EasyChair Preprint

№ 8818

The European Approach to Artificial Intelligence Across Geo-Political Models of Digital Governance

Jeroen van den Hoven, Giorgia Pozzi, Marc Stauch, Iryna Lishchuk, Francesca Musiani, Josep Domingo-Ferrer, Salvatore Ruggieri, Francesca Pratesi, Roberto Trasarti and Giovanni Comandè

September 6, 2022

The European Approach to Artificial Intelligence across Geo-political Models of Digital Governance

Jeroen van den Hoven and Giorgia Pozzi,[1]
Marc Stauch and Iryna Lishchuk,[2]
Francesca Musiani,[3]
Josep Domingo-Ferrer,[4]
Salvatore Ruggieri,[5]
Francesca Pratesi and Roberto Trasarti,[6]
Giovanni Comandé[7]

[1] Delft University of Technology, Jaffalaan 5, 2628BX, Delft, The Netherlands
[2] Gottfried Wilhelm Leibniz Universität Hannover, Welfengarten 1, 30167 Hannover, Germany
[3] CNRS - Centre national de la recherche scientifique, 3 Rue Michel Ange, 75016 Paris, France
[4] Universitat Rovira i Virgili, Av. Catalunya, 35, 43002 Tarragona, Spain
[5] Università di Pisa, Lungarno Antonio Pacinotti, 43, 56126 Pisa, Italy
[6] National Research Council of Italy (CNR), Via Giuseppe Moruzzi, 1, 56124 Pisa, Italy
[7] Scuola Superiore Sant'Anna di Pisa, Piazza Martiri della Libertà, 33, 56127 Pisa, Italy
iryna.lishchuk@iri.uni-hannover.de

Abstract. Digital technologies are crucial in many high-stakes fields and should follow the principle of transparency. At the same time, technologies are inescapably value-laden. In fact, values are built into algorithms, technical standards, and protocols. Adopting a geo-political perspective, this paper aims to investigate how the main state actors (i.e., Russia, China, the USA, and Europe) further the advancement of digital technologies in ways that mirror their political, cultural, and societal structures. We propose a comprehensive analysis that encompasses a legal, ethical, and technical assessment. Furthermore, we consider a case within the SoBigData++ research infrastructure as an example of successful synergy of digital technologies and fundamental ethical and legal principles underpinning the European society.

Keywords: Digital Governance, Artificial Intelligence, Geo-political Models.

1. Introduction

The current paper builds on and furnishes an example for the claim, made in the paper by Jeroen van den Hoven et al. (2021), that the largest state actors (i.e., the USA, China, Russia, and Europe) adopt ways of promoting technological advancement that mirror their cultural, political, economic, and social structures. In this respect, its purpose is to provide a comparative study of the different geo-political approaches to one particular technology, namely artificial intelligence (AI). We carry out this analysis under different perspectives encompassing the ethical, legal, and technical dimensions relevant to regulating AI. The paper includes analysis of legislative initiatives and national AI policies (OECD database of national AI policies, 2021), opinions in the literature, public reports, real-life developments.

In this context, we consider how the model adopted by the USA that is characterized by limited regulations of technology mirrors the libertarian values and individualistic model of citizens that finds its most suitable expression in the ideal of the *homo economicus*. For its part, Chinese socialism adopts digital technology to centralized surveillance and control technology aligned with behaviourist and utilitarian ideas. We also consider how Russian illiberalism, anti-individualism, conservatism, and 'guided democracy' are mirrored in its digital governance. Finally, we scrutinize how the European approach that sees at its center liberal democracies translates into strong AI regulations and data protection. Moreover, we consider how technological innovation is advanced in accordance with a conception of the person as autonomous, with particular weight assigned to human freedom and respect for dignity. We further argue that Europe's strong focus on pushing forward technological advancement while sticking to widely shared and fundamental ethical principles and strong regulations is not an obstacle to innovation but rather the best way to its fulfilment (Agius et al., 2021). In order to substantiate our claims, we consider a case within the SoBigData++ research infrastructure (RI). This should enable us to show that it is possible to achieve crucial knowledge of relevant social practices while remaining faithful to the core ethical and legal principles that underpin the European approach towards digital advancement.

2. Legal Perspective

From the perspective of protected values, the diverse approaches, i.e. the EU model of protecting individuals, the U.S model of corporate control, the model of state control adopted by Russia and China, are described further below.

2.1. EU Model of Protecting Individuals

The EU approach to regulating artificial intelligence, signalled in the recently proposed AI Regulation (COM(2021) 206 final, published by the European Commission in April 2021), reflects an underlying concern with protecting the rights and freedoms of individual EU citizens. In this respect, it is of a piece with other key pieces of EU legislation relating to use of digital technologies, such as the General Data Protection Regulation (Regulation (EU) 2016/679). In all cases, the undoubted potential benefits promised by the new technologies must be set against the risks they may pose – either by misuse, or simply inadvertence (unintended effects), to individual or social interests[1].

The EU approach to AI presents a combined model that builds on strategic complex regulation of AI and sector-specific norms of direct effect[2]. Accordingly, the draft Regulation opts for an *ex ante* regulatory approach, but one which differentiates, with respect to the applicable rules and safeguards, according to the level of risk that diverse AI applications pose to relevant rights and interests. In the first place, some uses of AI, where the risk is considered unacceptable are straightforwardly prohibited. This includes AI systems that manipulate human opinions or decisions through choice architectures, leading people – as individuals or groups - to act to their detriment, as well as technologies for indiscriminate surveillance, or social scoring (COM(2021) 206 final, Article 4). Secondly, other applications, which contain foreseeable risks to the health, safety or fundamental rights of natural persons, are classified as 'high risk' (Annex II, COM(2021) 206 final). In this case, their development will be subject to a stringent risk assessment and accreditation process to ensure the risks are appropriately minimized and managed before the applications go to market. Developers will need to demonstrate inter alia the quality, representativeness and suitability of datasets used, transparency in how the system operates, and its accuracy, robustness and cybersecurity (COM(2021) 206 final, Title III). In this regard, there are already various health AI solutions with CE marking – a regulatory requirement for putting a medical device on the market (Regulation (EU) 2017/745) - in Europe[3]. Further such AI-driven health solutions are in the pipeline (Gerke et al., 2020), which will be required to undergo similar certification in due course.

