



PARTICIPATORY RIGHTS IN THE REGULATION OF TRANSNATIONAL PHENOMENA: BIG DATA, TRADE AND SURVEILLANCE*

di Maria Francesca De Tullio **

TABLE OF CONTENTS: 1. Introduction – 2. The International Trade Law Through the Lenses of Big Data
Players' role – 3. The Persisting Relevance of Nations and Territories in Discriminatory Counter-
terrorism Surveillance – 4. Conclusions: Towards and Inclusive (Digital) Citizenship

1. Introduction

This paper, from the viewpoint of the European Union law, observes how private actors are involved in public decisions, concerning a transnational phenomenon: the circulation of big data. The core question is how much, and in which ways, non-nationals can participate in the elaboration and implementation of the relevant rules. The research investigates if there is a linear tendency towards the involvement of all foreigners in decision-making; in case of negative answer, it highlights the reasons – and especially the possible social reasons – underlying the choice of inclusion-exclusion in the enjoyment of political rights.

Traditionally, citizenship is supposed to be the cleavage along which political rights are granted or denied. This is due to the traditional assumption of coincidence between a State territory and a political community. Hence, citizenship is understood as a “space of equals”; composed of people who share a unitary interest and set of values and thus hold the same duties of obedience and participatory rights.¹ Nowadays, this construction is being

*Contributo sottoposto a *double blind peer review*.

** Dottoressa di ricerca in “Diritti umani. Teoria, storia, prassi” presso l’Università degli Studi di Napoli Federico II.

¹ The normal assumption is that citizens are the ones who are mainly interested in the destiny of the Country and, therefore, hold voting rights: Adriana Ciancio, ‘I diritti politici tra cittadinanza e residenza’ (2002) 1 Quaderni costituzionali, 54-55. Even if sometimes there are some breakthroughs towards the recognition of the right to vote for foreigners, its effectivity largely depends upon the immigration laws: Lara Trucco, ‘Il permesso di soggiorno nel quadro normativo e giurisprudenziale attuale’, in Pasquale Costanzo, Silvana Mordeglia and Lara Trucco (eds.), *Immigrazione e diritti umani nel quadro legislativo attuale* (Giuffrè 2008), 43.

rethought in light of the contradictory tensions of globalization, following the increase of migratory flows and transnational movements of capitals, commodities and people. Namely, there is a growing involvement of international private actors in decision-making. «The difficulties of political mediation of social conflict have suggested to recur to mechanisms based on civil society's self-regulation, also through appropriate public institutions, able to be (rather than a place of authoritative decision) the place of that self-regulation (it is the case of independent authorities)².

Moreover, different stakeholders are involved through *sui generis* participatory processes, that have generated a flexible public-private cooperation, with ongoing *ad hoc* adjustments³. Private actors intervene upon invitation of the public sector, after selected groups have been identified on the basis of the decisions to be taken.⁴ Sometimes, they are also involved as experts⁵: «a crucial government decision is made neither by a government official nor even by a specific nongovernmental person or organization, but rather by the collective practices of a profession—that is a group of persons defined by their possession of a particular body of knowledge»⁶. In the field of international agreements, even judicial review is entrusted, sometimes, to public-private arbitration bodies, using informal, if not secret, procedures.⁷ So, clearly participation is understood as , which rests upon citizens' spontaneous engagement.

As to modalities, doctrine has highlighted a dominance of market rationality in rule-making. This parameter has become the principal tool of evaluation and interpretation:⁸

² Massimo Luciani, 'Il paradigma della rappresentanza di fronte alla crisi del rappresentato', in Nicolò Zanon and Francesca Biondi (eds.), *Perversi e vicende attuali della rappresentanza e della responsabilità politica* (Giuffrè 2001), 113. Cfr. Giovanna De Minico, *Regole. Comando e consenso* (Giappichelli, 2005), 10-54.

³ Helmut Willke, 'Societal Guidance through Law?', in Gunther Teubner and Alberto Febbrajo (eds.), *State, Law and Economy as Autopoietic Systems* (Giuffrè 2002), 382-383; Maria Rosaria Ferrarese, 'La governance e la democrazia postmoderna', in Alessandro Pizzorno (ed.), *La democrazia di fronte allo stato : una discussione sulle difficoltà della politica moderna* (Feltrinelli, 2010), 63, 72; Valeria Giordano and Antonio Tucci, *Razionalità del diritto e poteri emergenti* (Giappichelli, 2013), 89; J. Chevallier, 'La gouvernance, un nouveau paradigme étatique?' (2003) 1, 105-106 *Revue française d'administration publique*, 216.

⁴ EU MP Molly Scott Cato, allowed to see the procedures of TTIP partially, and in a room with limited access, noticed that: «92% of those involved in the consultations have been corporate lobbyists. Of the 560 lobby encounters that the commission had, 520 were with business lobbyists and only 26 (4.6%) were with public interest groups. This means that, for every encounter with a trade union or consumer group, there were 20 with companies and industry federations»: Molly Scott Cato, 'I've seen the secrets of TTIP, and it is built for corporations not citizens' (*TheGuardian.com*, 6 February 2015) <www.theguardian.com/commentisfree/2015/feb/04/secrets-ttip-corporations-not-citizens-transatlantic-trade-deal>.

⁵ Maria Rosaria Ferrarese, 'La governance e la democrazia postmoderna', in Alessandro Pizzorno (ed.), *La democrazia di fronte allo stato : una discussione sulle difficoltà della politica moderna* (Feltrinelli, 2010), 68.

⁶ Martin Shapiro, 'Administrative Law Unbounded: Reflections on Government and Governance' (2001) 8 *Indiana Journal of Global Legal Studies*, 370.

⁷ Probably, the most relevant examples are related to ISDS (Investor-State Dispute Settlement): Alessandra Algostino, 'ISDS (Investor-State Dispute Settlement), il cuore di tenebra della global economic governance, e il costituzionalismo' (2016) 1 *Costituzionalismo.it*, 135-174.

⁸ Gino Scaccia, 'Il territorio fra sovranità statale e globalizzazione dello spazio economico' (2017) 3 *RivistaAic.it*, 15-16; Roberto Bin, 'Contro la governance: la partecipazione tra fatto e diritto', Speech at the congress *Il federalismo come metodo di governo. Le regole della democrazia deliberativa*, Trento, November 25-26, 2010, <www.robertobin.it>, 4; Thomas

each State is influenced by an «economic constituency», prevailing over the political one, who exerts pressure on institutions, through the threat of withdrawing from investments.⁹ Hence, beyond national boundaries, what appears to matter most in national States is to «create the conditions and formal, but also material, prerequisites [...] for the continuation of production and accumulation, as well as for their preservation, notwithstanding the phenomena of material, temporal and social instability that are intrinsic to the anarchical socialisation of capitalist processes»¹⁰.

In sum, the transnational scenario highlights a «disarticulation: on the one hand, a society without State, the *business community*, ruled by a new *lex mercatoria*, which consolidates its planetary dimension, by concentrating in itself normative function and, with international arbitration chambers, also judiciary functions; on the other hand, the multitude of national society, organised as a State, holding the internal interests that are not represented in the *societas mercatoria*, but progressively deprived of normative and judicial function».¹¹

Internet is an emblematic case for such issue, because compels each national system to relate to subjects and jurisdictions outside its boundaries: the World Wide Web is a global network hosting communication and trade among people, and organizations, outside the national limits. Hence, the growth of digitalization leads the States to allow foreign actors to participate in decision-making processes, or to seek extraterritorial implementation of their rules. Mostly, these ones are businesses, that claim decisional powers because of their market share.¹²

Not hazardously, different models of Internet governance have been proposed,¹³ outside of the traditional patterns of State authority. The nature of this work does not allow to give full account of this debate; though, a synthesis is possible, in order to explain the scope of the discussion. Some proposals aim at leaving digital behaviours under complete

G. Weiss, 'Governance, good governance and global governance: conceptual and actual challenges' (2000) 5, 21 *Third World Quarterly*, 796 ss. With particular reference to rating agencies: Adriano Cozzolino, 'Rating Agencies, Symbolic Capital and the Evaluation of Nation-States. A Preliminary Exploration' (2019) 8.4 *Cartografie sociali. Rivista di sociologia e scienze umane*, 142 ss.

⁹ The expression is in Gianni Ferrara, 'La sovranità popolare e le sue forme' (2006) 1 *Costituzionalismo.it*, 270-271. Cfr. Id., L'indirizzo politico dalla nazionalità all'apolidia, Speech at the congress *Esposito, Crisafulli, Paladin. Tre costituzionalisti nella cattedra padovana*, June 19-20-21, 2003, Padua, in *archivio.rivistaic.it*, 13-15.

¹⁰ Gianni Ferrara, 'Democrazia e stato nel capitalismo maturo. Sistemi elettorali e di governo' (1979) 4-5 *Democrazia e diritto*, 518-533 (quotation is at p. 518). Indeed, scholars have noticed that capitalism is not based on *laissez faire*, but needs a legal order, instrumental to the economic system: Peter Nahamowitz, 'Difficulties with Economic Law : Definitional and Material Problems of an Emerging Legal Discipline', in Gunther Teubner and Alberto Febbrajo (eds.), *State, Law and Economy as Autopoietic Systems* (Giuffrè 2002) 549.

¹¹ Francesco Galgano, *La globalizzazione nello specchio del diritto* (Il Mulino 2009), 73.

¹² Eric Brousseau, Jean-Michel Glachant, 'Regulating networks in the "new economy": organizing competition to share information and knowledge', in Eric Brousseau, Meryem Marzouki and Cécile Méadel (eds.), *Governance, Regulation and Powers on the Internet* (Cambridge University Press 2012), 82-92.

