Panopticon* to the Surveillance Society: Data-sorting and the principle of equality.

The increasing use of information technologies for surveillance purposes is a fact. It could be that they are dedicated to protecting our safety and ensuring our rights rather than spying on us and invading, at the bequest of the capitalist economy, our privacy, but that does not change the fact itself: Our societies are societies that are under surveillance. The myriad of actions that each of us carries out every day and through which we relate to the world, such as using credit cards, passing through toll booths, opening a bank account, talking on the phone, surfing the net, posting our pictures on Facebook or Instagram and many others, are actions which are potentially being monitored. In fact, surveillance has two sides: The ambivalent character of today's computer technology must be borne in mind, recognising its positive and negative aspects.[16]

The idea of surveillance for the purposes of social control is not new. The text in which Jeremy Bentham theorised and designed a model prison which he called *Panopticon,*[17] a round building in which a single guard can see all the detainees, is dated 1791. This design allows control, as well as impeding detainees from establishing relationships among themselves, each being locked in a cell that only faces the central tower. In fact, according to Bentham's description, there is a central tower surrounded by cells. In the central tower is the watchman. In the cells are prisoners – or workers, or children, depending on the use of the building. The tower shines bright light so that the watchman is able to see everyone in the cells. The people in the cells, however, aren't able to see the watchman, and therefore have to assume that they are always under observation. These cells are divided from one another, and the prisoners by that means excluded from all means of communication with each other, by partitions in the form of radii issuing from the circumference towards the centre, and extending as many feet as shall be thought necessary to form the largest dimension of the cell[18]. The *Panopticon Letters* thoroughly described how the inspection principle could be applied to penitentiaries, hospitals, schools and other kind of institutions alike. As Bentham and Božovič underline:

> *No matter how different, or even opposite the purpose: whether it be that of punishing the incorrigible, guarding the insane, reforming the vicious, confining the suspected, employing the idle, maintaining the helpless, curing the sick, instructing the willing in any branch of industry, or training the rising race in the path of education: in a word, whether it be applied to the purposes of perpetual prisons in the room of death, or prisons for confinement before trial, or penitentiary- houses, or houses of correction, or work-houses, or manufactories, or mad-houses, or hospitals, or schools*.[19]

Nevertheless, the *Panopticon or The Inspection House* is the Benthamite opus that elicited the largest number of dissenting opinions and it is still considered full of controversy and ambiguity: Indeed, the project can be interpreted either as an architectonic concept leaving no room for human dignity or an attempt to reform prisons and establish a universally-recognized educational model.

This concept, for example, was adopted by Foucault as a metaphor with which to describe and explain how discipline and the control of individuals work in modern times.

In view of this interpretation, the Benthamite project will be connected to a darker twist of everyday life and will become the synonym of surveillance. The panoptic model is interpreted as a kind of input emission code with the aim of changing the behaviour of those monitored through the use of so-called "disciplinary strategies".[20] More use is made of these than of "physical force". In fact, from its creators' perspective, continuous surveillance induces those under surveillance to interiorise specific rules of conduct. The detainees in a Panopticon, while not being coerced into behaving in certain ways, appear to act in line with the directives imposed by the power that determines the horizon within which they act. Thus, the concept of power changes: It is no longer seen as being merely a violent or ideological imposition, but a complex strategy that is inevitably linked to the concept of knowledge.[21]

Power is interpreted as something which is reticular, conveyed through a number of bodies, both political and administrative, and is perpetuated by the individuals themselves, invested by laws, social conventions, thought and action patterns and also by new information and communication technology. What matters is the establishment of a *mechanism of self-discipline* because you may be under observation at any time. The individual's state of conscious and continuous visibility is the guarantee that power works automatically. Foucault describes the prisoner of a Panopticon as being at the receiving end of asymmetrical surveillance: *He is seen, but he does not see; he is an object of information, never a subject in communication.*[22] The parallels between the Panopticon and contemporary information technology may be obvious, but what happens when you step into the world of digital surveillance and data capture? Are we still "objects of information" as we swipe between cells on our smartphone screens? The relevance of the Panopticon as a metaphor begins with when we start thinking about whether contemporary types of technology (effectively digital and data-driven) are analogous to the central tower concept. For example, whether this type of visuality is asymmetrical, and being co-opted for the same political exercise. Does the fact that we don't know we're being watched mean we are being normalized in the way the Panopticon was intended to correct behaviour?

These days, the panoptic model, as originally conceived, is considered obsolete by contemporary society. It needs to be "upgraded" and integrated. The "disciplinary society" itself evolves, becoming a society of surveillance and (big) data control.[23] The dynamics and liquidity of the new society needs new "devices", computer, smartphones and anonymous ones, able to make the body increasingly docile.[24] Fluid modernism has replaced traditional static patterns and describes a world where power has splintered from politics; where discipline is not located in the institution, but diffuse; where *social forms disappear before new ones are cast,*[25] leaving us without strategies for navigating the inside or outside of these shifting social systems. Technology has also contributed to this dilemma. Constant technological change can no longer be considered a transient phenomenon – it is, indeed, the norm.[26] Consequently, also surveillance has become fluid: The old, relatively solid institutions of marketing or crime control have softened, becoming malleable and rapidly adaptive in an interconnected world of software and networks. The means of tracing and tracking the mobilities, of collecting and processing personal data, of profiling and mining identities of the Twenty-first Century are going global, invisible, ubiquitous.[27] We live so much of our lives online, share so much data, but feel nowhere near as much attachment for our data as we do for our bodies. Without physical ownership and without an explicit sense of exposure I do not normalise my actions. If anything, the supposed anonymity of the Internet means I do the opposite. My data, however, is under surveillance, not only by my government but also by corporations that make enormous amounts of money capitalising on it.

There is no question that technology has dramatically changed how we live, work, socialize, etc. The current problem is overseeing and managing the flow of data and information and, through these, being able to monitor individuals. New social control is continuous, unlimited, potentially open to anyone and, at the same time, perceived as *routine.*[28] So far from the single all-seeing eye of an Orwellian '*Big Brother*', myriad agencies now trace and track mundane activities for a plethora of purposes. George Orwell's *Nineteen-Eighty-Four*[29] painted a terrifying picture of detailed, damning surveillance by the nation-state, personified by the sinister, looming figure of "Big Brother". These highlighted the crucial role of information (or lack of it, for the surveilled) within bureaucratic governments, alongside the constant threat of totalitarianism. But, in the era of information technology and digitization, "Big Brother" has grown: not only is he watching you, he is also potentially reading your emails, listening to your phone calls, mapping your personal data, and tracking your every move. And all of us are unconscious accomplices.

> *Today's Big Brother is not about keeping people in and making them stick to the line, but about kicking people out and making sure that when they are kicked out that they will duly go and won't come back* […].[30]

Even Lyon himself speaks instead of *social orchestration*,[31] cross-checking and a *power that plays its part*,[32] but also of *ordinary people who usually cooperate*.[33] Nowadays, social control instead tends to drive individuals into adapting to the group's expectations, towards self-discipline, towards normalising their behaviour, making it conform to normality or to common behaviour, without the need to deviate.

The development of information technology which is used for the purpose of monitoring plays an essential role because it allows fine-grained and extended control. It responds, primarily, to a need for security: Increasing the perception of safety also increases freedom, namely the right not to be enslaved by fear and terror. Living in a society of risk and uncertainty increases demand for security, which is often and deceptively achieved by increasing control. The paradox of new surveillance and new social control is that they increasingly affect personal freedom, with continuous intrusions into the privacy of citizens, but the fact that they exist makes us feel safer. It is the supersession of the classic panoptic model by a new form of surveillance and control. The increasing flexibility of individuals imposes a greater need to control them: Less invasive, less visible, but at the same time more comprehensive and detailed. The advent of the information age, in which, thanks to databases, it is possible to find and record an increasing amount of data (the so-called '*big data*'), allows the reconstruction of a more accurate profile for each individual citizen (the so-called '*body as information*'). Indeed, it is possible to reconstruct the profile of an individual, weaving a collection of data-images of each single individual-user. One must then ask oneself whether, in addition to reconstructing, by reading and indexing past and present actions, it is also possible to construct, providing input for the future, thereby directing the user's profile towards predefined norms and values.[34]

If we accept the idea that social control also means the ability to drive individuals towards adapting to the social and cultural expectations of the dominant group,[35] it follows that gender, as well as race, ethnic origin, language, religion, age, disability and sexual orientation, become particularly sensitive information. They affect surveillance techniques that, in turn, will operate according to logic that conforms to the dominant patterns of thought, tending towards reproducing those same social paradigms. In other words, individuals who are controlled in a culturally oriented manner will tend to discipline themselves, to "normalise" their behaviour in accordance to more common behaviour, in order to avoid being left vulnerable.

