III.2

# The Algorithmic Governance of Administrative Decision-Making: Towards an Integrated European Framework for Public Accountability

SUMMARY: 1. Introduction and Outline of the Study- 2. Context and Features of the 'Algorithmized' Public Administration- 2.1 The Private-Public Partnerships for the Delivery of Algorithm-driven Public Services- 3. Legal Obstacles to Accountable Algorithmic Public Decision Making- 3.1. The Subjective Obstacle: the Unsuitability of Administrative Law Principles of Accountability and Transparency- 3.2 The Objective Obstacle: the Intellectual Property Protection of Privately-Developed Algorithms- 4. The General Data Protection tools of Transparency and Accountability- 5. Conclusions

**1.** The shift from a big data- to an algorithm-driven economy, currently changing the face of many private domains, is ultimately touching also upon the public sector. Here, the growing use of algorithms for the purposes of decision-making in the field of public services is sensitively transforming the way in which public action is carried out.

Examples of algorithm-driven public decisions are blossoming in the USA and are starting to become apparent also in the European Union. In the USA, for example, and more specifically in the city of New York, the local government has employed algorithms in order to carry out the most various activities, ranging from the allocation of police officers, firehouses, public housing, food stamps[525]. Also within European Union Member States, examples of algorithmic employment in the public sector are proliferating. In these regards, mention must be made of the practice of profiling the unemployed done by the Ministry of Labour and Social Policy in Poland[526]. In France, with the declaration of the state of emergency after the last terror attacks, the police has started employing a software that predicts where and when crime is going to occur[527]. Also the Dutch tax authority is relying on algorithm-driven correlations to increase the efficiency of the tax system[528].

All these examples show that the enhancement of computational capabilities is structurally changing the ways in which public services are delivered. This paper moves from this acknowledgment and enquires the legal pitfalls of this newly emerging scenario from a European Union law standpoint.

Against this backdrop, the paper is structured into two sections.

525 J. Powles, *New York City's Bold, Flawed Attempt to Make Algorithms Accountable*, published on the 20th December 2017 on the New Yorker, online available at https://www.newyorker.com/tech/elements/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable.

526 This is documented by J. Niklas, K. Sztandar-Sztanderska, K. Szymielewicz, *Profiling the unemployed in Poland: Social and Political Implications of Algorithmic Decision-making*, 2015, online available at https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf, *passim*.

527 K. Kubler, *Surveillance, Power and Algorithms in France's State of Emergency*, in *Big Data & Society*, July-December 2017, p. 1 ff..

528 C. Quelle, *Privacy, Proceduralism and Self-Regulation in Data Protection Law*, in *Teoria Critica della Regolazione Sociale*, 2017, p. 3.

The first section illustrates the features of the 'algorithmized' public administration, showing how the increasing reliance on data-driven systems, obliges the public sector to lean on private companies' technical expertise and infrastructure. In light of the peculiarities of the emerging environment, the second section will enquire the (in)effectiveness of traditional European administrative law tools in respect to accountability objectives. Hence, the analysis will turn to the consideration of the new provisions of the General Data Protection Regulation. The study will conclude with some systemic considerations regarding the need to adopt an integrated approach between traditional administrative law tools and business-centred provisions entailed in the GDPR.

**2.** Algorithm-driven decision-making has first proliferated in the private sector where it has become the major business model in so-called digital markets, exploiting users' personal data for commercial purposes- *i.e.* is primarily for predicting and thus orienting users' commercial behaviour- and thus with the primary aim of maximising companies' profits[529]. The employment of such massive processing techniques in the public sector has come behind and has sensitively different features and outcomes in respect to the private and commercial-oriented sphere.

Lately, algorithmic processing infrastructures have triggered governments' attention that have over time become large depositories of citizens' personal data[530]. The digitisation of public administrations' databases has soon enabled a faster consultation of collected and available datasets.

These patterns have been amplified with the increasing employment of algorithms as processing infrastructures of public administrations' collected data. Through processing algorithms, data are not any more a static evidence merely working as a support of public decision making carried out by public officials, but have themselves become, in those sectors where algorithms are employed, the centre and the source of decision-making[531].

The increasing quantitative and qualitative importance of algorithms for the purposes of decision making in various fields of the public sector is transforming algorithms into outright governance tools: algorithms are indeed employed as a means for authorities to manage "individual behaviour and allocate resources" It thus appears that, similarly to the private sector, also the public sector is being overtaken by a new form of algorithmic governance[532].

Through the 'algorithmisation' of public action, public affairs begin to be regarded as technical problems that need to be addressed through technical solutions[533]. With algorithms becoming the engines of public affairs' management, and thus exerting control over society[534], a new form of technocratic public governance emerges, apparently providing impartial and scientifically-grounded decisions on the basis of data-driven models. These data-driven models are

529 G. Comandè, *The Rotting Meat Error: From Galielo to Aristotele in Data Mining?*, in *EDPL*, 2018, 4, 3, p. 270.

530 G. Carullo, *Big Data e Pubblica Amministrazione nell'era delle banche dati interconnesse*, in *Concorrenza e Mercato*, 2016, 23, p. 181 ff..

531 K. Yeung, *Algorithmic Regulation: a Critical Interrogation*, in *Regulation & Governance*, July 2017, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972505, p. 20 ff..

532 The term 'algorithmic regulation' was first coined by T. O'Reilly, *Open Data and Algorithmic Regulation*, in B. Goldstein, L. Dyson (ed.), *Beyond Transparency - Open Data and the Future of Civic Innovation*, San Francisco, 2013, p. 289-300.

