Social Mining & Big Data Analytics

SoBigData

RESEARCH INFRASTRUCTURE ++

Deliverable D2.3

Ethics and Legality Framework activities 2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871042

DOCUMENT INFORMATION

PROJECT	
PROJECT ACRONYM	SoBigData-PlusPlus
PROJECT TITLE	SoBigData++: European Integrated Infrastructure for Social Mining and Big Data Analytics
STARTING DATE	01/01/2020 (60 months)
ENDING DATE	31/12/2024
PROJECT WEBSITE	http://www.sobigdata.eu
TOPIC	INFRAIA-01-2018-2019 Integrating Activities for Advanced Communities
GRANT AGREEMENT N.	871042

DELIVERABLE INFORMATION	
WORK PACKAGE	WP2 NA1 - Responsible Data Science
WORK PACKAGE LEADER	TUDelft
WORK PACKAGE PARTICIPANTS	CNR, UNIPI, SSSA, KCL, LUH, CNRS, URV
DELIVERABLE NUMBER	D2.3
DELIVERABLE TITLE	Ethics and Legality Framework activities 2
AUTHOR(S)	Juan M. Durán (TUDelft)
CONTRIBUTOR(S)	Giorgia Pozzi (TUDelft), Francesca Pratesi (CNR), Denise Amram (SSSA), Roberto Pellungrini (SNS), Mark Coté (KCL), Josep Domingo-Ferrer (URV), Iryna Lishchuk (LUH), Francesca Donati, Giovanni Comandé (SSSA), Ilaria Barsanti (CNR)
EDITOR(S)	Valerio Grossi (CNR)
REVIEWER(S)	Marco Braghieri (KCL), Roberto Pellungrini (SNS)
CONTRACTUAL DELIVERY DATE	31/12/2022
ACTUAL DELIVERY DATE	09/01/2023
VERSION	V1.0
TYPE	Report
DISSEMINATION LEVEL	Public
TOTAL N. PAGES	42
KEYWORDS	Privacy, ethics, data science

EXECUTIVE SUMMARY

This deliverable provides a full report of the relevant activities carried out, ongoing, and planned during the period 1st July 2022 - 31st December 2022 by Work Package 2: NA1 - Responsible Data Science (hereby WP2) and its Tasks.

The document is structured as follows. Section 1 reports on the relevance of WP2 for the other work packages within the consortium SoBigData++. Section 2 reports on the general activities carried out by all the members of WP2. Section 2 is subdivided into the following sections: subsections 2.1 to 2.4 report on each individual task's activities as well as collaborations; subsection 2.5 reports on the publications by the members of WP2. Finally, the appendixes include extra details about activities mentioned in this deliverable. Appendix A reports on the statistics of TransNational Access and Micro-Projects (as indicated in sections 2.1 to 2.4) and appendix B contains the white paper to be published by the High-Level Advisory Board.

DISCLAIMER

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871042.

SoBigData++ strives to deliver a distributed, Pan-European, multi-disciplinary research infrastructure for big social data analytics, coupled with the consolidation of a cross-disciplinary European research community, aimed at using social mining and big data to understand the complexity of our contemporary, globally-interconnected society. SoBigData++ is set to advance on such ambitious tasks thanks to SoBigData, the predecessor project that started this construction in 2015. Becoming an advanced community, SoBigData++ will strengthen its tools and services to empower researchers and innovators through a platform for the design and execution of large-scale social mining experiments.

This document contains information on SoBigData++ core activities, findings and outcomes and it may also contain contributions from distinguished experts who contribute as SoBigData++ Board members. Any reference to content in this document should clearly indicate the authors, source, organisation and publication date.

The content of this publication is the sole responsibility of the SoBigData++ Consortium and its experts, and it cannot be considered to reflect the views of the European Commission. The authors of this document have taken any available measure in order for its content to be accurate, consistent and lawful. However, neither the project consortium as a whole nor the individual partners that implicitly or explicitly participated the creation and publication of this document hold any sort of responsibility that might occur as a result of using its content.

GLOSSARY

EU	European Union
EC	European Commission
H2020	Horizon 2020 EU Framework Programme for Research and Innovation
VA	Virtual Access
TA	Transnational Access
BOEL	Board for Operational Ethics and Legality
XAI	Explainable Artificial Intelligence

TABLE OF CONTENTS

1 Relevance to SoBigData++

This document provides a full report of relevant activities carried out, ongoing, and planned during the period 1st July 2021 - 31st December 2022 by Work Package 2: NA1 - Responsible Data Science (hereby WP2) and its Tasks.

1.1 Purpose of this document

The document corresponds to deliverable **D2.3: Ethics and Legality Framework activities** according to WP2. The deliverable must be a report describing activities performed in the WP2 as a whole and specifically activities carried out in the various boards and tasks.

1.2 Relevance to project objectives

This document complies with the objectives established for WP2 consisting in gathering innovative and proactive responses to structural problems currently emerging in social and cultural data analytics, such as online information disorder, the Facebook data privacy breach and algorithmic bias and discrimination. This is ensuring that the project not only develops best practices and resources for social and cultural data analytics practitioners, and it is granting a wider, informed, engaged and equitable participation and impact. To this end, the tasks related to WP2 have carried out a series of activities as described in Section 2.

1.3 Relation to other work packages

WP2 carried out and planned different activities independently as well as in close collaboration with several other WPs. These activities focus on emerging ethical and social concerns that transpire from the analysis and validation of usage of data mining resources. Of particular relevance are the following WPs:

- WP3: Dissemination, Impact, and Sustainability
- WP4: Training
- WP5: Accelerating Innovation
- WP6: Transnational Access
- WP7: Virtual Access
- WP8: Social Mining and Big Data Resource Integration
- WP10: Exploratories

Naturally, the BOEL as well as the High-Level Advisory Board is attending all ethical and legal consultations required within SoBigData++ by any WP and/or its members.

