Journal of Ethics and Legal Technologies – Volume 3(2) – November 2021

Special Section introduction: Identity and Citizenship in the Algorithmic Society

Guido Gorgoni

Dipartimento di Scienze Politiche, Giuridiche e Studi Internazionali Università degli Studi di Padova
guido.gorgoni@unipd.it

Short Title: Identity and Citizenship in the Algorithmic Society

Keywords: Algorithmic Society, Artificial Intelligence, Digital Citizenship

Introduction

The focus theme of this special issue is on "identity and citizenship in the Algorithmic Society", along the definition proposed by Jack M. Balkin:

> [...] a society organized around social and economic decision-making by algorithms, robots, and Al agents, who not only make the decisions but also, in some cases, carry them out[1].

The development of Artificial Intelligence (AI) under the form of automated decision-making, already targeted by the first legal instruments dealing with data protection, has nowadays reached a new qualitative step given its pervasiveness in our daily life, which is likely to increase in the near future.

The delegation of decisions to algorithms affects the very idea of the law affecting the legal experience built on it:

> The study and practice of [Modern] law have thus been focused on establishing the meaning of legal norms and their applicability to relevant human interactions, while establishing the meaning of human action in the light of the applicable legal norms. Data-driven agency builds on an entirely different grammar, its building blocks are information and behavior, not meaning and action. We need to face the possibility that this will drain the life from the law, turning it into a handmaiden of governance (that fashionable term meaning anything to anybody), devouring the procedural kernel of the Rule of Law that enables people to stand up for their rights[2].

The characters of the Algorithmic Society question not only the idea of personal identity, but the very idea and nature of the law: "explainability matters because the process of reason-giving is intrinsic to juridical determinations – not simply one modular characteristic jettisoned as anachronistic once automated prediction is sufficiently advanced"[3]. In particular, the developments of AI raise concerns on the loss accountability in the decision-making process given the role played by automated decision-making processes.

Whilst the issues raised by data collection and automated processing are already part of the current debate, especially after two years of COVID-19 pandemic crisis which exasperated not only the collection and the use of data, but also the use of automated data processing techniques and devices the sense of connecting identity and citizenship may not emerge clearly at first glance and needs some clarification.

[1] Balkin 2017, 1219.
[2] Hildebrandt 2016, 2.
[3] Pasquale 2017, 1252.

In the next subsections I will try to provide some quick insights on the terms of the debate, in particular focusing on three core concepts characterizing the debate around the Algorithmic Society hosted here: datafication, identity and citizenship.

Datafication

The datafication of personal information[4] implies the traditional problems of surveillance and control, taking them to another level, but also – and more radically – directly affects the very construction of the identity:

> […] people's lives are subject to a cascade of algorithmic judgments that fashion identity, opportunities, and vulnerabilities over time […] The central problem we face today, therefore, is not intentional discrimination, but cumulative harm to identity and opportunities[5].

Datafication means a further step beyond digitalization, marking a substantive transformation, comparable to a major infrastructural advance such as the ones represented by aqueducts or the *Enciclopédie* [6]:

> […] datafication represents an essential enrichment in human comprehension. With the help of big data, we will no longer regard our world as a string of happenings that we explain as natural or social phenomena, but as a universe comprised essentially of information.

Datafication is therefore not a technical but a societal phenomenon; in particular the datafication of personal information leads to the emergence of a new kind of society:

> Digitization was the process of taking the analog world to the digital environment; it allowed society to store more information and process it more rapidly. In the digitized era, digital information was still treated as if it was analog, and it was often used within the same " singular purposes for which it was collected and to which its "value was tied" […] Datafication allows analysis of information in more sophisticated ways and allows analyses across large data sets. It breaks down the traditional understanding of data as numbers and information as texts, movies, music, and so on[7].

Despite not being explicitly presented in the debate, it is clear that datafication is ongoing not only within the socio-technical context of big data,

[4] Mai 2016, 193.
[5] Balkin 2017, 1235–36.
[6] Mayer-Schönberger and Cukier 2013.
[7] Mai 2016, 194.

but also within the economical-political context of the well-known formula of the "surveillance capitalism"[8], which is accompanied and sustained by the generalization of a broad "surveillance culture"[9], which locates the debate beyond the traditional perspective of state surveillance and social control[10].