533 R. Kitchin, *The real-time city? Big data and smart urbanism*, in *GeoJournal*, 2014, 79, 1, p. 9.

534 M. Janssen, G. Kuk, *The Challenges and Limits of Big Data Algorithms in Technocratic Governance*, in *Gov. inform q.*, 2016, 33, p. 371.

ultimately creating a new form of "technological determinism" given by algorithms' predictions triggering public action[535]. Algorithms indeed rely on "actuarial predictions" given by the correlations between the features or characteristics drawn from the data[536]. As framed in these terms, the "algorithmised" public governance is drastically overturning the traditional manners of conduction of public affairs[537], ordinarily based on what some strand of the literature has called "clinical predictions", consisting in public officials' management of specific situations[538].

Conversely, in the current technological environment, the human evaluative factor is increasingly being replaced by machine-driven calculations[539]. Hence, in respect to these automated processing systems and the readily usable knowledge they generate, public administrations and public officials specifically in charge of exercising public action become mere executors of evaluations entirely carried out through automated systems. In other terms, algorithms are being deferred the substantial part of the decision-making process, whereas public officials maintain only the function of formalising and practically enacting judgements taken by the machine-driven model.

**2.1.** Governments' technical limitations make private contractors key components of data-driven decision making processes[540]. The technological support provided by private corporations has thus become of primary importance for addressing the public need in an era of technological disruption, and thus for acquiring the analytics necessary for "smart" urban systems.

The outsourcing of processing infrastructures needed for the handling of the enormous available datasets is formally occurring through public-private partnerships[541], which have been defined in the literature as "any arrangement between government and the private sector in which partially or traditionally public activities are performed by the private sector"[542].

These private-public partnerships create a bi-directional flow of datasets that benefits both the private and the public stakeholders involved. Indeed, through these service contracts, publicly owned data flow into the processing infrastructures offered by private companies. In this way, these companies acquire control of such data, which thus come to aliment and thus enrich their processing

535K. Yeung, *Algorithmic Reguation: a Critical Interrogation*, cit. p. 20.

536 R. Brauneis, E.P. Goodman, *Algorithmic Transparency for the Smart City,* in *YJoLT*, 2018, 103, p. 111 ff..

537 M. Tenney, R. Sieber, *Data-Driven Participation: Algorithms, Cities, Citizens, and Corporate Control*, in *Urban Planning*, 2016, 1, 2, p. 101 ff..

538 R. Brauneis, E.P. Goodman, *Algorithmic Transparency for the Smart City,* cit. p. 111 ff..

539 This is the general definition of governance given by J. Black, (2014) *Learning from Regulatory Disasters*. LSE Law, Society & Economy Working Papers 24/2014, online available at http://eprints.lse.ac.uk/60569/1/WPS2014-24_Black.pdf.

540 T. Filer, *Developing AI for Government: What Role and Limits for the Private Sector?,* online available at https://www.bennettinstitute.cam.ac.uk/blog/developing-ai-government-what-role-and-limits-priv/. For a general assessment, see P. Vincent-Jones, *The Regulation of Contractualization in Quasi-Markets for Public Services*, in *Pub. L.*, 1999, p. 304.

541 For a deeper assessment over the issue of private-public partnerships, although specifically focused on the police sector, see N. Purtova, *Between GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public-Private Partnerships*, in *IDPL*, 2018, 8, 1, p. 52 ff..

542 E.S. Savas, *Privatization and Public-Private Partnerships*, Chatham House, 2000, 4. See also European Commission, *Green Paper on Public-Private Partnerships and Community Law on Public Contracts and Concessions*, April 2004, p. 9.

systems[543]. On the other side, private corporations' data- and the information they entail-, originally feeding the provided algorithmic infrastructure, become equally relevant for the purposes of public actors: this privately-owned data that has originally trained the algorithmic model has a sensitive impact on the results rendered by the processing system; it is thus this data that ultimately defines public decision-making. In addition to this, governments also often make specific agreements for accessing privately held data in order to strengthen the evidence given by public datasets[544]. The agreements specifically designed for the transfer of datasets from private actors to public bodies often accompany the private-public partnerships aimed at providing the processing infrastructure[545].

The proliferation of private-public partnerships for the allocation of "algorithmised" public services are giving rise to an interesting process of infiltration of market rationales in the determination of public actions' courses. With privately-constructed algorithms shaping public interventions, private corporations are gaining an increasing important role in the organization and orientation of the public sector[546]. The related spillover effect is that the growing involvement of private corporations in public affairs causes the marketization of public services given that corporations increasingly provide these processing services to public actors in order to increase their profits. This phenomenon has been elsewhere called 'corporisation' of city governance[547], bringing about the risk of corporate capture of public power[548].

The delegation of the decision making site governing the allocation of public services to private actors requires a robust regulation and a strong enforcement in order to avoid an uncontrolled interference of the technology sector in public matters: with the rise of public-private partnerships for the machine-driven delivery of public services, governments' accountability results to be intrinsically connected to- and thus depends on- the transparency of companies' processing activities.

**3.** The above-outlined paragraphs have shown how the rising employment of algorithms in the public sector is sensitively transforming the dynamics of public decision-making.

