DOI: 10.17573/cepar.2022.1.01 *1.01 Original scientific article*

Social Aspects of Democratic Safeguards in Privacy Rights: A Qualitative Study of the European Union and China

Polonca Kovač
University of Ljubljana, Faculty of Public Administration, Slovenia
polonca.kovac@fu.uni-lj.si
http://orcid.org/0000-0002-7743-0514

Grega Rudolf
Information Commissioner of the Republic of Slovenia, Slovenia
grega.rudolf@ip-rs.si
http://orcid.org/0000-0001-9449-6905

Received: 14. 1. 2022
Revised: 11. 4. 2022
Accepted: 16. 4. 2022
Published: 31. 5. 2022

ABSTRACT

Purpose: The primary objective of the present research is to identify the basic tools and restrictions concerning the protection of privacy and personal data in the EU and China as two fundamentally different cultural systems. Based on the socio-cultural analysis of backgrounds, trends and expert assessments, the research aims to examine whether privacy protection standards, such as those provided by the GDPR in the EU, are sufficiently robust to endure the digital age. Two different cultural frameworks have been analysed in order to understand their influence on practical behaviours regarding the democratic safeguards in privacy rights enforcement in the EU compared with China. This is accomplished by comparing social control in the EU and the social credit system in China.

Design/Methodology/Approach: Considering the administrative context, a combined qualitative approach is applied, including normative and dogmatic methods, literature analysis, sociological and historical methods, expert interviews, and comparative and axiological methods.

Findings: The results of both theoretical and empirical parts of the research suggest that the stricter regulation in the EU compared to China – in the sense of more consistent protection of privacy and personal data as well as transparency rights – can be attributed to its democratic protection of human rights and more definitive regulations, particularly the GDPR. These major differences seem to create an even deeper gap in the future, to be explored scientifically and in practice. The authors conclude that authorities must actively guarantee the rights related to privacy and

personal data protection, or else effective governance will lead to a surveillance society and erosion of individuals' freedom as a valuable civilizational asset.

Academic contribution to the field: The research contributes to administrative science by addressing one of the key concepts of modern public governance, namely the collision between the principles of effectiveness and transparency on the one hand and privacy on the other. The use of scientific methods paves the way for further comparisons.

Practical Implications: The article provides a concise overview of the relevant literature and an analysis of the rules that underpin the implementation, evaluation and improvement of regulations, especially in the light of ICT development, e.g. in times of the Covid-19 pandemic.

Originality/Value: The paper bridges the gap created by the differences in the understanding of privacy and public governance in the field in the EU and China based on cultural differences. The usual general or merely law- or technology-based analyses are upgraded with a combination of various research methods.

Keywords: privacy rights, personal data protection, EU, democratic safeguards, China, control society, socio-cultural analysis.

JEL: K23, K38

1 Introduction

Society and the public governance of community affairs are in a state of constant change. Good administration is deemed to respect and balance different principles. Over the past decades, however, in the light of modern processes such as globalisation, digitisation or delegation of public tasks to various public and private entities, this has implied also proportionate respect for transparency as well as privacy (Kierkegaard, 2009; Fisher, 2010; Kovač, 2014, Galetta et al., 2015; Pirc Musar et al., 2020; Erkkilä, 2020). The protection of or interference with privacy and the regulation of related rights, particularly personal data protection, are highly dependent on regional values, traditions, principles, and the legal arrangements in individual communities. This is not only the case for individual countries but also broader settings such as the European or (North) American system, the Asian and specifically the Chinese model.

Lately, the greatest impact on public governance and the concept of privacy has been demonstrated by the rapid and intensive development of information and communication technology (ICT), raising a number of challenges concerning legal certainty, democracy, fundamental human rights, social control and the role of public administration. This applies in general and in particular in the context of the COVID-19 pandemic (see literature review and findings in Aristovnik et al., 2021). The technological development of society often results in technology colliding with fundamental human rights (see, for example, Kent, 2013; Cullen, 2016; Zhao, 2015; Čebulj and Pirc Musar in Pirc Musar, 2020). Therefore, the need for a careful substantive and procedural as well as institutional regulation aimed to prevent or resolve such collisions in advance