In fact, the possibility of these huge databases not only containing information on identity, but also on inclinations, purchases, activities and personal relationships is often underestimated. According to Poster's study,[36] we stand before a surveillance system capable of controlling every detail, at all times, of the daily lives of individuals thanks to a control system known as *dataveillance*. Among the techniques of dataveillance is "profiling", the creation of individual profiles, processed by putting together as much information as possible on individuals and based on their past experiences. Cross-checking of data, however, is not solely carried out by the investigating authorities, but also by large financial groups, banks, insurance companies, marketing companies, etc. Very often, we ourselves provide information voluntarily (e.g. social networks), making ourselves increasingly visible and transparent to an electronic eye that, instead, remains hidden.

These days, the link between surveillance and the collection of personal data, including gender, race and sexual orientation, is becoming increasingly close and significant. The fact that personal data can be sorted at a distance and checked for matches thanks to increasingly sophisticated algorithms is a key feature of the "new" surveillance.[37] Abstract data, including video, biometric, and genetic as well as computerized administrative files, are manipulated to produce profiles and risk categories in a liquid, networked system. The point is to plan, predict, and prevent by classifying and assessing those profiles and risks. In particular, we talk about "data sorting" to refer to any process that involves arranging the data into some meaningful order to make it easier to understand, analyse or visualize.

When working with research data, sorting is a common method used for visualizing data in a form that makes it easier to comprehend the story the data is telling.[38] Similarly these data manipulation techniques are also applied to our digital alter egos (the so-called "body as information"). "Social sorting" highlights the classifying drive of contemporary surveillance:[39] A key trend of today's surveillance is the use of searchable databases to process personal data for various purposes and to classify people – citizens, workers, customers, detainees, and so on – into categories to facilitate management and control (or discrimination) through the differential treatment of those groups.[40] In this way, individuals leave traces of behaviour that are then memorized into the databases of numerous agencies and institutions, which produce the electronic image of these real bodies.

Social control is exercised through the classification of individuals, who are separated along an axis running from "normal" to "deviant". Those able to influence how people are classified and categorised tend to be in positions of greater power. According to this depiction, surveillance is a valuable instrument for categorising and classifying populations, not just invading the personal sphere or violating the individuals' privacy. Scholars like Lyon argue that the most concerning facet of surveillance is the reinforcement of divisions by arranging people into social categories. All things considered, social sorting grants different opportunities to different groups and often amounts to subtle and malleable ways of ordering societies. As a result, *these categories assume material force because they include and exclude, declare eligible or not, and everyone continuously participates in this process*.[41]

Social sorting presupposes difference; in that sense it reifies pre-existing differences in society and preserves the *status quo*. The recent example of Amazon's recruiting algorithm reproducing gendered hiring patterns involved collection from a pre-existing dataset, i.e. a workplace where women were already underrepresented, and creating "favourable" profiles on that flawed basis.[42] Gender, thus, became a marker for employability and the social sorting reflected the status quo that was a result of systemic sexism and patriarchal barriers.

This process is now somewhat occluded, especially in the current era of surveillance, by the use of information technology in the sorting processes. The question that needs to be asked is how the highly consequential coding that distinguishes between one group and another is carried out? How does data sorting operate? Is it a gender-neutral process? Probably not.[43] First of all, *The act of classification is a moral one because each standard or category valorises one viewpoint and silences another; it can create advantage or suffering*.[44] Secondly, *There are risks inherent to surveillance technology systems whose crucial coding mechanisms invoked categories derived from stereotypical and prejudicial sources*.[45] Modern systems of technological surveillance share the ability to filter out social context and reduce social figures and practices to data that can be analysed and sorted according to *objective* criteria. These systems and practices exactly reproduce the masculine and hetero-sexist logic of the social context in which they operate, because *They depend upon disembodied representations of the world and an evacuation of social relations and contexts*.[46]

The fact that modern surveillance technology assimilates social inequalities and reproduces them in the way personal data is collected and analysed, in the way "suspicious" social groups are identified and in the way social figures and space are controlled at a distance, should not surprise. In fact, even before surveillance, there is another system of social control that is affected by masculine and heterosexist logic: The law.[47] Even theorised legal instruments for the elimination of inequalities and social discrimination themselves end up by being one of the causes. Non-discrimination law and data protection law are the main legal regimes that could protect people against AI decision-making and dataveillance discrimination. Non-discrimination law, for example, makes use of the categorisation of individuals to identify groups "to protect". Discrimination is prohibited in many treaties and constitutions,[48] including the European Convention on Human Rights.

Article 14 of the European Convention on Human Rights states:

> *The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status*.[49]

Both direct and indirect discrimination are prohibited by the European Convention on Human Rights. Direct discrimination (or disparate treatment) means, roughly summarised, that people are discriminated against on the basis of a protected characteristic, such as racial origin. The European Court of Human Rights describes direct discrimination as follows: *There must be a difference in the treatment of persons in analogous, or relevantly similar, situations*, which is based *on an identifiable characteristic*.[50] Indirect discrimination (or disparate impact) occurs when a practice is neutral at first glance but ends up by discriminating against people of a certain racial origin (or another protected characteristic).

Indirect discrimination is described as follows by the European Court of Human Rights:

(*A) difference in treatment may take the form of disproportionately prejudicial effects of a general policy or measure which, though couched in neutral terms, discriminates against a group. Such a situation may amount to "indirect discrimination", which does not necessarily require a discriminatory intent*.[51]

Therefore, the *grounds* on which discrimination is prohibited are already indicated: However, since legal reasoning proceeds by categories and is therefore constantly and predominantly occupied in establishing boundaries, there is a risk that the principle of equality, in a purely anti-discriminatory manner, will result in a classificatory way of thinking that proceeds by selection and exclusion.[52] It is precisely here that cultural influence bursts forth in all its arrogance and pervasiveness: If culture, and specifically the social constructs of sex and gender, operates on legal categories and classifications, affecting them more or less consciously, the result will be discrimination, inequality and exclusion. It follows that legal reasoning and vocabulary will be unable to understand the differences that do not fit into the rigid classification schemes and as such will reproduce them in a vicious circle.

The principle of equality, as it has developed, protects by reaffirming the superiority of the reference model ("equal" describes a value only in relation to something equal to whom? Equal to what?): The problem is the norm, the standard against which the difference is measured as a standard deviation, a deviance. It is thus shown to be very inefficient when it comes to understanding human differences in the social sphere, given that it proposes that they should conform to that standard. With something of a paradoxical turn, the modern principle of equality, theorised to overcome social structures and thought patterns that produce discrimination, hierarchies and inequalities, ends up by being one of the causes. Both the American and European anti-discrimination law seem anchored to Martha Minow's concept of the "Dilemma of Difference"[53], as it contradictorily protects minorities (from any of the protected categories), while in practice underlining their distance from "normality": A form of protection introduced through the formulation of bans on behaviour, actions and practices listed on the basis of different *grounds* of discrimination and that, while setting itself the objective of safeguarding their diversities, ends up stigmatising them, marking them as negative.

According to Martha Minow, the problem is the "norm", when it is seen as stated, neutral and self-evident; it absolutises some points of view, experiences and interests and, at the same time, leaves out any other point of view, experience and interest. In fact, *The ideal of objectivity itself suppresses the coincidence between the viewpoints of the majority and what is commonly understood to be objective or unbiased*.[54] In Minow's words,

> *The law has tended to deny the mutual dependence of all people while accepting and accentuating the dependency of people who are "different", [because] law has relied on abstract concepts, presented as if they have clear and known boundaries, even though the concepts await redefinition with each use*.[55]

A criticism, therefore, of the abstract nature of the classic subject of rights (male, white and heterosexual), the supposed neutrality of the law (and surveillance!) and the inadequacy of protection that is firmly anchored to the categorisation of differences, rather than based on the more inclusive notion of human dignity evaluated on a case by case basis and the reality of different circumstances.

In effect, in classical liberal thinking, the law is supposed to be rational, objective, abstract and oriented towards principles; these are dichotomous characteristics that in Western societies have always been associated with the masculine gender and, therefore, at a higher-level than their opposites, identified as feminine. This assumption was the starting point for many feminist thinkers in order to criticise the law which was structured in a masculine and

patriarchal manner. Such law *Not only reflects a society in which men rule women, [but it also governs] in a male way;*[56] the law sees and treats women the way men see and treat women.

The liberal state coercively and authoritatively constitutes the social order in the interests of men as a gender, through its legitimating norms, forms, relation to society, and substantive policies.[57] Carol Smart identifies three stages in feminist positions on the law, effectively summarised in three slogans: The law is sexist, the law is male, the law is gendered.[58] As part of our line of reasoning, we are mainly interested in the third phase. In fact, it allows a more transversal reflection, which begins with sexual differences and crosses all the others. It is no longer an investigation on how law can transcend gender, but an analysis of how gender operates on the law and how the law, in turn, contributes to reproducing gender. It is, therefore, an analysis of how law clashes a far more complex and intricate reality than social constructivism would like it to appear and is unable to make its own, discriminating and stigmatising, on the contrary, that which falls outside out gender and sexual binarism.