The increasing involvement and role of private informational and technological assets in the delivery of public services has two main effects. On the one hand, indeed, it "neutralizes" the administrative law rules of accountability and transparency that traditionally guard the traceability of public administrations' actions. This occurs because these rules only apply to public administrations- that, as illustrated above, are emptied by algorithms of substantial decision making functions-, and thus cannot be applied to private contractors (*subjective obstacle*).On the other hand,

543 See L. Edwards, *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*, in *EDPL*, 2016, 2, p. 28-58.

544 For an analysis regarding government access of privately held data in the UK, see I. Brown, *Government Access to Private Sector Data in the United Kingdom*, in *IDPL*, 2012, 2, 4, p. 230 ff..

545 F.H. Cate, J.X. Dempsey, I.S. Rubinstein, *Systematic Government Access to Private-sector Data*, in *IDPL*, 2012, 2, 4, p. 195 ff..

546 R. Brauneis, E.P. Goodman, *Algorithmic Transparency for the Smart City*, cit. p. 114, where the Authors recall the registration by IBM of the trademark 'smart city".

547 R. Kitchin, *The real-time city? Big data and smart urbanism.*, cit. p. 5. See also J.S. Hiller, J. M. Blanke, *Smart Cities, Big Data, and the Resilience of Privacy*, in *Hastings L.J.*, 2017, 68, p. 309.

548 R. Brauneis, E.P.Goodman, *Algorithmic Transparency for the Smart City*, in *YJoLT*, 2018, 103, p. 20. See L. Edwards, *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective,* cit. p. 32.

conversely, it operationalizes the whole set of intellectual property tools that companies have at their disposal in order to protect the products of their technological research & development, thus raising substantial barriers for public administrations that turn out to be incapable of accessing the logic underlying the privately-originated machine-driven processes (*objective obstacle*).
These two points will be enquired in the following paragraphs.

**3.1.** The private algorithmic processing infrastructures to which public bodies are increasingly resorting and the private-public partnerships that govern the transfer of such technology call into question some fundamental principles that rule both the political and administrative action, and more precisely the ones related to the accountability and the transparency of public administrations' action. These principles are foundational principles of good governance[549].

The notion of public accountability relates to the political legitimacy of public institutions in democratic systems. More precisely, public institutions' political legitimacy implies a responsabilization of these same institutions in the sense that their actions have to satisfy the public mandate received and that they have to signal such compliance to the citizens who bear the effects of public actions. In this perspective accountability contributes to strengthening the principle of democracy as expressed in art. 6 of the European Treaty and in the Charter of Fundamental Rights of the European Union.

In these regards, it is interesting to recall that the 1998 OECD Principles for managing Ethics in Public Services explicitly acknowledges the principle of accountability, stating that "public servants should be accountable for their actions to their superiors and, more broadly, to the public. Accountability should focus both on compliance with rules and ethical principles and on achievement of results (…)"[550]. Along these lines, also the European Commission's White Paper on European Governance stresses the need for clarity with regards to "the roles in the legislative and executive processes" as well as the need for European institutions to "explain and take responsibility" for their actions[551]. Accordingly, the Paper affirms the "need for greater clarity and responsibility from Member States and all those involved in developing and implementing EU policy at whatever level"[552].

Against this backdrop, accountability implies openness of public authorities' interventions, requiring institutions and administrative bodies and agencies to open their activities to the public[553]. The principle of openness not only requires these actors to conduct their work as openly as possible, but also to proactively open their operations to the public. As will be assessed below, administrative

549 C. Harlow, *Global Administrative Law: the Quest for Principles and Values*, in the *EJIL*, 2006, 17, 1, p. 187 ff..
550 OECD, *1998 Recommendation of the OECD Council on Improving Ethical Conduct in the Public Service, including Principles for Managing Ethics in the Public Service*, online available at http://www.oecd.org/gov/ethics/Principles-on-Managing-Ethics-in-the-Public-Service.pdf, p. 76.
551 European Commission, *European Governance- A White Paper*, 25 July 2001, online available at https://ec.europa.eu/europeaid/sites/devco/files/communication-white-paper-governance-com200142820010725_en.pdf, p. 10.
552 *Ibid.*.
553 In these regards, see A. Alemanno, *Unpacking the Principle of Openness in EU law- Transparency, Participation and Democracy*, in *European Law Review*, 2014, 39, 1, p. 72.

openness has an instrumental value for it ensures the participation of civil society in public decision-making and with that the more fruitful enactment of democratic ideals.

Against this backdrop, the principle of accountability is intimately connected to the principle of transparency[554], which is explicitly acknowledged in art. 41.2 of the Charter of Fundamental Rights as part to the right of good administration, requiring institutions to "maintain an open, transparent and regular dialogue with representative associations and civil society".

The principle of transparency is enshrined in art. 15.3 TFEU, providing substantive and procedural rules for the operationalization of such principle. Transparency is highly context-dependent and thus varies depending on the activities that are carried out[555]. The public information released must be up to date, complete- that is, ready for consultation-, and consistent with the original documents held by the administration. It moreover needs to contain the indication of its origin and of how it can be reused.

The quality of transparency is strictly related to the administrations' use of a clear and understandable language of the information posted on the institutional channels of information. The requirement of a clear and plane language of the public information released to the public has been widely acknowledged by the case law of the Court of Justice of the European Union[556], which has stressed that clarity of language in the documents of the public institutions is strictly related to the principles of legal certainty and the protection of legitimate expectations. In these terms, transparency enables the predictability of policy action and is thus the more important the more the specific public action is the result of discretionary powers[557].

Public transparency's golden rule is given by the right of access to public documents, enshrined in art. 15 TFEU, in art. 42 of the ECHR, and in Regulation EC N. 1049/2001 of the European Parliament and of the Council on public access to EU institution documents[558].