Identity

What characterises the Algorithmic Society is not only the fact of the automated decision-making, but also its extent, since the digital profile of a person becomes an integral part of her legal identity (and sometimes, but this is out of the scope of our current discourse, of her psychological identity). On the digital sphere identity is unilaterally attributed more than intersubjectively negotiated in social interactions[11] in that it results from the processing of data which escapes the mastering of the data subject.

> A central concern is how identity – the association of persons with positive and negative associations and traits – is constructed and distributed in the Algorithmic Society [...] people's algorithmically constructed identities and reputations may spread widely and pervasively through society, increasing the power of algorithmic decision-making over their lives[12].

Among the most prominent scholars in the field of the legal, ethical and societal impacts of machine learning and automated data processing, Mireille Hildebrandt in one side recalls the distinction between identity-idem and identity-ipse in order to preserve the idea of the incomputable nature of personal identity, whilst at the same tine advocating for an "agonistic machine-learning" as a form of negotiation of the algorithmically-defined identity[13].

What links directly identity and citizenship is the issue of the representation of oneselves, as well as of others, as citizens beyond the membership of a particular legal system; under this respect the question of the identity and that of citizenship do not belong to separate fields, ethics on one side and politics on the other, but are part of the same reflection: that of the anthropological and political construction of the self mediated by the interactions wit the others through the internet.

[8] Zuboff 2019.
[9] Lyon 2019.
[10] Rodotà 1973.
[11] Swann Jr 2005.
[12] Balkin 2017, 1236.
[13] Hildebrandt 2019.

Citizenship

In line with the arguments exposed above, the recent years show an increasing reflection on the subject of digital citizenship, flourished in particular after the "Snowden turn", which led to take into account not only the surveillance coming from the side of the States, but more profoundly obliged to rethink the impact of surveillance practices, included self-surveillance, on the very idea of (digital) citizenship[14]. In particular the most promising and inspiring theorizations of digital citizenship aim explicitly at going beyond the usual definition of the digital citizen as "those who use the Internet regularly and effectively—that is, on a daily basis"[15].

This latter approach puts the focuses of digital citizenship on participation in society online:

> Digital citizens are those who use technology frequently, who use technology for political information to fulfill their civic duty, and who use technology at work for economic gain"[16].

The Snowden revelations and the development of the surveillance capitalism show how this perspective is not sufficient for configuring a satisfactory figure of the digital citizen, able to cope with the imbalance of power relations at the (geo)political as well as at the economic level[17]. Therefore, instead of focusing on the inclusion of the citizen in existing forms of participation which are already defined and which therefore are considered as satisfactorily implementing the citizenship idea in the digital sphere, some of the more prominent constructions of citizenship purport a portrait of the digital citizen as one who is engaged in struggles for *claiming* rights, i.e. in co-defining the very spaces of participation, if necessary subverting the existing ones from within. What emerges is therefore an active, critical and subversive figure of the citizen, a figure certainly not yet fully existing, apart a growing number of prominent examples, but a citizen "yet to come"[18].

The contributes in this special session

The special session of this issue presents a multifaceted picture of some of the core issues characterizing the shape of identity and digital citizenship.

[14] Hintz, Dencik, and Wahl-Jorgensen 2019.
[15] Mossberger 2008, 1.
[16] Mossberger 2008, 15.
[17] Bauman et al. 2014.
[18] Isin and Ruppert 2020.

Raphaël Gellert opens the debate on the algorithmic society by directly dealing with the current issue of the regulation of AI, in particular by examining the risk-based approach adopted in the recent Regulation proposal of the European Commission "Laying Down Harmonised Rules on Artificial Intelligence" (AIA, Artificial Intelligence Act), comparing it with the risk-based regulatory approach adopted by the GDPR.

The author highlights how these two complementary regulations (although one already in force, one only proposed) are inspired to different types of risk-based regulation models which play different functions, leading to considerably different outcomes; but at the same time the author proposes a way to hermeneutically deal with this structural difference so as to practically reduce the concrete impacts of the different logic animating two regulatory acts that shall work together.

Far from being a pure legal technicality, "risk regulation has become an inherent feature of the EU internal market" and therefore plays a crucial role in shaping European legislation, in particular the one dealing with scientific and technological innovation.

From the proposed analysis it emerges how in the AIA the role of risk-based approach is that of determining the thresholds of (high) risks above which AI systems require regulatory (or legislative) intervention, whilst on the other side the risk-based approach in the GDPR has a different rationale, aiming at determining the intensity of the compliance measures (along the data protection impact assessment).