¹³ Lawrence B Solum, 'Models of Internet governance', in Lee A. Bygrave and Jon Bing (eds.), *Internet Governance. Infrastructure and Institutions* (Oxford University Press 2009), 55; Eric Brousseau, Meryem Marzouki and Cécile Méadel, 'Governance, networks and digital technologies: societal, political and organizational innovations', in Id (eds.), *Governance, Regulation and Powers on the Internet* (Cambridge University Press 2012), 3.

self-regulation, of users and operators¹⁴. Secondly, ‘westfalian models’ have been considered, implying inter-governmental agreements. Other paradigms rely on hybrid public-private models on supranational scale, as transnational quasi-private cooperatives or international organisations. Finally, another position is to consider Internet governance as a technical matter, to be addressed by experts from the governmental or corporate sectors.

As in many other fields, these models are intertwined, and create new forms of regulation, characterised by the fact of being produced with a significant influence of the private sector upon the public one, and sometimes an even position between the two. Though, such horizontality is not an absence of hierarchies: here, as in other fields, participatory rights are not distributed in an equal way, but substantially attributed to the ‘over the top’ players, who control the highest market share online.

For the sake of conciseness, the questions emanating from this paper are analyzed through a specific subtheme of the Internet law, e.g. the regulation of big data. This lens seems to be fitting with the scope of this study because data carries with itself the vocation of transnationality of the Internet, as well as its multi-purpose usability, allowing it to serve both economy and human rights.

As to the first element – transnationality – big data has an intrinsic tension to unrestrained circulation, from both technical and economic point of view. Firstly, as scholars clarified, the raw substance of data approximates it to non-rival and non-excludable goods¹⁵, because they can be duplicated and transferred virtually everywhere at almost no cost, and they are not consumed by utilization. Furthermore, the innovativeness of the most advanced data analysis instruments derives exactly from the possibility of reusing data sets. Indeed, “data mining” – as explained below – does not need specific samples, fitting to each experiment, but allows us to scrutinize huge quantities of data collected from different sources with different aims, even in absence of a working hypothesis prior to the creation of the data sets¹⁶. Then, not only is information non-rival, but it also delivers its highest potential value if shared, reused, and linked with other databases.

As to the second element – multifunctionality – data can serve multiple aims that meet different and sometimes contrasting interests, involving the economic, personal or public sphere. This means that data regulation is not neutral, oppositely, has to balance constitutional values. For example, information can be gathered and sold for advertising purposes or can build artificial intelligences or become a shared industrial asset in

¹⁴ J.P. Barlow, ‘A Declaration of the Independence of Cyberspace’, (*eff.org*, 8 February 1996) <<https://www.eff.org/it/cyberspace-independence>>. *Contra*, G. De Minico, ‘Towards an Internet Bill of Rights’ (2005) 37, 1 *Loyola Los Angeles International & Comparative Law Review*, 28-29.

¹⁵ Katarzyna Śledziowska and Renata Wloch, ‘Should We Treat Big Data as a Public Good?’, Mariarosaria Taddeo and Luciano Floridi (eds.), *The responsibilities of online service providers* (Springer 2017), 265-268.

¹⁶ Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (Houghton Mifflin Harcourt 2013), 11-70, 147-158.

agricultural and manufacturing sectors¹⁷. Yet, the discipline of data is linked to fundamental rights and especially privacy, too.

For these reasons, this paper analyzes two emblematic examples of the legislation in the EU concerning data: trade law and counter-terror law. The first one is an example of how regulatory processes can involve foreign private actors, granting them participatory rights. As observed in the following paragraph, free market is the primary basis of such laws, overriding other principles, and, accordingly, stakeholders that have a part in the process are chosen on the basis of their economic power, rather than rationality. Oppositely, counter-terror law is driven by the idea of national security, with a mistrust against foreigners, who are surveilled as potential enemies. Though, paradoxically, intelligence services cooperate with other multinational private actors for this aim.

These factors also highlight new boundaries in participatory rights, since data control is strictly linked to sovereignty.

Here, a clarification shall be made, concerning the right to privacy. The latter is not the main object of this work. Though, it is central in the reasoning, as a point of reference through which discrimination is assessed.

In accordance with the EU framework,¹⁸ privacy it is not only a protection of what is normally “secret”, like the person’s private sphere or domicile. Rather, it is a right to “informational self-determination”, i.e. everyone’s possibility to control one’s own information. The pivot of this system is the mechanism of informed consent: as a general rule, personal data can only be processed with the individual’s consent, qualified by specific requirements that such consent is freely given, specific, informed and unambiguous (Articles 6 ss., GDPR). This discipline is provided because information is the natural expansion of the individual sphere itself, and then it is embedded in the overall right to personal autonomy.

Of course, the enjoyment of this right can be limited, if needed to fulfill other rights, like economic ones, as in trade law, or security ones, as in counter-terror law. This is also stated in the GDPR, which allows some exception to the requirement of consent, when deemed necessary for national security¹⁹ (Article 23). Though, in this case a balance is needed,

¹⁷ Josef Drexler, ‘Designing Competitive Markets for Industrial Data - Between Propertisation and Access’ (2016) Max Planck Institute for Innovation & Competition Research Paper No. 16-13. <<https://ssrn.com/abstract=2862975>>, 30-38.

¹⁸ Privacy is stated specifically in stated in Charter of Fundamental Rights of European Union [2012] OJ C 326, 26.10.2012, Article 8. Such right shall have at least the same meaning and scope as European Convention for the Protection of Human Rights and Fundamental Freedoms [1950], Article 8. The discipline, shaped as a normative on informational self-determination is detailed in: European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] O.J. L 119/1 (hereinafter GDPR).

¹⁹ [Specific norms for these cases are provided in Directive \(EU\) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council](#)

according to the principle of proportionality. As specified by EU Court of justice,²⁰ limitations of privacy are only accepted if provided by the law, apt, necessary and proportionate in relation to the counterposed value.

Apparently, there are cases where reasonableness and proportionality cannot be assessed, since in some contexts police is bound to act before having any information about “how” of the danger, but also about “if”, “when” and “where”. This is exactly the case for counter-terror: the peculiarity of the new terrorism is that it can hit in an unforeseeable way – with regard to time, modalities and targets – and is able to organize its actions on transnational scale²¹. Hence, ignorance of the potential event impedes a proper evaluation of the measures, in terms of reasonableness.

In this case, action is not forbidden, for the same reasons stated by the precautionary principle,²² i.e. to avoid political choices being completely subordinated to scientific certainty. Though, such rule is not an outright exclusion of the obligation to strike a proportional balance. Rather, such principle shall be enacted through a slightly different referral rule, adjusted to the situation: ‘the more severe is the intervention against a fundamental right, the higher shall be the certainty about the premises supporting the intervention’,²³ and *vice versa*.

[Framework Decision 2008/977/JHA, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=IT>](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=IT)

²⁰ See, lastly, Cases c-293/12 and c-594/12, Digital Rights Ireland Ltd v Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] European Court of Justice, ECLI:EU:C:2014:238. Concerning the requirement of “provision by the law”, the respective balance of Judiciary and Parliamentary powers is controversial: Antonio D’Andrea, *Autonomia costituzionale delle camere e principio di legalità* (Giuffrè 2004), 1 ss.; Oreste Pollicino, ‘Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale’ (2014) 3 *Federalismi.it*. <[²¹ In the legal literature, see Giovanna De Minico, *Costituzione. Emergenza e terrorismo* \(Jovene 2016\), 188 ss.; A. Vidaschi, ‘Da Al-Qaida all’IS: il terrorismo internazionale si è fatto Stato?’ \(2016\) 1 *Rivista Trimestrale di Diritto Pubblico*, 43-46.](http://www.federalismi.it/AppOpenFilePDF.cfm?artid=28017&dpath=document&dfile=25112014121445.pdf&content=Interpretazione+o+manipolazione?+La+Corte+di+giustizia+definisce+un+nuovo+diritto+alla+privacy+digitale+-+stato+-+dottrina+-+>, 5-8.</p>
</div>
<div data-bbox=)

²² Consolidated Version of the Treaty on European Union [2008] OJ C115/13, Treaty on the Functioning of the European Union, Article 191; Communication from the European Commission COM(2000) 1 final on the precautionary principle [2000] <<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0001:FIN:EN:PDF>>.

²³ Robert Alexy, *Theorie der Grundrechte* (tr. Leonardo Di Carlo, Suhrkamp 1985), 651; Rosario Serra Cristóbal, ‘The Impact of Counter-terrorism Security Measures on Fundamental Rights: The Need for Supranational Common Standards of Rights Protection to respond to terrorism risk’ (2014) Speech at IX IACL International Congress, *Constitutional Challenges: Global and Local*, Oslo, June 16-20, 2014. <<http://www.jus.uio.no/english/research/news-and-events/events/conferences/2014/wcclmcd/wccl/papers/ws1/w1-crist%C3%B3bal.pdf>>, 4, commenting D Ennis et al. v. United States, Supreme Court of United States, No. 336 [June 4, 1951].

Moreover, another criterion not stated in the Charter appears to be slowly emerging in some recent decisions of the EU Court of Justice²⁴: a hierarchy that privileges personality rights over economic ones has to be recognized.²⁵

What is most important, here, is that informational self-determination is also an essential part of social and democratic inclusion and, consequently, exercise of political rights. Such observation is due to at least three reasons.

Firstly, gathering data about a person's life allows to influence her with the threat of revealing compromising details;²⁶ and this is not a mere hypothesis, since in many instances governments have attempted to use this strategy to blackmail their opponents.²⁷ Secondly, as witnessed in periods of dictatorship, espionage – if enacted by people in position of power – can lead to self-censorship, because of the fear of possible consequences which could derive from some claims or behaviours.²⁸ Thirdly, the controller can also influence other's decisions,²⁹ to the extent that, according to some theories, governments ought to learn fallacies in average citizens' reasoning and exploit them to discretionarily guide the personal choices³⁰.