As objectified in the right to access, transparency is itself functional to the right of defence and thus directly serves due process rationales[559]. This is well expressed in art. 41 ECHR defining the components of the right to good administration, entailing according to para 2 of the same article i) citizens' right to defence and due process, ii) the right to access to administrative documents and iii) the right to receive explanations regarding public actions.

554 For a theoretical reconstruction, see C. Harlow, *Global Administrative Law: the Quest for Principles and Values*, cit. p.187 ff..

555 *Ibid.*.

556 See, for example, Court of Justice of the European Union, *Administration des douanes v Société anonyme Gondrand Frères and Société anonyme Garancini,* C-169/80, 9 July 1981, online available at http://curia.europa.eu/juris/showPdf.jsf?text=&docid=90884&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=319462, para 17; Court of Justice of the European Union, *Amministrazione delle finanze dello Stato v Srl Meridionale Industria Salumi and others* and *Ditta Italo Orlandi & Figlio and Ditta Vincenzo Divella v Amministrazione delle finanze dello Stato,* C-212/80, 12 November 1981, online avalable at http://curia.europa.eu/juris/showPdf.jsf?text=&docid=91124&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=321098.

557 S. Prechal, M. de Leeuw, *Dimensions of Transparency: the Building Blocks for a new Legal Principle?*, in *REALaw*, 2007, 1, p. 51 ff.

558 So art. 2 para 1 of the Regulation EC N. 1049/2001 of the European Parliament and of the Council on public access to EU institution documents.

559 In these regards, see S. Prechal, M. de Leeuw, *Dimensions of Transparency: the Building Blocks for a new Legal Principle?*, cit. p. 55.

III.2

According to the interpretation given by the literature[560], art. 298.1 TFEU, by stating that "the institutions, bodies, offices and agencies of the Union shall have the support of an open, efficient and independent European administration", extends the principles of accountability and transparency to the entirety of EU administrations, *i.e.* the administrations that act within the territory of the European Union[561].

The emergence of a horizontal chain of stakeholders governing public decision-making courses relying on algorithmic processing infrastructures sensitively challenges the above-outlined framework[562]. As has been demonstrated, indeed, in the networked algorithmised public decision-making environment, the role of the public authority is lessened and substantially substituted by private companies who do not have the typical democratic accountability requirements that, in a representative democracy, traditionally belong to public administrations[563]. Private entities contracting with public authorities for the purposes of delivering algorithmic processing infrastructures are not subject to the accountability and transparency requirements of public subjects. These entities can indeed hardly be considered as "bodies governed by public law", since the definition of such notion under art. 1.9 Directive 2004/18/EC excludes the industrial or commercial character of these bodies[564]. To the contrary, the entities that provide algorithmic processing infrastructures as a support to public authorities' decision-making mostly have a strong commercial and industrial characterization.

Against this backdrop, hence, the achievement of public accountability and transparency in the illustrated terms appears to be primarily obstructed by a subjective obstacle, that is the inapplicability of the principles of good administrative governance to the private entities that are progressively taking the reins of such governance. This means that in the networked algorithmic environment accountability of the public authority diminishes. As a consequence, control of the policy address through traditional administrative law tools becomes less effective.

560 A. Alemanno, *Unpacking the Principle of Openness in EU law- Transparency, Participation and Democracy,* cit. 72.

561 For the notion of EU administrations, see H. Hoffman, G. Rowe, A. Turk, *Administrative Law & Policy of the European Union*, Oxford, 2012, p. 171 ff..

562 For an empirical analysis of the challenges to democratic accountability posed by the contracting activities of public administrations with private entities, see C. Di Martino, J. Scott, *Private Sector Contracting and Democratic Accountability*, in *Educational Policy*, 2012, p. 1 ff..

563 On the issue see P.R. Verkuil, *Public Law Limitations on Privatisation of Government Functions*, Cardozo Legal Studies Research Paper N. 104, 1 March 2005, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=681517, p. 8, affirming that "delegations to private hands in our society come with strings attached that ensure fairness at the individual level and accountability at the political level".

564 Conversely, according to art.1.9 Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public work contracts, public supply contracts and public service contracts, "(…) a body governed by public law means any body: (a) established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; (b) having legal personality; and (c) financed, for the most part, by the State, regional or local authorities, or other bodies governed by public law; or subject to management supervision by those bodies; or having an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law". The provision thus clearly excludes the industrial or commercial nature of the contracting entities in order to be considered a body governed by public law.

In addition to this, public administrations relying on privately-developed algorithmic models are themselves incapable of accessing the information needed to satisfy normative transparency and thus accountability requirements because of the existence of a strong set of intellectual property tools, which run contrary to transparency duties and thus to the enactment of effective public accountability mechanisms.

**3.2.** The European intellectual property framework provides several tools for the protection of corporations' developed algorithms. These are to be found in copyright, database rights and trade secret rights.

Although there have been long discussions regarding the patentability of "computer implemented inventions" [565], the option of patenting softwares has soon been put aside, due to the legal and practical difficulties related to such an extension[566]. The exclusion of the eligibility of the patent as a tool for the protection of algorithms has caused the shift of focus onto other tools of protection.