In fact, in the GDPR risk is calculated by paying attention to the properties of the processing, which are considered as a proxy for the extent of the risk, on the contrary the AIA put the emphasis on the harms potentially or actually experienced by the individuals. Nevertheless the considerable divergence at the theoretical level between these two different approaches to measuring risks can be mitigated in practice, in particular by reading the proposed AIA in the light of some relevant recitals of the text.

At the end of this exercise the distinction between the two different approaches to risks regulation might be rendered less strong as the two regulation models might suggest. Indeed both acts deal with risks affecting fundamental rights, which lend themselves much less easily to scientific and quantitative analyses of risk and do require a different, qualitative and evaluative, approach.

So whilst at a first glance the proposed AIA seems to be inspired to a logic of traditional command and control regulation, rather than the risk-based system of compliance, more flexible and discretionary, characterizing the GDPR, a careful interpretation of its provisions shows that the opposition

between a system of flexible compliance (characterizing the GDPR) and rigid compliance (characterizing the proposed AIA) is not as sharp as it may appear.

The similarity between the concerns which inspire the two regulations lead us to question the considerable difference between these two regulatory approaches, which in turn lead to ask whether the European Commission in determining what counts as a high risk AI system "should be more risk averse (with the chance of wrongly including non-high risk systems) or should it be more risk friendly (with the chance of omitting some high risk AI systems)"?

This leads to question the "solidity" of the European Commission's approach used in the AIA, be it at the theoretical and methodological level, as well as at the legal and political one, since "what is deemed to count as a high risk [...] is context-dependent and therefore susceptible to change through time", being dependent on the risk appetite of the regulator. In this sense, focusing on high risks as triggers for regulation – as in the AIA – appears to be quite risk-friendly and deviates from the approach to risk regulation used in other acts similarly dealing with risks to health, safety and fundamental rights: "it could have been perfectly possible to require that all AI systems comply with a minimum or essential level of health, safety, and fundamental rights protection, which in this case would be undertaken through the quality management system (instead of the safety assessment)".

The analysis shows how a different regulatory approach to AI is possible; in particular how it would be possible to dress a uniform approach concerning all AI systems much less risk friendly than the existing proposal and instead more aligned with the precautionary principle, which not only is a fundamental principle of European law, not only inspiring many instruments of the New Legislative Framework, but also indicated as extremely important by the High-Level Expert Group on Artificial Intelligence, which explicitly recommended that the future AI Act shall be based on the logic of the precautionary principle. Nevertheless, despite these solid normative and scientific anchorages, the precautionary principle does not seem to be taken in adequate consideration for the regulation of the algorithmic European society.

The issues of regulating and in turn being regulated by AI systems are at the core of the contribution by **Alberto Cammozzo** proposing a topology of the socio-technical as well as economical and political spaces as they are configured in the algorithmic society (he speaks of an "algorithmic turn"), in which "social, communicative and informative space is shaped together by humans and machines, further deepening the ethical issues about the ecological responsibility".

Building on a classification of the spatial location of social machines, the author suggests four possible alternative spatial dimensions focusing on the impact that social machines have on the communicative, informative and relational environment, along *an axis where the spatial dimension of the social machine action becomes more and more closer to the individual.*

The proposed taxonomy is not spatial but "ecological" and "semiotic" since it puts the accent on the *relational* habitat, distinguishing accordingly between four basic "spaces": *a-topies*, *hetero-topies*, *iso-topies*, and *soma-topies*.

This approach is extremely interesting and relevant in that it highlights the ethical issues that arise around the spaces of social machines along two axes: the physical, geographically located one, expressing *where* social machines components are situated (infrastructures, people, knowledge, labour, payments).

The second, semiologic, is tied to the four spatial dimensions mentioned above and regards *what kind of* cultural environment social machines are designed to respond to: "what are the algorithms, codes, interfaces, possible encoding variables of the content the machine handles".

This allows to draw in one side some "geographies of inequality" as far as social machines play a key role in producing inequalities.

On the other side, along the semiotic axis, this leads to sketch a relational ecology focused on some fundamental ethical issues, such as context puncturing, reduction of variety and pollution.

This highlights some major concerns not only for the legal system and for regulation (such as those examined by the article of Raphaël Gellert in this section), but also – and possibly mainly – for the identity of the individuals and their constitution as a (digital) citizens. To grasp them the author invites us to reflect on the fact that under the socio-technical architecture:

> "Whole languages, cultures, social norms and legal systems, forced in the moulds of standardized interfaces often forged in topologically and culturally concentrated environments, may be challenged".