1.4 Structure of the document

The document is structured as follows. Section 1 reports on the relevance of WP2 for the other work packages within the consortium SoBigData++. Section 2 reports on the general activities carried out by all the members of WP2. Section 2 is subdivided into the following sections: subsections 2.1 to 2.4 report on each individual task's activities as well as collaborations; subsection 2.5 reports on the publications by the members of WP2. Finally, the appendixes include extra details about activities mentioned in this deliverable. Appendix A reports on the statistics of TransNational Access and Micro-Projects (as indicated in sections 2.1 to 2.4) and appendix B contains the white paper to be published by the High-Level Advisory Board.

2 Report on WP2 activities

Activities carried out by WP2 partners under SBD acknowledgment:

UNIPI: On September 19th 2022 ECML PKDD hosted the 4th Int. Workshop on eXplainable Knowledge Discovery in Data Mining (XKDD).
XKDD was organised by UNIPI members Riccardo Guidotti and Anna Monreale. The proceedings will be soon available in Springer's Lecture Notes in Computer Science.

URV: The main SoBigData++ event organised during the period 1 July - 1 November 2022 was the organisation of the PSD 2022 conference, which was held in Paris, France. The conference was attended by over 70 individuals and its proceedings have been published by Springer in the Lecture Notes in Computer Science series 13463.
https://link.springer.com/book/10.1007/978-3-031-13945-1

CNR: With SNS, CNRi co-organized a *workshop*, i.e. the 1st International Workshop on Imaging the AI Landscape After the AI Act (in conjunction with the first International Conference on Hybrid Human-Artificial Intelligence, physically held at the Vrije Universiteit Amsterdam, Netherlands, on June 13, 2022. This workshop's goal was to assess from a multidisciplinary point of view (i.e., law experts and technicians) how the new EU regulation proposal could shape AI technologies of the future. The event was structured with 2 invited talks from international experts, 11 peer-reviewed papers presentations, and one group activity. The participants in the event were 30 in total, roughly half male and half female, mostly early career researchers, PhD students, and academics. More information in the event can be found at: http://iail2022.isti.cnr.it/

TU Delft:
In the timeframe between July 1st 2021 and December 31st 2022, TU Delft carried out the following activities:

- On november 12th, 2021 TU Delft organised an online workshop in collaboration with the World Health Organization entitled: *Ethics and Governance of Artificial Intelligence for Health: The Importance of Design for Values.* More details regarding the workshop can be found in a contribution published in the SoBigData magazine no. 7 / Winter 2021-2022 (authors: Giorgia Pozzi, Jeroen van den Hoven, Juan M. Durán).
- From May 23rd to May 25th 2022, TU Delft organised a workshop on XAI (Explainable Artificial Intelligence) entitled: Workshop series Issues in XAI 4: "Explanatory AI: Between Ethics and Epistemology" (https://juanmduran.net/xai4/)
- On November 25th, 2022 TU Delft organised a hybrid workshop in collaboration with the World Health Organization entitled "Design for Values in AI for Medicine and Healthcare" (https://www.tudelft.nl/evenementen/2022/tbm/design-for-values-in-ai-for-medicine-and-healthcare).

2.1 Task 2.1. Board of Operational Ethics and Legality

Task leader: TUDelft
Participants: LUH, CNR, SSSA

The Board of Operational Ethics and Legality is promoting the Micro-Project "BOEL Works", which is providing a recommendation service to all the members of SoBigData++. This service is exclusively focused on assisting the consortium members' concerns regarding legal, ethical, and societal questions brought about by their research. This recommendation service could be used to seek advice on the methodological approach (references, tools, standards, and policies etc.) to be applied in several contexts of their research (e.g. for grant applications, academic essays, databases, and research outreach, workshops etc) in order to successfully deal with the ethical-legal and societal-related aspects. In this context, the BOEL provides first assistance to improve individual as well as groups awareness on the ethical, regulatory, and societal implications in data science and to facilitate an accountable problem-solving approach towards the research.

The "BOEL Works" Micro-Project is a continuous MP, renewed every 6 months. In the following, we report an overview of the service provided by the BOEL regarding the requests received in the timeframe 1st July 2021-1st January 2023. In this timeframe, the requests received were almost exclusively TNA requests. We specify in the following when a particular request was not a TNA request. For practical reasons, we report the activity of the BOEL in the timeframe previously indicated according to the different phases in which the MP took place.

MP1
On 15 July, the BOEL received a request on Twitter data, i.e., the Societal Debates exploratory, and it has ETH as destination. On July, 19th (4 days later), sub-group 2 positively answered. However on 27 July the applicant provided further details to the BOEL and we provided an updated evaluation on 3 August (after 7 days).

On 21 July, an application on conversational assistant systems (again, the Societal Debates exploratory is involved) was received. CNR was the chosen destination. This time, sub-group 1 asked for additional information after 15 days, i.e., on 8 August.

The same application also regards another project concerning medical data, i.e., related to the Network Medicine exploratory, with UNIROMA as final destination. The details on this application are the same as the previous one.

Finally, on 29 July , we received a project, again on Twitter data (Societal Debates); this time USFD was the selected destination. This request is managed by sub-group 2, but due to the summer break we were not able to finish before the MP ended. This request was quite problematic, and it required more effort and internal discussion by the BOEL sub-group 2.

MP2
Except for the request received on 18 October all other requests come from the Transnational access program.

The first request was received on 12 October 2021. The proposal aimed at extracting the dynamics of social activities on Twitter with the overarching goal of analysing social phenomena such as polarisation,echo chambers, etc. The proposal received a green light from the BOEL.

The second request was received on 13 October 2021. The proposal addressed the topic of scalable interpretable document ranking. The response of the BOEL was positive and was provided on 3 December.