With regards to copyright protection, the Directive on the legal protection of computers of 2009[567], replacing the previous 1991 Software Directive[568], has redefined the scope of copyright protection of computer programs. The persisting uncertainties around such forms of protection have triggered the intervention of the European Court of Justice in the case *Sas Institute Inc. c. World Programming Ltd*[569]. Here, the Court has clarified that the protection under copyright law of computer programs applies only to "the forms of expression of a computer program and the preparatory design work capable of leading, respectively, to the reproduction or the subsequent creation of such a program[570]", but does not include the functionalities, the programming language of the program, and the format of data files used in a computer of it[571]. By stating so, the European

565 Cf. *Proposal of a directive of the European Parliament and of the Council related to the patentability of computer implemented inventions*, released on the 20th February 2002, online available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52002PC0092. See J Drexl, RM Hilty et. al., *Data ownership and access to data, Position statement of the Max Planck Institute for Innovation and Competition of the 16th August 2016 on the Current European Debate*, Max Planck Institute for Innovation and Competition Research Paper No. 16-10, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165, p. 5-6, stressing that patent "protection (of algorithms) would pose a risk of two negative effects: first, protection of abstract subject-matter would cause needless – and, in the case of algorithms, unreasonable – restraints on competition that, according to current knowledge, would not be economically justified. (…) Second, it is barely foreseeable what markets and sectors would be affected. This makes finding suitable approaches to a regulation seem unrealistic".

566 The Supreme Court of the United States, in *Alice Corp. v. CLS Bank International*, clarified that abstract inventions, such as algorithms, do not become patentable merely because they are implemented on a computer. So *Alice Corp. Pty. V. CLS Bank Int'l*, 134 S. Ct. 234, 2358 (2014). For a comment see Nicholson Price II, *Expired Patents, Trade Secrets and Stymied Competition,* cit. p. 1425.

567 Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L. 111, 5-5-2009.

568 See Council Directive of 14 May 1991 on the legal protection of computer programs, 91/250/EEC, OJ 17-5-91, N.L. 122/42.

569 Court of Justice of the European Union, *Sas Institute Inc. c. World Programming Ltd*., C-406/10, 2 May 2010, online available at http://curia.europa.eu/juris/document/document.jsf?docid=122362&doclang=EN.

570 *Ibid.*, para 37.

571 *Ibid*., para 39. For a comment, see P. Samuelson, T. Vinje, W. Cornish, *Does Copyright Protection Under the EU Software* Directive *Extend to Computer Program Behaviour, Languages and Interfaces?,* in *EIPR*, 2012, 34, 3, p. 158.

Court of Justice has reaffirmed the basic copyright law principle on the basis of which copyrights protects only the original expression of an idea[572].

Through licensing terms, copyright protection can be used in order to restrict the ability of a third party to use the protected parts of the computer program. Indeed, in case the licenses are established through valid contracts, uses that do not respect the license terms may constitute breach of contract. Hence, copyright protection of algorithms has an important restrictive function regarding the use of the protected technology[573]. This means that copyright restrictions can well be used for impeding governments to employ the provided algorithms for purposes that are different from the ones indicated in the licensing terms.

Shifting from the processing infrastructure to the object of the processing, copyright can be employed for the protection of aggregated digital data processed by algorithms[574] in case the selection and arrangement of it meets the originality threshold[575].

Irrespectively of any inventiveness, digital datasets can find protection under the 1996 Directive on legal protection of databases[576], establishing an exclusive *sui generis* right over databases resulting from a "substantial investment"[577].

However, the strongest tool of protection that algorithms' developers have is trade secret protection as recently reformed by the Trade Secret Directive 2016/943. The new Directive provides indeed very broad conditions for protection, encompassing nearly every business confidential information[578]. Despite formal declarations[579], the Directive provides a proprietary-styled protection over information[580], which thus offers strong grounds for big data companies to obscure both the

572 See J. Litman, P. Samuelson, *The Copyright Principles Project: Directions for Reform*, in *BTLJ*, 2010, 25, p. 1190-1191.

573 Highlighting the function of copyright as a means to restrictively regulate the use of the protected object, N. Shemtov, *Beyond the Code: Protection of non-Textual Features of Softwares*, Oxford, 2017, p. 151.

574 For a reflection upon the copyrightability of so-called computer-generated works, see R. Abbott, *Artificial Intelligence, Big Data and Intellectual Property*: *Protecting Computer-Generated Works in the United Kingdom*, in T. Aplin (ed.), *Research Handbook on Intellectual Property and Digital Technologies*, forthcoming, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064213.

575 It should be however recalled that it is very difficult for a database to accomplish the originality threshold required under European copyright law. On the issue see DJ Gervais, *The internationalisation of Intellectual Property: New challenges from the very old and the very new*, in *Fordham Intellectual Property, Media & Entertainment Law Journal*, 2002, 12, p. 929-935.

576 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal Protection of Databases, online available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML.

577 Cf. art 7, 4 par. Database Directive. Recently, see I. Gupta, *Footprint of Feist in European Database Directive: a Legal Anaysis of IP making in Europe*, Springer, 2017, p. 11-37.

578 See art. 2 of the Directive where trade secrets are defined as any information that i) is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; ii) has commercial value because it is secret; and iii) has been subject to reasonable steps to keep it secret. See D. Sousa Silva, *What exactly is a trade Secret under the proposed Directive*?, in *JIPLP,* 2014, 9, p. 11-15.

579 See recital 10 of the Directive affirming that its "provisions (...) should not create any exclusive right on the know-how or information protected as trade secrets"

580 Trade secret protection and enforcement is confined to cases of conducts of "acquisition, use and disclosure" that are to be considered "unlawful". The notion of unlawfulness is very broad and comprehends also any "unauthorised access to, appropriation of, or copy of any documents, objects, materials, substances or electronic files (…) containing

processed health data and the procedural information regarding algorithm-driven processing activities. This procedural information encompasses information regarding how algorithms are developed, how they are validated and the data on which they are trained[581].