is becoming all the more crucial for the democracy of government. This applies at the level of the highest legal acts, i.e., international and constitutional law (see Galetta et al., 2015, Avbelj et al., 2019). With the development and proliferation of ICT and large-scale data gathering, a plethora of questions arises regarding the appropriate processing of personal data, ICT regulation, and restriction of excessive ICT interference with the rights of individuals. Social control enabled by ever more easily accessible technology and increasingly large databases poses a key challenge for modern society balancing between the provision of privacy and freedom of expression and thought (and other human rights) on the one hand and the desire to regulate as effectively as possible and maximise citizen conformity on the other. According to various sources, the purpose of social control is to identify and regulate non-conforming behaviour of individuals in the society that, in turn, could deter them from such behaviour with punishments and rewards (see Peerenboom, 2005, pp. 72–162; Kent, 2013; Zhao, 2015, pp. 29–52; Kasl, 2019, pp. 349–358).

The article explores privacy and personal data protection by comparing two large entities stemming from different societal values and hence different public governance systems and legal regimes – the European Union (EU) and the People's Republic of China. A brief summary of the legal rules in force in the European and Chinese orders is a starting point for a qualitative study, which is conducted on administrative scientific bases, focused on the analysis of the influence of different cultural backgrounds on concrete and practical behaviours. In the EU, the area of privacy has recently been marked by the adoption of the General Data Protection Regulation (GDPR),[1] directly applicable in all Member States since May 2018. In China, social surveillance is being enforced through what is known as the social credit system (Chen and Cheung, 2017; Dai, 2018; Mistreanu, 2018; Wong and Dobson, 2019; Ding, and Zhong, 2020; Shahin and Zheng, 2020). Quite clearly, the EU and China take the opposite stance in such regard, the former building on the restriction of interference – whether by public authorities or private actors – with people's privacy, while the latter governs the society through government interference with individuals' privacy.

However, the question occurs why to compare the EU and the Chinese systems, having in mind that EU is a supranational democratic entity and China a centralised and rather autocratic country. Nevertheless, as shown in the following sections, our intention is not to focus on the state-like mechanism themselves solely but mainly the cultural background leading to certain legal sources and administrative practices. Should we compare just one EU Member State to China, already the size scope would not be comparable, since the EU has 447 and China app. 1,402 million population, respectively, so the size is more equalised as would be the case if just one (European) country would be explored. And most importantly, as regards the EU legal framework through the GDPR, it is applied directly regardless of the national legal orders of Mem-

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119.

ber States. The primary objective of the present research is thus to identify the basic tools and restrictions concerning the protection of privacy and personal data in the EU and China and the trends of further development in the broader framework. We have examined to which extent such various cultural backgrounds critically contribute to development or erosion of democratic safeguards. By analysing the existing regulation, the article aims to examine whether the relevant protection standards are strong and robust enough to endure the upcoming digital era and whether there is a need for additional and stricter regulation in the future based on the cultural peculiarities attributed to European or Chinese system.

The structure of the article is as follows. After defining the methodological approaches in the second chapter and presenting the various complementary methods of qualitative social science research applied, the third chapter provides a sociological and theoretical framework of the regulation of privacy and personal data protection in the EU and China. This is based on an analysis of the latest scientific literature, especially from recent years. The fourth chapter denotes the empirical part providing a more detailed analysis of the Chinese and EU legal systems and their implementation, deriving from the comparison and analysis of regulations, summaries of expert interviews, and key findings from previously studied scientific literature. This chapter succinctly addresses the safeguards and standards of protection in the EU vis-à-vis China in the light of the research question concerning the extent to which privacy protection systems are related or differ in terms of ICT use and large-scale processing of personal data. The discussion in the fifth chapter addresses the main differences, the importance of their understanding, and future development trends in this field. It is followed by a conclusion.