In light of what has been said, one can better understand the parallelism between law/gender and surveillance/gender. Even modern surveillance technology is supposed to be neutral, objective and abstract. However, it is not. *Unequal power relations are reinforced and reproduced by technological means*.[59] Therefore, the same critical reasoning can also be applied to supervision and the techniques for collecting, processing and classifying personal data, as these processes are socially and culturally embedded and replicate the prejudices of big data and data mining experts. As a result, data subjects may unwittingly suffer discrimination (on the grounds of gender, race or sexual orientation etc.), or may be wrongly placed in categories to which they do not belong, because surveillance control is value-laden, heteronormative and male gendered.[60]

3. Gendered surveillance: The masculine and paternalistic logic of control.

Long before the development of contemporary surveillance technology, gender and sexuality were already intensely controlled firstly by moral and subsequently by social and legal regulations. Today, surveillance helps to reinforce sexual rules by creating pressure for self-regulation,[61] also because surveillance techniques are full of masculine and heteronormative assumptions and assorted gendered dynamics. It is important here not to mix gender with sex, even though they are connected in a very complex way. Also, the biological sexes of the people involved is relevant grounds for discrimination and creates lots of problems in terms of social control and dataveillance (for example, in the case of intersexed people). However, when we speak about gendered surveillance, we refer to a system that operates according to masculine logic and has a masculinising influence on the subjects and spaces under surveillance.[62] Surveillance systems, therefore, will claim to be “rational”, “objective”, “abstract”, “active”, “at distance” and generally “infallible”. This also means that not only women will be discriminated against, but also all the other categories of individuals who play havoc with the hierarchies of a society ordered according to masculine and heteronormative values. As Monahan’s study found:

> *These surveillance systems and practices are highly masculinised, at least on a theoretical level, because they depend upon disembodied representations of the world and an evacuation of social relations and contexts. Moreover, when the logic of these systems is applied back upon social space and used to govern people and practices, social inequalities are both solidified and obscured. Because social control through surveillance happens at a distance, or as an automated part of*

> *the system, these inequalities are more likely to be perceived as individual rather than collective problems*[63]

Contemporary surveillance technologies are, in fact, defined by characteristics culturally associated with masculinity (rationality, abstraction, objectivity); they are built with reference to a standard subject (which, by implication, is represented by the male, white, heterosexual, middle class, etc. individual); they are used in contexts that are already characterised by gender tensions in order to "protect" the most "vulnerable" group (thereby encouraging voyeuristic practices, as well as a masculinisation of space); they are based on categorisations that already exist on a social and legal plane (male/female, age, nationality, race, employment, sexual orientation, etc.). In particular, it is assumed that the criteria on which controls and data processing are based are *objective* and *neutral*. In practice, they are not. In the language of modern surveillance technology, as in the legal one, masculinity occupies both the neutral/objective position, as well as the masculine one. Therefore, everything that does not fall within this standard is categorised and labelled as "vulnerable", "handicapped", "suspect", or even "deviant".

A good example of masculine and paternalistic control logic is provided by video surveillance. Our lives are increasingly under the gaze of surveillance cameras as their use extends from the private areas of shopping centres and banks to residential spaces such as local authority housing schemes and, now, city centres. Furthermore, the diffusion of CCTV surveillance is set to continue. However, is it proper to apply CCTV to every public area and who decides where it is proper or not? Many authors[64] have emphasized the voyeuristic aspect (a typically masculine aspect) of video surveillance systems installed in specific areas (usually in traditionally feminine areas – e.g. shops, gyms, schools, public transportation, etc. and also private housing). The experience of "being watched", the "control from a distance", the idea of "victimisation of women who needs (male) protection" are highly gendered. In fact, camera operators are generally male and the people under surveillance are generally female:[65] This fact confirms the dominant position of males who, from their control rooms, can freely observe unsuspecting women, and others, from afar. One consequence is a masculinisation of space,[66] i.e. a space that is built according to masculine parameters and to which all others must adapt. So, women in these places are "vulnerable" by definition and are increasingly scrutinized, formally in order to provide additional protection from harassment or assault.

In fact, women are encouraged to take a daily number of precautions that men do not even think of having to adopt; many areas of the city (for example, remote or peripheral locations) and many hours of the night are highly discouraged when it comes to women. Most women find themselves living in a space that is built to be hostile and threatening, they are encouraged to avoid risks and to avoid certain situations and certain relations. In a nutshell, women see a part of their freedom restricted. Video surveillance systems reinforce this logic: Women are "vulnerable" subjects that need to be observed because they need to be in some way protected. To this effect, control assumes masculine and paternalistic characteristics and contributes to the construction of women as vulnerable and the masculinisation of public places.

As Koskela describes:

> *Such meanings reinforce the different ways that women are constructed as vulnerable. On one hand, surveillance equipment can be read as a sign of danger (distrust, need for control) and can thus amplify a sense of vulnerability. On the other hand, the promise of increased security generates a pressure for women to accept surveillance*.[67]

So, how do we protect ourselves from a system that has transformed the seemingly natural male virtues – such as strength, courage, security, honour, sense of command and superiority – into political virtues that are necessary to the global order of society, the legal system and the State? The myth of the universal subject has tended to erase the voices, experiences and contributions of those who fall outside this model and to transform social and legal context in a masculine way.[68]

Another interesting example of discriminatory and paternalistic logic of control is provided by "*profiling*" activities. Profiling, as defined by the Oxford English Dictionary, consists in the recording and analysis of a person's psychological and behavioural characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people. Criminal investigation and security control, but also marketing and advertising are increasingly based on big data analysis processed by AI technologies. The disappearance of real bodies has resulted in trust being put in the possession of a range of information and identification tools.

Information, which we often leave unwittingly, is key to the prevention of future risks. However, this type of surveillance reaffirms old inequalities and social discriminations, as well as creating new ones. Profiling has no interest in social causes or deep-seated motivations that lead to violence; what counts is the construction of models to predict future behaviour. Sometimes the police use AI systems for predictive policing: automated predictions about who will commit crime, or when and where crime will occur. We are all potential suspects in the eyes of public authorities, but some are more than others.[69] From the point of view of gender relations, dangers for women, as for men, have masculine connotations. Crime, violence and aggression are masculine qualities. Rapists, criminals and terrorists are commonly seen as males. Women are seen as prey, as victims. The social construction of masculinity as aggression, virility, strength and authority and femininity as weakness, vulnerability, sensitivity and submission are reproduced as natural and unchangeable. Fear of violence is a sensitive indicator of gendered, but complex power relations which make up society and space. Women's fear is generally regarded as '*normal*' and their boldness thought to be risky: The conceptualisation of women as victims is unintentionally reproduced.[70] Profiling is socially integrated and replicates the prejudices of data mining experts, not only from the point of view of gender, but also from racial, ethnic and religious points of view. For example, following the terrorist attacks of September, 11th 2001, being of Arab descent or the Muslim faith have become recurring characteristics of terrorist and religious fundamentalist profiles. In a very short space of time, terrorism, one of the most important issues in security, was automatically associated with the "Islamic world" and the Muslim communities in Western countries were seen as an actual or potential "enemy within"[71].

The gendered nature of surveillance technologies also becomes apparent in all situations in which virtual profiles do not respond to data criteria standards. Information-based

control forces people to deal with traditional social (and now virtual, too) classifications. For example, body screening technologies used in airport security checkpoints tend to disaggregate travellers into a hierarchy.[72] Passengers are subjected to gender, racial and behavioural profiling. In this way, *The various individuals at the airport are distributed into a complex hierarchy of "rank" and then circulated through the disciplinary space*.[73] In some international airports there are systems, such as the "Backscatter X-Ray Machines" and the "Millimeter Wave Scanner", which make almost three-dimensional images of the body possible and which, therefore, characterize bodies of the passengers as generic male or female bodies. These instruments are insistent on there being only two possible sexes/genders. The *gender-queer body* – the intersexed, hermaphroditic, transgendered, transsexual, and other non-normative bodies – is re-inscribed into the sex/gender binary and is viewed with suspicion.[74] Trans-people are still either "male" or "female" and intersexed and other non-normative bodies are still going to be made to fit in this binary.

4. Categorisation of the *body-as-information* and discrimination by abstraction. What protection is there by the law?

According to Ian Hacking's assertion that *The systematic collection of personal data about people [for surveillance purposes] has affected not only the ways in which we conceive of a society but also of the ways in which we describe our neighbour*,[75] we can affirm that surveillance is a way of imposing norms. As mentioned earlier, modern surveillance technology assimilates and reproduces prejudices and social discriminations in the way it collects and processes data and personal information, the way it classifies individuals into "suspicious" social categories and the way it controls space and social figures from a distance. In fact, the organisation and processing of information is carried out through the categorisation of data, thereby giving it a meaning.