The above-outlined intellectual property tools not only shield corporations' algorithmic assets from the eyes of competitors, but, in the dynamic of public-private partnerships, end up creating a substantial safeguard also in respect to the public counterpart[582]. Indeed, these tools and the contractual restrictions regarding them, block public contractors' access to the functional logic of the algorithms they get to employ, with the ultimate effect of rendering these same public administrations incapable of releasing to the wider public explanations regarding the process of the formation of public administrations' will.

In these regards, it is interesting to recall that access to document rules, such as the ones entailed in art. 41 ECHR, in art. 15 TFEU and in Regulation EC N. 1049/2001 regarding public access to European institutions documents provide specific exemptions with regards to the disclosure of those documents that "would undermine the protection of the commercial interests of a natural or legal person"[583]. The protection of business secrets has been recognised by the Court of Justice of the European Union as a general principle applicable in the context of public procurement[584]. Accordingly, these commercial confidentiality exemptions have been interpreted by the Court of Justice of the European Union in a very broad way[585] and also the latest rulings in these regards have confirmed the existence of an outright presumption of confidentiality in the case law of the Court of Justice of the European Union regarding access to public documents[586].

The obscurity of algorithmic decision-making courses renders it arduous for citizens to assert a claim of a right or a legitimate interest. Algorithms' intrinsic and extrinsic obscurity impedes a direct participation of citizens in machine-driven decisions carried out by governments.

the trade secret (…)" carried out "without the consent of the trade secret holder". See artt. 4 n. 56 and 6 of the EU Trade Secret Directive. See EU Directorate General for Internal Policies, *Trade Secrets*, 2014, online available at http://www.europarl.europa.eu/RegData/etudes/note/join/2014/493055/IPOL-JURI_NT(2014)493055_EN.pdf, p. 4; T Aplin, *Right to Property and Trade Secrets*, in C. Geiger, *Research Handbook on Human Rights and Intellectual Property* Cheltenham, 2015, p. 421-426.

581 All this information regarding algorithms constitute the so-called 'e-trade secrets'. R. Niebel, L. De Martinis, B. Clark, *The Eu Trade Secrets Directive: all change for trade secret protection in Europe?*, in *JIPLP*, 2018, p. 3.

582 D.S. Levine, *Secrecy and Unaccountability in Our Public Infrastructure*, in *Florida Law Review*, 200, 59, p. 149.

583 So art. 4.2 EU Access Regulation.

584 Court of Justice of the European Union, Case C-450/06, *Varec SA v. Belgian State*, 14 February 2008; online available at http://curia.europa.eu/juris/liste.jsf?language=en&num=c-450/06,para 49; Opinion of AG Kokott of 23 September 2010 in *Stichting Natuur en Milieu and Others*, C-266/09, online available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CC0266, para 77.

585 For the American perspective, see D.S. Levine, *The Impact of Trade Secrecy on Public Transparency*, in R.C. Dreyfuss, K.J. Stranburg, *The Law and Theory of Trade Secrecy. A Handbook of Contemporary Research*, Cheltenham, 2011, p. 406 ff.

586 See, for example, Court of Justice of the European Union, Case C-562/14 P, *Sweden v. Commission*, 11th May 2017, online available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130dc33afe3f799b84a4e9ab3c8c36aca0434.e34KaxiLc3eQc40LaxqMbN4Pb3uPe0?text=&docid=190582&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=715713. In the same sense, Court of Justice of the European Union, Case C-139/07, *Commission v. Technische Glaswerke Ilmenau*, online available at http://curia.europa.eu/juris/liste.jsf?language=en&num=c-139/07.

In this perspective, the opaqueness of privately developed algorithms implemented at governmental level brings about public disempowerment and loss of accountability. In respect to obscure algorithm-driven decisions shaping public interventions, citizens lose their participatory rights in collective ruling and become passive recipients of machines' determinations[587]. Against this backdrop, the acknowledgment of the unsuitability of traditional administrative "command and control regulation", suggests the need to look for new regulatory tools and governance mechanisms that are better capable of addressing the complexity of emerging algorithm-driven administrative decision-making patterns. The fact that algorithms who drive governments' decisions are privately controlled requires a shift in terms of systemic perspectives and thus of the tools needed to effectively pursue the accountability and transparency objectives. These tools are to be found in the General Data Protection Regulation, which provides specific tools with the aim of achieving accountability and transparency of algorithmic decision-making courses. As will be assessed in the following paragraph, these tools acquire a specific relevance for public accountability and transparency purposes in the "algorithmised" public environment.

**4.** In the effort to provide constructive regulatory responses to the phenomenon of massive machine-driven data processing, the General Data Protection Regulation has newly emphasized and reinvigorated the principles of accountability and transparency in the realm of data protection law. In this way, the two principles have acquired a new significance for the protection of data subjects' rights in the context of algorithmic processing activities.

The Regulation establishes an entire set of obligations born by entities that carry out personal data processing activities "wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system"[588]. The Regulation applies to both private and public entities. This reflected by recital 6, acknowledging that "technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities"; as well as by the definition of "controllers" and "processors" under art. 4.7 and 4.8 GDPR, encompassing a "natural or legal person, public authority, agency or other body". In light of these provisions, it seems that for the purposes of the Regulation, private and public entities are generally equalized[589].

