ISSN 2281-5147

Opinio Juris inComparatione

Studies in Comparative and National Law

Vol. 1, n. 1/2022

Pacini Giuridica

CONTENTS

Articles

Section 1

Section 2

ISSN 2281-5147

CITIZENSHIP AND MEMBERSHIP: THEORY AND CHALLENGES IN TIMES OF GLOBAL CRISES. DECISION MAKING AND ALGORITHM. THE EUROPEAN UNION'S PROPOSAL

Fulvio Costantino*

Abstract

Human beings all over the world are today more "post-national" thanks to technology, which is able to create even more intense bridges and bonds between people far away from the world than those close to us, and therefore on the one hand often makes it difficult understanding or accepting which law is applicable to a specific case, on the other hand, suggests treating subjects who use the same tools in the same way, beyond their formal citizenship. With the digital citizenship notion, we mean a set of rights and duties of citizens defined within the Internet. The following appear to be involved: the need for inclusion, as forms of exclusion may arise from the refusal or the impossibility of using technologies; the need for skills, above all technical and legal, to deal with the digital context; the need for participation, so that digitization can fully deploy its social and civic benefits. On the other hand, however, digitization can even lead to the situation in which men are deprived of the human rights guaranteed by citizenship and therefore find themselves without any rights. All these aspects are intended to be discussed in this paper.

* Fulvio Costantino is Associate Professor of Administrative Law at the Department of Political Science, Communication and International Relations – University of Macerata. fulviocostantino@gmail.com

ISSN 2281-5147

Indice Contributo

Keywords

Digital citizenship – Rights – Technological inclusion – Digitalization – European Union

ISSN 2281-5147

1. The notion of cd. digital citizenship

Human beings all over the world are today more "post-national" thanks to technology, which is able to create even more intense bridges and bonds between people far away from the world than those close to us, and therefore on the one hand often makes it difficult understanding or accepting which law is applicable to a specific case, on the other hand, suggests treating subjects who use the same tools in the same way, beyond their formal citizenship[1].

With the digital citizenship notion, we mean a set of rights and duties of citizens defined within the Internet[2]. In this sense, it is defined as an extension of "traditional" citizenship, possible thanks to information and communication technologies (ICT)[3]. It would therefore be a new and further typology of citizenship, not an alternative or opposite to the classic one, whose content can be considered aimed at simplifying the relationship between citizens, businesses and public administration.

Institutional documents refer to digital citizenship: the Council of Europe[4] defines a digital citizen as "a person who masters the competences for democratic culture in order to be able to competently and positively engage with evolving digital technologies; participate actively, continuously and responsibly in social and civic activities; be involved in a process of lifelong learning (in formal, informal and non-

[1] An interesting case of digital citizenship concerns Estonia. Since 2014, Estonia offers an "electronic residency" program, thanks to which one can digitally sign documents, pay taxes online, open a bank account, start a business, services generally available to its citizens. Estonia has one of the largest stateless populations in Europe, due to naturalization laws passed after the fall of the Soviet Union which required members of ethnic groups from the Soviet Union to reapply for citizenship. Many have not applied for or obtained citizenship and are subject to many forms of discrimination. https://www.e-resident.gov.ee/. See Taavi Kotka, Carlos Ivan Vargas Alvares del Castillo, 'Kaspar Korjus, Estonian e-Residency: Benefits, Risk and Lessons Learned' in E. Francesconi (ed.), *Electronic Government and the Information Systems Perspective. EGOVIS 2016. Lecture Notes in Computer Science*, Springer, 2016, https://doi.org/10.1007/978-3-319-44159-7_1.

[2] Karen Mossberger, Caroline. J. Tolbert, Ramona S. McNeal, *Digital Citizenship: The Internet, Society, and Participation* (Cambridge US, 2007).

[3] https://epale.ec.europa.eu/is/node/109784.

[4] Recommendation CM/Rec (2019) 10 of the Committee of Ministers to member States on developing and promoting digital citizenship education.

ISSN 2281-5147

formal settings) and be committed to defending continuously human rights and dignity"[5]. According to the European Union[6] "Digital citizenship is a set of values, skills, attitudes, knowledge and critical understanding citizens need in the digital era. A digital citizen knows how to use technologies and is able to engage competently and positively with them".

From these documents emerges the ideal of a citizen who knows how to orient himself in the new digital context. There is no doubt that this scenario carries within it a strong egalitarian instance (for example, access to the Internet for all), and proposes to citizens new forms of economic initiative, work, professional training and cultural expression. In particular, with reference to relations with public authorities, it facilitates citizens' access to issues of general interest, greater interactivity with institutions and disintermediation, greater information symmetry with public authorities, greater pluralism and circulation of dissent.

The following appear to be involved: the need for inclusion, as forms of exclusion may arise from the refusal or the impossibility of using technologies[7]; the need for skills, above all technical and legal, to deal with the digital context; the need for participation, so that digitization can fully deploy its social and civic benefits.

On the other hand, however, digitization can even lead to the situation in which men are deprived of the human rights guaranteed by citizenship and therefore find themselves without any rights[8]. All these aspects are intended to be discussed in this paper.

[5] And "Digital citizenship" is the capacity to participate actively, continuously and responsibly in communities (local, national, global, online and offline) at all levels (political, economic, social, cultural and intercultural).

[6] Council conclusions on digital education in Europe's knowledge societies (2020/C 415/10), §10.

[7] See Gerard Doppelt, 'Equality and the Digital Divide' (2002) 24 *Hastings COMM. & ENT. L.J.* 601.

[8] See Hannah Arendt, *The origins of Totalitarianism* (first published 1951, The World publishing Company 1958), chapter 9, 267 and 287.