In other respects, though, the EU legal framework evinces an open and accepting attitude towards AI applications. AI systems falling outside the prohibited and high-risk categories, i.e. 'low-risk' may be developed free from regulatory constraint. The only residual requirement here is that of transparency (Ibid, Article 41). The innovation-friendly stance of the Proposal is also underlined by the express provision for 'sandboxing' schemes, in order to allow high-risk applications to be tested subject to appropriate regulatory oversight at Member State level (Ibid., Article 44).

Overall, it appears that the draft AI Regulation provides for a framework that will strike an appropriate balance between the benefits and risks associated with the technology. The draft is presently proceeding through the EU legislative process, with the expectation that it will be enacted as law in 2023 and enter force some time in 2024. In the meantime, the centrality of EU citizen rights' protection in relation to AI applications is emphasized by the general 'European Declaration on Digital Rights and the Digital Decade' issued by the Commission in January 2022 (COM(2022) 28 final). Here it is stated that: "*Everyone should be empowered to benefit from the advantages of artificial intelligence by making their own, informed choices in the digital environment, while being protected against risks and harm to one's health, safety and fundamental rights*" (Ibid., Chapter III).

2.2. US Model of Corporate Control

Traditionally, the US has favoured a 'laissez faire' approach towards internet and digital technology regulation, with the state restraining itself from imposing onerous rules, so as to allow market-players to develop their business models relatively unhindered. Insofar as general legislative initiatives have occurred this has more been motivated by a desire to protect the operations of digital service providers, as with the 1998 Digital Millennium

[1] Recital 3 COM(2021) 206 final.
[2] France, however, attributes more importance to the norms of strategic planning, than to direct regulation. *See*: Neznamov, 2019)
[3] Health app Ada, Your personal health guide, assesses individual-specific symptoms and recommends steps (like visit a doctor or emergency care), is CE marked (class I) and compliant with the GDPR. *See* at: https://ada.com.

Copyright Act (DMCA), which establishes liability immunities for platforms and other providers (wider than those under the e-Commerce Directive in the EU), which host or transmit IPR-infringing content.

By contrast, restrictions on digital actors have taken a piece-meal form, covering certain specific high-risk activities, while otherwise leaving the field free for companies to innovate and prosper. Another factor here is the strong protection enjoyed by free-speech under the US Constitution (Johns, 2015). This is reflected, inter alia, in the tolerant attitude of the lawmaker towards the practice – essential to the business-models of many internet concerns - of large-scale data-collection, trading and analysis. Here one looks in vain for overarching data protection legislation akin to the EU's GDPR. Rather, the US has taken a 'pocket-based' approach limited to particular sectors, such as the rules to protect sensitive health data under the 1996 Health Insurance Portability and Accountability Act (HIPAA). Beyond these specific areas of coverage, it is felt sufficient protection is provided to individuals through the operation of the market (where rogue data uses are penalized by loss of consumer trust and goodwill), as well as *ex post* facto liability in case of proven individual harm, through privacy-based torts.

At the same time, there is also one mechanism, whose de facto effect is to impose *ex ante* regulatory duties on internet companies. This takes the form of possible action by executive agencies, notably the Federal Trade Commission (FTC) against companies, whose data practices are seriously deceptive or unfair towards consumers, or otherwise violate specific protective statutes. Here, even without proof of individual damage, the FTC has the power to impose significant fines. A number of large internet concerns have been the subject of such investigations, sometimes resulting in expensive settlements, as happened to Google in respect of its tracking of children's use of YouTube (Min, 2019) and to Facebook over its complicity in the Cambridge Analytica scandal (Federal Trade Commission, 2019). In 2020, the FTC issued a business guidance on AI and algorithms recommending that the use of AI should be transparent, fair, and accountable (Federal Trade Commission, 2020). Enforcement actions followed[4].

In relation to AI-based technologies, there is a similar starting point that government regulation should not unduly interfere with innovative business practices. This is reflected in the November 2020 guidance on approach to AI issued by the White House to federal agencies[5]. Subsequently, there are further indications that, at least in the case of AI, the US government may attempt to take a more overarching regulatory approach. In October 2021, the Presidential Office of Science and Technology suggested the need for a general 'Bill of Rights' in this area, to protect citizens from the risks posed by such technology accompanied by a public request[6].

In this regard, it appears that the executive intent, and possibly also the content of the rules would not be dissimilar to the present EU proposal for an AI Regulation. It is more likely here too, that the pockets-based approach (and largely at state, rather than federal level), will prevail[7] (Pereyra, 2021). In summary, it may be said that the US is likely, with AI as for other digital technologies, to stand by its free-market preference over the more *ex ante* regulatory approach – backed by concern for citizen rights – found in Europe. At the same time, there are at least hints that the US government – backed by an increasing distrustful public – may be willing to take a tougher approach towards the use of AI by the most powerful conglomerates.