There are only a few regulatory differences between public and private actors[590]. The most significant relates to the requirement of the appointment of a data protection officer[591], always compulsory for public authorities and only compulsory for private entities if their core activities "consist of processing operations which, by virtue of their nature, their scope and/or their purposes,

587 *Ibid*..

588 So art. 2.1 GDPR, defining the "material scope" of the Regulation.

589 However, as Recital 19 GDPR clarifies that the processing activities carried out by public authorities for the purposes of "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data" falls outside the specific scope of the Regulation.

590 In these regards, see O. Butler, *Obligations Imposed on Private Parties by the GDPR and UK Data Protection Law: Blurring the Public-Private Divide*, in *European Public Law*, 2018, 24, 3, p. 555 ff..

591 Art. 37 GDPR.

require regular and systematic monitoring of data subjects on a large scale" or "of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10"[592].

Under these premises, the GDPR becomes a highly important source of regulation of the conduct of public administrations that make use of algorithmic processing infrastructures for the purposes of public services' delivery[593].

However, the GDPR's regulatory potential for public authorities' algorithm-driven decision-making is to be perceived also from a different, *indirect* or *subsidiary*, perspective: by regulating private corporations' processing endeavors, the GDPR's provisions assure as a reflex the enhancement of the accountability and the transparency of public authorities actions that are defined by privately-generated algorithms.

Under these premises, it is extremely interesting to observe that the regulation of data processing activities enacted by the GDPR is achieved through reliance on the same foundational principles regulating public administrations' acts, *i.e.* the principle of accountability and transparency. Nonetheless, the notion of accountability outlined in the GDPR is sensitively different from the administrative law one that has been outlined above. Conversely, the principle of transparency shares some interesting common features with the administrative law principle.

In the GDPR, accountability has become a central principle governing machine-driven data processing operations. In respect to the administrative law notion, accountability is only indirectly related to the purpose of participation and empowerment. To the contrary, it is related to data controllers' and processors' 'responsabilization' and is primarily linked to the object of verifiability, which is, in turn, related to risk management concerns. The GDPR expressly affirms that the principle of accountability under data protection law serves the function of detecting- and thus of signaling- whether an occurred personal data breach "is likely to result in a risk to the rights and freedoms of natural persons".

The accountability principle is established under art. 5.2 GDPR, affirming that 'the controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 (accountability)'. By stating so, art. 5.2 GDPR establishes the autonomy of the principle of accountability in the data protection law ecosystem, and at the same time the strict operational connection to other principles relating to the processing of personal data- such as the principle of lawfulness, fairness, purpose limitation, data minimisation and ultimately of transparency.

As the same wording of art. 5.1 GDPR clarifies, the accountability parameter demands that compliance to normative requirements is externally verifiable, thus traceable. For these purposes, the principle of accountability is substantiated in the rules entailed in art. 22 GDPR, establishing that i) "the data 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

592 Other regulatory differences relate to enforcement and specifically relate to the exemption under art. 41.6 GDPR from the monitoring of approved codes of conduct with regards to the processing carried out by public authorities and bodies and the unavailability established under art. 79.2 GDPR of the option of bringing proceedings "before the courts of the Member State where the data subject has his or her habitual residence", in case the controller or processor is a public authority of a Member State in the exercise of its public powers".

593 O. Butler, *Obligations Imposed on Private Parties by the GDPR and UK Data Protection Law: Blurring the Public-Private Divide,* cit. p. 560 ff..

affects him or her"; ii) "the right to obtain human intervention on the part of the controller"; iii) the right "to express his or her point of view and to contest the decision"; in art. 13.2 lett. f GDPR and art. 14.2 lett. g GDPR, requiring the controller to inform the data subject about "the existence of automated decision-making, including profiling (…) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" (so-called 'right to explanation'); and ultimately in art. 58.1 lett. b GDPR that assigns to supervisory authorities the power to carry out "investigations in the form of data protection audits".

These measures strengthen the accountability regime of the GDPR respectively assuring a direct interaction between data subjects and data controllers (art. 22 GDPR); the release of information regarding the ratio and the legal effects of the data processing operations (art. 13.2 lett.f; art. 14.2 lett.g GDPR); the enactment of control mechanisms capable of signalling irregularities or system weaknesses in the management of personal data (art. 58.1 lett.b GDPR). All these measures encumber data controllers and processors with disclosure obligations that render processing activities transparent and thus traceable. In these regards, also in data protection law, transparency is a fundamental means to achieve accountability and is thus to be considered a key component of it[594].

As the same GDPR states, transparency "requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used (…)"[595]. More precisely, transparency "requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used"[596].

As in the context of administrative law, also in the data protection law ecosystem, transparency is primarily achieved through the right of access, which is established under art. 15 GDPR.