ISSN 2281-5147

2. Citizenship rights promoted by technologies

El Growing digitalization has an impact on the exercise of political, civil and social rights, on the legal situations recognized to citizens and businesses, in particular towards the public authorities[9]. Access to services provided by the administration on a platform can ensure a better result in terms of time and costs; digitization can have positive effects on education, health, social services, the conduct of economic activities; more legal guarantees can be recognized.

In this context, the notion of digital citizenship can be useful[10]. Among the main legal profiles involved, we can identify: among the rights, the right to digital identity[11], i.e. the availability of a unique digital identity assigned to citizens by administrations; the protection of personal data[12]; digital access and inclusion[13]; training for the acquisition of digital skills[14]; the information and use of public digital content[15]; citizen

[9] Caroline Fischer, Moritz Heuberger, Moreen Heine, *The impact of digitalization in the public sector: a systematic literature review*, 14 2021, 1-21, https://www.researchgate.net/publication/351216766_The_impact_of_digitalization_in_the_public_sector_a_systematic_literature_review.

[10] Arne Hintz, Lina Dencik, Karin Wahl-Jorgensen, *Digital citizenship in a datafied society* (Wiley, 2018); Giovanni Pascuzzi, *La cittadinanza digitale. Competenze, diritti e regole per vivere in rete* (Mulino, 2021).

[11] Clare Sullivan, 'Digital citizenship and the right to digital identity under international law' (2016) 32/3 *Computer Law & Security Review*, 474.

[12] Adam Thierer, 'The Pursuit of Privacy in a World Where Information Control Is Failing. Privacy, Security, and Human Dignity in the Digital Age (2013) 36/2 *Harvard Journal of Law & Public Policy*, 409.

[13] Clare Sullivan, 'Digital Citizenship and the Right to Identity in Australia', (2013) 41/3 *Federal Law Review*, 557.

[14] Viviane Devriesere, 'La Citoyennete Numerique' (2019) *Revista Universitara de Sociologie*, 82.

[15] Karen Mossberger, 'Towards digital citizenship: Addressing inequality in the information age' in Andrew Chadwick and Philip N. Howard (eds), *Routledge Handbook of Internet Politics* (Routledge, 2009), 173.

ISSN 2281-5147

participation in political decision-making[16]; the daily use of the benefits of digital technologies[17]. The responsibilities include respecting the rules of the web and sharing one's digital content[18].

The rights related to digital identity and digital domicile are necessary for the dialogue between citizens and public authorities. Digital identity is used to access services safely. The digital domicile allows you to receive communications, send requests or documents, make payments. The digitization of proceeding implies the right to digitally access services and to submit files through online portals through accessible technology.

These are instrumental rights with respect to underlying claims, such as starting an economic activity, enrolling in school services, booking medical examinations, etc., which however deserve protection. A further effect is uniformity, as conditions and requirements must be the same throughout the national territory[19].

---

[16] Jorge Francisco Aguirre Sala, '*Citizenship.com 2.0: A Link to Participative Democracy (The Evolution of Citizenship in a Project Instrumentalized by New Media)*', (2014) 11/4 *US-China Law Review*, 461.

[17] *Ibidem*.

[18] Clare Sullivan, 'Digital Citizenship and the Right to Identity in Australia*', cit.*

[19] In Italy there is a regulatory text of reference for digital rights, the Digital Administration Code (Legislative Decree 82/2005 - CAD) which entitles Section II of Chapter I the "Digital Citizenship Charter". It affirms the right to use technologies (art. 3), the right to digital identity and digital domicile (art. 3-bis), the right to make payments using computerized methods (art. 5), to communications between businesses and public administrations (art. 5-bis), simple and integrated online services (art. 7), computer literacy of citizens (art. 8), connectivity to the Internet network in offices and public places (art. 8-bis), to electronic democratic participation (art. 9). The Italian Constitutional Court (Sentence 251/2016) has framed digital rights in the category of essential levels of services (l.e.p.) concerning civil and social rights, to be guaranteed uniformly throughout the national territory. See R. Cavallo Perin and D. U. Galetta (eds), *Il diritto dell'amministrazione digitale* (Giappichelli 2021). In Spain, a Digital Rights Charter was launched, which provides for many rights for citizens and indications for the public authorities, even if it is a non-binding act. Tools have also been put into operation that try to make inclusion effective. For example, the Barcelona digital platform Decidim! aims to encourage citizen participation through the management of citizens' involvement activities in democratic processes in political institutions, businesses and associations. The same platform in Italy is used by the Department of Public Administration and the Department for Institutional Reforms to develop the «ParteciPa» platform, which manages consultation processes on certain issues of public interest and is taken into consideration by Italian movements and parties. The platform commits the user to sign a "social contract". Pablo Aragón et al., 'Deliberative Platform

ISSN 2281-5147

3. The centrality of data transparency

Digitization has its fuel, which is data[20]. Digital citizenship implies the right to transparency of that data as a prerequisite[21].

Data is a tool for producing knowledge and wealth. Just as the principle of transparency is an expression of the democratic principle, an instrument of guarantee of individual and collective freedoms, of civil, political and social rights, of good administration. It allows to implement the principles of equality, impartiality, good performance, integrity, responsibility, optimal use of public resources[22].

Design: The Case Study of the Online Discussions in Decidim Barcelona', Giovanni Luca Ciampaglia, Afra Mashhadi and Taha Yasseri (eds), (2017) 10540 *Social Informatics. SocInfo 2017. Lecture Notes in Computer Science* (Springer 2017). See also *Advancing civic participation in algorithmic decision-making*, which examines the impact it has already had and which institutions such as Citizens assemblies, citizens juries, participatory budgeting (https://datajusticelab.org/wp-content/uploads/2021/06/PublicSectorToolkit_english.pdf).