2.3. Russian Model of State Control

Russia was 'largely disinterested in strong Internet regulation until the 2010s' (Kolozaridi & Muravyov, 2021). However, approaches aimed at strengthening of Russia's technological and digital sovereignty have given way, since the early 2010s, to a number of laws and initiatives aiming to shape an 'autonomous Russian Internet'. Since 2014, the Russian government has invested considerable resources in redesigning its internet infrastructure (labelled as 'RuNet'), to both limit access to specific website addresses or block messaging platforms (such as

[4] An action brought by the FTC against the photo-app developer concerns the latter's non-consensual use of customer data to develop facial recognition technology, which led to a settlement requiring it to delete the associated algorithm. In the face of growing public pressure and congressional scrutiny, especially regarding the use of facial recognition, Facebook announced later in 2021 that it would voluntarily shut down its program developing such technology. *See:* Pereyra, 2021.

[5] "*to consider ways to reduce barriers to the development and adoption of AI technologies [and] to support the U.S. approach to free markets, federalism, and good regulatory practices (GRPs), which has led to a robust innovation ecosystem…. [A]gencies should continue to promote advancements in technology and innovation, while protecting American technology, economic and national security, privacy, civil liberties, and other American values, including the principles of freedom, human rights, the rule of law, and respect for intellectual property." See:* White House, 2020.

[6] *"information about technologies used to identify people and infer attributes, often called biometrics—including facial recognition, but also systems that can recognize and analyze your voice, physical movements and gestures, heart rate, and more. We're starting here because of how widely they're being adopted, and how rapidly they're evolving, not just for identification and surveillance, but also to infer our emotional states and intentions*." *See:* Lander and Nelson, 2021.

[7] Initiatives include the Artificial Intelligence Video Interview Act passed in Illinois in 2019, regulating use of AI by employers when conducting video interviews, as well a 2021 Colorado Act that restricts the uses insurers may make of potentially discriminatory predictive algorithms. *See:* Pereyra, 2021.

Telegram), and also with the aim of controlling more directly the Internet traffic across Russian territory. This trend has further accelerated in the wake of the war in Ukraine.

The AI strategy, introduced by the Decree of the President dd 10.10.2019 N 490, follows the approach of strategic planning (*ex ante* approach). The central elements of the Russian AI strategy include (a) favourable legal conditions; (b) special regimes for data access (including personal data); (c) simplified testing and deployment of AI solutions; (d) removal of export barriers; (e) uniform standardization and compliance assessment systems; (e) stimulation of investments, including by PPPs; (f) ethics rules. *De jure*, the Russian AI strategy should adhere to the principles of protecting human rights and freedoms guaranteed by the Russian and International laws, minimisation of risks, transparency and explainability, but also technological sovereignty to ensure independence of Russia in the field of AI. *De facto*, the European Court of Human Rights assessed the Russian legal framework in the field of communications in breach of the right to privacy protected by Article 8 of the Convention[8]. The "war blockings" concerned also internet resources, including EuroNews, Facebook, Twitter, Instagram upon the Russian intervention into Ukraine (Gainutdinov and Chikov, 2022). The respect and enforcement of human rights by Russia remains questionable, as Russia has been excluded from the Council of Europe, and will depart from the Convention on Human Rights on September, 16th, 2022.

Implementing the AI strategy in Russia requires some legislative amendments and testing. For the legislative part, e.g., the storage of data sets (inter alia, sound, speech, medical, video surveillance) for the purposes of AI on the public platforms (point 38 Decree N 490) and ensuring protection of data generated in economic and R&D activities, data localization in Russia and priority access by the state authorities (point 39 Decree N 490) (Neznamov, 2019) lack normative foundations. For the testing part, the experimental regimes (also referred to as digital sandboxes) have been enacted by the Federal Law No. 123-FZ (in force from July, 2020) and the Federal Law No 253-FZ (in force from January, 2021). The others are in the pipeline. In particular, healthcare, agriculture, logistics, construction, municipal services are identified as potential R&D and testing sites for AI. For instance, in the course of implementing the AI strategy in medicine, the legal regulation of electronic health records was amended in a way to allow storage of de-identified data for the purposes of machine learning and formation of AI-driven systems in support of clinical decision-making, both as access to the AI solutions by medical institutions (Order No 2174). While Europe is concerned with deconvoluting algorithmic black-box in light of the transparency requirement and the right to explainability, the Russian state, similarly to the U.S., seems to follow here the *ex post* regulation approach under the slogan "build fast, fix later". This position can be explained against the background of legislative developments towards digital governance in Russia.

Most notably, the ambitions towards digital governance have translated into the Law FZ-90, which called for a 'sovereign RuNet' in 2019 and mandated passing of internet traffic within Russia through internet exchange points (IXPs) pre-approved by Roskomnadzor (Claessen, 2020); obligatory measures on ISPs to ensure the security and integrity of the RuNet (such as DPI technologies); the National Domain Name System (NDNS)[9] (Kolozaridi & Muravyov, 2021). To sum up, Russia has improved and centralized its capabilities to control its national online information space, as well as key internet resources at the domestic level. This has played out at different levels: attempts to deploy surveillance and filtering technologies, attempts to control access to online information (such as DPI), as well as policy measures aimed at censorship of online content and blacklisting of specific internet resources. This has contributed to the development of a burgeoning domestic market for internet 'black boxes', including systems for intercepting telecommunications[10]. At the internet governance level, Russia illustrates the attempt of a state to reassert sovereignty over cyberspace (after an initial period of non-intervention in the same). In line with China, Russia now tends to support a state-centric model of global internet governance favouring multilateral agreements rather than multi-stakeholder settings (Nocetti, 2015).

2.4. The Chinese Model of State-controlled Internet and AI Development

Since 2013, China has published several documents on national policy on AI and Internet (Roberts et al., 2021). In 2015, the country's State Council defined the "Internet +" action, which sought to integrate the internet into all elements of the economy and society. In 2017, the State Council outlined the country's strategy to develop artificial intelligence and become the world's leader in AI by 2030.