The third request was received on 18 October 2021. . The goal of the proposal is to investigate whether people returned to their habits regarding physical activity and quality of life post lockdown, compared to the pre-lockdown. The response provided by the BOEL on 3 December .

The fourth request was received on 20 December. The proposal is on the topic of ordinal quantification methods inspired by astro-particle physics. The BOEL provided a positive response on 2 February 2022

The fifth request was received on 20 December. The original request's goal was on improving the explanation of sentiment analysis in the NLP context. After reviewing the request, the BOEL deemed the proposal as lacking details, particularly regarding data collection and processes. This answer was provided on 1 February. In the face of the BOEL's comments, the applicant resubmitted the application on 8 February. Unfortunately, the BOEL deemed also this second application as incomplete and lacking details, in particular regarding the data collected. This response was provided on 1 April..

The sixth request was submitted on 20 December on the topic of bitcoins price bubbles on Twitter. Besides the advice of ensuring compliance with the ETHZ, the BOEL did not find this submission problematic. The reply was provided to the applicant on 3 February.

On 11 January, BOEL received an integration to an application originally submitted on29 July. As indicated in the previous report, this application was quite problematic and required particular attention from BOEL members. In this novel integration, the applicant provided more information regarding the data collection process, as requested by the BOEL. The answer was provided on 23 March. .

The seventh application was received on 4 February. The topic of the application was interpretability by design.The request received green light from the BOEL. The reply was sent on 23 March.

The eighth request was received on21 February. The request was on the topic of Explainable AI (XAI). The BOEL responded positively to the request on 23 March

The ninth request was submitted on28 February. The BOEL sent a positive reply on 5 April.

Finally, the tenth application was received on 29 March. The goal of the project is to develop an agent-based opinion formation model over dynamic social networks. The BOEL did not approve the request in its original form due to a lack of information regarding the data gathered. In view of the BOEL's feedback, the applicant resubmitted an integration to her application on 11 April. The BOEL approved this updated version of the application. The reply was sent a day later, on 12 April.

MP3

In the period starting from 10 May 2022 to 10 November 2022 the BOEL received a total of 15 new requests and 8 integrations. Moreover, 5 requests and 1 integration were received in the period of the previous BOEL MP but were unswered during the current BOEL MP. For this reason, we include these in this report.

We shall begin with the request received in the timeframe of the previous MP but answered during the current MP.

On 14 April the BOEL received an integration. This application received a positive reply by the BOEL on 17 May.

On 29 April a request was received on explainable and trustworthy AI for anomaly detection in cellular networks. The BOEL replied negatively on 17 May to this request due to a lack of information regarding the dataset used in the study. The applicant submitted an integration on 23 May. The BOEL replied with a green light on 30 May.

On 29 April the BOEL received a request on the topic of sustainable cities for citizens. The BOEL deemed the request unproblematic and responded with a green light on 30 May.
A further request was received by the BOEL on 2 May . This request received the BOEL's approval on 30 May.

On 2 May the BOEL received a request on the topic of how to summarise information in an extended time of crisis on social media. The reply of the BOEL was sent on 30 May . In this reply, the BOEL requested more information from the applicant. On 15 August, the applicant submitted an integration to her application. After re-evaluation from the BOEL, the application received the green light on 1 September.
On 2 May, a further request was received on the topic of measuring and modelling algorithmic bias and fairness. The BOEL replied on 30 May with concerns regarding data protection and the need for further information. On 15 August the applicant replied to the BOEL ensuring that all data will be anonymized in the research. Upon this clarification, the BOEL replied positively on 1 September.

On 11 May a request was received for a study investigating the relationship between human mobility behaviour and socio-economic, environmental, and epidemiological factors. The BOEL's reply on 30 May required further information in order to grant approval. Following on the BOEL's request for further information, an integration to the original request has been submitted by the applicant on 31 May. A positive reply from the BOEL (even though under the heading of "attention needed") was sent to the applicant on 16 June.

On 12 May a request was received on the topic of integrating trajectory data. In its response sent on 30 May, the BOEL did not approve the request since it was missing an ethical self-assessment. The applicant submitted an integration to her application on 2 June. The BOEL approved the request on 23 June, even though some points still require the applicant's attention.

On 31 May, a request was received on the topic of efficient querying of special data. The response provided by the BOEL on 16 June was positive, but the applicant has been encouraged to pay attention to the fact that the data he deals with can be potentially re-identifiable.

On 4 July a request was received on the topic of echo chambers in politics using Reddit data. The BOEL provided a positive response on 15 July, however suggested to the applicant to pay attention to possible re-identification issues.

On 6 July a request was received on the topic of biclustering in Telecom data. The response of the BOEL reported possible issues in terms of data protection and lack of clarification regarding the ethical self-assessment. For these reasons, theBOEL's first response was not positive (it was sent on 15 July). The applicant submitted an integration to the application on 25 July and received green light from the BOEL on 9 August.

On 21 July a request was received regarding a research proposal on the generation of cellular network traffic. The response of the BOEL (sent on 9 August) was negative due to issues in terms of transparency and regarding an incomplete self-assessment. The applicant submitted an integration on 29 August. In the face of the integrations, on 1 September the BOEL deemed conditional approval acceptable at discretion of the supervisor.

On 21 July BOEL received a request on "Analyzing raw tweets in a rumor detection task". Unfortunately, due to a lack of information, the request has not been granted approval by the board on 9 August. The applicant submitted an integration to the original application on 17 August. Considering the integration made to the application, the BOEL granted approval on 1 September September.

On 16 August, an application entitled "Balancing centrality measures in social networks by rewiring" was received by the board. The BOEL positively replied on 1 September yet raising some relevant points for the applicant.

On 23 August, an application was received on the topic of the spreading of misinformation on social networks. The BOEL positively replied to the request on 1 September.

On 23 August, a further request was received on "Privacy preserving ambient sensor data analysis in smart home platforms". The applicant received a green light from the BOEL on 1 September.