With regards to the content of the right to access, art. 15 GDPR provides a specific list of the information that needs to be made available to the data subjects. First of all, data subjects shall have the right to "obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to personal data"[597]. In addition to this, the right to access encompasses a variety of other types of information regarding, amongst others, "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject"[598]. The provision of "meaningful information about the logic involved" as well as of "the significance and the envisaged consequences of such processing for the data subject" concretises what has been

594 B Goodman, *A Step towards accountable algorithms?: Algorithmic Discrimination and the European General Data Protectio*n, 29th Conference on Neural Information Processing Systems (NIPS 2016), Barcelona, Spain, online available at http://www.mlandthelaw.org/papers/goodman1.pdf, p.7-9.
595 Recital 39 GDPR.
596 Recital 58 GDPR.
597 Art. 15 GDPR.
598 *Ibid*..

appointed as "the right to explanation"[599]. As some strand of the literature[600] has suggested, the expression "meaningful information" is to be interpreted as "legibility" of "architecture" and "implementation" of algorithmic processing[601]. Overall, it can be said that meaningful information about the logic involved must provide clarity with regards to the causal connections and the inference processes that orient the data-driven system so that the data subject may evaluate what type of consequences arise from the processing and thus exploit the remedies needed to address such "envisaged consequences". In this light, the proposed concept of "legibility" of the information to be provided under art. 15.1 lett. h GDPR is systematically consistent with the call for accessibility and understandability of the information regarding the processing entailed in the above-recalled recitals[602].

The right to access under art. 15 GDPR with its related transparency and explanation functions enables data subjects to verify the processing entities' conducts and more specifically their compliance with the data protection rules established by the Regulation. In this perspective, it is a primary tool for responsabilizing processing businesses and thus for achieving their accountability as defined in art. 5.2 GDPR.

Finally, it needs to be clarified that the effectiveness of the so-defined right to access is not destined to be blurred by the statements under recital 63 GDPR, affirming that the right to access "should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software". Although the balancing between individuals' right to data protection and businesses' intellectual property rights is debated in the literature[603], some strand of the scholarship[604] has convincingly argued in favour of the prevalence of the right to access over the protection of intellectual property rights, observing- amongst others- that the same recital 63 GDPR specifies that "the result of those considerations should not be a refusal to provide all information to the data subject", suggesting in this way that the right to access can be limited but never totally rejected.

As interpreted in these terms, the transparency rules entailed in the GDPR turn out to be precious regulatory tools for the networked algorithm-driven public decision-making, shedding light over the first stage of the complex public decision-making chain, that is the stage of the algorithmic processing carried out by private corporations. Since the outcomes of such processing activities come to define the courses of public decision making, the information provided on the basis of the mentioned GDPR's provisions to data subjects, become a useful means to empower citizens in respect to automated public adjudications and to control public interventions. The acknowledgment of the complexity of the "algorithmised" public administration decision-making

599 See, generally, M. Kaminski, *The Right to Explanation, Explained*, University of Colorado Law Legal Studies Research Paper, 18-24, 15th June 2018, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3196985, *passim*.

600 G. Comandè-G. Malgieri, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *IDPL*, 2017, 7, 4, p. 243-244.

601 *Ibid*..

602 Recitals 39 and 58 GDPR.

603 S. Wachter, B. Mittlestandt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation*, in *IDPL*, 2017, 7, 2, p. 76.

604 G. Comandè, G. Malgieri, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation,* cit. p. 263-264.

courses and of the structural and functional features of the new data protection law tools offered by the GDPR, thus ultimately reveals the significance of these same tools for public accountability purposes. With private parties assuming an increasingly important role in the performance of public functions through the grant of technological support, technical verifiability becomes an important source of political accountability.

**5.** The above-outlined analysis leads to two final considerations, one of practical and the other of more theoretical nature.

From a practical standpoint, the study has demonstrated that the increase in the private-public partnerships for the delivery of public services through algorithmic models, sensitively challenges the effectiveness of traditional administrative law tools of accountability and transparency of administrative decision-making. The unsuitability of traditional administrative law tools is mainly given by the fact that they cannot be applied to private processing entities and that public authorities cannot themselves access the relevant information concerning the algorithmic models employed for their decision-making since these are protected by strong intellectual property safeguards. In this light, transparency provisions entailed in the GDPR, and especially the right to access under art. 15 GDPR, assure the release of information regarding the privately conducted processing activities that increasingly orient public interventions. In this perspective, they become thus essential tools for data subjects to trace complex public decision-making courses and thus indirectly enhance political accountability as promoted by traditional access to public documents channels.

Against this backdrop, it appears that an integrated approach between new data protection law tools and traditional administrative law tools is needed in order to achieve a satisfying level of political accountability in respect to "algorithmised" public interventions. Such integrated approach is ultimately deemed to be essential for an effective protection of citizens' legitimate interests and fundamental rights that a short-sighted conception of public accountability would undermine in the shadow of algorithm-driven administrative rulings.

Ultimately, at a deeper level, the traced analysis reveals the complexity of the private-public divide in the algorithmic economy, requiring a rethinking of the interaction between different regulatory branches of European law and more precisely between different regulatory tools provided by these. The increasing intertwining between private and public parties for the algorithm-driven delivery of public services raises profound questions regarding the ways of integrating administrative and data protection law, the opportunity and limits of the applicability of general data protection law to public actors' processing activities as well as the functions to be assigned to traditional administrative law tools in the algorithmic environment[605].

***GIULIA SCHNEIDER***

605 In these regards, it is interesting to recall that the Administrative Tribunal of Lazio with the ruling has granted access to the information regarding the algorithms of a software employed by the Italian Public Administration for the purposes of the transfer of teachers under the Italian law 10/2015 under the right to access to public documents as established by art. 22 of the Italian law n.241/1990. So TAR Lazio-Roma, Sez. III bis, ruling 22 March 2017 n. 3769. For a comment see M. Iaselli, *Diritto di accesso all'algoritmo, TAR Lazio apre nuovi scenari*, published on the 17th May 2017, online available at http://www.altalex.com/documents/news/2017/05/17/diritto-di-accesso-algoritmo.