The next step is to decide inclusions and exclusions according to predetermined standards and categories, enhancing some and silencing others. The standard, as mentioned, is always male, white, heterosexual, middle class, etc. characterized. Inevitably, that which does not fit into established categories (male/female, for example) is considered "deviant" or "suspect". Thus, even when bodies become data (the so-called "*body as information*") and there is a separation from the materiality of the real world, the same discriminations and social inequalities continue to be reproduced. Torin Monahan speaks of *discrimination by abstraction*, meaning *The ways that technological systems, especially those that produce representations of data, strip away social context, leaving a disembodied and highly abstract depiction of the world and of what matters in it*.[76] The data and information that form the bodies-as-information, i.e. the virtual identities of individuals, are extrapolated from social and material context. It could be held that abstraction neutralizes the various characteristics (sex, gender, race, ethnicity, age, sexual orientation, etc.) that, socially and culturally, characterize individuals and differentiate them. In reality, it is the very absence of a social and cultural background that makes these differences even more pronounced and turns them into instruments of discrimination that are even more dangerous because they are decontextualized. For example, in some countries the '*datafication*' of transgender bodies resulted in their identities being reified as "other" or "third gender".[77]

While granting of computerized national identity card bestows several benefits onto citizens – the ability to vote, apply for a passport, access to government jobs, obtain a mobile SIM, governmental financial support schemes – it also brings citizens into the categories and databases constructed to not only monitor their activities, but also constrain their identities, stripping their existing fluidity. In several jurisdictions, recognition of transgender identities has not necessarily translated into an accurate reflection of their lived experience on official records.

The system still sees gender identities as fixed and the freedom to self-determination without becoming for this reason a "special" object of surveillance is not conceived.

The flow of information that each individual leaves behind, whether voluntarily or involuntarily, can also be used for the purposes of control by both public and private organisations. The identification, classification and evaluation of big data by computer systems have become routine. However, these procedures appear problematic, especially in terms of their neutrality. The choice between individuals and groups (and consequently favouring certain groups over others) is inevitably based on a judgment of value that by its very nature is not objective. Who decides? What criteria do AI systems use? Using computers for the classification of individuals and groups on the basis of decontextualized information and criteria that reflect a dominant culture can only exacerbate social inequalities. Is it not discrimination when an employer prefers to hire a worker instead of another on the basis of statistics such as, for example, black people being more prone to violence and dishonesty than whites?[78] Is it not discriminatory for an algorithm to *insist* on classifying individuals as either male or female? In this sense, surveillance technology contributes to the reinforcement of social norms both by facilitating the exposure of deviances, which are then considered suspect, and by promoting self-discipline and concealment by those who fall outside these norms. As Kathryn Conrad describes, *The virtual body created by data, in the case of a transsexual person [or intersexual], appears contradictory, confusing; the data history for a trans person comprises two bodies (male and female) rather than one gender-queer body*[79]; surveillance and dataveillance technologies, relying on traditional stereotypes, tend to reinforce the traditional social system (as well as the gender/sexual binarism) and, therefore, the material body is put under pressure to conform or be excluded from the system.

As mentioned before, non-discrimination law appears insufficient when it comes to protecting people. It emphasizes, in turn, the differences between individuals and their "distance" from the standard model. Although it is forbidden to discriminate on the basis of "*protected grounds*" established by law or by the courts through case law (see the many judgments which, in some countries, have extended the ban on discrimination to categories not covered by the law (for example, in *Egan v. Canada,*[80] the Supreme Court of Canada included sexual orientation among the protected categories), *It's important to understand that no one escapes the expanding web of statistical discrimination*.[81] Non-discrimination tools show several weaknesses, especially in the context of information technologies. Although we can invoke the indirect discrimination to combat the discriminatory effects of AI automated decisions, the prohibition of indirect discrimination does not provide a clear and easily applicable rule. The concept of indirect discrimination results in rather open-ended standards, which are often difficult to apply in practice. It needs to be proven that a seemingly neutral rule, practice or decision disproportionately affects a protected group and is thereby *prima facie* discriminatory. In many cases, statistical evidence is used to show such a disproportionate effect but often it's not enough.[82] Suppose that somebody applies for a loan on the website of a bank.

The bank uses an AI system to decide on such requests. If the bank automatically denies a loan to a customer on its website, the customer does not see why the loan was denied. Moreover, the customer cannot see whether the bank's AI system denies loans to a disproportionate percentage of, for instance, women.[83] So even if customers knew that an AI system rather than a bank employee decided, it would be difficult for them to discover whether the AI system is discriminatory.

Another weakness relates to non-discrimination law's concept of protected characteristics. Non-discrimination statutes typically focus on (direct and indirect) discrimination based on protected characteristics, such as gender, race or sexual orientation. But many new types of AI-driven differentiation seem unfair and problematic – some might say discriminatory – while they remain outside the scope of most non-discrimination statutes. Hence, non-discrimination law leaves gaps.

Even the right to privacy is insufficient for protecting people. Citizens are very worried by their "digital body", a life increasingly entrusted to the abstract dimension of the electronic processing of their information. People are now known to public and private entities almost exclusively through their data, which makes them something of a disembodied entity. Our identity is thus entrusted to the way in which this information is processed, connected and circulated. For these very reasons, new protection requirements arise. Hence the invocation of the right to privacy. Recently, talk has begun of *Habeas Data*, an indispensable development of the *Habeas Corpus* from which personal freedom has historically developed. This is the perspective in which privacy can now be found, confirming that the protection of personal data is a fundamental human right and an essential component of new citizenship.[84] In Europe, for example, it should be noted that Article 8 of the Charter of Fundamental Rights of the European Union attributes autonomous importance to the protection of personal data. We are interpreting the law as also containing *Habeas Data*, not only to repel illegal or undesirable invasions, but also to avoid being "constructed" and "classified" by others. The *Habeas Data* writ itself has a very short history, but its origins can be traced to certain European legal mechanisms that protected individual privacy. *Habeas Data* has been described as *A procedure designed to safeguard individual freedom from abuse in the information age*.[85] The importance of this figure is stressed by the fact that it can be a mechanism available to citizens that will insure real control over sensitive personal data, stopping the use and abuse of such information, which would be detrimental to the individual.[86]

More recently, the European legal framework has been enhanced with an additional instrument for the protection of fundamental rights, the *General Data Protection Regulation* (GDPR).[87] It grants rights to people whose data are being processed (data subjects) and imposes obligations on parties that process personal data (data controllers). Eight principles form the core of data protection law; they can be summarised as follows: (a) Personal data may only be processed lawfully, fairly and transparently; (b) Such data may only be collected for a purpose that is specified in advance, and should not be used for other unrelated purposes; (c) Such data should be limited to what is necessary for the processing purpose; (d) Such data should be sufficiently accurate and up-to-date; (e) Such data should not be retained for an unreasonably long period; (f) Such data should be secured against data breaches, illegal use etc.; (g) The data controller is responsible for compliance.[88] So, the basic premise of GDPR is that consumers must give their consent before a company such as Facebook can start to collect personal data. The company must explain why data is collected and how it's used. The firm also isn't allowed to use the data for a different reason later on.

Data protection law could help mitigate risks of unfair and illegal discrimination. For instance, data protection law requires transparency about personal data processing: Article 22 of the GDPR, sometimes called the Kafka provision, contains an in-principle prohibition of fully automated decisions with legal or similar significant effects and applies, for instance, to fully automated e-recruiting practices without human intervention. In other words, people may not be subjected to certain automated decisions with far-reaching effects.[89]

The question that arises is once again whether such protection is effective. There are problematic aspects, in particular with *automated databases* and *online information*: It is very difficult to control the flow of information via the web, especially when it goes from one country to another, from one company to another. There are discussions on the need for uniform provisions common to all the different areas of the world, even for reasons of cost related to privacy policy management by companies. The debate is still very open, both in Europe and the United States, also because a right such as keeping personal information confidential can conflict with other rights, like freedom of speech and other privileges related to the free use of the web. On the other hand, it may be useful to prevent certain information from being used with prejudicial or discriminatory intent to "construct" and "classify" individuals,[90] also considering that it is increasingly difficult to contain information about us once it has entered the web.

It is equally true, however, that it is not a foregone conclusion to expect legal instruments, designed to protect individuals as socially positioned and physical persons, to also work effectively in the protection of decontextualized and disembodied entities such as "*bodies-as-information*". People are now largely known and "*managed*" by public and private entities almost exclusively through their related data. Therefore, the electronic body requires *ad hoc* legal instruments for its effective protection. Perhaps it is necessary to progress to a "law 2.0", a new way of conceiving the law and legal protection of the person: A more dynamic and flexible type of protection, no longer anchored to the categorisation of differences, but based on the notion of universal human dignity evaluated on a case by case basis, in the face of different circumstances. Equality must instead fully refer to the principle of anti-subordination that recognizes the fundamental need to eliminate the subordination of the black race to the white one, the female gender to the male one, homosexual orientation to heterosexual orientation and so on.[91] In the light of surveillance studies, we are witnessing the gradual computerisation of the body and an increasingly pervasive and widespread use of information technology (including for the purposes of social control). The law is struggling in the face of such rapid developments. There is a need to identify legal remedies capable of protecting the rights of the individual in both his/her physical and "virtual" versions, i.e. at the moment in which it is abstracted from reality and reassembled as a mass of data and information through which the individual is now regarded/managed/controlled.