On 5 September, the BOEL received the only request in the MP period that is not related to a TNA application. Indeed, the request is from a researcher, who desired to improve his ERC research proposal on data-driven and user-centred content moderation. The BOEL positively evaluated the request on 28 September.

On 7 September a request was received on "Local and global explanations for federated learning models". The BOEL replied positively on 22 September.

On 20 October, the BOEL received an application on "A network approach to study historical figures and geographical regions of the Yore". The request received a green light by the BOEL on 26 October.
A further request was received on 20 October. The request received approval by the BOEL on 26 October.

On 21 October, an application was received for a project entitled "Towards a local-density corrected Homophily in networks". The request has been approved by the BOEL on 2 November.

2.2 Task 2.2 Bottom-up Ethics and Legality for Data Science

Task leader: SSSA
Participants: TUDelft, CNR, URV, KCL, SSSA, LUH

The SSSA team (Giovanni Comandè, Magali Contardi) has actively taken part in the meetings that have been scheduled on 27 July 2021 and 27 September 2022. SSSA has also planned two additional SoBigData++ and LeADS joint Awareness Panels. One titled "*Data portability: integrating the notion in the legal framework*", which was held on 28 November 2022 and the other entitled "Further processing of health data for research

purposes: the interplay between the GDPR and the MDR" (13 December 2022). SSSA has designed two other Awareness Panels for the upcoming months. From a scientific viewpoint, SSSA contributed to the debate on AI, big data, ethics and regulation with scientific publications (see Section 2.5).

2.3 Task 2.3 High-Level Advisory Board

Task leader: LUH
Participants: TUDelft, CNR, UNIPI, URV, CNRS, SSSA

2.3.1 Activities performed

Dissemination panel: Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal implications, 9 March, 2022, Conference call (Microsoft Teams), co-organised by Re-Imagine Europa.
Another activity performed by WP2 within Task 2.3 was the production of a white paper. The white paper is entitled "The European Approach to Artificial Intelligence Across Geo-political Models of Digital Governance" and was authored by Jeroen Van den Hoven, Giorgia Pozzi, Marc Stauch, Iryna Lishchuk, Francesca Musiani, Josep Domingo-Ferrer, Salvatore Ruggieri, Francesca Pratesi, Roberto Trasarti and Giovanni Comandé. WP2 completed the white paper and submitted it for publication on 31 August 2022 to IFDaD2022, the International Forum on Digital and Democracy. The publication was unfortunately rejected on the 13th of October 2022. Thus, WP2 has engaged in finding a different journal for the white paper's publication. At present, WP2 is considering a submission to Big Data and Society (https://journals.sagepub.com/description/BDS) - impact factor 8.7) which has a fair review speed (11 weeks on average). This activity will be carried in order to publish the white paper in 2023.
As for WP2 work in Progress, there is a white paper on AI and data models is in progress, scheduled for submission for publication in March 2023.

2.3.2 Participants involved

Task leader: LUH
Participants: TUDelft, CNR, UNIPI, URV, CNRS, SSSA

The High-Level Advisory Board consists of the following members:

1) TUDelft: Jeroen van den Hoven (Chair)
2) LUH: Marc Stauch (Vice Chair)
3) SSSA: Giovanni Comandé (Vice Chair)
4) CNR: Fosca Giannotti (regular member)
5) UNIPI: Salvatore Ruggieri (regular member)
6) URV: Josep Domingo-Ferrer (regular member)
7) CNRS: Francesca Musiani (regular member)
8) Giovanni Sartor – UEI (external expert)

2.3.3 Goals of the activities

Production of annual white papers to be published and disseminated via different channels (T.3.2, T.3.4, and T.5.1) to impact European society at different levels

2.3.4 Possible sponsorships other than SoBigData++ (if applicable)

N/A

2.3.5 Outcome(s) produced

White paper 2022: "The European Approach to Artificial Intelligence Across Geo-political Models of Digital Governance" and was authored by Jeroen Van den Hoven, Giorgia Pozzi, Marc Stauch, Iryna Lishchuk, Francesca Musiani, Josep Domingo-Ferrer, Salvatore Ruggieri, Francesca Pratesi, Roberto Trasarti and Giovanni Comandé. Under review.

2.3.6 Possible follow up activities

Annual white papers:

(a) white paper 2022/2023;
(b) white paper 2023/2024

2.3.7 Contribution to the task and WP2 in general

Annual reporting on best-practice, emerging trends, innovative approaches resulting from the Project. Advice, formation of high-level opinions on the legal and ethical matters emerging within the project. All members of the HLAB are actively engaged in the debate and writing of the second and third whitepaper regarding activities and positioning of SoBigData++

2.4 Task 2.4 Critical Data Literacy

Task leader: KLC
Participants: LUH, TUDelft, CNR, SSSA

In accordance with project partner CNR and the project management team, KCL was tasked with the update of the SoBigData Literacy section of the Research Infrastructure. At present, the SoBigData Literacy section contains 149 items, comprising 43 training materials. The items regarding Data Literacy are distributed as such:

Journal Article	76
Conference Paper	26
Book Chapter	2
Deliverable	1
Research Article	1

KLC collaborated with CNR and the project management team to identify identify all Open-Access articles that were published before June 2022 that also had acknowledged SoBigData++ in the correct manner [i.e., "acknowledge support from EU HORIZON 2020 INFRAIA-2019-1(SoBigData++) No. 871042"].

The number of articles was, in June 2022, 63. All files were downloaded from their hosting platforms, renamed, and uploaded in a dedicated folder in the RI at the following folder: https://data.d4science.net/WXLZ.

A test-page was created for a sample article, which can be found here: https://sobigdata.d4science.org/group/sobigdataliteracy/literature?path=/dataset/ba441f5d-0260-43d2-b1cd-c418ff2c01a3. Once it was uploaded, WP3 and the project management team both agreed that a new item page should be developed, providing further emphasis on the authors of the paper, its green access status and eliminating some of the visible fields that in the item creation interface process are currently compulsory.