Enforcing the above guidelines and regulations can be very effective in China, because the state has succeeded in creating national IT champions that can compete at the international level. This has been an

[8] See ECHR, Case of ROMAN ZAKHAROV v. RUSSIA, Judgment of 4.12.2015

[9] The main idea behind the NDNS, a 'state DNS-resolver', is 'to ensure that RuNet sites will still be accessible from Russia in case of any problems with the global DNS' but its actual implementation and deployment remains unclear given the complexity of its internet architecture. *See:* Stadnik, 2021.

[10] Known in Russia as systems for operative investigative activities, SORM) and traffic filtering solutions, *See:* Ermoshina et al., 2021.

extremely swift process combining a huge market with state support to local companies and restrictions to foreign companies. Indeed, big US players such as Google, Facebook or Netflix are largely absent.

The IT development pace in China has entirely taken place in the last 35 years. The first e-mail in China was sent in 1987 and the first cable connection to the World Wide Web was built in 1994. Twenty years later, about half of the nation's population regularly used the Internet. At present, nine of the world's ten biggest IT companies (in terms of market capitalization) are based in China (Melnik, 2019).

In the country's current plans for AI, different AI national champions have been tasked with different endeavours: Baidu with anonymous driving, Alibaba with smart cities, and Tencent with computer vision for medical diagnoses (Jing and Dai, 2017). Furthermore, the government intends to use AI for moral governance, as made explicit by the social credit system promoted by the State Council since 2014, and by the deployment of surveillance technologies heavily relying on facial recognition (Anderlini, 2019). Also noteworthy are the country's strides towards "general AI" that can act autonomously in novel circumstances (Hannas et al., 2022). China's Standardization Administration states three ethics principles for AI technologies (Ding and Triolo, 2018):

1. Human interest. The ultimate goal of AI should be to benefit human welfare.
2. Liability. Accountability is a requirement for both developing and deploying AI systems and solutions. In particular, this implies a requirement of transparency, that is, of understanding how AI systems operate.
3. Consistency. On the one hand, data should be properly recorded with adequate oversight, but commercial organizations should be able to protect their intellectual property.

3. Ethical Perspective

As noted at the outset of the Paper, technology is not neutral, and the way in which technological advancement is being pushed forward by the major forces acting on the international scene is the expression of political, societal, and moral values that underlie their social structure. The historic rivalry between the US and China in the race to establish themselves as geopolitical powers "*is the expression of identity on a larger geographic scale than that of the individual nation; using the possibilities, both present and future, brought about by technological change it is the practical assertion of a distinct value-system*." (Gould, 2021, p. 2). It is interesting to see how this tension mirrors how these technologies are regulated and developed, and which values and ethical principles are at its basis.

For example, China's authoritarian system of one-party control is mirrored in surveillance technologies and internet censorship - China's "Great Firewall" allows avoiding access to information that is not in the interest of the regime to be accessed and shared (Lippert, 2020, p. 36). In doing so, it strongly constrains the freedom of individuals and their possibility to form a regime-independent opinion. This also represents a considerable constraint to human autonomy: in fact, having access to information diversity can be considered an important enabling condition for autonomy (Mittelstadt et al. 2016). This points to the concern of having a "socialism with Chinese characteristics" (Piccone, 2018, p. 7) as a viable alternative to the European model focusing on the respect of individual rights and human dignity and further stresses the need for the EU to establish itself on the international digital scene as guardant of liberal democratic values.

Even though competition among China, the USA, and the EU is increasing to establish digital spheres of influence, it can be said that *"(f)or the EU, it is not so much a question of winning or losing a race between the USA and China, but of finding the way of embracing the opportunities offered by AI in a way that is human-centered, ethical, secure, and true to our core values*" (Annoni et al., 2018, p. 120). However, Europe is, to a large extent, dependent on the US regarding social media, communication platforms, and other network-based platforms in which the US is obviously leading. The EU has positioned itself at the forefront of AI and data regulations, and this regulatory approach that sees respect for the fundamental values of the EU and the rule of law as paramount does not hinder its technological advancement. Two clear examples of how basic values are shaping the diplomatic, legal, and trade relations with Europe are the struggles with Meta and Google and the European Commission in the context of the Digital Markets acts. In this regard, the so-called 'gate-keepers' (like Google and Meta) will have to be more open to competition with smaller apps and will have to be more open about their algorithms and less aggressive and predatory with their behavioural advertising techniques. Both the applications of social media platforms with their surveillance capitalist affordances that are US-based as well as the state surveillance technologies and standards that are China-based are correctly seen as antithetical to an EU conception of the good society.

4. Technical Perspective

Standards are an essential policy instrument in the field of Internet, AI and more broadly digital governance and are aimed at providing a number of benefits and safeguards to users, ensuring expected quality and safety, informing and allowing for comparison, optimizing costs, favouring interoperability and trading, etc. A (technical) standard is a normative document describing *technical specifications*[11] of processes or of products/services. Their implementation is usually driven by market dynamics and they often have to rely on voluntary adoption obtained by consensus between experts taking part in their formulation (Rossi, 2021), which is the main difference with respect to legal documents.

Internet governance literature has demonstrated the extent to which standards and protocols are notoriously political (DeNardis, 2009), even more so as digital technologies become pervasive across the world and throughout society. Some of them are "control points" and can serve as a form of public policy (formulated mostly by private organizations), for instance by determining how innovation policy and economic competition can proceed at both national and global levels, or by constituting substantive political issues (DeNardis, 2009). As such, they are shaped by a complex web of simultaneous negotiations (Radu, 2019) aimed at improving and transforming the way users, companies and states connect online, and form an integral part of the Internet governance field. Digital standards are primarily defined by a myriad of Standard Developing Organizations (SDOs)[12]. These standardizing organizations may be understood as a (distributed) field of struggle (Pohle & Voelsen, 2022) for companies and states alike, and they are arenas where powerful actors deploy their influence efforts to defend their political and economic interests through the formulation of technical standards and protocols (Zittrain, 2008).