Thus, any public or private actor who engages in bulk metadata collections enacts a form of surveillance, where public powers can know people and phenomena without being in turn observed by society. This is especially true when such entity does not disclose the way in which data is used, since in this case it is not, in turn, controllable. Such informational

²⁴ Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González [2014] European Court of Justice, ECLI:EU:C:2014:317, paras. 97 e 99.

²⁵ Carlo Iannello, 'Il «non governo» europeo dell'economia e la crisi dello stato sociale', 2 *Rassegna di Diritto Pubblico Europeo Online*, 12 ss.; A. Lucarelli, 'Beni comuni. Contributo per una teoria giuridica' (2015) *Costituzionalismo.it*.

²⁶ Paul M Schwartz, 'Internet Privacy and the State' (1999-2000) 32 *Connecticut Law Review*, 841-842; Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 (3) *University of Pennsylvania Law Review* [https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477\(2006\).pdf](https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf), 539-541.

²⁷ Shaun B Spencer, 'Security Versus Privacy: Reframing the Debate' (2002) 79, 4 *Denver University Law Review* <<http://ssrn.com/abstract=2015040>>, 572; and, as to corporations surveillance, Jack M Balkin, 'Information Fiduciaries and the First Amendment' (2016) *Yale Law School, Public Law Research Paper No. 553* <http://ssrn.com/abstract=2675270>, 4-5.

²⁸ Jean-Claude Paye, 'France: An Algorithmic Power' (2016) 67, 9 *Monthly Review* <<https://monthlyreview.org/2016/02/01/france-an-algorithmic-power/>>; Karen Turner, 'Mass Surveillance Silences Minority Opinions, According to Study' (*WashingtonPost.com – The Switch*, 28 March 2016) <https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/?utm_term=.b75fe1352fdf>; Nicole Perloth, 'Governments Turn to Commercial Spyware to Intimidate Dissidents' (*NewYorkTimes.com*, 29 May 2016) <http://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html?_r=0>. This issue is also the object of important jurisdictional decisions: *Whalen v. Roe*, U.S. Supreme Court, No. 75-839, 429 U.S. 589 [February 22, 1977], in <<https://www.law.cornell.edu/supremecourt/text/429/589>>.

²⁹ Bert-Jaap Koops, 'Some Reflections on Profiling, Power Shifts and Protection Paradigms', in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizen* (Springer 2008) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1350584, 2; Andrew J Roberts, 'A Republican Account of the Value of Privacy' (2013) *University of Melbourne Legal Studies Research Paper No. 673* <<http://ssrn.com/abstract=2369680>>, 17-26.

³⁰ Cass Sunstein, *Laws of fear: beyond the precautionary principle* (Cambridge University Press 2005), Ch. VIII.

asymmetries are an interference with individual freedom, and, on a massive scale, with popular sovereignty, because governments are provided with a form of unaccountable power.

For these reasons, one can fairly assume that data control is central in assessing the enjoyment of political rights. So, with reference to the parameter of privacy – understood as informational self-determination – the research will assess how regulations affect the respective status of nationals and non-nationals. Eventually, the central issue will become if, and how, the global nature of the Internet lowers discriminations in the enjoyment of participatory rights, and, in case of negative answer, which critical points shall be addressed for a more equal involvement of civil society in decision-making.

2. The International Trade Law through the Lenses of Big Data Players' Role

As mentioned before, the Internet is a field where the community of reference, advocating for a democratic participation, is only partly linked to the territory, and mostly thinks of itself as an a-territorial collectivity. Moreover, due to the key infrastructural and economic value of the World Wide Web, netizens are not the only ones who claim decisional powers. Other actors are involved, such as other States, corporations of the Internet and many forms of sectorial and territorial international organizations. So, clearly State powers cannot exercise the traditional internal and external sovereign authority. Firstly, such matters often exceed the national jurisdiction: nor the players or the infrastructures of the web are located in one single territory. Secondly, sometimes the online word even questions the States' monopoly of the legal force. In the digital environment new “functional” private powers have emerged³¹. These ones, due to their economic position, are able to hold peer-to-peer relations with States and impose their rules to a plurality of the Internet users on global scale.

This situation has caught the attention when a European State established an Ambassador in the Silicon Valley for the relationships among the ‘over the top’ Internet businesses.³² However, other instances show that such actors are considered as allies in the enforcement of internal sovereignty, rather than average components of civil society. One case is given by national elections, hindered by the dangers of foreign “trolls”, or voter profiling by corporations like Cambridge Analytica, on behalf of politicians.³³ Eventually, pending the imminent EU Parliamentary elections, the first regulatory reaction to the latter

³¹ Frank Pasquale, ‘From Territorial to Functional Sovereignty: The Case of Amazon’ (*Lpeblog.org*, 6 December 2017) <<https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/>>.

³² Tech Ambassador of Denmark <<http://techamb.um.dk/>>.

³³ Hannes Grassegger and Mikael Krogerus, ‘The Data That Turned the World Upside Down’ (*Motherboard.vice.com*, 28 January 2017) <https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win>. D

distortion of public sphere was the big players' self-regulation³⁴. For example, Facebook³⁵ gave its own political direction to the measures: the transparency measures on paid advertising, through open archives on the sponsored campaigns and their financiers; the de-indexation and labelling of fake news. In the context of this research, it is interesting to notice that the company also banned paid political advertising from abroad, thus enacting a provision that reinforces the exclusion of foreigners from the political community.

Such examples give a sufficient account of the novelty of the Internet as a regulatory field. The huge debate on the Internet governance, mentioned above, is a clear indicator of the fact that offline government cannot be immediately taken as a model for digital issues.

New technologies create unprecedented horizons for the territorial and material expansion of digital freedom. Moreover, as mentioned, the web is a new kind of space, where many enclosures are virtually avoidable, because many digital goods, as data, information or source codes, are non-rival in nature.

Nevertheless, this circumstance has not brought the Internet community to question property. Oppositely, new forms of property were created to generate an artificial scarcity of such goods, with the aim of providing incentives for their production. Not by hazard, the most noticeable leaps towards global harmonization of rules and participation of international civil society seem to happen, paradoxically, in the regulation of economic matters.

The Internet is an increasingly important issue in trade law. Concerning big data, for example, «as more business models and practices move onto the digital platform and data becomes increasingly shared and exchanged on an international scale, its relationship to international trade intensifies. Since data are gathered, digitized, stored, and moved on a truly global basis by a multitude of parties, restrictions and regulations concerning data directly effect on global trade».³⁶

Therefore, market needs have been the engine of many experiments of international regulation, which are perhaps the most successful, in terms of obligation and involvement of stakeholders.

Normative harmonization is required by global trade because differences among law systems bring strong incentives to restrain the circulation of commodities. Indeed, if safeguards are not homogeneous, each State seeks to apply its own rules and so protect

³⁴ The EU has promoted a process of self-regulation: see 'Code of Practice on Disinformation', 26 September 2018, <<https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>>. For the implementation, see European Commission, Analysis of the 'Annual self-assessment reports of signatories to the Code of Practice on Disinformation 2019', 29 October 2019 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62698>.

³⁵ Anika Geisel, 'Protecting the European Parliament Elections' (*Newsroom.fb.com*, 28 January 2019) <<https://newsroom.fb.com/news/2019/01/european-parliament-elections/>>.

³⁶ United Nations Conference on Trade and Development (UNCTAD), 'Data protection regulations and international data flows: Implications for trade and development' (United Nations 2016) <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf>, 3-4. See also Harsha Vardhana Singh, Ahmed Abdel-Latif and L. Lee Tuthill, 'Governance of International Trade and the Internet: Existing and Evolving Regulatory Systems' (2016) Global Commission on Internet Governance, Paper Series: No. 32 <https://www.cigionline.org/sites/default/files/gcig_no32web_0.pdf>, 2.

fundamental rights according to their own balancing decisions. For example, foodstuffs that can be legally commercialized in their Country of origin might be prevented from being sold in another State, if the latter has stricter norms for human health.

Well, the European Union has full competence over the negotiation of trade agreements, even if there are controversies over the scope of such power, especially when they affect national regulations concerning fundamental rights. In these cases, some States have claimed the need of a parliamentary ratification of decisions.³⁷

However, in this research, what matters most is the peculiar legal rationality of trade agreements. These ones have market as a primary objective, and use this aim as a point of reference when they choose the actors and the approaches. Of course, trade negotiations are part of the broader system of EU law, and therefore they are also bound by the «democracy, the rule of law, human rights and the principles of international law» (Article 21 TEU). Though, doctrine have highlighted that such regulatory contexts rather tend to act as a detached legal order, with a systemic bias in favour of economic freedoms. Not surprisingly, authors have highlighted the tension – almost a schizophrenic one – between the system of free trade, on the one hand, and the entire system of fundamental rights, rule of law, and judicial redress, on the other hand³⁸.

A paradigmatic example is the use of National Treatment and Most-Favoured-Nation Treatment clauses, which are both in the General Agreement on Trade in Services (Articles II and XVII) and in the General Agreement on Tariffs and Trade (Articles I and III)³⁹. According to the former, the conditions applied to the delivery or circulation of national products or services shall also be applied to the other contracting parties. The latter provides that, in principle, any advantage or privilege granted by a State to another State – which is part of the agreement – shall be accorded also to the other contracting parties.

Per se, the two principles are not limited in scope, so they rise a problem of coordination with the system of protection of fundamental rights, which also does not have material limits. The formers give rise to uncertainties in the application of the latters, since any limitation to transnational commerce is a potential infringement of the engagements contracted with other parties. This is why their contents, other than their procedures, have been contested by civil society in different fields, like, for example, health protection, food security, access to medicines,⁴⁰ biodiversity...