2 Research design, question and methods applied

The research relies on the usual research process structure with the following basic steps: defining the research problem and research objectives, designing an analysis plan, collecting data, analysing data, and interpreting the results (Neumann, 2006). The analysis is part of broader research on the effectiveness and efficiency of public administration in Slovenia and the EU (cf. Aristovnik et al., 2021).[2]

As regards research design, the definition of the research problem, objectives, and the resulting research question was followed by the definition of the key units of scientific literature, be it in the form of scientific articles, monographs, commentaries on regulations, relevant case law or internet analyses. We proceeded from the objective of the research, which is to gain an insight into the commonalities and, in particular, differences between the European and Chinese privacy regimes by studying political, sociological, and

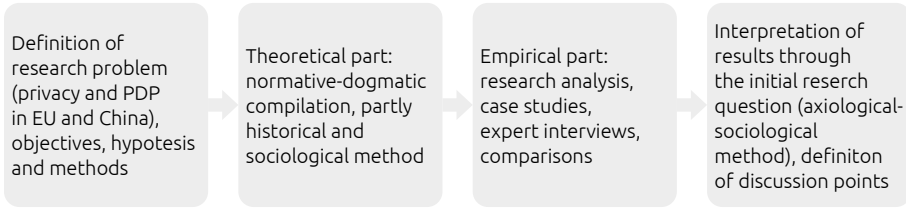
2 Hereby, we acknowledge the financial support from the Slovenian Research Agency, especially regarding research funding of the core programme no. P5-0093 implemented at the Faculty of Public Administration, University of Ljubljana. See also COVID-19 Social Science Lab available at: https://www.covidsoclab.org/home/>.

legal aspects in order to provide a basis for better mutual understanding and greater convergence in the future. The central research problem addressed by the article is how the concept of privacy can be understood in the context of entities as politically, sociologically, and legally different as the EU and China, and what its limitations are. The last part of the problem implies the identification of safeguards set by the EU to prevent the creation of a society of (by European standards) excessive control. The EU related regulation, literature and studies tend to take European privacy and transparency standards for granted, which should not be so; in fact, it is unfortunately not the case anymore already in some European countries when facing carious crises and enforcing the measures, such as corona disease fight. The study therefore aims to show the respective developments in the direction of control society if not enough attention is paid to democratic values, as they are understood in the European context. Given the above, the following research question is addressed: *To which extent the EU regulates the protection of individuals' privacy rights more strictly than China, and what are the basic grounds thereof?*

The comparative analysis of the sociological context, legal regulation and its implementation in the EU and China is based on several complementary methods of social science research, characterised by a qualitative approach. It is recognised in the literature that structural constraints, cultural backgrounds included, shape actors' behaviour and that actors respond to isomorphic pressures from their institutional environments and adopt structures, practices, and routines that have high social value (Nitzl et al., 2020). Considering that the topic is addressed from the perspective of administrative law, normative and dogmatic methods, analysis of scientific literature, sociological and historical analysis, expert interviews, and comparative and axiological methods are used. The normative method, in particular, is frequently combined with sociological and axiological methods, especially in the chapter comparing the EU and China. When using the normative method, the study is limited to an analysis of relevant pieces of legislation in the EU and China and their scope as regards privacy rights. There is no detailed analysis of specific rules in force provided since this is not the core aim of this study and exceeds the research question posed. Here, legal regulations with the GDPR at the forefront were taken as the benchmark for assessing the applicable rules. As the latter are based on community values, they must be interpreted with an axiological approach, while the sociological method serves to examine society's influence on the law and law's influence on the future development of society.

The definition of research objectives and the study of the relevant literature were followed by normative and dogmatic analysis and definition of the basic concepts of research, after which came the empirical part. The basic steps of the research are presented in Figure 1.

Figure 1. Basic research steps with methods applied



Source: own.

