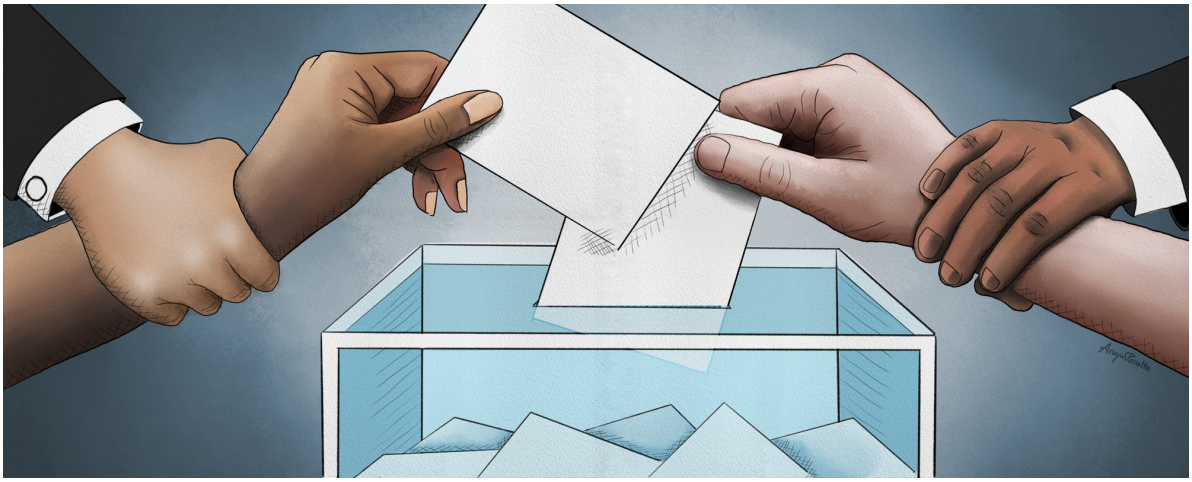
SOCIAL AND DEMOCRATIC IMPACTS

# The Redefinition of Power

## Artificial Intelligence and Legal Ecosystems

Pompeu Casanovas



Araya Peralta

The European Commission refers to artificial intelligence as ‘systems that display intelligent behaviour […] — with some degree of autonomy — to achieve specific goals’ [1]. Together with robotics and big data analytics, it represents a key line of research, with billions invested in it [2]. ‘Big data analytics’ is not a technical term. It refers to data that can be aggregated, added to and managed by algorithms, and which feed artificial intelligence systems.

The six Vs: value, volume, velocity, variety, veracity and variability, are sometimes used to define the concept. I prefer to talk about structured, semi-structured and unstructured data and meta-data that delimit the scope of the web and so-called dark web for their practical representation. Gartner’s reports and predictions for 2018 and 2019 identify artificial intelligence, ethics and governance as at a peak in their expectations hype cycle. Ethics is one of the new points theyidentify as essential in the next five years in theirwidely-usedcycle of technological expectations for industrial development. For the first time, ethics and governance are considered regulatory elements in the 2018 hype cycle. The most recent cycle for 2019 confirms this trend and adds a key emerging field: regulatory ecosystems and regulatory compliance [3] . What does this mean?

I will use recent examples of the impact of technology and then focus on the new regulatory models we require. I will put the horse before the cart: first the social effects, then the technical aspects.

## Some examples

The best known case is that of Cambridge Analytica: the identification of voter profiles in the UK Brexit referendum and the later USA presidential elections. Voters received personalised information based on their profile, without realising they had previously been analysed. If a company is capable of aggregating all a person's data on the web without their consent, it can acquire rare power, not only over the data but also over the person, because it can control their feelings, wishes and decisions. How is this done?

Before the case blew up and the videos and seminars were removed from YouTube, the company's engineer Jack Hansom provided an explanation: using data aggregation algorithms.

'Knowing an average is not very useful, what we really want is the individual. […] How can this be scaled? Well… traditionally, a survey is used. A set of questions are asked after which we can infer something about the personality. But to obtain a reliable estimate, you might need hundreds of people […]. However, what we want is to make use of Facebook information, using it as input for machine learning models to predict personality and thus go beyond surveys'.

The strategy worked. Carole Cadwalladr, the journalist who uncovered Cambridge Analytica's malpractice, has pointed out that lack of public control over gathered and analysed data is a direct threat to democracy [4] . In this she agrees with other analysts who have studied the use of AI techniques in the causes of the global financial crash [5].