In relation to big data, the applicable law often depends on the localization of information. This means that regulatory differences incentivize governments to keep data

³⁷ For an essential account of the debate: Dirk De Bièvre, 'The Paradox of Weakness in European Trade Policy: Contestation and Resilience in EU CETA and TTIP Negotiations' (2018) 53(3) *The International Spectator*, Italian Journal of International Affairs, 10-11.

³⁸ In that sense, doctrine has used a comparison with the character of Dr Jekyll and Mr. Hyde: Ernst-Ulrich Petersmann, 'Democratic Legitimacy of the CETA and TTIP Agreements?', in Thilo Rensmann (ed.), *Mega-Regional Trade Agreements* (Springer 2017), 39-56 (the expression is at p. 54).

³⁹ Catherine A Brown, 'The General Agreement on Trade in Services', in Ead. (ed.), *Non-discrimination and Trade in Services* (Springer, 2017), 21-25.

⁴⁰ Roberto Caso and Paolo Guarda, 'Copyright Overprotection Versus Open Science: The Role of Free Trade Agreements?', in Lilian Corbin and Mark Perry (eds.), *Free Trade Agreements* (Springer 2019), 41-50.

sets within their territory.⁴¹ For instance, the General Data Protection Regulation (or GDPR) of the European Union forbids personal information to be transferred to third Countries that do not ensure an ‘adequate’ level of protection (Articles 44-47). Moreover, that ‘adequacy’ has been interpreted in a rigid way by the EU Court of Justice. Indeed, this Judge in the *Schrems* decision reads the requirement as imposing an ‘essentially equivalent level of protection’.⁴² Thus, in this case the absence of equivalence between regulatory systems impedes the transfer and selling of data.

To address such issues, a vast range of Free Trade Agreements (FTAs) has taken place, with the aim of building common rules and so remove barriers to trade. This kind of regulation is not “neutral” or merely “technical”, but has an impact on the reciprocal coexistence of fundamental rights. The process of harmonizing disciplines is also a decisional process, which chooses a discipline, and so sets its own balance among the different fundamental and economic rights involved. In other words, despite its economic ratio, it has to be recognized as a real coercive juridical system⁴³, which could even be considered the embryo of a new paradigm of the Internet Governance.⁴⁴

This is particularly evident in the latest wave of FTAs (including, e.g., the Comprehensive Economic and Trade Agreement - CETA and the Transatlantic Trade and Investment Partnership - TTIP), which are only a species of the broader genus of Free Trade Agreements, but seem to be particularly emblematic here because they attain a very advanced institutionalization of the international State-business cooperation.⁴⁵ In other words, free market, in this case, fosters a fully original juridical order – produced at international level – whose objectives, procedures and actors are different from the establishment of traditional Constitutional States.⁴⁶

Here, the topic is analysed by taking into account the arrangements over data flows in Trade in Services Agreement (TiSA), a FTA in course of negotiation, seeking to minimize

⁴¹ Eg, the Brazilian *Marco Civil* demanded a forced localisation in the country of all data of Brazilian users that are collected by foreign companies: Lei N° 12.965, de 23 de Abril de 2014, Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>.

⁴² Case C-362/14, Maximilian Schrems v. Data Protection Commissioner [2015] European Court of Justice, ECLI:EU:C:2015:650 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ10362>>. See Giovanna De Minico, *Costituzione. Emergenza e terrorismo* (Jovene 2016), 136-137.

⁴³ John H. Jackson, *Sovereignty, the WTO and Changing Fundamentals of International Law* (Cambridge University Press, 2006), 1-78.

⁴⁴ Maria Francesca De Tullio and Giuseppe Micciarelli ‘Trade Agreements and Internet Governance: Data Flow and Politics in the TiSA’s Governmental Rationality’ in Meryem Marzouki and Andrea Calderaro (eds), *Global Internet Governance as a Diplomacy Issue* (Rowman & Littlefield, forthcoming). To this shared reflection is due much of the reasoning that has been later developed here on Free Trade Agreements.

⁴⁵ Giuseppe Micciarelli, ‘CETA, TTIP e altri fratelli. Il contratto sociale della post democrazia’ (2017) 2 *Politica del diritto*, 257 ss. This is true, not only in the rule-making phase, but also in the application of such rules, often entrusted to private dispute settlement organisms: Alessandra Algostino, ‘Isds (Investor-State Dispute Settlement), il Cuore di Tenebra della Global Economic Governance, e il Costituzionalismo’ (2016) 1 *Costituzionalismo.it*, 103-115.

⁴⁶ Rory Van Loo, ‘The Corporation as Courthouse’ (2016) 33 *Yale Journal on Regulation* <<http://digitalcommons.law.yale.edu/yjreg/vol33/iss2/5>>, 554 ss.

non-tariff barriers to the international trade in services.⁴⁷ This case is interesting because its geographic scope is exceptionally broad: it would involve twenty-three Parties – including the EU – accounting for about seventy percent of international trade in services, and it is conceived as an open Treaty, susceptible to be integrated in the World Trade Organisation (WTO) framework, in case a critical number of WTO Members would adhere.

As to the aims, TiSA – differently from other forms of regulation – is built around the central value of free trade, and so its whole structure is crafted to favour this principle over the others. In juridical terms, this is translated into a straightforward mechanism of rule-exception to address all the conflicts between economic and fundamental rights.⁴⁸ Namely, free trade – and so free flow of data – is stated as a general overarching principle, with the establishment of clauses of National Treatment and Most-Favoured-Nation Treatment.⁴⁹ Oppositely, basic freedoms, where ensured, are provided as an authorization for the Parties to derogate the Treaty⁵⁰. This is not secondary, because, according to the juridical science, exceptional rules have a narrow application, that shall be punctually justified and cannot be interpreted extensively or analogically.⁵¹ On the contrary, general rules can only be set aside when they are expressly excluded.

This settlement is radically opposite to democratic Constitutions, where personality rights – and not free trade – are “fundamental” and so enjoy an “assumption of maximum extension”.⁵² Which is to say that freedoms are applied in all occasions, unless an exception is clearly provided by the law, is apt to pursue an equally fundamental principle, and results necessary and proportional to the benefit provided⁵³. In other words, the rule-exception mechanisms appear completely specular to each other: TiSA reverts the value given to the

⁴⁷ The content of FTAs negotiations is classified. However, drafts have been partly leaked by civil society organisations (eg, Wikileaks and Greenpeace) and some Parties’ official positions have been voluntarily released. This research is based on these sources.

⁴⁸ Jane Kelsey and Burcu Kilic, ‘Briefing on US TISA proposal on E-commerce, Technology Transfer, Cross-border Data Flows and Net Neutrality’ [2014] Public Services International <http://www.world-psi.org/sites/default/files/documents/research/briefing_on_tisa_e-commerce_final.pdf>, 7, 16; Israel Tamir, ‘TISA Annex on Electronic Commerce: A preliminary analysis by the Canadian Internet Policy & Public Interest Clinic (CIPPIC)’ (2015) <https://wikileaks.org/tisa/analysis/Analysis-of-20150220_Annex-on-Electronic-Commerce/Analysis-of-20150220_Annex-on-Electronic-Commerce.pdf>, 14-16; Jane Kelsey ‘TiSA: Updated Analysis of the Leaked “Core Text” from July 2016’ (2016) https://wikileaks.org/tisa/analysis/201609_TiSA_Analysis-on-Core-Text/201609_TiSA_Analysis-on-Core-Text.pdf, 2.

⁴⁹ See Articles I-4 and the un-numbered Article between I-2 and I-3 of the core text, together with Articles 2 and 8 of the Annex on Electronic Commerce.

⁵⁰ Article I-9 of the Core Text.

⁵¹ Among many, *Klass v. Germany* App no 5029/71 (ECHR), para. 42; paras. 66-8, 81.

⁵² Pierfrancesco Grossi, *Introduzione ad uno studio sui diritti inviolabili nella Costituzione italiana* (Cedam 1972), 16; Paolo Caretti, *I diritti fondamentali. Libertà e diritti sociali* (Giappichelli 2005), 104.

⁵³ Among many, *Halford v. the United Kingdom*, App no 20605/92 (ECHR), paras. 66-8, 81; European Court of Justice, *Digital Rights Ireland Ltd c. Ireland*, para. 38.

personal sphere in democratic orders, and place trade as general principle, while relegating rights to narrow exceptions.⁵⁴

Basically, the possibility to enact the aforementioned Articles 44-47 GDPR would be actually doubtful under the TiSA regime, because every implementing act would have to fit a system where free circulation of data is the norm, and privacy the exception.

The pivot of this system is the general rule of free data traffic, provided in the *Annex on Electronic Commerce* of the TiSA, as a corollary of the wider principles of National Treatment and Most-Favoured-Nation Treatment, contained in the *Core Text* (Articles I-4 and the un-numbered Article between I-2 and I-3). Indeed, Article 8 of the *Annex on Electronic Commerce* forbids location requirements for computing facilities and Article 2 contains the right of ‘transferring, accessing processing or storing information, including personal information, within or outside the Party’s territory, where such activity is carried out in connection with the conduct of the service supplier’s business’. Here ‘connection’ is a broad term able to account for all the different hypotheses where economic activities require the transfer of data: data can be an accessory, the object or even a remuneration for the service.

Namely, data protection measures must not be a ‘means of arbitrary or unjustifiable discrimination among countries where these conditions prevail, or a disguised restriction on trade in services’ (Article I-9, chapeau, Core Text), must be ‘necessary’ and ‘not inconsistent with the provisions of this Agreement’ (Article I-9(c), Core Text). This is a risk for privacy, since – as mentioned – a general principle of law is that exceptions are subject to very strict interpretation. Further confirmation comes from the jurisprudence under Article XX of *General Agreement on Tariffs and Trade*⁵⁵ and Article XIV of *General Agreement on Trade in Services*,⁵⁶ whose wording is similar to the Article I-9 of TiSA. Indeed, in some decisions the exercise of the State authority to legislate in favour of fundamental values has been ruled unlawful.⁵⁷

The data subject’s privacy is somehow recognised in Article 2, but not entrenched with specific safeguards. More precisely, informational self-determination is mostly protected as a consumerist entitlement, instrumental to ‘consumer’s confidence in electronic commerce’ (Article 4, *Annex on Electronic Commerce*). Consequently, a real – although weak – consent requirement is only set for unsolicited commercial electronic messages (Article 5, *Ibid.*). In the remaining fields, instead, there is only a broad-termed obligation prescribing to the Parties the adoption of a ‘domestic legal framework’ of protection (Article 4, *Ibid.*).