Conclusion.

In summary, this paper has tried to address the issue of surveillance under two guises: That of (in)equality of gender and that of the law and the protection of people. In fact, as we have seen, on one hand, surveillance has increasingly become part of the everyday experience of people throughout the world and, on the other hand, social stereotypes and prejudices also affect information technology and reproduce the same inequalities and discrimination in the virtual space as exist in the real one. We are witnessing the progressive computerisation of the body and the progressive advancement of computer technology that has led to an increasingly pervasive and widespread dissemination of surveillance and control techniques. Nowadays, however, the electronic body, the "*body-as-information*", is monitored (and discriminated) more than the physical one: Thanks to computer databases, it is possible to find and register an increasing amount of data and this allows the reconstruction of an increasingly accurate and easily controlled profile for each individual. As we have tried to highlight, even information technology is contaminated by cultural paradigms and gender stereotypes (as well as other grounds) that are still rooted in Western society. Surveillance (through data-sorting and data-mining processes, for example) turns out to be one of those *gendered-mechanisms* that

reproduce gender differences and the discrimination associated with it. The design of modern surveillance technologies and the way in which they operate reveal masculine, paternalistic and heterosexist logic which has an adverse practical effect on all individuals, especially those who do not conform with predefined standard categories. In addition to a masculinisation of space,[92] they trigger (at least implicitly) processes of "normalisation", i.e. driving towards self-discipline in order to uniform behaviour to traditional dichotomies and social categories (of gender and others), to avoid being left vulnerable.

On the other hand, the law does not seem to provide appropriate means for protecting the individual and for social change. Neither the principle of equality, interpreted in an anti-discriminatory sense, or the right to privacy seem to be able to face the new challenges that society provides them with, including the issue of surveillance and social control. It must be said that such legal remedies, designed to protect the real subject in its physicality and space, cannot be expected to work properly or be as effective when applied to the protection of the individual's virtual identity. It should be acknowledged that we are moving towards a new concept of "personal identity", one which is increasingly detached from the social and biographical dimensions of the individual. Even the protection of *virtual body identity* must be taken seriously. Our identity is thus entrusted to the way in which this information is processed, connected and circulated. So, as Frank Pasquale suggests, "*(e)ven if algorithms at the heart of these processes "transcend all understand*ing", *we can inspect the inputs (data) that go into them, restrict the contexts in which they are used, and demand outputs that avoid discriminatory impacts.*[93] A reflection must therefore be made on the dangers of big data's bias, social sorting and control, automated decisions, invasion of privacy and lack of concern for the integrity and dignity of the people targeted and it is with reference to this that the law is called upon to provide more convincing solutions.

[1] See, in particular, LYON, D. (2001). *Surveillance society: monitoring everyday life.* Buckingham: Open University Press; *Id.*, (2007). *Surveillance studies: An overview*. London: Polity.

[2] MONAHAN, T. (2010). *Surveillance in the time of insecurity*. New Brunswick: Rutgers University Press.

[3] MATHIENSEN, T. (1999). *On globalization of control: towards an integrated surveillance system in Europe*. London: Statewatch.

[4] WARREN, S.D., BRANDEIS, L.D. (1890). "The right to privacy", in *Harvard Law Review*, vol. 4, p. 193-220.

[5] See, for example, BOEHME-NEßLER, V. (2016). "Privacy: a matter of democracy. Why democracy needs privacy and data protection", in *International Data Privacy Law*, 6.3, p. 222-229; MAI, J. (2016). "Big data privacy: The datafication of personal information", in *The Information Society*, 32.3, p. 192-199; YU, S. (2016). "Big privacy: Challenges and opportunities of privacy study in the age of big data", in *IEEE Access*, 4, p. 2751-2763.

[6] RODOTÀ, S. (2004). "Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati", 26th International Conference on Privacy and Personal Data Protection, Poland, Wroclaw, September 14-16,
in *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1049293*, p. 2.

[7] See, in particular, RESTA, G., ZENO-ZENCOVICH, V. (Eds.) (2016). *La protezione transnazionale dei dati personali. Dai "Safe harbour principles" al "Privacy shield"*, Roma: Roma Tre Press.

[8] See, for example, NOBLE, S.U. (2018). *Algorithms of oppression. How search engines reinforce racism*, New York: NYU Press; BARTLETT, K. (2018). *Feminist legal theory: readings in law and gender*. New York: Routledge.

[9] See, among others, BALL, K., GREEN, N., KOSKELA, H., & PHILLIPS, D.J. (2009). "Editorial: Surveillance studies needs gender and sexuality". *Surveillance & Society*, 6(4), p. 352-355.

[10] MINOW, M. L. (1990). *Making All the difference: inclusion, exclusion, and American Law*. Ithaca: Cornell University Press.

[11] See, for example, CONRAD, K. (2009). "Surveillance, gender and the virtual body in the Information Age". *Surveillance & Society*, 6(4), 380-387.

[12] MONAHAN, T. (2010). *Surveillance in the time of insecurity*. New Brunswick: Rutgers University Press, p. 288.

[13] Indeed social sorting has very real consequences for subjects. For example, errors occur when databases are combined, inaccurate or unrepresentative data are used and missing data are "filled in", leading to the observation that social sorting is nearly always "wrong" at the level of the individual. Also the production of profiles is socially embedded and replicates the prejudices of data mining experts. Potential is created for prejudices to be written into algorithms which identify risk, entitlement and criminality. As a result data subjects may unwittingly suffer discrimination, or may be wrongly allocated to categories they do not belong. Social sorting is often based on geo-demographic information, and ascribes value judgement to different groups of people. For example, particular consumption preferences, whilst forming distinct groups, are mapped onto places when combined with information such as a postcode. Lifestyles and places hence begin to merge and neighbourhood characteristics come to determine the products and services offered to individuals living there. Some of these characteristics include discriminatory categories the likes of which would be illegal in other settings.

For example, in *Cherry vs. Amoco Oil Co*. (490 F. Supp. 1026 (N.D. Ga. 1980)), a noteworthy legal case in the US, it was revealed that a white woman who lived in a predominantly black neighbourhood was refused a credit card not because of her personal

credit history, but because the postcode in which she lived was considered too risky in the credit checking system. See, *inter alia*, DANNA, A., GANDY, O.H. (2002). "All that glitters is not gold: digging beneath the surface of data mining", in *Journal of Business Ethics* 40(4), 373-386.

[14] See, for example, GANDY, O.H. (1993). *The panoptic sort: a political economy of personal information*. Boulder, CO: Westview; LYON, D. (Ed.) (2003). *Surveillance as social sorting: privacy, risk, and digital discrimination*. New York: Routledge.

[15] See, on this last point, GIACOMELLI, L. (2018). *Ripensare l'eguaglianza. Effetti collaterali della tutela antidiscriminatoria*. Torino: Giappichelli.

[16] See LYON, D. (2001). *Surveillance society: monitoring everyday life.* Buckingham: Open University Press.

[17] BENTHAM, J. (1791). *Panopticon or the inspection house, Vol. 1*. London: T. Payne.

[18] *Idem*.

[19] BENTHAM, J. & BOŽOVIČ M. (1995). *The panopticon writings*. 1st ed. London: Verso, p. 3.

[20] FOUCAULT, M. (1975). *Discipline and punish: the birth of the prison*, New York: Random House.

[21] See, in particular, FOUCAULT, M. (1979 [1976]). *The history of sexuality. Volume 1: An introduction*. London: Allen Lane.

[22] FOUCAULT, M. (1975). *Discipline and punish: the birth of the prison*, New York: Random House, p. 200.

[23] LYON, D. (2001). *Surveillance society: monitoring everyday life.* Buckingham: Open University Press.

[24] See, in particular, BAUMAN, Z. & LYON, D. (2012). *Liquid surveillance: A conversation*. Cambridge: Polity Press.

[25] BAUMAN, Z. (2000). *Liquid modernity*. Cambridge: Polity Press, p. 3.

[26] *Idem*.

[27] See, among others, ANDREJEVIC, M. (2012). "Ubiquitous surveillance". In BALL, K., HAGGERTY, K.D., & LYON, D. (Eds.). *Routledge handbook of surveillance studies* (p. 125-132). London: Routledge; *Id*. (2014). *Book review: BAUMAN, Z. and LYON, D.. "*Liquid Surveillance. Media", *Culture & Society,* 36(3), 409–411.

[28] BAUMAN, Z. & LYON, D. (2012). *Liquid surveillance: A conversation*. Cambridge: Polity Press.

[29] ORWELL, G. (1948). *Nineteen-Eighty-Four*. London: Secker & Warburg.

[30] BAUMAN, Z. (2006). *Liquid fear*. Cambridge: Polity Press, p. 25.