Further activity was outlined, planning an interaction with WP7 (Virtual Access) and WP9 (E-Infrastructure and Supercomputing Network) in order to develop an ad-hoc item creation page for Data Literacy.

2.5 Publications by members of WP2

1. Jeroen van den Hoven, Giorgia Pozzi, Marc Stauch, Iryna Lishchuk, Francesca Musiani, Josep Domingo-Ferrer, Salvatore Ruggieri, Francesca Pratesi, Roberto Trasarti, Giovanni Comandè, (forthcoming) "The European Approach to Artificial Intelligence Across Geo-Political Models of Digital Governance" *IfDad*.
2. Anna Monreale, Roberto Pellungrini (forthcoming) "A Survey on Privacy in Human Mobility", *Transactions on Data Privacy*.
3. Najeeb Jebreel, Josep Domingo-Ferrer, Alberto Blanco-Justicia, and David Sánchez (forthcoming) "Enhanced security and privacy via fragmented federated learning", *IEEE Transactions on Neural Networks and Learning Systems*.

4. Alberto Blanco-Justicia, David Sánchez, Josep Domingo-Ferrer and Krishnamurty Muralidhar (forthcoming) “A critical review on the use (and misuse) of differential privacy in machine learning”, *ACM Computing Surveys*.
5. Rami Haffar, Najeeb Jebreel, David Sánchez and Josep Domingo-Ferrer, (forthcoming) “Generating deep learning model-specific explanations at the end user’s side”, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*.
6. Francesca Pratesi, Roberto Trasarti, Fosca Giannotti, (2022) “Ethics in smart information systems, Ethical Evidence and Policymaking: Interdisciplinary and International Research”, *Policy Press*
7. Josep Domingo-Ferrer and Maryline Laurent (eds.), (2022) *Privacy in Statistical Databases-PSD 2022,* Lecture Notes in Computer Science, vol. 13463, Springer, ISBN 978-3-031-13944-4
8. Josep Domingo-Ferrer (2022) “Tit-for-tat disclosure of a binding sequence of user analyses in safe data access centers”, in *Lecture Notes in Computer Science*, vol. 13463, pp. 133-141. Vol. Privacy in Statistical Databases-PSD 2022, Paris, France.
9. Alberto Blanco-Justicia, Najeeb Moharram Jebreel, Jesús Manjón, and Josep Domingo-Ferrer, (2022) “Generation of synthetic trajectory microdata from language models”, in *Lecture Notes in Computer Science*, vol. 13463, pp. 172-187. Vol. Privacy in Statistical Databases-PSD 2022, Paris, France.
10. Rami Haffar, Ashneet Khandpur Singh, Josep Domingo-Ferrer and Najeeb Jebreel (2022) “Measuring fairness in machine learning models via counterfactual examples”, in *Lecture Notes in Computer Science*, vol. 13408, pp. 119- 131. Vol. Modeling Decisions in Artificial Intelligence-MDAI 2022, Sant Cugat del Vallès, Catalonia.
11. William Seymour, Mark Cote, and Jose Such (2022) “Can you meaningfully consent in eight seconds? Identifying Ethical Issues with Verbal Consent for Voice Assistants”. In *Proceedings of the 4th Conference on Conversational User Interfaces (CUI '22)*. Article 15 pp 1–4. Association for Computing Machinery.
12. Tom van Nuenen, Jose Such, and Mark Cote (2022) “Intersectional Experiences of Unfair Treatment Caused by Automated Computational Systems” *Proc. ACM Hum.-Comput. Interact*. 6, CSCW2, Article 445 pp 1-30.
13. Jeroen van de Hoven, Giovanni Comandé, Salvatore Ruggieri, Josep Domingo-Ferrer, Francesca Musiani, Fosca Giannotti, Francesca Pratesi, Marc Stauch, (2021) “Towards a digital ecosystem of trust: Ethical, legal and societal implications”, *Opinio Juris In Comparatione*.
14. Roberto Pellungrini (2021) “Privacy Risk and Data Utility Assessment on Network Data”. *DataMod* 93-106

3 Conclusions

This document reports the scope, activities, and members involved in the most recent activities carried out, ongoing, and planned by Work Package 2: NA1 - Responsible Data Science during the period 1st July 2021 - 1st January 2023.

This document includes a full report on the Micro-Projects that this Work Package was involved as member as well as those that lead. It also includes a complete report of the activities involving the Task leaders and participants. These are: dissemination in academic venues as well as public outreach; publications in academic journals as well as articles of public interest (many as open access). Let it be noted that, among the publications, this Work Package as also produced a White Paper that expresses in clear form the overall ethical and political position about Big AI as represented by the member of SoBigData++. Finally, this report includes a draft of the mentioned White Paper.

Appendix A. TransNational Access - Statistics

A link to every project is available upon request.