⁵⁴ Rolf H Weber, ‘Regulatory Autonomy and Privacy Standards under the GATS’ (2012) 7 Asian Journal of WTO & International Health Law and Policy, 32-34; Kristina Irion, Svetlana Yakovleva and Marija Bartl, ‘Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements’ (2016) Independent study commissioned by BEUC et al., published 13 July 2016, Amsterdam, Institute for Information Law (IViR) <https://ssrn.com/abstract=2877166>, 57.

⁵⁵ 1986 <https://www.wto.org/english/docs_e/legal_e/gatt47.pdf>.

⁵⁶ 1994 <https://www.wto.org/english/docs_e/legal_e/26-gats.pdf>.

⁵⁷ United States – Measures Affecting The Cross-Border Supply Of Gambling And Betting Services [2004] WTO Panel, WT/DS285/R; United States - Standards for Reformulated and Conventional Gasoline [1996] WTO Appellate Body, WT/DS2/AB/R.

In practice, the Parties of the treaty can have privacy legislation, but only insofar as its approval or enforcement does not alter the substance of the free economic initiative. Indeed, any conflict that may arise between the two values is settled – as anticipated – through a rule-exception mechanism, where privacy is an exceptional norm, and can derogate to free trade only if very strict requirements are met.

In sum, these rules are radically divergent not only from traditional Constitutional orders, but also from other pieces of international regulation on data protection, such as the OECD Privacy Principles. Thus, the pivotal aim of these ones is to impose a plafond of minimal safeguards for liberties, even if their *occasio legis* is to foster trust as a precondition to free exchange. On the contrary, FTAs are a negotiating field where some Parties – seeking to access new markets – accept limitations of their demand to safeguard individual rights.⁵⁸

Contents, as described above, are linked to the procedures followed and actors involved, which are at the core of this essay. Traditionally, in democratic Constitutions, the identification of a balance among fundamental rights is strictly entrusted to representative organisms and Parliaments above all, acting through public procedures, regulated by an overarching fundamental Chart. Moreover, oversight powers are entrusted to independent organisms, and primarily to the judiciary, usually burdened by obligations to motivate their decisions and means of appeal.⁵⁹

In comparison, TiSA shows an outright shift of paradigm. Here negotiations are conducted by different actors, coming from both governmental and private sectors, who do not need to be part of the representative circuit or even of the relevant democratic community. To be precise, Parliaments are not even able to fully observe and oversee the proceedings, which are kept under a strict secret.⁶⁰ Nor is it clear what are the enforcement organisms and procedures of TiSA, which are barely sketched in the latest draft.⁶¹

So, the vertical form of representative democracy is substituted with the horizontality of public-private negotiation, which seeks to legitimize itself through the stakeholders' participation⁶². Though, horizontality does not always mean absence of hierarchy, because contracts, in absence of constitutional (or quasi-constitutional) guarantees, favour those who have most bargaining powers, which are not necessarily the States. Indeed, in the neoliberal market order, these ones are subject to competition as well, because they are in

⁵⁸ Graham Greenleaf, 'The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy?' (2016) UNSW Law, Research Paper No. 08 <https://ssrn.com/abstract=2732386>, 3; Cristophe Leroy, 'Existe-t-il un marché du droit public ?' (2016) 100 Petites affiches, 3-4.

⁵⁹ Cases c-293/12 and c-594/12, Digital Rights Ireland Ltd v Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] European Court of Justice, ECLI:EU:C:2014:238. Concerning the tool of the appeal: Giovanni Serges, *Il principio del "doppio grado di giurisdizione" nel sistema costituzionale italiano* (Giuffrè 1993).

⁶⁰ Susan Aaronson, 'Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security' (2015) 14, 4 World Trade Review, 678.

⁶¹ EU Proposal, TiSA - Dispute Settlement Chapter.

⁶² See also R. Bifulco, 'Le sfide della crisi economica alla Costituzione: differenziazione e globalizzazione' (2012) 2 *Parolechiane*, 54 ss.

need of attracting investors and buyers, and so try to arrange the most favourable rules for commerce.

In conclusion, the example seems to be a sufficient example of how new forms of public-private regulations are emerging, which act according to market logics and are able to produce binding effects on States on a transnational scale. Namely, not only are foreign actors – like investors and businesses – effectively included in decision-making, against the nation State tradition; what is more, these players weigh even more than governments themselves.

Now, as mentioned in the introduction, this circumstance at first glance appears to expand democratic vindications outside of the national boundaries. Though, the real question is whether there are analogous participatory mechanisms when non-nationals are average persons, and not exponent of economic powers. From the above description, it seems that no such system is available in trade law. Hence, economic and social factors seem to be the real cleavage: foreign actors are involved in rule-making on selective basis, and more precisely according to their ability to represent vested interests.

In the following paragraph, the research observes that the same can be stated for human rights law.

3. The Persisting Relevance of Nations and Territories in Discriminatory Counter-Terrorism Surveillance

While negotiations over FTAs are ongoing, the same cannot be claimed for international Treaties concerning data protection. This tendency is clear if we consider, for instance, the aforementioned Articles 44-47, GDPR, in particular their application to data transfers towards the US. History shows that transatlantic relationships have never been easy on these matters, especially due to the US surveillance laws regarding crime prevention, which are utterly invasive, and even harsher on foreigners' data. The attempts to involve US in multilateral agreements – such as OECD privacy Guidelines, or the APEC Privacy Framework – have not succeeded in producing binding and enforceable language,⁶³ but only in obtaining an arrangement based on a mechanism of self-certification – the so-called *Safe Harbor*⁶⁴ – which has later been considered by European Court insufficient to safeguard personal information coming from EU. More recently, another pact has been signed –

⁶³ Graham Greenleaf, 'The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy?' (2016) UNSW Law, Research Paper No. 08 <https://ssrn.com/abstract=2732386>, 2.

⁶⁴ Commission Decision 2000/520/EC pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (Adequacy Decision) [2000] OJ L 215, 25/08/2000 <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000D0520&from=IT>>.

called *Privacy Shield*⁶⁵ – which is controversial as well,⁶⁶ especially in light of Trump’s policies, which provide even a step back in the safeguard of non-US people.⁶⁷

The need to have an efficient intelligence sector is obviously a constant in every nation State; though, it has had a sudden increase since the experience of 9/11 in New York. Counter-terror has opened a new state of emergency made of derogatory measures, which are not extraordinary and temporary, but become embedded in the ordinary law. Indeed, public authorities are forced to a state of permanent alert, because criminal cells, also due to technological evolution, seem to be able to organize themselves and strike at any time. Hence, the only useful strategy appears to be an ordinary “administration of the risk”, involving a total and permanent control, targeting everyone regardless of specific suspects.⁶⁸

Concerning the US, famous press investigations⁶⁹ have revealed that intelligence services engage in mass metadata harvesting and analysis, along with the legal basis provided by *Foreign Intelligence Surveillance Act* (FISA)⁷⁰. The aim of analyzing communication metadata is to identify suspected persons and keep them under observation to stop them before they commit an illicit act. Basically, this data is examined through “data mining” techniques, i.e. governmental statistics which extract subjective qualities and behaviours that are more frequently linked to a given crime, and so indicate any other person possessing such features as a likely criminal. In sum, snooping is possible even without having to demonstrate a reasonable link with a crime.

Such legislation does not concern contents, but only metadata, i.e. data on movements, behaviours and circumstances of communication. Though, it shall be considered as an interference with privacy, not less. Indeed, technology has generated new data analysis techniques and new devices, which produce a huge quantity of data on daily basis. In this context, even non-content information can reveal a person’s life with a great level of details:

⁶⁵ Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (Adequacy Decision) [2016], OJ L 207, 1.8.2016 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG>.

⁶⁶ Conseil National du Numérique, ‘Communiqué, Pourquoi l’accord « Privacy Shield » doit être renégocié’ (2017) <https://cnnumerique.fr/wp-content/uploads/2017/09/CNNNum_PrivacyShield.pdf>.

⁶⁷ Executive order. Enhancing public safety in the interior of the United States, January 25th, 2017, Sec. 14. <<https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united>>.

⁶⁸ John Yoo, ‘The Legality of the National Security Agency’s Bulk Data Surveillance Programs’ (2013) UC Berkeley Public Law Research Paper No. 2369192 <http://ssrn.com/abstract=2369192>. 5-11.

⁶⁹ Glenn Greenwald, ‘NSA collecting phone records of millions of Verizon customers daily’ (*TheGuardian.com*, 6 June 2013) <<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>>; Barton Gellman and Laura Poitras, ‘U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program’ (*WashingtonPost.com*, 6 June 2013) <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>.

⁷⁰ Pub. L. 95-511 – OCT. 25 (1978) 92 STAT. 1783 <<https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf>> and subsequent modifications.

data sets can ‘be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on’.⁷¹

These rules are very far from the ones stated by EU law, as interpreted by the Court of Justice, and this is why they raise an issue of adequacy of the US data protection. Therefore, they cast doubts on the possibility of transatlantic circulation of EU citizens’ data.