The second example is less well known, but no less real: identity cards based on violations of corporate or legal regulations, which are aggregated on a sort of traceable chart or portrait of our compliance with regulations. They are similar to driving licence points or credit cards, but create what might be termed an institutional portrait of users of a given public service. Listen to the warning to passengers on the Beijing to Shanghai high-speed train, as recorded by another journalist, James O'Malley (2018):

> "Dear passengers, people who travel without a ticket or behave disorderly, or smoke in public areas will be punished according to regulations, and the behaviour will be registered in an individual information credit system. To avoid a negative record of personal credit, please follow the relevant regulations and help with the order on the train and at the station' [6].

This system is part of a plan by the Chinese government to standardise a unified economic and social reputation system by 2020, based on large-scale information aggregation techniques for each citizen. This has very practical consequences, notably, the creation of

blacklists of ‘disaffected citizens’.

It is what is known as a system of mass surveillance of the population. The consequences are harsh for people on the discredited persons lists. For instance, limits are placed on what they can buy, they are not allowed to take high-speed trains or planes, stay in luxury hotels or go on holiday with travel agencies and they cannot send their children to private schools. The sanctions are social and economic, a form of ostracism that prevents offenders from climbing and enjoying the benefits of the social ladder [7] . Setting aside its consequences, behind it are automatic data collection, aggregation and management systems.

The third example is facial recognition, in the UK this time, at the heart of western democracies:

> “In 2017, the London Metropolitan Police tested a facial recognition algorithm on a million visitors to the Notting Hill carnival to identify people on their wanted lists. The technology found 35 ‘matches’. Human examiners rejected 30 of them. The police arrested the other five. Only one of them was actually the right person. To make matters worse, the police then realised the list was not up to date, and this person was no longer wanted for any crime”. [8]

The ethical and legal conditions for facial, as well as biometric, recognition are one of the hot topics in contemporary practical philosophy. It is an issue for which there is no simple solution, because it concerns the balance between individual freedom and the right to privacy, on the one hand, and the right to collective security on the other.

## The redefinition of power

These examples show that what is technically possible is not always socially desirable. All the above cases are different and respond to data use dynamics with differing constrictions. We could mentioned others, relating to data violation, data re-identification despite encrypting and cybersecurity [9] . They are all striking and have one element in common: *they demonstrate the weakness of the traditional instruments of law, politics and classic participative democracy to deal with these situations.*

The issue also involves redefining the 20th century theme of mass society (the crowd). But what we are discussing is, above all, the changing nature of the power that moves it. Jeremy Heimans and Henry Timms have written a book on this subject, titled precisely New Power (2018). They propose a redefinition of new power in relation to the old. They have

developed what they term a new power compass: flexible, connected, undemanding, inarticulate, informal, making use of how people connect, participate, share, empathise with ideas and feelings, or flee when overwhelmed by contradictions, have duties imposed on them or simply dislike what they see on the screen of their mobile, tablet or computer. By contrast, the old power is authoritarian, oppressive, bossy, taxing, bureaucratic and demands obedience. It is not suited for success on the web.

> Indeed, what is complex and new is the coexistence of a plurality of forms of power associated with technology

Indeed, what is complex and new is the coexistence of a plurality of forms of power associated with technology, which seek, as always, economic and political optimisation for their own benefit. I share Nigel Shadbolt and Roger Hampson's vision in The Digital Ape (2018). The species advances by developing social relations that are something more than technology. Unfortunately:

> "[…] the point is not that machines might wrest control from the elites. The problem is that most of us might never be able to wrest control of the machines from the people that occupy the command posts". [10]

Modern states have begun to behave like corporations: they defend themselves and tend to monopolise digital media. We do not have to look to states with totalitarian tendencies such as China or Putin's Russia for examples. In France, article 33 of the new Justice Reform Act [11] prohibits the use of advanced digital instruments in the study of complete judicial sentences with the names of the magistrates issuing them, in the name of privacy and data protection (protéction de la vie privée)[12].

We see here the new means by which the law is published: a universal unique identifier: the so-called European Legislation Identifier, or ELI. When we refer to identity, we mean the identification of digital entities, in other words, representation of identity in algorithms and semantic languages. To all intents and purposes, this is the same for people, organisations and objects.ISO/IEC 24760-1 defines identity as 'a set of attributes related to an entity'. Identity is an essential point. The US Department of Commerce's National Institute of Standards and Technology has also clearly stated: 'accessing a digital service may not mean that the subject's real-life identity is known'[13].