[31] LYON, D. (2001). *Surveillance society: monitoring everyday life.* Buckingham: Open University Press, p. 13.

[32] *Idem*, p. 40.

[33] *Ibid*.

[34] For example, a dataset that does not contain explicit data about people's sexual orientation can still give information about people's sexual orientation. "Facebook friendships expose sexual orientation", found a study from 2009. The study *demonstrates a method for accurately predicting the sexual orientation of Facebook users by analysing friendship associations (...). [T]he percentage of a given user's friends who self–identify as gay male is strongly correlated with the sexual orientation of that user*. See, *inter alia*, JERNIGAN, C. & MISTREE, B.F. (2009). "Gaydar: Facebook friendships expose sexual orientation". 14(10), *First Monday.*

[35] See, for example, ROSS, E.A. (1969). "Social Control: a survey of the foundations of order". *Cleveland, OH: The Press of Case Western Reserve University.*

[36] POSTER, M. (1990). *The Mode of Information. Poststructuralism and Social Context*. Cambridge: Polity Press.

[37] See, among others, LYON, D. (Ed.) (2003). *Surveillance as social sorting: privacy, risk, and digital discrimination*. New York: Routledge.

[38] See, in particular, ANDREJEVIC, M. (2012). "Ubiquitous surveillance". In BALL, K., HAGGERTY, K.D. & LYON, D. (Eds.). *Routledge handbook of surveillance studies* (p. 125-132). London: Routledge.

[39] See LYON, D. (2001). *Surveillance society: monitoring everyday life.* Buckingham: Open University Press.

[40] Artificial Intelligence systems are often "black boxes": It is often unclear for somebody why a system makes a certain decision about him or her. Because of the opaqueness of such decisions, it is difficult for people to assess whether they were discriminated against on the basis of, for instance, sex, gender identity or racial origin. AI-driven decision-making can lead to discrimination in several ways. In a seminal paper, BAROCAS and SELBST distinguish five ways in which AI decision-making can lead, unintentionally, to discrimination. The problems relate to (i) how the "target variable" and the "class labels" are defined; (ii) labelling the training data; (iii) collecting the training data; (iv) feature selection; and (v) proxies. In addition, (vi), AI systems can be used, on purpose, for discriminatory ends. See BAROCAS, S. & SELBST, A.D. (2016). "Big Data's disparate impact", in *Californian Law Rev*., 105, 671.

[41] LYON, D. (2001). *Surveillance society: monitoring everyday life.* Buckingham: Open University Press, p. 152.

[42] See ZUBOFF, S. (2015). "Big other: surveillance capitalism and the prospects of an information civilization", in *Journal of Information Technology*, 75-89.

[43] See, among other, BAROCAS, S. & SELBST, A.D. (2016). "Big Data's disparate impact", in *Californian Law Rev*., 105, 671.

[44] BOWKER, G. C. & STAR, S. L. (1999). *Sorting things out: classification and its consequences*. Cambridge, MA: MIT Press, p. 5.

[45] LYON, D. (Ed.) (2003). *Surveillance as social sorting: privacy, risk, and digital discrimination*. New York: Routledge, p. 2.

[46] MONAHAN, T. (2010). *Surveillance in the time of insecurity*. New Brunswick: Rutgers University Press, p. 117-118.

[47] See, amomg others, MACKINNON, C.A. (1983). "Feminism, Marxism, Method, and the Sate: Toward Feminist Jurisprudence". *Signs 8*, 4, 635-658; *Id*., (1989). *Toward a Feminist Theory of the State*. Cambridge, MA: Harvard University Press; *Id*., (2000). "Disputing Male Sovereignty: On United States v. Morrison". *Harvard Law Review* 114, 1, 135-177; SMART, C. (1992). "The Woman of Legal Discourse". *Social and Legal Studies*, 1, 29-44; GIACOMELLI, L. (2012). "Quando la vita infrange il mito della 'normalità': il caso dei minori intersessuali", in *Rivista Critica del Diritto Privato*, 4, 597-636; BARTLETT, K. (2018). *Feminist legal theory: Readings in law and gender*. New York: Routledge.

[48] See e.g. Article 7 of the United Nations Declaration of Human Rights; Article 26 of the International Covenant on Civil and Political Rights; Article 21 of the Charter of Fundamental Rights of the European Union; Article 3 of the Italian Constitution; Section 9 of the South Africa Constitution etc.

[49] Protocol 12 to that Convention lays down a similar prohibition, with, regarding certain aspects, a broader scope. *The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status*. Article 1, Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, European Treaty Series - No. 177, Rome, 4.XI.2000.

[50] ECtHR, *Biao v. Denmark* (Grand Chamber), No. 38590/10, 24 May 2016, para. 89.

[51] *Idem*, para. 103.

[52] See, in particular, GIACOMELLI, L. (2018). *Ripensare l'eguaglianza. Effetti collaterali della tutela antidiscriminatoria*. Torino: Giappichelli.

[53] MINOW, M. L. (1990). *Making all the difference: inclusion, exclusion, and American Law*. Ithaca: Cornell University Press.

[54] *Idem*, p. 60.

[55] *Idem*, p. 10.

[56] MACKINNON, C.A. (1989). *Toward a feminist theory of the State*. Cambridge, MA: Harvard University Press, p. 162.

[57] See, for example, MACKINNON, C.A. (2000). "Disputing male sovereignty: on United States v. Morrison". *Harvard Law Review* 114, 1, 135-177; *Id.*, (2003). "Women and Law: The Power to Change". In R. MORGAN (Ed.). *Sisterhood is forever: The women's anthology for a new millennium* (p. 447-55). New York: Washington Square Press; *Id*. (2006). *Are women human?: and other international dialogues*. Cambridge: Harvard University Press.

[58] SMART, C. (1992). "The woman of legal discourse". *Social and Legal Studies*, 1, 29-44.

[59] MONAHAN, T. (2010). *Surveillance in the Time of Insecurity*. New Brunswick: Rutgers University Press, p. 114.

[60] See, in particular, BALL, K., GREEN, N., KOSKELA, H., & PHILLIPS, D.J. (2009). "Editorial: surveillance studies needs gender and sexuality". *Surveillance & Society*, 6(4), 352-355; CONRAD, K. (2009). "Surveillance, Gender and the Virtual Body in the Information Age". *Surveillance & Society*, 6(4), 380-387; NOBLE, S.U. (2018). *Algorithms of oppression. How search engines reinforce racism*, New York: NYU Press; BARTLETT, K. (2018). *Feminist legal theory: Readings in law and gender*. New York: Routledge.

[61] See, among others, KOSKELA, H. (2012). "*You shouldn't wear that body*: The Problematic of Surveillance and Gender". In BALL, K., HAGGERTY, K.D., & LYON, D. (Eds.). *Routledge handbook of surveillance studies* (p. 49-56). London: Routledge.

[62] See MONAHAN, T. (2010). *Surveillance in the time of insecurity*. New Brunswick: Rutgers University Press.

[63] *Idem*, p. 117-118.

[64] See, among others, NORRIS, C., & ARMSTRONG, G. (1999). *The maximum surveillance society: the rise of CCTV*, Berg, Oxford and New York; KOSKELA, H. (2002). "Video surveillance, gender, and the safety of public urban space: "Peeping Tom" goes high tech?" *Urban Geography*, 23, 257-278; MONAHAN, T. (2010). *Surveillance in the time of insecurity*. New Brunswick: Rutgers University Press.

[65] KOSKELA, H. (2012). *"You shouldn't wear that body:* The Problematic of Surveillance and Gender". In BALL, K., HAGGERTY, K.D., & LYON, D. (Eds.). *Routledge handbook of surveillance studies* (p. 49-56). London: Routledge.

[66] *Id.*, (2000). *"*The gaze without eyes": video-surveillance and the changing nature of urban space". *Progress in Human Geography*, 24, 243-265; *Id.*, (2002). "Video surveillance, gender, and the safety of public urban space: "Peeping Tom" goes high tech?", in *Urban Geography*, 23, 257-278.

[67] *Id*., (2012). *"You shouldn't wear that body:* The Problematic of Surveillance and Gender". In BALL, K., HAGGERTY, K.D., & LYON, D. (Eds.), *Routledge handbook of surveillance studies* (p. 49-56). London: Routledge, p. 52-53.

[68] See, for example, CONRAD, K. (2009). "Surveillance, gender and the virtual body in the Information Age". *Surveillance & Society*, 6(4), 380-387.

[69] A notorious example of an AI system with discriminatory effects is the system known as "Correctional Offender Management Profiling for Alternative Sanctions" – COMPAS. The COMPAS system is used in parts of the US to predict whether defendants will commit crime again. The idea is that COMPAS can help judges to determine whether somebody should be allowed to go on probation (supervision outside prison). The COMPAS system does not use racial origin or skin colour as an input. But research by Angwin et al., investigative journalists at ProPublica, showed in 2016 that COMPAS is "biased against blacks".