The sketched double topology permits also to draw an analogy between the pollution affecting the natural environment and the practice of dumping costs on the social environment is also pertinent when considering algorithms. In this case, pollution is the result of a negligent use of computational capacities that externalizes costs onto innocent others (in terms of, e.g. harms to reputation, discrimination, normalization or manipulation of behaviour, lack of transparency/accountability).

This emphasizes how "social machines may change the relational capabilities embedded in these ecosystems exerting a structural power in

shaping space and relations in space", clearly drawing responsibilities on those who design and employ them.

The identity of the person is at the core of the analysis proposed by **Enrico Maestri** which is dealing with the issue whether or not it is still possible to introduce new effective forms of governance for protecting individuals, and in particular children, as digital persons, in particular their rights to dignity, habeas data and personal data privacy.

In line with the analyses proposed by Alberto Cammozzo, the author locates the discourse within the sort of *digital promiscuity produced by the fact that people live simultaneously online and offline, a "dual realm"* where experimentation with relationships produces a digital neighborhood without the need for relational depth.

In the cyberspace, – a "space without place and without bodies" – "a person becomes a flow information that is continuously exchanged in a coded system, so that the questin raises on how is it possible to discern the identity of any particular individual, in a context where the only identifiable element is digitised information.

This way

> "a person loses every re-putation (every ontological thinkability) and becomes an informational organism destined to mutate in every instant" so that it becomes "virtually impossible for an institutional entity aiming to protect the digital person, to reconstruct that person's identity and establish whether an injury to their reputability has occurred."

We shall therefore take into account, following Stefano Rodotà, that "a new entity – the digital person – has made its appearance in the digital ecosystem, as a technological outcome of the reconfiguration of the classical concept of person".

The point is that digital persons are taken in a web of connections without spatial constraints or the need for a shared physical presence, and currently play a crucial role in cultural praxis and in a primary socialization, in forms which are located far away from the idea of privacy.

This is particularly visible if we consider the rules of the GDPR aiming at protecting the personal data of children, which illustrates paradigmatically the tendency to contractualise the legitimization of personal data processing.

Three years after its full implementation, the GDPR has not proved itself to ensure adequate harmonisation of the rules regarding the protection of children, so that substantial restrictions are still established by pre-existing or new laws or codes of conduct at a national level. Far from being an

accident, the author emphasizes how indeed the GDPR was not constructed in such a way as to enable complete protection of individual privacy.

Recalling the fact that "cyberspace is an architectural system that implements the codifying of human normative spaces, i.e. the channelling of modes of action, of the logical and functional governance of cognitive processes, of possible motivations and practicable or available alternatives", the author underlines the tendency to transform personal data into a commodity, so that "once they go online the rights recognised in the real world become more fragile and blurred", since "they are subjected to the pressure of supranational private actors which, in order to get around certain legal constraints, choose the most advantageous jurisdiction for the purpose of forum shopping in the regulatory space". This represents "an ideal habitat for anyone who wishes to exercise global surveillance over digital bodies".

Consequently the need arises to protect the rights of a new entity – the digital person – who inhabits a place – the cyberspace – where temporal and spatial limits no longer apply.

"The digital person travels continuously between two worlds interconnected by platforms, veritable vehicles of transmission, memorisation and manipulation of every piece of information; this global digital nonplace is the World Wide Web".

The author echoes the topology illustrated in the essay of Alberto Cammozzo by reminding us that.

Within this reconfigured space the person (in the classic sense of subjective identity and psychological and physical integrity) is transformed into a *digital person*, i.e. into "a cluster of data in which corporeality, instead of disappearing, is socially relocated and technologically governed", so that "we risk losing sight of the distinctive attributes of humans, such as the value of dignity and the moral sense of belonging to one's own species".

The author proposes a differentiation between the two notions of digital identity and digital persona as a crucial step in creating better future ICT systems.

Whilst digital identity does not seem to be linked to anything that people refer to as *identity*, "the digital person is a collection of information that the cognitive and sensory mechanics of a human being parses into an individual actor, a character".

Within this context young teenagers are more vulnerable than adults: "as a consequence of dataveillance via mobile and wearable devices, social media platforms and educational software, children are considered like algorithmic assemblages, with the risk that their complexity, potentialities and opportunities may be profiled".

The architectures of cyberspace has an impact on legal constraints, they also end up supplanting the fundamental values and principles of law, allowing data to be transformed from a fundamental component for the construction of an individual's digital *personality* into an intangible *object* of exchange.