If we look at the phenomenon from the point of view of data subjects, FISA appears of particular concern mainly because of the scope and firepower that the US intelligence is able to put in place. Though, from a barely legal point of view, EU Member States’ laws do not ensure a greater level of protection, when it comes to crime prevention and repression.⁷² For instance, one can consider UK, with *Data Retention and Investigatory Powers Act 2014* (DRIP)⁷³ and *Investigatory Powers Act 2016*,⁷⁴ or France, with *LOI n° 2015-912 du 24 juillet 2015 relative au renseignement*⁷⁵ and the *LOI n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales*.⁷⁶

In the case of the UK, both the mentioned laws allow the government to require by notice a public telecommunications operator to retain relevant communications data, even in absence of a clear suspicion. No provision requires an oversight of any judicial or independent organism. Such acts are being reiterated in clear breach of European and internal Courts statements, which until now have censored, respectively, the so-called Data Retention Directive⁷⁷ and the UK laws of 2014 and 2016. In 2014, the intention of not complying with European Court’s order was blatant: the Prime Minister in its press release (10 July 2014) declared that the aim of the DRIP was to ‘enable agencies to maintain existing capabilities’ after a ‘recent development’, which is that «the European Court of Justice (ECJ) has struck down regulations enabling Communications Service Providers (CSPs) to retain communications data for law enforcement purposes for up to 12 months. Unless they have a business reason to hold this data, Internet and phone companies will start deleting it which has serious consequences for investigations – investigations which can take many months and which rely on retrospectively accessing data for evidential purposes».

As far as France is concerned, Article 5 of the French *LOI n° 2015-912* has introduced – exclusively for counter-terrorism needs – “black boxes” in communication channels. The

⁷¹ Justice Sotomayor, concurring opinion in *United States v. Jones*, Supreme Court of the United States, No. 10-1259 [January 23, 2012] <<http://www.law.cornell.edu/supremecourt/text/10-1259>>.

⁷² Daniel Bigo and others, ‘Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law’ (2013) CEPS Paper in Liberty and Security in Europe Papers No. 61 <<http://ssrn.com/abstract=2360473>>, 12-18.

⁷³ 2014 c. 27 <<http://www.legislation.gov.uk/ukpga/2014/27/contents>>.

⁷⁴ 2016 c. 25 <<http://www.legislation.gov.uk/ukpga/2016/25/contents>>.

⁷⁵ JORF n° 0171 du 26 juillet 2015 <<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id>>.

⁷⁶ JORF n° 0278 du 1 décembre 2015 <<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031549747&categorieLien=id>>.

⁷⁷ Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [2006] OJ L 105/54 13.4.2006 <<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>>.

disposition gives to the Prime Minister, after consultation of the *Commission nationale de contrôle des techniques de renseignement*, the power to order to communication service provider in their networks to activate devices able to surveil communication metadata in bulk, to ‘find connections susceptible of revealing a terrorist menace’. In other words, a broad authority is given to government, who is allowed to control communication also in absence of a specific connection with a demonstrated crime or attempt.

This is relevant in this work, especially because of the effects that the use of such strategies has on equality.

To be sure, even citizens are subject to the same surveillance powers, and are similarly not entitled to oversee decisions. Though, there is evidence that such restriction of privacy and self-determination, even when formally does not discriminate foreigners, results in a substantial inequality. It is undeniable that preventive data-driven measures create and deepen discriminations based upon nationality and residence. As stated in literature, ‘the use of algorithmic profiling [...] is, in a certain way, inherently discriminatory: profiling takes place when data subjects are grouped in categories according to various variables, and decisions are made on the basis of subjects falling within so-defined groups’.⁷⁸ Indeed, as explained above, algorithms of data mining automatically find recurrent correlations and deduct predictions from them. For example, a bank could infer – by applying such automatic calculations to its customers’ history – that 70% of the people living in a neighbourhood have been insolvent; hence, it could decide to refuse conceding loans to the residents of that area. Sure, a single individual could be among the 30% of people who would have been able to pay back, but this is not essential in the activity of a bank, because accepting a percentual of mistake is still more convenient than spending time and money to analyze each particular instance.⁷⁹ What is more, sometimes “non-interpretable” procedures are used, i.e. algorithms which work well on big numbers, because they use a particularly high number of variables, but, for the same reasons, are not explicable and understandable for a human brain.⁸⁰

Such discrimination – that is hardly acceptable in inter-private relationships – is even more critical in counter-terror intelligence. Firstly, intelligence decisions affect fundamental rights. So, an algorithmic analysis cannot determine an outright presumption of guiltiness, because this would contrast with the equal application of *habeas corpus*, that imposes a presumption of innocence. Rather, in every democratic system disparity has to be rationally explained in light of the objective of the norm. Secondly, some legal differentiations are particularly critical in democracies, and race and nationality – which are the object of this research – are exactly among them. This is one of the reasons why, in principle, the data

⁷⁸ Bryce Goodman and Seth Flaxman ‘EU regulations on algorithmic decision-making and a «right to explanation»’ (2016) Paper presented at the ICML Workshop on Human Interpretability in Machine Learning of 2016, 28/6/2016 <<http://arxiv.org/pdf/1606.08813v1.pdf>>, 27.

⁷⁹ Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (tr. Roberto Merlini, Houghton Mifflin Harcourt 2013), 25.

⁸⁰ Tal Zarsky, ‘Transparent Predictions’ (2013) 4 University of Illinois Law Review <<http://ssrn.com/abstract=2324240>>, 1519-1521.

subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (Article 22, GDPR). As well-known, this provision is among the ones that can be derogated for security reasons; though, as explained before, this does not allow a total neglect of the proportionality principle. Rather, reasonableness has been recognized by the Court of Justice as a fundamental principle, still in place when it comes to crime prevention.

Hence, surveillance laws shall contain strict provisions posing limits and independent oversights to the police access to data. Though, such regulations are lacking in the aforementioned Acts. In their absence, reasonableness is hard to ascertain and ensure.

The first motivation is that some algorithms make it impossible to give an account of the decisions, because some formulas bring to “non interpretable” choices, which cannot be reconstructed by human brain. A solution could be to avoid employing such methods in a counter-terrorism context, and only use procedures that can be explained and argued. But, once again, laws do not provide a similar ban, so that the choice is left almost exclusively to intelligence services and to enterprises to which data mining is outsourced.

The second motivation is that the very same preventive approach is problematic in this sense. Indeed, while sanctions are visible and act against visible and proofed facts, prevention restrains human rights before the violation, and it is bound to use the truth of intelligence in substitution of the factual one.⁸¹ The same occurs for free speech: surveillance generates mechanisms of self-censorship. These ones sometimes hit illicit expressions, susceptible of triggering or encouraging a crime, but some other times strike the bare dissent, which is precious for democracy. In both cases, if the limitation of rights happens before the facts, no judiciary proceeding or political analysis can be able to state in a definite way what is the real danger brought by that person and, thus, if the preventive measure has actually saved human lives.

Such risks are not speculative. Counter-terror provides immediate examples of possible discrimination: probably statistics would reveal that attackers are mainly young males, coming from Arabic Countries and adhering to Islamic religion.⁸² According to these calculations, everyone having these characteristics shall be specially surveilled. Moreover, such predictions tend to induce ‘self-fulfilling cycles of bias’:⁸³ the fact of spying certain categories with greater attention means by itself that more crimes will be discovered within them, even if the criminality rate is not much higher than the average one. Though, the

⁸¹ Antoinette Rouvroy and Thomas Berns, ‘Le nouveau pouvoir statistique’ (2010) 40 *Multitudes* <http://www.cairn.info/revue-multitudes-2010-1-page-88.htm>, 92-93; Giorgio Agamben, ‘Giorgio Agamben: « De l’Etat de droit à l’Etat de sécurité »’ *Le Monde* (23 July 2015). <http://www.lemonde.fr/idees/article/2015/12/23/de-l-etat-de-droit-a-l-etat-de-securite_4836816_3232.html>.

⁸² Francesca Bignami, ‘Toward a Right to Privacy in Transnational Intelligence Networks’ (2007) 48 *Boston College Law Review*, 6.

⁸³ Alessandro Mantelero, ‘Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection’ (2016) 32, 2 *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 3-4.

mere frequency of crime attempts discovered is a circumstance that can impress and strengthen social stigma towards a given community.

However, in some cases, foreigners are expressly excluded from some privacy safeguards. This is what happens, for example, to the French *LOI n° 2015-1556*, which only applies abroad, or in the US, where the guarantees of FISA are not applicable to foreigners which are not located in the national territory. Still, discrimination does not effectively protect nationals, because repressive rules – once introduced – can be easily expanded, and, however, their limitations are easily circumvented by governments.⁸⁴ For example, as to FISA, the bulk metadata collection of communication abroad also allows to gather US persons' data “incidentally”, i.e. while U.S. persons are communicating with foreign people. Moreover, States stipulate mutual agreements with each other, in which one Party engages to provide the other Party with the latter citizens' data, and *vice versa*. So, each Party can spy on its own nationals by availing itself of the other Party's more favourable surveillance conditions.⁸⁵

This casts a shadow on the reasonableness of this kind of discrimination: it does not effectively safeguard citizens, but rather causes a “race to the bottom”. Being circumvented by governments, they provide loopholes to nationals' privacy safeguard, since eventually the harsher rules, approved for foreigners, are also used for citizens. What is more, differentiating on the basis of nationality is not even consistent with the intrinsic rationality of security measures. A terrorist ought not to be an alien, and in facts many attacks have been brought by “lone wolves” who are born and grown up in the same territory. Hence, the only plausible rationality of such norms is in the rhetoric of emergency: harsh measures are better accepted if they appear to hit some “others” perceived as clearly separate from “us”,⁸⁶ and lacking of the right to vote.