> *COMPAS (...) correctly predicts recidivism 61 percent of the time. But blacks are almost twice as likely as whites to be labelled a*

higher risk but not actually reoffend. It makes the opposite mistake among whites: They are much more likely than blacks to be labelled lower risk but go on to commit other crimes

See ANGWIN, J. & AL. (2016), "Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks". *ProPublica,* May 23, 2016, https://www.ProPublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (accessed August 2019).

See also GIACOMELLI, L. (2019), "Big Brother is «gendering» you. Il diritto antidiscriminatorio alla prova dell'intelligenza artificiale: quale tutela per il corpo digitale?", in *BioLaw Review*, 2.

[70] See KOSKELA, H. (1997). "*Bold walk and breakings*: Women's spatial confidence versus fear of violence". *Gender, Place and Culture*, 4, 3, 301-319.

[71] See, among others, JACKSON, R. (2007). "Constructing enemies: *Islamic terrorism*" in *Political and Academic Discourse*. *Government and Opposition*, 42, 3, 394-426.

[72] MACMAHON, J. (2012). *Normalizing Gender, Performing the State: Disciplinary Power and Biopower at the Airport Security Checkpoint*, New York State Political Science Association Annual Conference, April 20-21, https://www.academia.edu/2367414/Normalizing_Gender_Performing_the_State_Disciplinary_Power_and_Biopower_at_the_Airport_Security_Checkpoint (accessed August 2019).

[73] *Idem*.

[74] See CONRAD, K. (2009). "Surveillance, gender and the virtual body in the Information Age". *Surveillance & Society*, 6(4), 380-387.

[75] HACKING, I. (1990). *The taming of chance*. Cambridge and New York: Cambridge University Press, p. 3.

[76] MONAHAN, T. (2010). *Surveillance in the time of insecurity*. New Brunswick: Rutgers University Press, p. 116.

[77] In recent years some countries like Nepal, Australia, Germany have introduced the possibility of indicating a third gender (or not to specify it) at the registry public office. See, for example, DUNNE, P. & MULDER, J. (2018). "Beyond the Binary: Towards a Third Sex Category" in Germany?, in *German Law Journal*, 19.3, 627-648; HERPOLSHEIMER, A. (2017). "A Third Option: Identity Documents, Gender Non-Conformity, & the Law!", in *Women's Rts. L. Rep*., 39: 46.

[78] See GANDY, O.H. (2012). "Statistical surveillance: remote sensing in the Digital Age". In BALL, K., HAGGERTY, K.D., & LYON, D. (Eds.), *Routledge handbook of surveillance studies* (pp. 125-132). London: Routledge.

[79] CONRAD, K. (2009). "Surveillance, gender and the virtual body in the Information Age". *Surveillance & Society*, 6(4), 380-387, p. 385.

[80] Supreme Court of Canada, *Egan v. Canada*, [1995] 2S.CR 513.

[81] GANDY, O.H. (2012). "Statistical surveillance: remote sensing in the Digital Age". In BALL, K., HAGGERTY, K.D., & LYON, D. (Eds.), *Routledge handbook of surveillance studies* (p. 125-132). London: Routledge, p. 127.

[82] See, in particular, COLLINS, H. & KHAITAN, T. (2018). "Indirect discrimination law: Controversies and critical questions", in COLLINS, H. & KHAITAN, T. (Eds), *Foundations of Indirect Discrimination Law*. London: Hart Publishing. See, also, FREDMAN S. (2016)."Intersectional discrimination in EU gender equality and non-discrimination law, European network of legal experts in gender equality and non-discrimination". Report for European Commission, Directorate-General for Justice and Consumers, in https://publications.europa.eu/en/publication-detail/-/publication/d73a9221-b7c3-40f6-8414-8a48a2157a2f/language-en (accessed August 2019).

[83] See, for example, LARSON, J. et Al.. *These are the job ads you can't see on Facebook if you're older*, The New York Times, 19 December 2017; HACKER, P. (2018). "Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law", in 55 *Common Market Law Review*, Issue 4, 1143–1185.

[84] See, above all, RODOTÀ, S. (1997). *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma and Bari: Laterza.

[85] FALCÓN, E. (1996). *Hábeas Data. Concepto y procedimiento*. Buenos Aires: Editorial Abeledo-Perrot, p. 28.

[86] GUADAMUZ, A. (2001). "Habeas Data vs the European Data Protection Directive", in *The Journal of Information, Law and Technology*, 3.

[87] The General Data Protection Regulation (GDPR), nº. 2016/679, agreed upon by the European Parliament and Council in April 2016, has replaced the Data Protection Directive nº. 95/46/EC in Spring 2018 as the primary EU law regulating how companies and institutions protect EU citizens' personal data. For a comparative overview see GELLERT, R., DE VRIES, K., DE HERT, P., & GUTWIRTH, S. (2013). "A comparative analysis of anti-discrimination and data protection legislations", in CUSTERS, B., CALDERS, T., SCHERMER, B. & ZARSKY, T. (Eds.). *Discrimination and privacy in the information society. Data mining and profiling in large databases*. Berlin: Springer.

[88] Article 5 of the GDPR and, also, Articles 5, 7, and 10 COE Data Protection Convention 2018. See MANTELERO, A. (2018). "Artificial Intelligence and data protection: Challenges and possible remedies. Draft report for the Council of Europe's Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", T-PD(2018)09Rev, in https://rm.coe.int/report-on-artificial-intelligence-artificial-intelligence-and-data-pro/16808d78c9 (accessed August 2019).

[89] See, for example, MENDOZA, I. & BYGRAVE, L.A. (2017). "The right not to be subject to automated decisions based on profiling", in SYNODINOU, T., JOUGLEUX, P., MARKOU, C. & PRASTITOU, T. (Eds.). *EU Internet Law: Regulation and Enforcement*. Berlin: Springer.

[90] See, among others, SELBST, A.D. (2017). "Disparate impact in Big Data policing", in 52 *Ga.L.Rev*., 109; O'NEIL, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Crown Publishing Group; SCHAUER, F.F. (2003). *Profiles, probabilities, and stereotypes*. New York: Harvard University Press.

[91] See, in particular, GIACOMELLI, L. (2018). *Ripensare l'eguaglianza. Effetti collaterali della tutela antidiscriminatoria*. Torino: Giappichelli.

[92] See KOSKELA, H. (2000). "*The Gaze without Eyes:* Video-surveillance and the changing nature of urban space. Progress" in *Human Geography*, 24, 243-265; *Id*., (2002). "Video surveillance, gender, and the safety of public urban space: "Peeping Tom" goes high tech?" *Urban Geography*, 23, 257-278.

[93] PASQUALE, F. (2016). "Bittersweet Mysteries of Machine Learning (A Provocation)", in *London Sch. Econ. & Pol. Sci.: Media Pol'y Project Blog*,
In
http://blogs.lse.ac.uk/mediapolicyproject/2016/02/05/bittersweet-mysteries-ofmachine-learning-a-provocation/ [https://perma.cc/XSS9-2D58] (accessed August 2019); see, also, GIACOMELLI, L. (2019). "Big Brother is «gendering» you. Il diritto antidiscriminatorio alla prova dell'intelligenza artificiale: quale tutela per il corpo digitale?", in *BioLaw Review*, 2.

References

ANGWIN, J. & Al. (2016). "Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks". *ProPublica,* May 23, 2016, https://www.ProPublica.org/article/machine-bias-risk- assessments-in-criminal-sentencing.

ANDREJEVIC, M. (2012). *Ubiquitous surveillance*. In BALL, K., HAGGERTY, K.D., & LYON, D. (Eds.). *Routledge handbook of surveillance studies* (p. 125-132). London: Routledge.

ANDREJEVIC, M. (2014). "Book review: Zygmunt Bauman and David Lyon, Liquid surveillance*"*. *Media, Culture & Society,* 36(3), 409–411.

BALL, K., GREEN, N., KOSKELA, H., & PHILLIPS, D.J. (2009). "Editorial: surveillance studies needs gender and sexuality". *Surveillance & Society*, 6(4), 352-355.

BAROCAS, S. & SELBST, A.D. (2016). "Big Data's disparate impact", in *Californian Law Rev*., 105, 671.

BARTLETT, K. (2018). *Feminist legal theory: Readings in law and gender*. New York: Routledge.

BAUMAN, Z. (2000). *Liquid modernity*. Cambridge: Polity Press.

BAUMAN, Z. & LYON, D. (2012). *Liquid surveillance: a conversation*. Cambridge: Polity Press.

BENTHAM, J. (1791). *Panopticon or the inspection house, Vol. 1*. London: T. Payne.

BENTHAM, J. & BOŽOVIČ M. (1995). *The panopticon writings*. 1st ed. London: Verso.

BOEHME-NEßLER, V. (2016). "Privacy: a matter of democracy. Why democracy needs privacy and data protection", in *International Data Privacy Law*, 6.3, 222-229.

BOWKER, G. C. & STAR, S. L. (1999). *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: MIT Press.