Date	Type	Answer Date
2021-07-15	TA project	2021-07-19
2021-07-21	TA project	2021-08-05
2021-07-21	TA project	2021-08-05
2021-07-27	TA integration	2021-08-03
2021-07-29	TA project	2021-09-13
2021-09-13	TA integration	2021-10-14
2021-09-13	TA integration	2021-10-14
2021-09-22	TA integration	2021-10-14
2021-10-12	TA project	2021-10-22
2021-10-13	TA project	2021-10-27
2021-10-18	Dataset in SBD++ Catalog	2021-12-03
2021-12-20	TA project	2021-12-03
2021-12-20	TA project	2022-02-01
2021-12-20	TA project	2022-02-03
2022-01-11	TA integration	2022-03-23
2022-02-04	TA project	2022-03-23
2022-02-08	TA integration	2022-04-01
2022-02-21	TA project	2022-03-23
2022-02-28	TA project	2022-04-05
2022-03-29	TA project	2022-04-01
2022-04-11	TA integration	2022-04-12
2022-04-14	TA integration	2022-05-17
2022-04-29	TA project	2022-05-17
2022-04-29	TA project	2022-05-30
2022-05-02	TA project	2022-05-30
2022-05-02	TA project	2022-05-30
2022-05-02	TA project	2022-05-30

2022-05-11	TA project	2022-05-30
2022-05-12	TA project	2022-05-30
2022-05-23	TA integration	2022-05-30
2022-05-31	TA integration	2022-06-16
2022-05-31	TA project	2022-06-16
2022-06-02	TA integration	2022-06-23
2022-07-05	TA project	2022-07-15
2022-07-06	TA project	2022-07-15
2022-07-21	TA project	2022-08-09
2022-07-21	TA project	2022-08-09
2022-07-25	TA integration	2022-08-09
2022-08-15	TA integration	2022-09-01
2022-08-15	TA integration	2022-09-01
2022-08-16	TA project	2022-09-01
2022-08-17	TA integration	2022-09-01
2022-08-23	TA project	2022-09-01
2022-08-23	TA project	2022-09-01
2022-08-29	TA integration	2022-09-01
2022-09-07	TA project	2022-09-22
2022-09-05	Research project	2022-09-28
2022-10-20	TA project	2022-10-26
2022-10-20	TA project	2022-10-26
2022-10-21	TA project	2022-11-02

Appendix B. White paper 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]
Centre Internet et Société, CNRS - Centre national de la recherche scientifique, 59-61 rue Pouchet, 75017 Paris, France
[4] Universitat Rovira i Virgili, Av. Països Catalans 26, 43007 Tarragona, Catalonia
[5] Università di Pisa, Largo B. Pontecorvo 3, 56127 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 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

[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)

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.

Subsequently, the Commission has also published a draft AI Liability Directive that would require EU member states to amend their domestic private law liability rules to give claimants the benefit of certain evidential presumptions in cases where they allege injury from the faulty performance of an AI-system, but face difficulty – due to the opaqueness of AI-systems - in proving this in line with the ordinary rules of civil proof; this includes both information disclosure duties on the defendant AI operator (in the case of a high-risk AI-system) under Article 3, and in some cases a presumption of causation between the established faulty input of the system-builder or -operator and the system's injurious output (Article 4).[15]

As these initiatives demonstrate, the EU law-maker is centrally concerned that the development and deployment of AI should not occur at the expense of the rights of individual citizens, especially those injured through the shortcomings of high-risk systems. 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 and AI Liability Directive provide for a framework that will strike an appropriate balance between the benefits and risks associated with the technology. The drafts are presently proceeding through the EU legislative process, with the expectation that they will be enacted as law in 2023 and enter force some time in 2024. In the

[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.

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).

Table 1: A comparative table of the AI model from perspective of an individual, industry and the state

	PROS	CONTRAS
Perspective of an individual	Strong legal protection of rights. and freedoms.	Scarcity of EU-made information technology.
Perspective of industry	Financial support from the European Commission and the national governments. Strong legal framework may protect against non-European players.	Market fragmentation. Legal constraints may hamper innovation.
Perspective of the state	Leadership in global protection of human rights and freedoms in the information society.	Slow enactment and deployment of new regulations. The main IT actors in Europe are headquartered elsewhere (US, China, etc.).

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 been more motivated by a desire to protect the operations of digital service providers, as with the 1998 Digital Millennium 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 piecemeal 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 that 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.

The effect of these laws has arguably been to concentrate rights and privileges in the hands of a powerful few: indeed it does not appear coincidental that the US is the home of the 'GAFAM' 'big five IT conglomerations of Google, Apple, Facebook (Meta), Amazon and Microsoft. In this regard, in the US too, there are ongoing legislative attempts to curb the anti-competitive potential of such entities, such as the 2021 'Ending of Platform Monopolies Act'.[28] At the same time, there is also an existing mechanism, whose *de facto* effect is to impose *ex ante* regulatory duties on IT 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

[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.

citizens from the risks posed by such technology accompanied by a public request[6]. As part of a 'National Artificial Intelligence Initiative' (NAII) it has also recently published a Blueprint for an 'AI Bill of Rights, containing a set of non-binding principles to guide the development and deployment of AI[7].

In the above regards, 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[8]. 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.

Table 2: A comparative table of the AI model from perspective of an individual, industry and the state

	PROS	CONTRAS
Perspective of an individual	Strong protection of free speech.	Little legal protection vs abuse by digital actors. Privacy protection only in certain sectors.
Perspective of industry	Few restrictions to large-scale data collection, analysis and trading. Little interference with AI innovation.	Government agencies may impose significant fines without proof of damage.
Perspective of the state	Legal capacity to leverage national digital actors as sources of intelligence.	Piecemeal control on digital actors.

[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] Issued in October 2022; see: [https://www.whitehouse.gov/ostp/ai-bill-of-rights/].

[8] 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.

2.3. The Russian Model of State Control

Russia was 'largely disinterested in strong Internet regulation until the 2010s' (Kolozaridi & Muravyov, 2021). However, approaches aimed at the 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 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), in accordance with the authoritarian and centralising turn imposed by the Russian government on its digital economy over the last decade, as well as the willingness to promote exclusively "made in Russia" technology. 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[9]. 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 has departed 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

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

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 strategy needs to be understood in the frameposition can be explained against the background of the broader legislative developments towards digital governance in Russia that were mentioned in the introduction to this section, and which unfold in accordance with socio-political and economic principles of increased authoritarianism, centralization, and promotion of national "digital champions".

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)[10] (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[11]. 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).

[10] 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.