What I am trying to point out is that the new forms of power imply control over these languages of representation and techniques of authentication, encryption and privacy, because these are what structure the potential relation between digital and real entities. In

other words, they manage references and co-references of words and discourses that up to now have only flowed through natural languages.

> Whoever controls the relationship between the data and meta-data of elements in a system is also capable of constructing their power of implementation

To put it simply: whoever controls the relationship between the data and meta-data of elements in a system is also capable of constructing their power of implementation; i.e. the scope of the ecosystem of their use. And this is an asymmetric relationship: while citizens, consumers and users can be closely identified and scenarios and contexts profiled, rarely can they obtain the general knowledge that the system and its administrators possess.

## Ethic and legal ecosystems, more than just regulatory models

This is why we cannot just use systems of values, principles and standards to regulate this complex hybrid consisting of our data and meta-data. The same is true for ethical or legal systems. There is (i) this intermediate element between semi-formal and formal languages that cannot be overlooked (if we wish to avoid or mitigate against further cases such as those described above); and (ii) the middle ground between constructing the public space and the collective coordination of behaviours through individual decisions and actions.

As we have seen, the ethics of artificial intelligence is one of the new points identified by Gartner as essential over the next five years. For the first time, ethics and governance are considered regulatory elements. But how? By incorporating ethics principles and legal protections in behaviour systems (artificial and human)?

The traditional strategy used to do so is to draw up a set of general principles that can be developed through regulatory systems, such as systems of standards, that permit their implementation. Among many other examples, Europe, UK, USA and Australia are drawing up ethical principles for application to AI legislation. The principles of transparency, accountability, and explainability of algorithms aim to go beyond the protection offered by good professional practices, industrial ISOs, professional standards and Federal Information Processing Standards (FIPs). This, if nothing else, is the intention of the recent General Data Protection Regulation (EU) 2016/679 (commonly known as the GDPR), which came into effect on 25 May 2018 in Europe, and which expressly includes so-called data protection by design. Compliance by design is a further strategy, explored in several European projects and various business and legal initiatives.

> Traditional laws and regulatory legal systems must also be modified to match instruments whose social effects cannot yet be precisely predetermined.

I am not questioning whether such formalisation is a good path towards achieving the goal of preserving individual rights. I am merely indicating that their application requires something else, because it is the social and political nature of these principles that needs to be specified, which can only be done through interrelations and interfaces between humans and machines. To put it another way: traditional laws and regulatory legal systems must also be modified to match instruments whose social effects cannot yet be precisely predetermined.

What we have termed *meso-level* [14] and *middle-out approach* [15] refer to the set of technical and human resources we need to implement in order to build a community, a socio-technical system and a human group that uses technology. I also think that this is what we need to focus on if we want to bring a little order to the application of artificial intelligence to existing regulatory systems.

Jurists and political philosophers from the 18th, 19th and 20th centuries often linked the concept of authority to the state or the representatives of government chosen by citizens (parliament). In fact, authority can also be associated with the market, or society as a whole. The idea that can guide us is finding a balance between all these different sources of authority, including what the individual can decide for him or herself (this latter point being an essential one). In a hyperconnected world, objects become the transmission channel for information. All the everyday objects that surround us will in the not-so-distant future transmit information about their users: cars, fridges and even toasters. How should we deal with this and the world of nanotechnology (microprocessors) that accompanies it? It is literally impossible to know right now.

Limits cannot come from restrictions but from conscious decisions on how to integrate them into the diverse range of social scenarios and contexts. Once again we return to identity: how to make it a priority. And this means being able to define (as far as possible) relations between the entities, attributes and values of the attributes that make up our digital and personal identity. This is not easy, because numerous points of support with personal and social networks already form a continuum from which it is difficult to escape. The idea would be to integrate all these scenarios in a way that can be controlled by each and every individual who experiences them. In short: finding polycentric points in the plurality of ecosystems that make up our lives, and agreeing on the regulatory ecosystems.