[20] The centrality of data is clear in the 2016 French law on the so-called République Numérique, which contains provisions for the modernization and digitization of public administration and to strengthen the protection of citizen-consumers in the digital space. It has established that public administrations must mutually make the data in their possession available to each other, in order to exercise the public functions assigned by law more easily and more quickly, streamlining and speeding up the administrative investigation. It is envisaged that the data may be the subject of an access request submitted by private individuals pursuant to the local transparency law (Code des relations between the public and the administration). The establishment of a new office, dependent on the Prime Minister, Commissioner for digital sovereignty, is envisaged (art. 29), with the aim of guaranteeing "the exercise, in cyberspace, of national sovereignty and of individual rights and freedoms and collective that the Republic protects. " It provides (art. 48) the right to "data portability" and the right to access the content of the user profile. It also provides (art. 63) a discipline of "digital successions", ie the right of the interested party, for the time following his death, to decide on the data entered in online platforms and services and the right for the heirs of the interested in accessing the same data. Philippe Mouron, 'La loi pour une République numérique', 2017 *Revue européenne des médias et du numérique*, 15. See Giovanni Comandè, 'The Fifth European Union Freedom', Hans Micklitz (ed.), *Constitutionalization of European Private Law*, XXII/2, (Oxford, 2014) https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780198712107.001.0001/acprof-9780198712107-chapter-3

[21] It is precisely from the aforementioned French law that not only the centrality of data is evident, but also the importance of data transparency.

[22] See art. 2, of the Italian d. lgs. 33/2013.

ISSN 2281-5147

Based on the principle of transparency, public authorities are required to make data, documents and procedures accessible. Accessibility and transparency equalize the relationship between citizens and administrations. The knowledge of times, costs, formalities, the provision of uniform forms, help citizens who deal with public authorities.

The data and documents to access services and services, or to obtain the necessary consents to start a business, should be available in an open format, unless there are reasons to justify a licensing or to protect privacy or particularly relevant interests. The data should be complete, provided in real time, remotely accessible and free of charge.

4. Citizenship rights put at risk by technologies: algorithms

After all, data are essential for governing, making decisions, intervening quickly and efficiently, as well as for communicating with citizens. To this end, the public authorities are making an increasingly wide use of computer algorithms, which are pre-set operations that probe, intertwine and process huge amounts of data (the so-called big data) and, through calculations, provide predictions, recommendations, decisions[23].

The speed of the computers and the lower incidence of mistakes compared to carrying out the same activities in analog mode has also led the public authorities to a massive use of algorithms. There are many uses of algorithms, but it is evident that public services are naturally characterized by equal requests, connected to repetitive activities without discretion and therefore are easily applicable to them.

Algorithms stand out for their undoubted effectiveness, and are able, if properly trained, to make decisions, or in any case to advise the decision makers. In this second case, the recommendations, based on predictions, indicate to the decision maker where to focus his attention (surveillance, investment, maintenance tasks). The

[23] With reference to the most recent forms of data analysis see Michael Veale and Irina Brass, 'Administration by Algorithm? Public Management Meets Public Sector Machine Learning', Karen Yeung and Martin Lodge (eds.), *Algorithmic Regulation* (OUP 2019).

ISSN 2281-5147

predictions thus also shape the decision that belongs entirely to human beings (checks on expenses, tax returns, travelers).

Algorithms are also successful because they have a semblance of neutrality[24] and objectivity[25]: due to the desubjectivization of computers, their work is perceived by decision makers and users as more objective than it is. Yet these are tools that are functional to the interests and ideologies of their clients. Neutrality can thus constitute an expedient to elude the problem of the decision maker's democratic accountability[26].

According to human parameters, even algorithms can be wrong, due to design errors, which poses a problem of responsibility. Rand Hindi (entrepreneur and data scientist) said: "Artificial intelligence makes fewer mistakes than humans, but it makes mistakes that humans would not have made" (referring to the fatal accident of a Tesla car that did not identify a truck in the middle of the road, which any driver would notice)[27].

More deceitful, however, is the structural error. Precisely because of the way they are constructed or operate, algorithms can incorporate prejudices or be a source of discrimination (the best known cases concern certain ethnic groups, women,

---

[24] Erika Giorgini, 'Algorithms and Law' (2019) *Italian Law Journal* 145.

[25] Paul Schwartz, 'Data Processing and Government Administration: The Failure of the American Legal Response to the Computer' (1992) 43 *Hastings L.J.* 1321, 1342 describing the deference of the individuals give to computer results.

[26] The role of those who have to make a decision and receive the recommendation from the algorithms is problematic, even and above all if they do not have adequate computer skills. The decision maker, in fact, even beyond the hypothesis of fully automated measures, may find himself in a position to formally take a decision substantially taken by artificial intelligence, without being able to understand, integrate or correct it.

With respect to this issue, the current legal framework does not provide a solution: art. 22 of the GDPR in fact prohibits the adoption of a fully automated act and refers to the final administrative decision: therefore, the level of attention on the direct use of algorithms in the adoption of decisions is high, not so much its use o in the investigation stage.

[27] *How Can Humans Keep the Upper Hand? The Ethical Matters Raised by Algorithms and Artificial Intelligence Report on the Public Debate Led by The French Data Protection Authority (Cnil) as Part of the Ethical Discussion Assignment Set by the Digital Republic Bill*, December 2017, 30.

ISSN 2281-5147

minorities) on a large scale[28]. Some "biases" underlying algorithms cannot be removed, also because they may be unintentional[29]. Visions of society resulting from stereotypes and prejudices can be perpetuated through decisions[30]. The programmer also affects how the algorithm works, and each algorithm is only one of the possible, which raises the problem of the relationship between scientist and public decision-maker[31].