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

Table 3: A comparative table of AI model from perspective of an individual, industry and the state

	PROS	CONTRAS
Perspective of an individual	Job creation in digital industries.	Censorship. Interception of communications. Limited access to foreign websites and internet services.
Perspective of industry	Favourable legal conditions. Special regimes for personal data access. Removal of export barriers. Stimulation of investments. Simplified testing.	State control of internet traffic. Restrictions on technology imports.
Perspective of the state	Strong control of internet traffic. Unlimited regulatory power.	Restrictions on technology imports.

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 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).

Yet, the relationships between those state-sponsored enterprises and the government are not free of tensions. In 2020, the Chinese government opened an investigation into e-commerce giant Alibaba, to examine whether the company was abusing its dominant position. The media

attributed such an attack to Alibaba's founder Jack Ma's open critique to President Jinping, when Ma said that the government's latest strategy is detrimental to innovation[12]. Also, the zero-tolerance policy against Covid19 has reduced the spending capacity of consumers and consequently the revenue of the Chinese internet giants. On the other hand, Huawei is facing export bans in the West because of (so far unsubstantiated) suspicions that their telecommunications equipment might be under the Chinese government's control[13]. Whereas the protection of the internal market against foreign competitors was key to the development of the Chinese IT champions, the continued growth of these companies is now hampered with the government's will to keep a tight control on information technology[14].

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.

It remains unclear to what extent the above ethics principles are motivated by genuine ethical concerns or rather by the ambition of Chinese companies to render their products and services acceptable in Western markets.

[12] https://thediplomat.com/2021/09/the-real-cause-of-chinas-alibaba-crackdown/

[13]https://harrisbricken.com/chinalawblog/the-huawei-export-ban-moves-to-europe-because-there-is-no-place-to-hide/

[14] https://www.insiderintelligence.com/content/alibaba-s-sluggish-growth-heralds-larger-problems

Table 4: A comparative table of AI model from perspective of an individual, industry and the state

	PROS	CONTRAS
Perspective of an individual	Wide range of Internet services offered by national champions.	Censorship. Interception of communications. Limited access to foreign websites and internet services.
Perspective of industry	Huge growth made possible by a protected market. Government support to create IT champions.	Tensions with the government, which retains ultimate control on the industry. Reluctance or even banning of Chinese suppliers in Western countries.
Perspective of the state	Strong control on a very powerful IT industry. Legal capacity to leverage national digital actors as sources of intelligence.	Difficult conciliation between national control on IT champions and global expansion of those champions.

3. Ethical Perspective

In the current era of Big Data, digital societies, and cutting-edge AI-based systems, the development, deployment, and regulation of technologies have become crucial ways for the main geopolitical powers to establish themselves on the international scene. In fact, the economic gain

ensuing from new technologies along with their ubiquitous use in almost every domain of public and private life motivates the political need to establish and protect one's own digital sovereignty (Hobbs, 2020). To secure a technopolitical sphere of influence (going beyond the meaning of this term usually understood in a territorial sense) has become fundamental (Lippert, p. 6): models of governance determine the way in which technological leadership is pursued and, conversely, technological leadership finds clear expression in political discourse and diplomacy.

In fact, the incentives to shape the digital landscape has a considerable impact on the power relations of state actors players on the international scene. The strategic rivalries, particularly between the USA and China, are not only shaped by conflicts over trade relations and financial policy (Lippert 2020), but they are now prominently shaped by huge investments that aim at competitive advantages in AI, Semiconductors, and quantum computing, battery technology, as well as the infrastructure, science and materials that are necessary. Technological autonomy in these and other areas has become decisive and paramount to the political relationships between geopolitical powers. The situation particularly sees China and the US[15] as main rivals regarding the hegemony on technological advancement in artificial intelligence. The way in which the systemic tension among these nations is managed in view of digital technologies is fundamental for the geopolitical order in the years to come. Of particular interest is the role played by the EU against this background.

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. In fact, normative standards can also be established *through* technology: the concept of "politics by default" points exactly to the value-ladennes of technologies and to the fact that they are "always permeated by political ideas, values and norms. These become embedded in a technology as standard ("default") configuration, for example in the software code, and as such create political and economic effects." (Lippert, p. 32) These considerations depict a situation in which the values underlying these technologies remain entrenched with the way in which they are further developed and regulated.

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

[15] Also interesting to investigate would be the role of Russia as a further player entering the scene. For example, Russia's intention to render the internet infrastructure state controlled to avoid dependence from China or US surely mirrors the ideology of censorship and oppression that is palpable also on the political scene (Lippert, p. 33). However, in this section we focus on the interplay between China, the US and Europe.

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).

However, party rule and ubiquitous and large scale surveillance and control have not hindered Chinese technological progress and economic growth. On the contrary, China is experiencing an increasing economic rise and is positioning itself as one of the main powers in the digital sphere. The fact that this is possible under an authoritarian regime - socialism with chines characteristics - that disregards liberal values and principles that characterize the European way of life and the European Union's political and legal system could be a concerning indicator of the fact that political stability and technological advancement can be achieved while not sticking to fundamental values. As Hilpert points out, "China shows state leaders and developments planners in Asia, Africa and Latin America very clearly that economic progress and globalisation must not necessarily rely on the Western paradigm." (Lippert, p. 37). 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[16] 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)[17]. 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[18]. 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

[16] 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'.

[17] 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).

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

ISO/IEC JTC 1/SC 42[19], the IEEE P7000[20], the ETSI SAI[21], and the ITU-T standard series on Machine Learning for 5G[22].

Several national pathways for the standardization of AI have been issued, such as the US NIST plan for federal AI standards engagement[23], the EU rolling plan for ICT standardization[24] (Chapter on AI), the China Standards 2035[25], the German roadmap of AI standardization[26], and the Australian AI Standards roadmap[27]. 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).