In the EU, only standards developed by European Standards Organizations (ESOs) are recognised as European Standards[13]. Harmonized standards are produced by ESOs based on a formal request issued by the European Commission. The survey by (Nativi and De Nigris, 2021) investigates the alignment between twenty-two AI standards by ISO/IEC and ETSI, and the eight requirements proposed in the proposal of the EU Artificial Intelligence Act: data and data governance; technical documentation; record keeping; transparency and information to users; human oversight; accuracy, robustness and cybersecurity; risk management; quality management. In the outcome, while there is not a single standard covering all of the requirements, for five of them there is some standard with a very high level of operationalisation of the requirement (making it hard to measure its fulfilment in practice) and for the remaining three requirements there is some standard with high level of operationalisation. Around 140 AI-related standard specifications are expected to be published in the period 2022-2024 (Nativi and De Nigris, 2021). The key initiatives include the ISO/IEC JTC 1/SC 42[14], the IEEE P7000[15], the ETSI SAI[16], and the ITU-T standard series on Machine Learning for 5G[17].

Several national pathways for the standardization of AI have been issued, such as the US NIST plan for federal AI standards engagement[18], the EU rolling plan for ICT standardization[19] (Chapter on AI), the China Standards 2035[20], the German roadmap of AI standardization[21], and the Australian AI Standards roadmap[22]. The development and adoption of one standard over another can confer a competitive advantage to companies or to national economies, or even put them in a dominance position in the global market. Thus, standardization becomes a strategic value, and standards can become a source of power in international politics (Wei 2021) - especially after the state-directed approach of China (Rühlig, 2020).

---

[11] The IETF defines standards as 'a specification of a protocol, system behavior or procedure that has a unique identifier' (RFC 3935, IETF), while the W3C usually refers to the word 'specification' instead of 'standard'.

[12] The Internet Engineering Task Force (IETF); the World Wide Web Consortium (W3C); the Internet Corporation for Assigned Names and Numbers (ICANN); the ITU Telecommunication Standardization Sector (ITU-T); the Organization for the Advancement of Structured Information Standards (OASIS); the Institute of Electrical and Electronics Engineers (IEEE).

[13] ESOs include: the European Committee for Electrotechnical Standardisation (CENELEC); the European Committee for Standardisation (CEN); the European Telecommunications Standards Institute (ETSI).

[14] Standardization committee on Artificial intelligence is organized into five working groups covering foundational standards (WG1), data (WG2), trustworthy AI (WG3), use cases and applications (WG4), and computational approaches (WG5), See: https://www.iso.org/committee/6794475.html

[15] IEEE P7000 standards being developed by the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems focus on ethical aspects of the implementation of intelligent systems, See: https://ethicsinaction.ieee.org/p7000/

[16] ETSI Securing Artificial Intelligence (SAI) standard series consider using AI to enhance security, mitigating against attacks that leverage AI, and securing AI itself from attacks, See: https://www.etsi.org/committee/1640-sai

[17] ITU-T standard is specialized in the field of telecommunication networks, See: https://www.itu.int/hub/2020/07/international-standards-for-an-ai-enabled-future/

[18] https://www.nist.gov/artificial-intelligence/plan-federal-ai-standards-engagement

[19] https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2022

[20] https://www.horizonadvisory.org/chinastandards

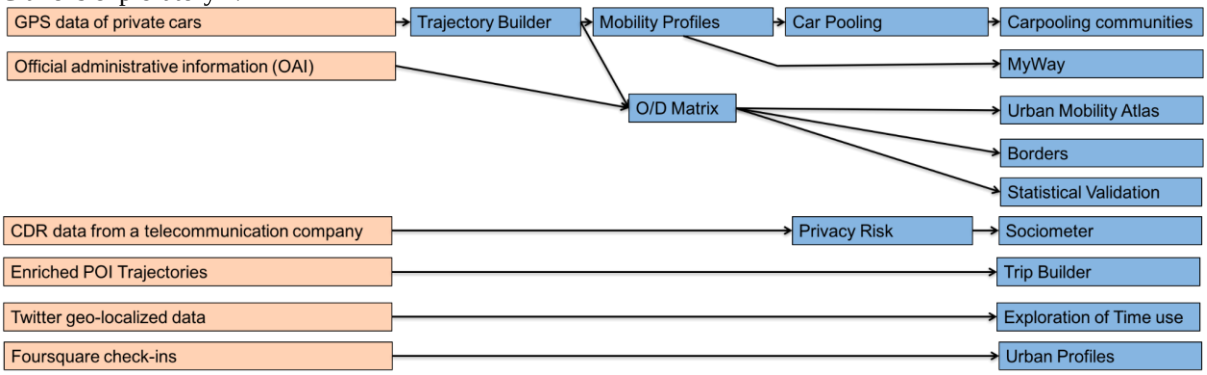
[21] https://www.din.de/en/innovation-and-research/artificial-intelligence/ai-roadmap

[22] https://www.standards.org.au/news/standards-australia-sets-priorities-for-artificial-intelligence

5. Implementations within SoBigData++ Research Infrastructure

Within the SoBigData++ initiative, the consortium applied the EU ethical framework in terms of legal compliance (e.g., with respect to the GDPR) and the ethical framework that we built on top of the law. The legal framework has been translated into concrete implementations (Forgó et al. 2020), such as compliance with intellectual property rights via SoBigData Gateway Terms of Use[23], a privacy risk assessment methodology to quantify the empirical risk of re-identification of data subjects in a particular dataset.

The application of main legal and ethical principles can be illustrated by the Sustainable Cities for Citizens exploratory[24]:



Here, one can see several sources and kinds of data (the left column) and the possible steps we included in the SoBigData RI, i.e., methods that can be found in the SoBigData Catalogue, ready to be applied to other similar data. At the end of the workflow, a specific service (indicated in the right column) can be developed. More details can be found in (Gionis and Mathioudakis, Trasarti and Grossi).