Ultimately, human error, bias in data entry or programming or malfunctions produce discriminatory algorithms. Discriminatory effects occurred in particular in the processes applied to the dynamics of the labor market[32], to the credit sector[33], in criminal proceedings[34].

---

[28] Jon Kleinberg, Jens Ludwig, Sendhil Mullainathan and Cass R. Sunstein, 'Discrimination in the Age of Algorithms' (2018) 10 *Journal of Legal Analysis*, 1; Stephanie Bornstein, 'Antidiscriminatory Algorithms' (2018) 70/2 *Alabama Law Review*, 519.

[29] Mirko Bagaric, Dan Hunter and Nigel Stobbs, 'Erasing the Bias against Using Artificial Intelligence to Predict Future Criminality: Algorithms Are Color Blind and Never Tire' (2020) 88/4 *University of Cincinnati Law Review*, 1037. Joshua A. Kroll, Joanna Huey et al., 'Accountable Algorithms' (2017) 165/3 *University of Pennsylvania Law Review* 633.

[30] 'Antidiscriminatory' *cit.*, 571.

[31] Karni Chagal-Feferkorn, 'The Reasonable Algorithm', (2018) *University of Illinois Journal of Law, Technology & Policy* 111; Ernest Schaal, 'What to Say to a Computer Programmer' (1982) 28/2 *Practical Lawyer* 71; Karni Chagal-Feferkorn, 'How Can I Tell If My Algorithm Was Reasonable?' (2021) 27/2 *Michigan Technology Law Review* 213.

[32] Matthew U. Scherer, Allan G. King and Marko J. Mrkonich, 'Applying Old Rules to New Tools: Employment Discrimination Law in the Age of Algorithms' (2019) 71 *South Carolina Law Review*, 449.

[33] Sahiba Chopra, 'Current Regulatory Challenges in Consumer Credit Scoring Using Alternative Data-Driven Methodologies' (2021) 23/3 *Vanderbilt Journal of Entertainment & Technology Law* 625.

[34] Aleš Završnik, 'Algorithmic justice: Algorithms and big data in criminal justice settings' (2021) 18/5 *European Journal of Criminology* 623; Mirko Bagaric, Jennifer Svilar, Melissa Bull, Dan Hunter, and Nigel Stobbs, 'The Solution to the Pervasive Bias and Discrimination in the Criminal Justice: Transparent Artificial Intelligence' (2022) 59/1 *American Criminal Law Review* 95; Danielle Kehl, Priscilla Guo and Samuel Kessler, *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing Responsive Communities Initiative*, *Berkman Klein Center for Internet & Society, Harvard Law School*, 2017; Michael Brenner, Jeannie Suk Gersen, Michael Haley et al., 'Constitutional Dimensions of Predictive Algorithms in Criminal Justice' (2020) 55/1 *Harvard Civil Rights-Civil Liberties Law Review* 267; Spencer S. Hsu, '*Symposium - From the Crime Scene to the Courtroom: The Future of Forensic Science Reform'* (2018)

ISSN 2281-5147

It should be added that algorithms have an impact not only on citizens who are recipients of public decisions, but also on how citizens exercise the rights and freedoms that the legal systems recognize them.

In fact, algorithms designed to recommend information and products in line with the presumed individual preferences may mean that the preferences on user information and subsequent exposure to content over time constitute cages, the so-called bubbles[35]. Users are confined to their profiles. Citizens are less free to self-determine and to choose, because freedom is exercised in relation to what 'offered' by profiling. This affects the free construction of the personality of individuals, and also their social representation, because profiling can produce the creation or perpetuation of stereotypes, as well as social segregation.

Finally, the algorithmic decisions that shape the flows of information can induce certain behaviors, modify the preferences and values of users, even lead them to radicalization[36]: in other words, they can manipulate the way of thinking and choices of citizens, who are also voters[37].

On the one hand, the algorithms involved in these problems are not mainly those used by public authorities, but those used by companies, primarily big techs (Amazon, Google, Facebook, just to name a few)[38].

34/4 *Georgia State University Law Review*; Carolyn McKay, 'Predicting Risk in Criminal Procedure: Actuarial Tools, Algorithms, AI and Judicial Decision-Making' (2020) 32/1 *Current Issues in Criminal Justice* 22.

[35] Kerri A. Thompson, 'Commercial Clicks: Advertising Algorithms as Commercial Speech' (2019) 21/4 *Vanderbilt Journal of Entertainment & Technology Law* 1019.

[36] Shaun B. Spencer, 'The Problem of Online Manipulation' (2020) 2020/3 *University of Illinois Law Review* 959; Allyson Haynes Stuart, 'Social Media, Manipulation, and Violence' (2019) 15/2 *South Carolina Journal of International Law and Business* 100; Gina-Gail S. Fletcher, 'Deterring Algorithmic Manipulation' (2021) 74/2 *Vanderbilt Law Review* 259.

[37] Jaeho Cho, Saifuddin Ahmed et al., 'Do Search Algorithms Endanger Democracy? An Experimental Investigation of Algorithm Effects on Political Polarization' (2020) 64/2 *Journal of Broadcasting and Electronic Media* 150.

[38] Swati Srivastava, 'Algorithmic Governance and the International Politics of Big Tech' (2021) *Perspectives on Politics* 1 doi:10.1017/S1537592721003145

ISSN 2281-5147

But profiling is even more problematic if used in the public sector, to prevent tax, social security and social welfare fraud, and above all for the so-called 'predictive police'. It is also used in the judicial sector: the Compas software was adopted in the State of Wisconsin to calculate the risk of recidivism or to define the amounts of bail to be paid[39].