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[28], a

[19] 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

[20] 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/

[21] 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

[22] 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/

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

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

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

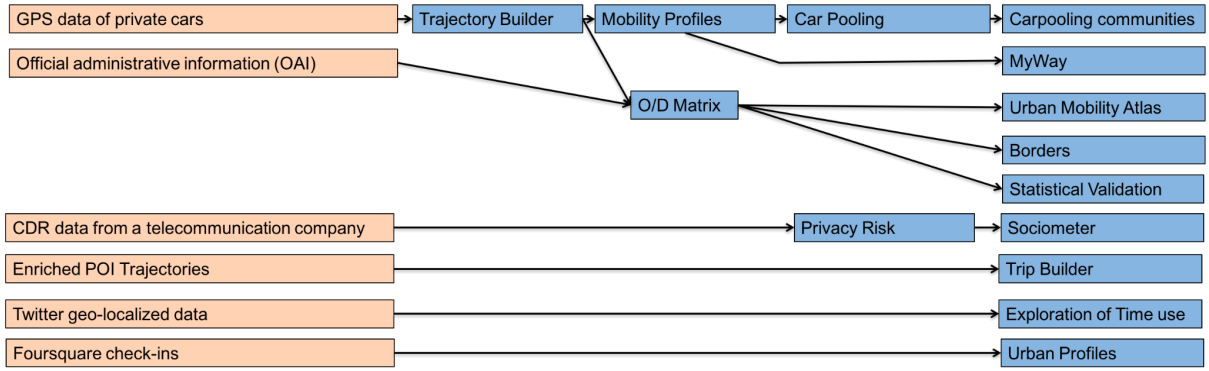
[26] https://www.din.de/en/innovation-and-research/artificial-intelligence/ai-roadmap

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

[28] https://sobigdata.d4science.org/catalogue-sobigdata

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[29]:



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) to be delivered by a Service Developer, i.e., an entity who want to have access to some data to design a service or a particular analysis. Note that the original data (i.e., CDR) are usually collected by a telco operator for billing purpose, but the Service Developer can be either an external organization or an untrusted department within the telco operator itself.

This kind of data is suitable for the development of the *Sociometer*[30], a service in which we are interested in quantifying residents, commuters, and visitors in a certain area. Indeed, ICPs are aggregated 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

[29] https://sobigdata.d4science.org/web/cityofcitizens

[30] http://data.d4science.org/ctlg/ResourceCatalogue/sociometer

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*[31], a service in which we are interested in quantifying residents, commuters, and visitors in a certain area. Indeed, Thus, a resident can be recognized because he/she could 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). Having in mind that we want to enable a trusted ecosystem for data sharing, Aas a middle passage between the ICP generation and the Sociometer deployment, a *Privacy Risk Assessment* module[32] has been deployed based on the framework PRUDEnce (Pratesi et al. 2018), 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. After this passage, if the data owner is satisfied about the privacy guarantees it obtained, can share aggregated data without risk of compromising users' privacy, otherwise, some mitigation strategies can be applied to remove the residual risk, possibly acting only (or mainly) on data related to users at risk in order to maximize the utility of the data after the transformation. An example of mitigation strategy tailored on ICPs can be found in (Pratesi et al. 2020), where ICPs are first clustered and then clusters are joined together until they do not respect the privacy guarantees set by the data provider, i.e., creating anonymity sets, like in (Sweeney 2002).

The Privacy Risk Assessment module is based on the simulation of attacks where the hypothesis is that the adversary knows all the call activities performed by his/her target in a certain territory and in a specific time window, which in our experiments varies from 1 to 4 weeks. The goal of the adversary is to link the real identity of his/her target to a specific ICP, and the goal of the Privacy Risk Assessment module is to measure empirically the probability of success of this attack, i.e., what is the actual risk for each individual in the dataset of being re-identified. 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

[31] http://data.d4science.org/ctlg/ResourceCatalogue/sociometer

[32] http://data.d4science.org/ctlg/ResourceCatalogue/privacy_risk_on_sociometer

limited to pocket areas such as healthcare. Russia and China favour state control internally and also at the international level; yet, their motivation 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[33].

[33] 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,

- 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[34], 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.
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.

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.

[34] 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.

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. H.R. Bill 3825 (introduced in Congress, June 11, 2021)
29. Jing, M., & Dai, S. (2019). China recruits Baidu, Alibaba and Tencent to AI 'national team'. South China Morning Post.
30. Johns, N, 'Regulating the Digital Economy' (Observer Research Foundation, 2015), 2.
31. 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.
32. 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.
33. 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
34. 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
35. Melnik, J. (2019). China's "National Champions" Alibaba, Tencent, and Huawei. Education About Asia, 24(2), 28-33.
36. 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/
37. 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.
38. 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.
39. 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.
40. 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.
41. Nocetti, J., 'Contest and conquest: Russia and global internet governance'. International Affairs, 91(1), 2015, 111-130.
42. OECD.AI (2021), powered by EC/OECD (2021), database of national AI policies, accessed on 8/06/2022" https://oecd.ai/en/dashboards
43. 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/
44. 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.
45. Piccone, T. (2018). China's long game on human rights at the United Nations. Brookings Institution, September, 7.
46. 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.

47. 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.
48. Radu, R. (2019). Negotiating internet governance. Oxford: Oxford University Press.
49. Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices.
50. 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.
51. 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.
52. Rühlig, T. M. (2020). Technical standardisation, China and the future international order: A European perspective. Heinrich-Böll-Stiftung European Union.
53. 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.
54. Stadnik, I. (2021). Control by infrastructure: Political ambitions meet technical implementations in RuNet. First Monday.
55. 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
56. 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
57. 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.
58. 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/
59. 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/
60. Wijermars, M. (2021). 'Selling internet control: the framing of the Russian ban of messaging app Telegram'. Information, Communication & Society,1-17.
61. 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.
62. Zittrain, J. (2008). The future of the Internet—And how to stop it. New Haven: Yale University Press.