## Interlinked democracy: a possible model of democracy

This is what I have termed ‘meta-rule of law’ [16] . It is not a term that can easily be translated into the Catalan continental legal culture, based on French civil and administrative law. It might be better to term it ‘ethical structure’, or the ‘rule of rights’ because it involves focusing on rights; i.e. the behavioural expectations our contacts, neighbours and counterparts have of us and us of them. There is a minimum possible level of protection, which defines the field that regulatory systems can cover

The aim is to extend and include protections and guarantees of rights in the structure of the Semantic Web (data/meta-data and web services) through semantic instruments and AI algorithms that we are able to apply (machine learning, privacy, etc.) Note that rights and obligations are not created by formal languages, but by interrelations (individual and collective) among members of social communities, the markets and civil society. But the transmission chain starts with identifiers.

Let us provide a basic definition of terms (Table 1):

1. The *Semantic Web* consists of any available data, raw, semi-structured or structured in a formal language, via application program interfaces (APIs) or information flows from the Internet of Things.
2. Linked data is a sub-set of the above for the networked publication and sharing of data, following the classic rules proposed by Tim Berners-Lee and developed by the W3C technological community (World Wide Web Consortium) [17] . The Semantic Web should not be confused with the internet. The former consists of information flows requiring regulation. The latter is the physical medium, a set of communication technologies.
3. Since the 1990s, deliberative democracy has been defined as ‘processes of judgement, preference formation and transformation within informed, respectful, and competent dialogue’ [18] . Thus it does not seek to limit the formal voting process. Epistemic democracy follows this path and has been defended by authors such as Jeremy Waldron and Josiah Ober. It assumes there is a collective decision-making process that can produce epistemically valid (true) results or reasonable decisions, largely based on or shaped by the participation of a large number of people.
4. The political processes of crowdfundingand crowdsourcing are based on this premise, as well as the methods of people’s assemblies (mini-publics). What we propose is to push the concepts of deliberative democracy or epistemic democracy a little further. Linked democracy is the concept by which we refer to the interrelation between a group of people, technology and data to create participation systems in which knowledge is aggregated, shared and aligned to make decisions and create lines of political and social action (Poblet, Casanovas and Rodríguez-Doncel 2019).
5. Linked democracy: (i) establishes and studies the contextual conditions of deliberative and epistemic democracy; (ii) is located on the intermediate meso-level

of implementation, as defined here; (iii) requires the human-machine interface; and (iv) addresses the institutional level that can be regulated and shaped. [19]

Democratic ecosystems are contextual, referring to networked interaction systems (meso-level). And they can interrelate to their environment to produce socially relevant knowledge and political decisions. This concept is similar to that of epistemic democracy, but based more on social innovations that can lead to participation that focuses on shared use of technologies to resolve common problems. Preserving individual rights in this process is what I have termed the meta-rule of law. [20]

Legal ecosystems are moving in this direction. It is not a matter of regulating only traditional instruments, laws, regulations and principles, but of making use of the elements offered by artificial intelligence to create stable, self-sustaining and agreed-upon regulatory systems. They consist of a variety of regulatory forms, from the traditional instruments of laws and regulations to 'soft' legal instruments (agreements and negotiations), public policies, industrial standards and technical protocols.

This is, of course, an institutionalist vision, but it is better than waiting until economic public policy (tax systems), migratory policy (systems of access to residency and nationality), health policy (organisation and transmission of health files) and criminal policy (organisation of police and criminal files) can be automated without public participation or discussion among citizens. As we have seen, this too is a perfectly viable route. It is up to us to avoid it.

## REFERENCES

1 — "Artificial Intelligence refers to systems that display intelligent behaviour by analysing their environment and taking action — with some degree of autonomy — to achieve specific goals. We are using AI on a daily basis, for example to block email spam or speak with digital assistants." (EU Commission 2018)
2 — "Public-private partnerships on robotics ('SPARC') and big data ('Big Data Value') represent EUR 1.2 billion in public investment plus EUR 3.2 billion in private investment for 2014-2020, giving EUR 4.4 billion in total." (ibid. EU Commission 2018).
3 — "Establish use-case-based accountability for AI solutions, outcomes and ethics. Develop methods for proactive regulatory compliance and outline reactive responsibilities, actions and procedures in the case of unanticipated and unintended consequences. Plan adaptive governance to support freedom and creativity in data science teams, but also to protect the organization from reputational and regulatory risks. Little or no governance in data science teams to facilitate freedom and creativity is an acceptable approach if this is a conscious governance decision." Gartner (2019). Svetlana Sicular, Jim Hare, Kenneth Brant, *Hype Cycle for Artificial Intelligence*, 2019. 25 July 2019 ID: G00369840.