More generally, the expression of *Jus algoritmi*[40] was used to describe a new form of citizenship, whose primary mode of operation is control through identification and categorization and which takes place through the increasing use of software to express judgments. on the status of citizenship of an individual, and therefore to decide what rights he has and what operations on his person are permitted.

The so-called social credit score also fits into this framework[41]: public authorities evaluate the social reliability of citizens on the basis of certain elements, including personality characteristics, social behavior, network of relationships or other elements, by means of a social score. Access to financial contributions or services is correlated to the score. For the Chinese State Council this is a fundamental component of the socialist market economy and social 'governance', which helps to create a "culture of sincerity", encourages "trust" and allows for the construction of a "harmonious socialist society"[42]. These are systems that have an impact on the construction of personality on behavior, with limitations of freedom and forms of exclusion.

---

[39] Hannah Bloch-Wehba, 'Access to Algorithms' (2020) 88/4 *Fordham Law Review* 1265; Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), 18 State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

[40] John Cheney-Lippold, 'Jus Algoritmi: How the National Security Agency Remade Citizenship' (2016) *International Journal of Communication* 10, 22.

[41] Lizzy Rettinger, 'The Human Rights Implications of China's Social Credit System' (2021) 21/1 *Journal of High Technology Law* 1; Bi Honghai, 'Old Regulatory Wine in a New Bottle of Technology - A Critical Analysis of China's Social Credit System' (2021) 16/2 *University of Pennsylvania Asian Law Review*, 282; Nizan Geslevich Packin and Yafit Lev-Aretz, 'On Social Credit and the Right to Be Unnetworked, Survey: The Evolving Landscape of Business and Media' (2016) *Columbia Business Law Review* 339; Daithì Mac Sithigh and Mathias Siems, 'The Chinese Social Credit System: A Model for Other Countries' (2019) 82/6 *Modern Law Review* 1034.

[42] https://www.eurozine.com/social-control-4-0-chinas-social-credit-systems/

ISSN 2281-5147

In this scenario, it is difficult to check and review the algorithms, first of all due to their complexity, as well as the complexity of the research and calculation activities they carry out[43]. Secondly, the debate on oversight has not yet reached shared solutions[44]. Thirdly, those who develop algorithms do not want to make them known[45]. And so also the principle of access to data, mentioned above, is not yet recognized, or at least not fully, and in some ways it is not even possible to guarantee it.

The term "algorithm dictatorship" was used to describe this situation[46]. The 'despotic domination' of algorithms, in fact, is an expression of the 'despotic domination' of public or private powers.

So much so that we can also ask whether it is appropriate to rely on algorithms, and if this does not involve a regression from the point of view of the ideals of justice. In this sense, the French National Bar Council (CNB) observes that "we must avoid the obsession with efficiency and predictability that motivates the use of the algorithm that leads us to design categories and rules no longer in consideration of our ideal of justice, but so that they can be more easily "codified"[47].

---

[43] Michael W. Monterossi, 'Algorithmic Decisions and Transparency: Designing Remedies in View of the Principle of Accountability' (2019) 5/2 *Hard Cases Italian Law Journal* 711.

[44] See *infra* about the European proposal.

[45] Mariateresa Maggiolino, 'EU Trade Secrets Law and Algorithmic Transparency' (2019) *Bocconi Legal Studies Research* available at SSRN: http://dx.doi.org/10.2139/ssrn.3363178; Michelle Azuaje Pirela and Daniel Finol Gonzalez, 'Algorithmic Transparency and Intellectual Property: Tensions and Solutions' (2020) 30 *Revista la Propiedad Inmaterial* 111.

[46]https://www.munichrefoundation.org/en/Climate_change_and_education/Dialogue_forums/Dialogue_forums_2018/23_January_2018_Globalisation_and_digitalisation_The_world_in_the_fast_lane.html

[47] *How can*, *cit.*, 30.

ISSN 2281-5147

5. Legal discipline and algorithms. Transparency

From a legal point of view, the algorithm appears similar to a regulation, drawn up by man and applied by the machine.

The Italian Consiglio di Stato considered the algorithm, that is the software, as a digital administrative decision[48]. It also established some requirements and limits on the use of algorithms: as they have legal value, even if in mathematical form, they must comply with the general principles of administrative activity, including publicity, transparency, reasonableness, proportionality. Administrative discretion can be exercised by the administration at the time of the algorithm development; the algorithm, on the other hand, must not leave room for discretion, but must provide a solution for all possible, even improbable cases, and must respond to the principle of reasonableness. The administration must play an *ex ante* role of mediation and settlement of interests, also by means of testing and improving the algorithm. Recourse to the judge must be envisaged for the evaluation of the correctness of the automated process and for the carrying out of evaluations and assessments made automatically.

In the US case Loomis vs Wisconsin, known as 'Compas', concerning the use of algorithms by the US criminal justice administration to assess the social dangerousness of the accused, it was argued that the use of technologies of this type cannot be "determinative" with respect to the decision, but it can be a "relevant factor", to be weighed. For this reason, the aim is to preserve a space for human decision-making, during control[49].

Two problematic issues of algorithms are those of accountability and transparency.

---

[48] https://www.giustiziaamministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=cds&nrg=201902936&nomeFile=201908472_11.html&subDir=Provvedimenti. Barbara Marchetti, 'La garanzia dello "human in the loop" alla prova della decisione amministrativa algoritmica' (2021) *BioLaw Journal - Rivista di BioDiritto* 367; Diana Urania Galetta 'Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia' (2020) *Rivista Italiana di Diritto Pubblico Comunitario* 501; Enrico Carloni, 'I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo' (2020) *Diritto amministrativo* 273.