The *digital person* is the result of data produced by a *natural person*: an electronic device, body-information, body-password: it is a receptacle of collected, processed data and information forming a person's digital biography.

The author provocatively concludes the analysis this way:

"Our existence as separate individuals and our personal identity are based on the fact that we *are* bodies. The network of computers has made the physical presence of participants redundant by omitting or simulating the immediacy of the body. The dark side of this cybernetic operation implies that it is the mind which governs our organic life. Yet can we ever be completely present when we live through a surrogate or virtual body that stands in our place?"

The intimate link between the bodily nature of our identity and the use of personal data in the algorithmic society is the central issue examined in the contribution of **Gianluigi Fioriglio** dealing with the some crucial aspects of the current evolutions in the field of the protection of health data. In particular the essay warns about the increasing tendency to reduce persons to a cluster of data, along the tendency to "dataism", including attempts to reconstruct some unpredictable emotional aspects characterising human beings.

Profiling is increasingly applied to human health, both regarding medical intervention as well as related services which may have a medical impact on health, like smartwatches providing health-related data. In particular reference is made to the widespread use of *Electronic Health Records* ("Fascicolo Sanitario Elettronico" in Italy), as well as to the development of precision medicine and individualized therapies.

The *mobile health* highlights a new form of vulnerability, that of users which may become victims of obsessive pressures on health and pervasive forms of medicalization, along standards which are not medically but socially and algorithmically defined, generating a subsequent, ofthen implicir, pressure to conform to these standards.

The IA therefore is increasingly given the task to define and tell "the truth", as Sadin warns. Two aspects of this process are increasingly problematic: on the one side, the fact that data are increasingly less controllable, given the overlapping phenomena of Big Data and cloud systems, which make them *inaccessible*; on the other side, the fact that data are not "taken" but are increasingly "built" through analytics and through automated decision-

making processes. Both these phenomena are not adequately tackled by the GDPR, as other authors in this section highlight, despite its apparently stringent provisions. Neither the regulatory initiatives undertaken in the field of health, such as the eIDAS (electronic IDentification Authentication and Signature) regulation, or the regulation proposal on a Single Market For Digital Services (Digital Services Act) seem to provide the necessary change of perspective in this field.

References

Balkin, Jack M. 2017. "The Three Laws of Robotics in the Age of Big Data (2016 Sidley Austin Distinguished Lecture on Big Data Law and Policy)." *Ohio State Law Journal*, no. 5: 1217–42.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2): 121–44. https://doi.org/10/gc8z96.

Hildebrandt, Mireille. 2016. "Law as Information in the Era of Data-Driven Agency." *The Modern Law Review* 79 (1): 1–30. https://doi.org/10.1111/1468-2230.12165.

———. 2019. "Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning." *Theoretical Inquiries in Law* 20 (1). http://www7.tau.ac.il/ojs/index.php/til/article/view/1622.

Hintz, Arne, Lina Dencik, and Karin Wahl-Jorgensen. 2019. *Digital Citizenship in a Datafied Society*. Polity. https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1985304.

Isin, Engin, and Evelyn Ruppert. 2020. *Being Digital Citizens (Second Edition)*. London: Rowman & Littlefield International. https://rowman.com/WebDocs/Being_Digital_Citizens_Second_Ed_Open_Access.pdf.

Lyon, David. 2019. "Surveillance Capitalism, Surveillance Culture and Data Politics." In *Data Politics: Worlds, Subjects, Rights. Abingdon: Routledge*, 64–77.

Mai, Jens-Erik. 2016. "Big Data Privacy: The Datafication of Personal Information." *The Information Society* 32 (3): 192–99. https://doi.org/10/gfz43k.

Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big data: a revolution that will transform how we live, work and think.* London: John Murray Publishers.

Mossberger, Karen. 2008. "Defining Digital Citizenship." In *Digital Citizenship: The Internet, Society, and Participation*, edited by Caroline J. Tolbert, Ramona S. McNeal, and Karen Mossberger, 1–19. MIT Press.

Pasquale, Frank. 2017. "Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society." *Ohio State Law Journal* 78: 1243.

Rodotà, Stefano. 1973. *Elaboratori elettronici e controllo sociale*. Bologna: Il mulino. http://127.0.0.1:8180/oseegenius/resource?uri=000001217322.

Swann Jr, William B. 2005. "The Self and Identity Negotiation." *Interaction Studies* 6 (1): 69–83.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY, USA: PublicAffairs.