Some implementations make use of the Call Detail Record (CDR) data stemming from telecommunication operators. This data originally tracks every single call a data subject performed in a time window, along with the timestamp in which the call starts/ends and the position of the antenna(s) managing the traffic, i.e., the area(s) in which the call is performed. In this case, data is aggregated in Individual Call Profiles (ICPs) according to three different time windows (i.e., morning, afternoon, and night), and it is summarized between weekdays and weekends. I.e., the ICP represents a spatio-temporal aggregation showing the presence of a user in a certain area of interest during different predefined time slots. This kind of data is suitable for the development of the *Sociometer*[25], a service in which we are interested in quantifying residents, commuters, and visitors in a certain area. Indeed, a resident can perform calls in every possible time slot, while a commuter will not be present during the nights or on the weekends; a visitor has a profile similar to a resident but for a limited amount of time (usually hours or days). As a middle passage between the ICP generation and the Sociometer deployment, a *Privacy Risk Assessment* module[26] has been deployed, where ICPs are tested by varying the possible background knowledge of the adversary (e.g., the adversary already knows the activity of his/her target during the first two weeks) offering, for each data subject, the actual risk to be correctly re-identified in the dataset. Our studies showed that, due to the aggregated nature of the data, this privacy risk is relatively low even if we consider strong background knowledge (Pratesi et al., 2017). For example, considering an Italian municipality, if we hypothesize that the attacker knows 1 week of calls of his/her target, the probability he/she succeeds in re-identification is extremely low, since for 95% of users the privacy risk is below 0.05 (i.e., they are indistinguishable from at least 199 others), while knowing 2 weeks, we have that only 10% of users have a risk greater than 0.2 (corresponding to an anonymity set of size 5), and knowing 3 weeks this risk is associated with 35% of individuals. However, even if the adversary knows 4 weeks of phone activities, the risk of re-identification of 60% of users is always below 0.05 (i.e., the anonymity set is greater than 20).

6. Outcomes

The above assessment suggests three main approaches to regulating Internet, AI and digital technologies. The US approach is basically market-oriented with government intervention being limited to pocket areas such as healthcare. Russia and China favour state control internally and also at the international level; yet, their motivation

[23] https://sobigdata.d4science.org/catalogue-sobigdata
[24] https://sobigdata.d4science.org/web/cityofcitizens
[25] http://data.d4science.org/ctlg/ResourceCatalogue/sociometer
[26] http://data.d4science.org/ctlg/ResourceCatalogue/privacy_risk_on_sociometer

is more to protect the state than to protect the citizens. Finally, the European Union puts the citizen at the center of its regulations. Although the EU approach can be construed as being more ethics-driven than the other two, it may also be less effective than the other two approaches, due to the lack of suitable incentives.

The US approach largely gives free rein to Internet companies and IT conglomerates, which have the usual corporate incentives to develop and deploy better, more attractive or more profitable technologies. Compliance with the pocket area restrictions can be enforced with sanctions aimed at deterring abuse. Furthermore, US government agencies can request cooperation of US-based Internet and IT companies in matters of national security.

The Russian and Chinese state-centered model is enforced by leveraging the extensive control mechanisms available to such authoritarian states. Foreign companies cannot operate in those countries unless they adhere to their regulations and, even so, their activity is subject to several constraints. Beyond ensuring state dominance, constraints on foreign corporations have been useful to protect national companies. As a result of this process, China has succeeded in creating national IT and Internet champions (Melnik, 2019), such as Alibaba, Tencent, Huawei and Baidu, among many others. Such champions have been able to thrive thanks to China's enormous internal market and state-protected capitalism, but they are tightly controlled by the Chinese government (Srinivasan, 2021). Today, they are not only instrumental at implementing the state control on information technologies, but they also extend China's worldwide influence in this domain.

The EU principle of protecting the individual is in line with the Union's foundational principles. At the same time, for several reasons, there are very few big IT corporations left that are headquartered in the EU, let alone Internet corporations. Hence, the European regulator has had, to a large extent, a free hand to impose constraints on the activity of Internet and IT companies without facing pressure from the European industry. A synergy between protecting the basic rights and enhancing the European IT industry vs foreign corporations is possible in view of fostering local IT champions in a more ethically aligned manner. Yet, the European model has a problem of incentives, both at the corporate level and at the individual level:

- The fragmentation of the European market and the tradition of national telecommunications monopolies are relevant factors. Whereas in the US and China a new IT product can be directly launched to a market with hundreds or thousands of millions of consumers, in the EU the language, cultural and political barriers make it harder for a new product to quickly reach all European member states (Baroudy et al., 2020). On the other hand, the European ecosystem of IT companies has been less innovative than its US counterpart and less state-backed/protected than its Chinese counterpart[27].
- The EU approach to IT regulation centered on individual rights and ethical values may also be a reason why new IT solutions are harder to deploy in Europe than in the other blocs. The COVID19 contact tracing apps are a case in point. While South Korea and China were able to quickly enforce the general adoption of such apps[28], the situation was quite different in the EU. For criticism for privacy reasons and privacy-preserving protocols introduced by academics and taken over by commercial Google and Apple apps, the effective use of automated contact tracing has stayed low in most European countries (Kahnbach et al., 2021). Being autonomous to decide whether to use contact tracing apps, the European citizen had little incentive to do so for energy consumption and negative news. Adoption of contact tracing apps was also low in the US, in this case mainly due to the libertarian tradition of distrusting governmental control (Zhang et al., 2020).