[49] Anne L. Washington, 'How to Argue with an Algorithm: Lessons from the COMPAS-ProPublica Debate' (2018) 17/1 *Colorado Technology Law Journal* 131.

ISSN 2281-5147

The French Conseil constitutionel, in the Décision n. 2018-765 DC, 12 June 2018 found that the so-called algorithms "Auto-apprenant", cannot in any case be used as an exclusive basis for an individual administrative decision, if they are not subject to control or validation[50]. The use of an algorithm in an administrative decision is allowed under three conditions: 1) the decision must expressly mention that it was adopted on the basis of an algorithm, in accordance with the provisions of the Code des relations entre le public et l'administration; 2) the main characteristics of this algorithm must, if requested, be communicated; 3) the decision cannot be made using an algorithm whose operating principles cannot be communicated without violating one of the secrets or protected interests identified by the Code des relations entre le public et l'administration. The decision must always be recourse.

The Italian Consiglio di Stato allowed the use of computer algorithms to take public decisions as long as the criteria applied are fully known. However, the decision must be attributable to the authority, which must be able to verify the logic and legitimacy of the choice entrusted to the algorithm. The identification of a subject is necessary to impute the choice and responsibility for damages; therefore the verification of the logic and correctness of the results must be guaranteed. The algorithm must therefore be known by the administration and by private individuals, as it is a rule expressed in a language different from the legal one: the authors, the processing procedure, the decision mechanism (the priorities assigned in the evaluation and the data selected as relevant) must be knowable, to allow verification. The technical formula must be accompanied by explanations that make it understandable. Confidentiality is not allowed[51].

The European Regulation 2016/679 (GDPR), to reduce the risk of discriminatory treatments for the individual, establishes in artt. 13 and 14 that in the information addressed to the interested party, notice is given of the possible execution of an automated decision-making process, both that the data collection is carried out by the interested party and by third parties. In the case of a fully automated process, the owner must provide " meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data

[50] Matteo Pressi, 'The Use of Algorithms within Administrative Procedures: National Experiences Compared through the Lens of European Law' (2021) 14/2 *Review of European Administrative Law* 69.

[51]https://www.giustiziaamministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=cds&nrg=201902936&nomeFile=201908472_11.html&subDir=Provvedimenti

ISSN 2281-5147

subject"[52]. Art. 15 provides for the principle of knowability and comprehensibility: according to the first, it is possible to receive information relating to the existence of any automated decision-making processes that concern him (paragraph 1, letter h) and, for the second, the possibility to obtain " meaningful information about the logic involved ".

It remains uncertain whether, despite the rules and judicial rulings, the demand for transparency will be met. Decisions can be made taking into account such a large number of data and parameters that it is practically impossible to reconstruct the logical process, and therefore the motivation, *a posteriori*: the more powerful the algorithm, the more opaque it becomes (as it calculates more variables and processes more data). The phenomenon appears even more pronounced in the areas of security and public order, in which secrecy and lack of motivation in decisions occur more frequently. Best algorithms are inherently dynamic, can change quickly, which makes them even more difficult to understand. There is a crisis of transparency and comprehensibility. The paradigm is even reversed: human beings become knowable (reified by algorithms) and machines become opaque[53].

The recipient of the recommendation does not know how the program arrived at that conclusion in cases where the algorithms recognize occurrences by learning themselves to weight the different components of the data entered. In these cases, the creators of the algorithms know the data in general terms, but in more advanced applications, they may not know the weight that has been attributed to particular inputs. It is difficult to think that in the future the public authorities will not want to use these more advanced algorithms.

6. Legal discipline and algorithms. Consent

Art. 22, paragraph 1, of the GDPR, according to the *Human in the loop* principle, provides that, if an algorithmic decision produces legal effects or significantly affects the person, the interested party has the right to have this not based solely on an

[52] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[53] See Hannah Bloch-Wehba, 'Access to Algorithms' (2020) 88 *Fordham Law Review* 1265; a possible solution is proposed by W. Nicholson II Price and Arti K. Rai, 'Clearing Opacity through Machine Learning' (2021) *Iowa Law Review* 775.

ISSN 2281-5147

automated process. The article contemplates in paragraph 2 some exceptions: cases in which the decision: a) is necessary for a contract; b) is authorized by Union or Member State law; c) is thbased on the subject's explicit consent.

If however, for art. 22 of the GDPR, exclusively automated processing and profiling activities can find a legitimate basis in the explicit consent of the interested party, the problem is to verify the same freedom of consent, when it is a necessary condition for obtaining a service.

The problem concerns the subject matter, since the relationship of citizenship cannot be reduced to the relationship between public power and the individual. It is no longer easy to use the distinction between public and private with reference to many private entities, which provide virtual spaces and services through which people meet, debate, inform themselves, form opinions, share data, documents, images and that they are not, due to the number of participants and the conditions of the service, replicated or replicable by public entities. In this case we are dealing with private powers[54].

According to art. 7, paragraph 4, of the GDPR, " When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. ".

Consent is often stolen, without informing the user about the collection and use of his data for remunerative purposes[55]: there is a risk to social life, in the event that the user wants to exclude some of the data offered by the use[56]. The conditioning is greater the more the service offered by the website operator is not provided by other operators and cannot be waived for the interested party. It is different when it comes to fungible goods or services, whereby the user can easily access similar services and

[54] *Ex multis*, Josh Simons and Dipayan Ghosh, 'Utilities for Democracy: Why and How the Algorithmic Infrastructure of Facebook and Google Must Be Regulated', (2020) https://www.brookings.edu/wp-content/uploads/2020/08/Simons-Ghosh_Utilities-for-Democracy_PDF.pdf

[55] CJEU Case C-645/19, Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit.