COLLINS, H. & KHAITAN, T. (2018). "Indirect discrimination law: Controversies and critical questions", in COLLINS, H. & KHAITAN, T. (Eds). *Foundations of Indirect Discrimination Law*. London: Hart Publishing.

CONRAD, K. (2009). "Surveillance, gender and the virtual body in the Information Age". *Surveillance & Society*, 6(4), 380-387.

DANNA, A., GANDY, O.H. (2002). All that glitters is not gold: digging beneath the surface of data mining, in *Journal of Business Ethics* 40(4), 373-386.

DUNNE, P. & MULDER, J. (2018). "Beyond the Binary: Towards a Third Sex Category in Germany?", in *German Law Journal*, 19.3, 627-648.

FALCÓN, E. (1996). *Hábeas Data. Concepto y procedimiento*. Buenos Aires: Editorial Abeledo-Perrot.

FOUCAULT, M. (1975). *Discipline and punish: the birth of the prison*, New York: Random House.

FOUCAULT, M. (1979 [1976]). *The history of sexuality Volume 1: An introduction*. London: Allen Lane.

FREDMAN S. (2016). "Intersectional discrimination in EU gender equality and non-discrimination law, European network of legal experts in gender equality and non-discrimination. Report for European Commission, Directorate-General for Justice and Consumers", in https://publications.europa.eu/en/publication-detail/-/publication/d73a9221-b7c3-40f6-8414-8a48a2157a2f/language-en.

GANDY, O.H. (1993). *The panoptic sort: A political economy of personal information*. Boulder, CO: Westview.

GANDY, O.H. (2012). "Statistical surveillance: remote sensing in the Digital Age". In BALL, K., HAGGERTY, K.D., & LYON, D. (Eds.). *Routledge handbook of surveillance studies* (p. 125-132). London: Routledge.

GELLERT, R., DE VRIES, K., DE HERT, P., & GUTWIRTH, S. (2013). "A comparative analysis of anti-discrimination and data protection legislations", in CUSTERS, B., CALDERS, T., SCHERMER, B. & ZARSKY, T. (Eds.). *Discrimination and privacy in the information society. Data mining and profiling in large databases*. Berlin: Springer.

GIACOMELLI, L. (2012). "Quando la vita infrange il mito della 'normalità': il caso dei minori intersessuali". *Rivista Critica del Diritto Privato*, 4, 597-636.

GIACOMELLI, L. (2018). *Ripensare l'eguaglianza. Effetti collaterali della tutela antidiscriminatoria*. Torino: Giappichelli.

GIACOMELLI, L. (2019), "Big Brother is «gendering» you. Il diritto antidiscriminatorio alla prova dell'intelligenza artificiale: quale tutela per il corpo digitale?", in *BioLaw Review*, 2.

GUADAMUZ, A. (2001). "Habeas data vs the European Data Protection Directive". *The Journal of Information, Law and Technology*, 3.

HACKER, P. (2018). "Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law", in 55 *Common Market Law Review*, Issue 4, 1143–1185.

HACKING, I. (1990). *The taming of chance*. Cambridge and New York: Cambridge University Press.

HERPOLSHEIMER, A. (2017). "A third option: identity documents, gender non-conformity, & the law", in *Women's Rts. L. Rep*., 39: 46.

JACKSON, R. (2007). "Constructing enemies: *Islamic terrorism*" *in Political and Academic Discourse*. *Government and Opposition*, 42, 3, 394-426.

JERNIGAN, C. & MISTREE, B.F. (2009). "Gaydar: Facebook friendships expose sexual orientation". 14(10), First Monday.

KOSKELA, H. (1997). *"Bold walk and breakings":* Women's spatial confidence versus fear of violence. *Gender, place and culture*, 4, 3, 301-319.

KOSKELA, H. (2000). *"The gaze without eyes:* video-surveillance and the changing nature of urban space. Progress" *in Human Geography*, 24, 243-265.

KOSKELA, H. (2002). "Video surveillance, gender, and the safety of public urban space: "Peeping Tom" goes high tech*?",* in *Urban Geography*, 23, 257-278.

KOSKELA, H. (2012). "*You shouldn't wear that body:* The problematic of surveillance and gender", in BALL, K., HAGGERTY, K.D., & LYON, D. (Eds.). *Routledge handbook of surveillance studies* (p. 49-56). London: Routledge.

LARSON, J. et Al., "These are the job ads you can't see on Facebook if you're older", The New York Times, 19 December 2017.

LYON, D. (2001). *Surveillance society: monitoring everyday life.* Buckingham: Open University Press.

LYON, D. (Ed.) (2003). *Surveillance as social sorting: privacy, risk, and digital discrimination*. New York: Routledge.

LYON, D. (2007). *Surveillance studies: An overview*. London: Polity.

MACKINNON, C.A. (1983). "Feminism, Marxism, method, and the State: toward feminist jurisprudence". *Signs 8*, 4, 635-658.

MACKINNON, C.A. (1989). *Toward a feminist theory of the State*. Cambridge, MA: Harvard University Press.

MACKINNON, C.A. (2000). "Disputing male sovereignty: on United States v. Morrison". *Harvard Law Review* 114, 1, 135-177.

MACKINNON, C.A. (2003). "Women and law: the power to change". In R. Morgan (Ed.). *Sisterhood is forever: the women's anthology for a new millennium* (p. 447-55). New York: Washington Square Press.

MACKINNON, C.A. (2006). *Are Women human?: and other international dialogues*. Cambridge: Harvard University Press.

MACMAHON, J. (2012). *Normalizing gender, performing the State: disciplinary power and biopower at the Airport Security Checkpoint*,
in
https://www.academia.edu/2367414/Normalizing_Gender_Performing_the_State_Disciplinary_Power_and_Biopower_at_the_Airport_Security_Checkpoint.

MAI, J. (2016). "Big data privacy: the datafication of personal information", in *The Information Society*, 32.3, p. 192-199.

MANTELERO, A. (2018). "Artificial intelligence and data protection: Challenges and possible remedies. Draft report for the Council of Europe's Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", T-

PD(2018)09Rev, in https://rm.coe.int/report-on-artificial-intelligence-artificial-intelligence-and-data-pro/16808d78c9.

MATHIENSEN, T. (1999). *On globalization of control: towards an integrated surveillance system in Europe*. London: Statewatch.

MENDOZA, I. & BYGRAVE, L.A. (2017). *The right not to be subject to automated decisions based on profiling*, in SYNODINOU, T., JOUGLEUX, P., MARKOU, C. & PRASTITOU, T. (Eds.). *EU Internet Law: regulation and enforcement*. Berlin: Springer.

MINOW, M. L. (1990). *Making all the difference: inclusion, exclusion, and American Law*. Ithaca: Cornell University Press.

MONAHAN, T. (2010). *Surveillance in the time of insecurity*. New Brunswick: Rutgers University Press.

NOBLE, S.U. (2018). *Algorithms of oppression. How search engines reinforce racism*, New York: NYU Press.

NORRIS, C., & ARMSTRONG, G. (1999). *The maximum surveillance society: the rise of CCTV*, Berg, Oxford and New York.

O'NEIL, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York: Crown Publishing Group.

ORWELL, G. (1948). *Nineteen Eighty-Four*. London: Secker & Warburg.

PASQUALE, F. (2016). "Bittersweet mysteries of machine learning (a provocation)", in *London Sch. Econ. & Pol. Sci.: Media Pol'y Project Blog*,
in http://blogs.lse.ac.uk/mediapolicyproject/2016/02/05/bittersweet-mysteries-ofmachine-learning-a-provocation/ [https://perma.cc/XSS9-2D58].

POSTER, M. (1990). *The Mode of Information. Poststructuralism and Social Context*. Cambridge: Polity Press.

RESTA, G., ZENO-ZENCOVICH, V. (Eds.) (2016). *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma: Roma Tre Press.

RODOTÀ, S. (1997). *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma and Bari: Laterza.

RODOTÀ, S. (2004). *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, 26th International Conference on Privacy and Personal Data Protection, Poland, Wroclaw, September 14-16, in
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1049293.

ROSS, E.A. (1969). *Social Control: A Survey of the Foundations of Order*. Cleveland, OH: The Press of Case Western Reserve University.

SELBST, A.D. (2017). "Disparate impact in Big Data policing", in 52 *Ga.L.Rev*., 109.

SCHAUER, F.F. (2003). *Profiles, probabilities, and stereotypes*. New York: Harvard University Press.

SMART, C. (1992). *The woman of legal discourse*. *Social and legal studies*, 1, 29-44. Warren, S.D., Brandeis, L.D. (1890). "The right to privacy", in *Harvard Law Review*, vol. 4, p. 193-220.

YU, S. (2016). "Big privacy: challenges and opportunities of privacy study in the age of big data", in *IEEE access*, 4, p. 2751-2763.

ZUBOFF, S. (2015). "Big other: surveillance capitalism and the prospects of an information civilization", in *Journal of Information Technology*, 75-89.