This mirrors the general approach of counter-terror, that has used the metaphor of “war on terror” to evoke an “us”- “them” dichotomy and the conflict with democratic values, but still remained unable to identify an external enemy, as any war would suppose. For example, in the United States after September 11th, 2001, terrorists from abroad have been included in a new juridical category, named “enemy alien”. Which is to say that they were not considered ordinary criminals, due to the severity of their acts, and so were not entitled to the ordinary guarantees of due process; though, they were even not external enemies in a traditional war, and so were not protected by Geneva Conventions. Hence, they were somehow conceived not only as foreigners, but also as “enemy of humanity”⁸⁷, not

⁸⁴ Privacy and Civil Liberties Oversight Board, ‘Report on the Telephone Records Program Conducted under Section 702 of the Foreign Intelligence Surveillance Act’ (2 July 2014) <<https://www.pclob.gov/library/702-Report.pdf>>, 137-140.

⁸⁵ Joshua Rozenberg, ‘Spies may not like the Anderson plan – but their world needs a revolution’ (The Guardian, 11 June 2015) <<http://www.theguardian.com/commentisfree/2015/jun/11/spies-gchq-anderson-snoopers-charter-bulk-surveillance-public-trust>>.

⁸⁶ Oren Gross, ‘Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?’ (2011) Minnesota Public Law Research Paper No. 03-2 <<http://ssrn.com/abstract=370800>>, 1082-1085.

⁸⁷ Carl Schmitt, *Begriff des Politischen* (tr. Pierangelo Schiera, Duncker & Humblot, 1932), 139 ss.

deserving guarantees at all:⁸⁸ as in the Agambenian metaphor of “camp”,⁸⁹ they were caught in the legal system only in a view of depriving them of both constitutional and international protections.

In conclusion, counter-terror shows that States have not completely abandoned their sovereign prerogatives with globalization and show, instead, their ‘gorgon’s head of the power’⁹⁰ when it comes to protect their unitary interests. So, a radically different attitude is used, compared to the internationalizing tendency of trade law: races and nationalities keeps being relevant for regulation, and foreigners – far from being involved in decisions – are, oppositely, caught in intelligence procedures that they cannot even observe. Moreover, there is no contradiction between the two tendencies; oppositely, private mass collections of data are instrumental to governments’ – and even businesses’ – surveillance.

As remarked before, this is also relevant with regard to self-determination and democratic control, since privacy is an essential part of personal autonomy, and transparency a necessary requirement for participation.

In light of these observations, the type of international participation described above – with regard to trade law – seems to be a narrow exception, rather than a general rule. Namely, such privilege is due to economic factors, that have intersected the traditional criterion of citizenship. Paradoxically, along with the first criterion, EU and Member States choose to discriminate some foreigners and negotiate with some others, putting at stake everyone’s fundamental rights.

Such gap is a contradiction in the EU law system, which is based on democracy and fundamental rights, as well as solidarity (Art. 27 and following, Nice Charter), inclusion (Art. 20-26, Nice Charter) and social cohesion (Art. 3 Treaty on European Union, Art. 174 Treaty on the Functioning of the European Union). This is especially true in the Internet, which could be the field, and the technical means, allowing to overcome national boundaries. Hence, from this point of view, the question becomes how participation can become more equal, especially in light of the nature of the web.

4. Conclusions: Towards an Inclusive (Digital) Citizenship

The brief account given has shown that non-citizens are not excluded from political rights in an equal manner; rather, some of them are involved – even in a leading role –

⁸⁸ Agustin José Menéndez, ‘Bush II’s Legal and Constitutional Theory: The Constitution of Emergency between Law and Propaganda’, in Bev Clucas, Gerry Johnstone and Tony Ward (eds.), *Torture: Moral Absolutes and Ambiguities* (Nomos 2009), 8-11.

⁸⁹ Giorgio Agamben, *Homo Sacer: Il potere sovrano e la nuda vita* (Einaudi 2005), 188-190.

⁹⁰ The expression has been used by Hans Kelsen, in *Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer*, Vol. 3 (Walter de Gruyter 1927).

in decision-making, while some others are targeted to violations of fundamental rights exactly because they cannot vote.

In sum, a new cleavage seems to emerge in the construction of the democratic community: in substance, the distinguishing factors are wealth and economic power.

Even more interesting is to notice that such phenomenon is verified not only among different classes of non-citizens, or among average citizens and powerful non-citizens, but also among citizens themselves. In other words, the globalization of legal phenomena highlights and formalizes a main flaw which is structural in our democracies: that the equation between citizenship and political participation has hardly ever corresponded to a concrete reality.⁹¹ Indeed, in our communities, even citizens have always experienced phenomena of social disparity which exclude them from the enjoyment of human rights and political participation. Indeed, a traditional challenge of democracy is that participation subtracts time from productive activities, and so prevents those who strive for a living wage from being fully included in the democratic life. More generally, citizenship has never proved to be a tool of inclusion, but, rather, an excuse to exclude certain non-nationals and so reinforce the Leviathan's authority. As wars and emergency show, an "external enemy" is often created to strengthen the idea of a "national general interest" and build consensus around State decisions. This construction is often fictional, used to pacify the internal lines of conflict and mobilise the have-nots, who otherwise would have little at stake in the haves' wars and security issues.⁹²

Though, this disparity will be even formalized, if governments engage in procedures of selective dialogue with stakeholders.

As to the regulation of the Internet, market law seems to drive to globalization, and even EU harmonization, more than the universality of rights. According to some authors, trade law is by now the most successful attempt to govern contested Internet issues through international legal regimes.⁹³

The World Wide Web, born as the realm of self-regulation and self-determination, has become an area where the State does not disappear, but enacts forms of pervasive

⁹¹ This is also true, sometimes, in a territorial meaning, where there are economic disparities within the different area of a State. Eg, as to the Italian debate, see: Michele Belletti, 'I "livelli essenziali delle prestazioni concernenti i diritti civili e sociali..." alla prova della giurisprudenza costituzionale: Alla ricerca del parametro plausibile...' (2003) 3 *Istituzioni del federalismo: rivista di studi giuridici e politici*, 614; Massimo Villone, *Italia, divisa e diseguale: Regionalismo differenziato o secessione occulta?* (Editoriale Scientifica 2019), provisional version <https://cambialmondo.files.wordpress.com/2019/04/20190316-villone-italia-divisa-e-diseguale-napoli-2019_compressed.pdf>, 83 ss.; Andrea Patroni Griffi, *Regionalismo differenziato e uso congiunturale delle autonomie* (2019) 1 *Rassegna di Diritto Pubblico Europeo Online*, 18-19. Concerning other 'unfulfilled promises of democracy', see: Lorenzo Chieffi, 'I paradossi del costituzionalismo contemporaneo e le "promesse non mantenute" dalle democrazie occidentali', in Id. (ed.), *Rappresentanza politica, gruppi di pressione, élites al potere : atti del Convegno di Caserta 6-7 maggio 2005* (Giappichelli, 2006), 11-46.

⁹² It has been noticed that security is a concern which affects more those who feel that they have an acquired status that they can lose, and *vice versa*: Conor Gearty, *Liberty and Security* (Polity Press, 2013), 38.

⁹³ Jack Goldsmith and Tim Wu, *Who controls the Internet? Illusions of a borderless world* (Oxford University Press 2006), 167.

surveillance and enforces a juridical space favourable to free market. This is also the consequence of regulatory processes, that have been privileging economic actors over the others. So, in this new regulatory field, inequalities have changed and interlaced with each other, but not disappeared.

Then – from the perspective of fundamental rights – the mindset shall not be to wonder, in general terms, how decision-making can be opened to international civil society actors. Rather, the main question is how to make the Web a space of equal participation, even for the disadvantaged and marginalized ones.⁹⁴ This would need a positive intervention of public powers, both at national and supranational level, able to remove the social and economic obstacles to inclusion.

Indeed, the horizontal and distributed architecture of the Internet is not decisive by itself. Democracy ‘does not follow automatically from the values associated with new technical arrangements for online information production and sharing’.⁹⁵

As a matter of facts, never has the Web been democratic, in the meaning of a social democracy. In its first phase, it was regulated by its users, which were indeed a “community of equals”, but were only an élite of experts, computer scientists and researchers. Hence, there was a form of ‘liberalism through protocols’, aiming at ‘organizing platforms in the most effective way possible, but also less hierarchical, to develop individuals’ autonomy’.⁹⁶ Though, when masses became able to access, the digital world turned inapt to be a space of equality. It was invaded by social, economic, political and geopolitical issues, as well as by disparity, that – online as offline – needed a public power. Though, at that time – exactly as now – a way to effectively govern these matters were yet to be found by States and supranational organizations. In few words, the fact of treating the Internet as a ‘virgin space’ has contributed to make it ‘appropriable’ from a juridical point of view: while great emphasis was given to the collaborative creation, less attention was paid to the either exclusive or collective appropriation of the final products⁹⁷

Later on, these dynamics of appropriation have generated a “tragedy of anti-commons”,⁹⁸ by subtracting to social utility non-rival goods, that could have been shared collectively without consuming the resource. Big data and algorithms have been concealed behind trade secrets. Even administrations sometimes are tempted to keep them as a private property, managed in an exclusive way or even destined to generate incomes.⁹⁹

⁹⁴ This involves an assumption of political responsibilities with regard to the issue of inequalities: Sandro Staiano, ‘Diseguaglianze e politiche dell’eguaglianza: profili teorici e istituzionali’ (2016) 144 *Sociologia del lavoro*, 115-116.

⁹⁵ Robin Mansell, *Imagining the Internet* (Oxford University Press 2012), 60.

⁹⁶ Benjamin Loveluck, *Réseaux, libertés et contrôle. Une généalogie politique d’Internet* (Armand Colin 2015), 63.

⁹⁷ Dominique Cardon, *La démocratie Internet. Promesses et limites* (Seuil/La République des Idées 2010), 32-33; Robin Mansell, ‘Power, hierarchy and the internet: why the internet empowers and disempowers’ (2016) *Global Studies Journal* <http://eprints.lse.ac.uk/64855/>, 22-23.