[56] Philip N. Yannella, 'The Differing US and EU Regulatory Responses to Rise in Algorithmic Profiling' (2018) 33/4 *Communications Lawyer* 1.

ISSN 2281-5147

therefore renounce without burdensome sacrifice[57]. On the other hand, social networks that allow you to stay in touch with people are not as fungible.

7. Legal discipline and algorithms. Profiling

With regard to profiling, art. 4, point 4, of the GDPR establishes that profiling is " any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"[58]. However, this is a discipline that has proved to be ineffective with respect to the cited risks posed by the algorithms.

[57] Lorena Barrenechea Salazar, 'Privacy, the Fallacy of Consent and the Need to Regulate Social Media Platforms' (2020) *Intergovernmental Organisations In-house Counsel Journal* 39.

[58] See the Recital n. 71 of the GDPR: "In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions" and recital 24 of the GDPR "The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes".

ISSN 2281-5147

8. The EU proposal for a regulation on AI

The European proposal for a regulation on AI intervenes in this scenario, and aims to reconcile the protection of fundamental rights and EU values with technological innovation, classifying AI systems according to the risk of use for health and security or for the fundamental rights of individuals[59]. A governance system is introduced at central and national level and measures are envisaged to support innovation (such as "regulatory sandboxes"). This defines a uniform legal framework for all Member States.

The proposal inherits many elements from the GDPR, including risk assessment and management, accountability and self-assessment mechanisms, sanctioning regimes and governance systems.

The proposal provides for a ban on placing on the market (or in service or using) AI systems that use subliminal techniques in order to significantly distort behaviour or that, for the same purposes, exploit the vulnerability of specific groups of people, for their age or for physical or mental disability (art. 5).

'Social scoring' systems, which lead to prejudicial or unfavorable treatment of certain individuals or entire groups of individuals in social contexts that have no relationship with those in which the data were originally generated or collected, are prohibited[60]. Real-time remote biometric identification systems are prohibited in spaces accessible to the public (for example facial recognition tools to control passers-by in public spaces), except in cases exceptionally authorized by law relating to crime prevention and contrast activities, in any case subject to specific guarantees[61].

---

[59] Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM(2021) 206 final. See also White Paper on Artificial Intelligence - A European Approach to Excellence and Trust COM/2020/65 final; Ethics Guidelines for Trustworthy AI High-Level Expert Group on Artificial Intelligence; Proposal for a Regulation of the European Parliament and of the Council on machinery products, COM(2021) 202 final.

[60] Recital 17.

[61] Art. 5. The use must: take into account the situation (severity, probability and extent of the damage), the consequences for the rights and freedoms of the persons concerned; be subject to temporal, geographical and personal limitations; be subject to prior authorization issued by a judicial authority or an independent administrative authority of the Member State, issued upon reasoned request and

ISSN 2281-5147

Other systems are classified as high risk but allowed as long as they comply with certain requirements before they are placed on the market or put into service (such as the use of high quality data sets, adequate documentation, adequate information to the user, adequate human surveillance and high standards in terms of robustness, security, cybersecurity and accuracy) and are subject to an *ex ante* conformity assessment (title III). These include critical infrastructures, like: education or vocational training (which can affect access to higher levels of education and professional life); labor (e.g. hiring procedures); essential public and private services (e.g. credit systems); transport (which could endanger life and health); the safety components of the products (e.g. robotic surgery); management of migration, asylum and border control (e.g. verification of the authenticity of travel documents); biometric identification and categorization of people; law enforcement activities that can interfere with people's fundamental rights; administration of justice and democratic processes (annex III). The list that can be extended by the Commission (art. 7).

There is an obligation to set up a risk management system for these technologies (art. 9). Data and data governance requirements are established (art. 10): training, validation and testing data must, inter alia, be relevant, representative, error-free and complete, have the appropriate statistical properties with respect to the recipients, they must take into account the geographical, behavioral or functional context in which the system is intended to be used. The drafting of the technical documentation of a high-risk AI system is required before the placing on the market or commissioning of this system (art. 11), the automatic recording of events ("log") during its operation (art. 12), conformity assessments for the most appropriate risk management measures (art. 19), the consistency of functioning with the intended purpose and compliance with the regulation. AI systems must be registered in an EU database, a declaration of conformity must be signed, and the AI system should bear the CE marking (art.19).

The suppliers of high-risk AI systems who believe that their system is not compliant must immediately take the necessary corrective measures, inform the distributors (art. 21), the competent national authorities of the States, the body that issued a certificate (art. 22).

---

in accordance with national law, if the authority has verified, on the basis of clear and objective evidence, that the use is necessary and proportionate; in a situation of justified urgency, it is possible to request authorization during or after use.

ISSN 2281-5147

Each Member State designates or establishes a notifying authority (art. 30 and 59), which supervises the market, provides guidance and advice, and supervises notified bodies, which carry out conformity assessment for high-risk systems. Depending on the system, the supplier follows the conformity assessment procedure based on internal control or with the involvement of a notified body. Biometric identification and categorization systems of natural persons are subject to a third party conformity assessment, except in cases where the supplier has used harmonized standards or - if applicable - common specifications, which would be part of internal control, including whether the point is the subject of debate.

For AI systems considered low risk, minimum transparency requirements are imposed (art. 52), so that individuals are informed that they are interacting with an AI system, if this is not evident: chatbots, recognition systems emotions or "deep fakes" (AI systems that generate or manipulate audio or video content that may appear authentic).

A European Committee for Artificial Intelligence is established, with the task of supporting cooperation between national supervisory authorities and the Commission, providing advice and expertise to the Commission and enabling the sharing of best practices (artt. 56-58) .