To conclude, since the EU has chosen an approach to IT regulation that puts individual rights and ethical values at the center of the stage, it has to take into account that autonomy is among those rights and values. This means that incentives for citizens must also be provided for if the EU wants to ensure an effective operation of the IT sector and stop lagging behind the other two main blocs.

References

1. Agius, E., Cambon-Thomsen, A., Carvalho, A. S., Gefenas, E., Kinderlerer, J., Kurtz, A., ... & van den Hoven, M. J. (2021) Values for the Future: The Role of Ethics in European and Global Governance by the European Group on Ethics in Science and New Technologies (EGE).
2. Anderlini, J. (2019). How China's smart-city tech focuses on its own citizens. Financial Times, 5.

[27] With some exceptions (notably in the Nordic countries), it has been dominated by risk-averse large players (Braga Malta, 2015), such as former national telecommunications monopolies (e.g. France Telecom, Deutsche Telekom, British Telecom, Telefonica, Telecom Italia, etc.) or big industrial conglomerates (e.g. Siemens, Alcatel, etc.) which did not place Internet or AI at the top of their priorities.

[28] Developing and deploying automated contact tracing in those countries was quick because apps were simple and centralized, no sizable opposition objected against such centralization, the governments of those countries were able to require their citizens to download and install contact tracing apps. *See:* Huang et al., 2020.

3. Annoni, A., Benczur, P., Bertoldi, P., Delipetrev, B., De Prato, G., Feijoo, C., ... & Junklewitz, H. (2018). Artificial intelligence: A european perspective.
4. Asmolov, G., & Kolozaridi, P. (2021). 'Run Runet runaway: The transformation of the Russian Internet as a cultural-historical object'. In The Palgrave Handbook of Digital Russia Studies, (pp. 277-296). Palgrave Macmillan, Cham.
5. Baroudy, K., Janmark, J., Satyavarapu, A., Strålin, T., & Ziemke, Z. (2020). Europe's startup ecosystem: Heating up, but still facing challenges. McKinsey and Company article, October, 11.
6. Bendett, S., & Kania, E. (2019). A new Sino-Russian high-tech partnership. Australian Strategic Policy Institute, 29.
7. Braga Malta, D. (2015) "4 things holding back European innovation - and 4 ways to unleash it", World Economic Forum.
8. Claessen, E. (2020). Reshaping the internet–the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU. Journal of cyber policy, 5(1), 140-157.
9. DeNardis, L. (2009). Protocol politics: The globalization of Internet governance. Mit Press.
10. Ding, J., & Triolo, P. (2018). Translation: Excerpts from China's 'White Paper on Artificial Intelligence Standardization'. New America.
11. Ermoshina, K., Loveluck, B., & Musiani, F. (2021). A market of black boxes: The political economy of Internet surveillance and censorship in Russia. Journal of Information Technology & Politics, 1-16.
12. Ermoshina, K., & Musiani, F. (2017). 'Migrating servers, elusive users: Reconfigurations of the Russian Internet in the post-Snowden era'. Media and Communication, 5(1), 42-53.
13. Ermoshina, K., & Musiani, F. (2021). 'The Telegram ban: How censorship "made in Russia" faces a global Internet'. First Monday, 26(5).
14. European Commission (2022). European Declaration on Digital Rights and the Digital Decade. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0028
15. European Commission (2021). Proposal for a Regulation of the European Parliament and the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. http://digital-strategy.ec.europa.eu/en/library/proposal-regulation-layingdown-harmonised-rules-artificial-intelligence-artificial-intelligence.
16. Federal Law of the Russian Federation (2020) "About carrying out experiment on establishment of special regulation for the purpose of creation of necessary conditions..." at: https://cis-legislation.com/document.fwx?rgn=124089.
17. Federal Law of the Russian Federation (2021) "About experimental legal regimes in the field of digital innovations in the Russian Federation" at: https://cis-legislation.com/document.fwx?rgn=126433.
18. Federal Trade Commission (2019). FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook
19. Federal Trade Commission. (2020). Using Artificial Intelligence and Algorithms. https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-algorithms
20. Forgó, N., Hänold, S., van den Hoven, J., Krügel, T., Lishchuk, I., Mahieu, R., ... & van Putten, D. (2021). An ethico-legal framework for social data science. International Journal of Data Science and Analytics, 11(4), 377-390.
21. Gainutdinov, D. and Chikov, P. (2022) Russia: human rights in the position of war. The first month of the armed conflict in Ukraine/Д. Гайнутдинов, П. Чиков, Россия: права человека на военном положении. Первый месяц вооруженного конфликта в Украине, Non-governmental report, published 26.03.2022
22. Gerke, S., Minssen, T., Cohen, G. (2020) Ethical and Legal Challenges of artificial intelligence-driven healthcare, Artificial Intelligence in Healthcare, Elsevier Inc., doi: https://doi.org/10.1016/B978-0-12-818438-7.00012-5.
23. Gionis, A. and Mathioudakis, M. D9.1 Social mining method and service integration 1, 654024 SoBigData Research Infrastructure Social Mining & Big Data Ecosystem, http://project.sobigdata.eu/material
24. Government of the Russian Federation (19.12.2020) N 2174/ Постановление Правительства Российской Федерации от 19.12.2020 № 2174 at: http://publication.pravo.gov.ru/Document/View/0001202012220048.
25. Hannas, W. C., Chang, H.-M., Chou, D. H., & Fleeger, B. (2022). China's Advanced AI Research: Monitoring China's Paths to "General" Artificial Intelligence. CSET-Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/chinas-advanced-ai-research/
26. Hobbs, C. (2020). Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry. European Council on Foreign Relations, 26
27. Huang, Y., Sun, M., & Sui, Y. (2020). How digital contact tracing slowed Covid-19 in East Asia. Harvard Business Review, 15(04).
28. Jing, M., & Dai, S. (2019). China recruits Baidu, Alibaba and Tencent to AI 'national team'. South China Morning Post.
29. Johns, N, 'Regulating the Digital Economy' (Observer Research Foundation, 2015), 2.
30. Kahnbach, L., Lehr, D., Brandenburger, J., Mallwitz, T., Jent, S., Hannibal, S., ... & Janneck, M. (2021). Quality and adoption of COVID-19 tracing apps and recommendations for development: Systematic interdisciplinary review of European apps. Journal of medical Internet research, 23(6), e27989.
31. Kolozaridi, P., & Muravyov, D. (2021). Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case. First Monday.
32. Lander, E., & Nelson, A. (2021). Americans Need a Bill of Rights for an AI-Powered World. Wired. https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/?tpcc=nleyeonai