⁹⁸ Barbara J. Evans ‘Barbarians at the Gate: Consumer-Driven Health Data Commons and the Transformation of Citizen Science’ (2017) 42, 4 *American Journal of Law and Medicine*, 15.

⁹⁹ Danièle Bourcier and Primavera De Filippi, ‘Vers un nouveau modèle de partage entre l’administration et les communautés numériques’, in Nicolas Matyjasik and Philippe Mazuel (eds.), *Génération Y et gestion publique : quels enjeux ?* (Comité pour l’histoire économique et financière de la France 2012), 4.

Exclusive appropriation of data by the Internet Service Providers (ISPs) has also generated informational oligopolies in the digital space. This is a consequence of indirect network effects, that make the advertising revenues flow towards the already dominant actors. Indeed, on the one side, advertisers prefer to invest in the most crowded platforms, since they acquire more data, thus guaranteeing a more effective targeted marketing. On the other hand, the incumbent's service is more appealing to consumers, because the dominant player hosts a larger community and has more profits to invest in quality. Therefore, a "snowball effect" hits the newcomers, who fail to gain customers and consequently are unable to gather data in order to procure advertising venues and cover the initial costs.¹⁰⁰ Moreover, oligopolists have started to gain control of information, until they have acquired enough power to become an equal partner for the States in law-making.

If inequalities online are linked to intellectual property, this is where positive action would be needed.¹⁰¹ Notwithstanding that, EU seems to still act mostly in favour of the Digital Single Market and the growth of European enterprises. This was evident with two of the most recent Acts, concerning the regulation of online communications and commerce: the GDPR and the Copyright Directive¹⁰².

The first one harmonises data protection law imposing more effective sanctions and stricter requirements to private data collection. That given, the Regulation facilitates circulation of data in the EU, by preventing restrictions based on national privacy laws. Though, it has failed to consider an issue crucial for substantial equality: the different bargaining power of parties. Article 7 states that «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». Though, it does not provide an outright ban of such contractual clauses. This circumstance makes it impossible to effectively ensure that consent is freely given, because in that case even the better-informed consumer, sensitive to his privacy, would accept to give data away, since some services are needed in everyday lives.¹⁰³

¹⁰⁰ Autorité de la Concurrence and Bundeskartellamt, *Competition Law and Data* (2016) <http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf>, 718-733; Maria Orefice, 'Big Data. Regole e concorrenza' (2016) 4 *Politica del diritto*, 17-51.

¹⁰¹ The turn towards putting enclosures in the Internet is largely due to the opinion that property rights are needed to encourage the production of such immaterial goods, by ensuring a remuneration to creators. Though, it is very controversial that intellectual property would be the best answer for this need: Dean Baker, Arjun Jayadev and Joseph Stiglitz, *Innovation, Intellectual Property, and Development: A Better Set of Approaches for the 21st Century* (*Accessibsa.org*, July 2017) <https://www.accessibsa.org/media/2017/12/Innovation-Intellectual-Property-and-Development.pdf>, 8-25.

¹⁰² COM (2016) 593: Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, Procedure 2016/0280/COD, <<https://data.consilium.europa.eu/doc/document/PE-51-2019-INIT/en/pdf>>.

¹⁰³ Article 29 Data Protection Working Party, 'Working Document 02/2013 providing guidance on obtaining consent for cookies' (1676/13/EN; WP 208, 2 October 2013) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf>, 5. Cfr. Agencia Espanola de Proteccion de Datos, 'Guía Sobre el Uso de las Cookies' (29 April 2013)

The Copyright Directive gives an answer to the most pressing instances of entertainment businesses,¹⁰⁴ by imposing measures that, according to different voices, threaten open access to culture.¹⁰⁵ In particular, the most contested ones are the provisions of Article 15, which creates new rights for publishers, and Article 17, which appears to oblige ISPs to install filters to impede the violations of copyright perpetrated by third parties' contents.

On one hand, it is true that such measures seem to hinder the mere *laissez-faire* economy of the Internet. Though, on the other hand, commentators have noticed that they eventually do not harm big ISPs, which already act as nearly monopolists in the respective markets. Indeed, most of them have already installed filtering mechanisms. Oppositely, such measures amount to a hardly sustainable burden for smaller enterprises, which could even discourage start-ups from growing beyond the threshold of application of the Article 13.¹⁰⁶ Hence, it risks reinforcing the strong ones and increasing the barriers to the entry of newcomers in the markets. This is why, even though every monopolist's preference is deregulation, 'their second preference was also always going to be lots of regulation, provided that they could afford the regulatory costs and no one who might challenge them could'.¹⁰⁷

Moreover, even if one of the declared objectives of the Directive is to safeguard the creators' rights, the final text failed to align with the best practices of the Member States in regulating the contractual relationships between authors and industries.¹⁰⁸ Yet, protecting the immaterial workers' labour shall be the first aim of a copyright regulation, as well as the only reason justifying the limitation of access to culture.

In sum, both instances – the GDPR and the Copyright Directive – show that, even on the Internet, the path of EU harmonisation is driven by economy, rather than social rights.

<https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf>, para. II.3.B).viii.

¹⁰⁴ Mike Masnick, 'Legacy Copyright Industries Lobbying Hard For EU Copyright Directive... While Pretending That Only Google Is Lobbying' (*TechDirt.com*, 12 December 2018) <<https://www.techdirt.com/articles/20181212/07074641205/legacy-copyright-industries-lobbying-hard-eu-copyright-directive-while-pretending-that-only-google-is-lobbying.shtml>>.

¹⁰⁵ 'Article 13 Open letter – Monitoring and Filtering of Internet Content is Unacceptable' (2017), Open letter from 57 signatories asking EU policy-makers to delete Article 13 of the new proposal on copyright in the digital single market <https://www.liberties.eu/en/news/delete-article-thirteen-open-letter/13194?utm_source=POLITICO.EU&utm_campaign=91f2de513a-EMAIL_CAMPAIGN_2017_10_16&utm_medium=email&utm_term=0_10959edeb5-91f2de513a-190133949>.

¹⁰⁶ Lenard Koschwitz, 'The European Parliament is discussing an expiry date for startups' (*Tech.eu*, 11 July 2017) <<https://tech.eu/features/16029/european-parliament-expiry-date-startups/>>.

¹⁰⁷ Cory Doctorow, 'Article 13: If You Want To Force Google to Pay Artists More, Force Google to Pay Artists More' (*EFF.org*, 21 November 2018) <<https://www.eff.org/deeplinks/2018/11/article-13-if-you-want-force-google-pay-artists-more-force-google-pay-artists-more>>.

¹⁰⁸ Directorate General for Internal Policies – Policy Department for Citizens' Rights and Constitutional Affairs Legal and Parliamentary Affairs, 'Strengthening the Position of Press Publishers and Authors and Performers in the Copyright Directive' (2017) PE 596.810 <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/596810/IPOL_STU%282017%29596810_EN.pdf>, 43 ss.

This points out that the Union has not overcome its original vocation, yet, and it is still more prone to markets than to equality and cohesion within and among the territories.

Now, the challenge is to go beyond the commercial ratio of the “four freedoms”, and start building a European digital citizenship as a tool of political and economic inclusion.

ABSTRACT

L'articolo, dal punto di vista dell'ordinamento dell'Unione Europea, osserva come gli attori privati sono coinvolti nella regolazione pubblica, usando come caso di studio un fenomeno transnazionale: Internet e, in particolare, la circolazione dei *big data*. L'obiettivo è di esplorare le contraddizioni e le disparità sociali che emergono nell'attribuzione di diritti politici agli stranieri.

In particolare, comparando due principali ambiti – i trattati di libero scambio e le norme antiterroristiche – la ricerca evidenzierà che non vi è corrispondenza biunivoca tra il fatto di non avere la cittadinanza e quello di essere esclusi dalla partecipazione democratica. Piuttosto, un criterio diverso sembra emergere: mentre, da un lato, vi sono ancora discriminazioni nel godimento dei diritti fondamentali, dall'altra parte, attori internazionali sono addirittura coinvolti nella decisione, quando sono esponenti di interessi forti.

In conclusione, lo studio mostra – nel campo dei *big data* – come il mercato sembra portare all'armonizzazione nell'UE più dell'universalità dei diritti. Alla luce dei principi di solidarietà (artt. 27 ss., Carta di Nizza), inclusione (artt. 20-26, Carta di Nizza) e coesione sociale (art. 3 TUE, art. 174 TFUE), questo solleva il problema di quali punti critici dovrebbero essere affrontati per un coinvolgimento più paritario della società civile nelle decisioni.

This paper, from the viewpoint of the European Union law, observes how private actors are involved in public rule-making, using a transnational phenomenon as a case study: Internet and, particularly, the circulation of big data. The objective is to explore contradictions and social disparities that emerge in the attribution of political rights to non-nationals.

In particular, by comparing and contrasting two main fields – i.e. free trade agreements and counter-terror regulations – the research will highlight that there is no strict coincidence between non-citizenship and exclusion from democratic participation. Rather, a different criterion seems to emerge: while, on the one hand, there are still discriminations in the enjoyment of fundamental rights, on the other hand, international actors are even involved in decision-making, when they are exponent of vested interest.

In conclusion, the study shows – in the field of big data – how market law seem to drive to EU harmonization, more than the universality of rights. Given of the principles of solidarity (Art. 27 and following, Nice Charter), inclusion (Art. 20-26, Nice Charter) and

social cohesion (Art. 3 TEU, Art. 174 TFEU), this raises the question of which critical points shall be addressed for a more equal involvement of civil society in decision-making.

PAROLE CHIAVE: *big data*, antiterrorismo, trattati di libero scambio, partecipazione, discriminazioni

KEYWORDS: big data, counter-terror, free trade agreements, participation, discriminations