An EU database for high-risk AI systems that may affect fundamental rights is envisaged, managed by the Commission and fed with data made available by AI system providers before placing them on the market or in service (art. 60); suppliers must report any serious incident or malfunction that may affect these rights to the supervisory authorities of the Member States where such incidents or violations have occurred, no later than 15 days after becoming aware of them. National authorities have the power to investigate and if they believe that, although compliant with the regulation, the AI system presents a risk, they ask the operator to take all appropriate measures, including withdrawal or recall from the market. For the most serious violations, fines of up to 30 million euros are envisaged or, if a company is responsible, up to 6 percent of the total annual worldwide turnover of the previous year, if higher.

There are many points under discussion. Beyond the need for more precise definitions and delimitations (on AI systems, on subliminal techniques, on the exploitation of vulnerabilities), there is no precise definition of high risk, which is an open standard and therefore must be interpreted.

The Economic and Social Committee has asked that the ban on social scoring extends to private organizations and semi-public authorities; a ban on the use of AI for

ISSN 2281-5147

automated biometric recognition even in spaces accessible to individuals; a mandatory third-party compliance assessments for all high-risk AI; appeal procedures for damage cases; the human prerogative for certain decisions.

9. Conclusions. Transparency, participation, collaboration

It was highlighted how being a citizen in a digital context provides unprecedented opportunities and risks. The principles that must govern the use of technology in the relationship of public authorities (and private individuals with citizens) are known, and are familiar to scholars of public law: legality, participation, transparency, proportionality, access to justice. And equally well-known tools are needed: regulation, authorization, supervision, sanctions. Much, however, needs to be interpreted in a new way.

Only a few examples will be given. There is a lot of emphasis on the principle of transparency, but the construction of the algorithms is the most important moment. It concerns above all the relationship between public interests: a reflection on the role of the same must be carried out in order to understand if, when, how and at what price they can be framed in predefined schemes. The programming of a computer requires, even when sensitive interests are involved, to carry out an abstract evaluation and therefore a weighting of the interests involved *ex ante*. This poses a crucial problem of the reliability of the algorithms: if they are not well calibrated, prejudices can be produced to the legal situations of the recipients of the decisions, and the algorithms will be able to replicate any errors for a potentially infinite number of times, until they (and provided that) are corrected. It therefore becomes necessary, first of all, to decide when to resort to them, in what ways and to assess which risks of prejudice the decision-maker is willing to accept, and such decisions must be documented[62].

The principle of participation can play an important role: a procedure similar to the one that characterizes rulemaking in the US system, characterized by transparency and participation, would be useful for the adoption of algorithms. Inclusive

[62] Ben Green, 'The Flaws of Policies Requiring Human Oversight of Government Algorithms' (2021) 45 *Computer Law & Security Review* https://ssrn.com/abstract=3921216 or http://dx.doi.org/10.2139/ssrn.3921216

ISSN 2281-5147

mechanisms of collective decision-making, with the involvement of stakeholders and civil society, can improve the correctness and validity of the models. The intervention of groups, organizations, research centers and universities makes it possible to reduce the information asymmetry. The examination and review by external and independent researchers, notice and comment procedures that subject the algorithms to public scrutiny may be useful.

Cases such as such as the one relating to the final marks of UK students[63], and the one relating the social benefits in the Netherlands[64] are examples of poorly designed, poorly constructed algorithms, not discussed with interested parties, not shared.

With regard to the principle of transparency: it is possible to predict the behavior of computers in the event that they operate on the basis of pre-programmed logical rules and known data sets. But on many aspects, the Regulation also appears simplistic: in the case of algorithms that adapt and develop new solutions to emerging and dynamic situations, the impossibility of monitoring every step of the machine must be accepted, and in exchange it must be requested that any action be carried out within the limits of the regulatory framework[65].

Technological innovation requires a rethinking of the role and tasks of the public decision maker, as well as adequate selection and training. The ability to communicate

---

[63] Sam Shead, 'How a computer algorithm caused a grading crisis in British schools' (2021)

https://www.cnbc.com/2020/08/21/computer-algorithm-caused-a-grading-crisis-in-british-schools.html

[64] Gabriel Geiger, 'How a Discriminatory Algorithm Wrongly Accused Thousands of Families of Fraud

Dutch tax authorities used algorithms to automate an austere and punitive war on low-level fraud' (2021)

https://www.vice.com/en/article/jgq35d/how-a-discriminatory-algorithm-wrongly-accused-thousands-of-families-of-fraud

[65] However, it has been noted that the decisions of computers are more transparent than those of humans. We have not written the code of human learning and we have very little control over the data entered in humans for their learning. Also, when it comes to understanding, we must take into account that many technologies (airplanes, drugs, medical interventions), although we depend on them, we do not understand how they work. Intellegibility must be such for experts, not necessarily for everyone, not even for the addressees of a decision or for public decision-makers.

ISSN 2281-5147

with AI suppliers, often external to the administration, must be developed so that the tools are built and adapted according to a logic that respects rules, principles and objectives[66]. Administrations, particularly local ones, do not have the skills and means to regulate and supervise the development and implementation of these tools[67]. Up to now, no registers relating to algorithmic procedures or transparency measures have been imposed, the industrial secrecy exception has been accepted for not publishing the source code[68], predictive software has been used secretly.

[66] See William S. Isaac, 'Hope, Hype, and Fear: The Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice' (2018) *Ohio St. J. Crim. L.* 543.

[67] Robert Brauneis and Ellen P. Goodman 'Algorithmic Transparency of the Smart City' (2018) *Yale J.L. & Tech.* 103.

[68] *Ibidem*.

ISSN 2281-5147