33. Lippert, B., & Perthes, V. (Eds.). (2020). Strategic rivalry between United States and China: causes, tragectories, andimplications for Europe (SWP Research Paper, 4/2020). Berlin: Stiftung Wissenschaft und Politik -SWP-DeutschesInstitut für Internationale Politik und Sicherheit. https://doi.org/10.18449/2020RP04
34. Melnik, J. (2019). China's "National Champions" Alibaba, Tencent, and Huawei. Education About Asia, 24(2), 28-33.
35. Min, S. (2019). Google to pay $170 million for violating kids' privacy on YouTube. CBS News. https://www.cbsnews.com/news/ftc-fines-google-170-million-for-violating-childrens-privacy-on-youtube/
36. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 2053951716679679.
37. Nanni, M., Andrienko, G., Barabási, A. L., Boldrini, C., Bonchi, F., Cattuto, C., ... & Vespignani, A. (2021). Give more data, awareness and control to individual citizens, and they will help COVID-19 containment. Ethics and Information Technology, 23(1), 1-6.
38. Nativi, S., De Nigris, S. (2021). AI Standardisation Landscape: state of play and link to the EC proposal for an AI regulatory framework, EUR 30772 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-40325-8, doi:10.2760/376602, JRC125952.
39. Neznamov, A., Legal Regulation of Artificial Intelligence. Legal aspects of the implementation of the national strategy for the development of Artificial Intelligence until 2030/ А. Незнамов, Правовое Регулирование искусственного интеллекта. Правовые аспекты реализации национальной стратегии развития искусственного интеллекта до 2030 года, Vector of legal science, N 12/2019, pp. 82-88.
40. Nocetti, J., 'Contest and conquest: Russia and global internet governance'. International Affairs, 91(1), 2015, 111-130.
41. OECD.AI (2021), powered by EC/OECD (2021), database of national AI policies, accessed on 8/06/2022" https://oecd.ai/en/dashboards
42. Pereyra, M. (2021). The State of Artificial Intelligence in the United States. Fordham Journal of Corporate and Financial Law, Law-Blog: https://news.law.fordham.edu/jcfl/2021/11/29/the-state-of-artificial-intelligence-in-the-united-states/
43. Pesapane, F., Volonté, C., Codari, M., & Sardanelli, F. (2018). Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. Insights into imaging, 9(5), 745-753.
44. Piccone, T. (2018). China's long game on human rights at the United Nations. Brookings Institution, September, 7.
45. Pohle, J. and Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order. Policy & Internet, 14(1), pp.13-27.
46. Pratesi, F., Monreale, A., Giannotti, F., & Pedreschi, D. (2017, November). Privacy preserving multidimensional profiling. In International Conference on Smart Objects and Technologies for Social Good (pp. 142-152). Springer, Cham.
47. Radu, R. (2019). Negotiating internet governance. Oxford: Oxford University Press.
48. Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices.
49. Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. AI & society, 36(1), 59-77.
50. Rossi, J. (2021). 'What rules the Internet? A study of the troubled relation between Web standards and legal instruments in the field of privacy'. Telecommunications Policy, 45(6), 102143.
51. Rühlig, T. M. (2020). Technical standardisation, China and the future international order: A European perspective. Heinrich-Böll-Stiftung European Union.
52. Srinivasan, R. (2021) "China's clampdown on national technology champions: Xi's new industrial statism, triumphalist hubris and art of jiu-jitsu", Swarajya, Aug. 13.
53. Stadnik, I. (2021). Control by infrastructure: Political ambitions meet technical implementations in RuNet. First Monday.
54. Trasarti, R. (CNR) and Grossi, V. (CNR), D9.2 Social mining method and service integration 2, 654024 SoBigData Research Infrastructure Social Mining & Big Data Ecosystem, http://project.sobigdata.eu/material
55. United Nations General Assembly (March 2021). Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final substantive report. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
56. Van den Hoven, J., Comandé, G., Ruggieri, S., Domingo-Ferrer, J., Musiani, F., Giannotti, F., ... & Stauch, M. (2021). Towards a digital ecosystem of trust: Ethical, legal and societal implications. Opinio Juris In Comparatione, (1/2021), 131-156.
57. Wei, K. (2021). China's Standards Development Strategy and Foreign Policy. FY2020 SSU-Working Paper No. 3. The University of Tokyo .https://ifi.u-tokyo.ac.jp/en/ssu-report/8993/
58. White House. (2020). Guidance for regulation of artificial intelligence applications. Memorandum For The Heads Of Executive Departments And Agencies. https://www.ai.gov/white-house-guidance-for-regulation-of-artificial-intelligence-applications/
59. Wijermars, M. (2021). 'Selling internet control: the framing of the Russian ban of messaging app Telegram'. Information, Communication & Society,1-17.
60. Zhang, B., Kreps, S., McMurry, N., and R. Miles McCain (2020) "Americans' perceptions of privacy and surveillance in the COVID-19 pandemic", Plos One, 15(2):e0242652.
61. Zittrain, J. (2008). The future of the Internet—And how to stop it. New Haven: Yale University Press.