4 — See:
• Cadwalladr, C. «Exposing Cambridge Analytica: "It's been exhausting, exhilarating, and slightly terrifying"». The Guardian, 28 de setembre del 2018.
• Cadwalladr, C. «Facebook's role in Brexit, and the threat to democracy», Ted Talk, 19 d'abril del 2019

5 — O'Neil, C. (2016). *Weapons of math destruction: how big data increases inequality and threatens democracy* (First edit). New York: Crown, 2016.

6 — Recorded by James O'Malley on 18 october 2018, at 12.24 am. "Dear passangers, people who travel without a ticket, or behver disorderly, or smoke in public areas, will be punished according to regulations, and the behaviour will be recorded in individual credit information system. To avoid a negative record of personal credit, please follow the relevant regulations and help with the orders on the train and at the station".

7 — Pack, J. «How does China's social credit system work?» Market Place, 13 de febrer del 2018

8 — Margetts, H., Dorobantu, C. «Rethink government with AI». *Nature* 568 (2019), 163-165.

9 — Berghel, H. «Equifax and the latest round of identity theft roulette». Computer, 50, 12 (2017), 72-76.

10 — Shadbolt, Nigel, and Roger Hampson (2018). *The Digital Ape: How to Live (in Peace) with Smart Machines*. Sydney: Pan Macmillan .

11 — LOI n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

12 — See:
• https://www.legifrance.gouv.fr/eli/loi/2019/3/23/2019-222/jo/article_33
• https://www.legifrance.gouv.fr/eli/loi/2019/3/23/JUST1806695L/jo/article_33
• https://www.legifrance.gouv.fr/eli/loi/2019/3/23/2019-222/jo/article_33

13 — "Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known." Grassi, P.A., Garcia, M.E., Fenton, J.L. *Digital Identity Guidelines*. NIST Special Publication 800-63-3.

14 — Poblet, M., Casanovas, P., Rodríguez-Doncel, V. *Linked Democracy. Foundations, methodologies, applications*. Cham: Springer Nature, 2019.

15 — Pagallo, U., Casanovas, P. and Madelin, R. (2019). "The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data." The Theory and Practice of Legislation, pp.1-25.

16 — Casanovas, P. *Sub lege pugnamus. De la gran guerra a les grans dades*. Barcelona: Publicacions de la Universitat de Barcelona, 2017.

17 — https://www.w3.org/DesignIssues/LinkedData.html

18 — Dryzek JS., Niemeyer N. «Deliberative Turns» (2009). In J. Dryzek, editor, *Foundations and Frontiers of Deliberative Governance*. Oxford: Oxford Scholarship Online, 2009, 3–17.

19 — Poblet, M., Casanovas, P., Rodríguez-Doncel, V. *Linked Democracy. Foundations, methodologies, applications*. Cham: Springer Nature, 2019.

20 — Casanovas, P. *Sub lege pugnamus. De la gran guerra a les grans dades*. Barcelona: Publicacions de la Universitat de Barcelona, 2017.

ACKNOWLEDGEMENTS

This article is part of the Meta-Rule of Law Project (DER2016-78108-P), of the Spanish Ministry of the Economy and Innovation . The article is based on the guest lecture to the 5th Catalan Philosophy Congress, 20 June 2019, Canillo, Andorra (video conference) and the guest lecture celebrating 300 years of the Catalan Mossos d'Esquadra police force at the Mollet del Vallès Police Academy on 27 September 2019. I have used material from the 'Compliance through Design' project carried out by the Data to Decisions Cooperative Research Centre (D2D CRC, Australia); and the EU Lynx project entitled 'Building the Legal Knowledge Graph for Smart Compliance Services in Multilingual Europe' (Grant agreement No 780602).

**Pompeu Casanovas**

El Dr. Pompeu Casanovas és Director de Recerca Avançada, professor de Filosofia i Sociologia del Dret a la Facultat de Dret de la UAB, fundador i president de l'IDT-UAB. Té vint anys d'experiència en recerca sobre sociologia del dret i filosofia, pragmàtica i IA i dret. Ha estat Investigador Principal de més de 50 projectes nacionals, europeus i internacionals. Ha publicat 10 llibres i més de 150 articles científics en les seves àrees d'interès. Les seves publicacions recents tenen a veure amb el desenvolupament d'ontologies legals per implementar tecnologies semàntiques de web; models de governança per implementar la seguretat i la protecció de dades a la Web; mediació, *Online Dispute Resolution* (ODR) i *crowdsourcing* per fomentar la participació democràtica ciutadana.