The normative and dogmatic methods served to define privacy and public governance as the framework concepts of analysis. These two terms are both rather ambiguous concepts that even the authors in the same space and time define differently. In our case, it was important to understand which types and rights of privacy are legally defined, especially to personal data protection related rights. We assumed that personal data protection is a key part of information privacy, whereby specifically in the exercise of the rights of individuals privacy and PDP are strongly intertwined, to the extent that they are mostly considered interlocking, especially in the EU but also globally (cf. Kuner et al., 2020; Pirc Musar et al., 2020; Avbelj et al., 2019). Moreover, we built on the need for proportional respect of the various principles of good administration, particularly the balance between transparency and privacy. From the point of view of governance and law, it is further important to distinguish between principles and enforceable rights, as the latter only become real through the procedures for their enforcement (cf. Kovač, 2014). Consequently, in the following sections upon European and Chinese systems, not only the relevant regulations and substantive privacy rights are analysed but also procedural issues are brought in the focus of attention. Additionally, the instutions responsible for enforcement of personal data protection are briefly described to emphasise their role in bringing the letter of the law into actual practice. This is of special importance when colliding transparency and privacy safeguards are in question (Erkkilä, 2020; Galetta et al., 2015). The theoretical part of the research studied the historical development of personal data protection and privacy, control society and other phenomena, all with the aim to shed light on the reasons for the current regulation.

Using interviews or a survey to answer research question could be criticized as being too subjective (Nitzl et al., 2020). However, subjective measures are often the only way to receive internal information from organizations or, as in our case, (supra) national system (Speklé and Widener, 2018). Prior research in public administration and management also indicates that subjective measures strongly correlate with objective measures in an organizational context (*ibid.*). In order to bridge this issue and given the complexity of the studied subject as well as the qualitative nature of the research in the central part of the analysis, the triangulation approach was used for the sake of increased objectivity (more in Neumann, 2006). In simple terms, triangulation means analysing a subject from multiple perspectives and with multiple methods and resources. Thus, especially for the comparison between the EU and China, a

combination of literature analysis, case studies and case law, and expert interviews was used, whereby the prevailing method was structured interviews with experts on European and Chinese regulation.

The experts were selected based on their theoretical knowledge and work experience in the relevant institutions, as well as on the impartiality of assessment. The interview concerning the EU system was held in the first half of 2021 with the Head of Inspections at the European Data Protection Supervisor (EDPS) Ms. Ute Kallenberger; the interview about the Chinese system was held with Dr. Yongxi Clement Chen, Researcher and Professor at the Faculty of Law of the University of Hong Kong. The EDPS is an independent European Union's supervisory institution ensuring that the EU institutions and bodies respect and ensure the rights to privacy and personal data protection. Dr. Chen was chosen after a review of professional and scientific literature on privacy, personal data protection and restrictions of rights, and above all owing to his research on transparency and control. He is also an expert in international comparative administrative law. Thanks to the chosen eligibility criteria and a balanced selection of experts, the interviews generated the desired results. Moreover, the interviews were standardised but still allowed the respondents to provide additional explanations, while the replies were evaluated descriptively and later quantified for the purpose of comparison. The results of the various approaches were eventually combined into discussion points based on the evaluation of the obtained results.

3 The sociological and legal framework of privacy and personal data protection in the EU and China

3.1 Baselines and legal framework of privacy and personal data protection in the EU

In modern democracies, public authorities are in possession of a vast body of information about citizens. They keep data on individuals as data custodians and are obliged to process it with due care and in accordance with personal data protection principles, such as accountability, proportionality, fairness, transparency, purpose limitation, integrity (Kierkegaard, 2009, p. 4). Hereby, privacy and transparency mechanisms in particular, are not just tools for applying legal rules but also extend the provinces of public administration and administrative law, contribute to architecture thereof, and provide new sources of conflict and dispute (Fisher, 2010).

When discussing privacy and transparency, the latter often declared as a contrast to privacy, so it has to be emphasised at the beginning that these are coincided concepts of good public governance and administration (Galetta et al., 2015). Privacy as well as transparency constitute democratic society only if both are proportionally enforced. Over time, however, various waves of transparency and privacy developments are characteristic for individual periods and countries or administrative traditions but convergent European and global understanding take all into account (Nikolić and Kovač, 2021). More-

over, these principles are associated with democratic accountability, but it also carries connotations of market efficiency. Although there are different modalities of (administrative) transparency, transparency holds promises for increased democratisation (Erkkilä, 2020). Transparency also implies access to public information, which can consist of various types of documents and registries and contradicts they system of principal data protection. Since especially administrative authorities manage significant amounts of personal data of citizens, transparency development, though, is raising additional concerns for privacy. Further, one can even claim that the attitude of the authorities towards the individual, individuals oversee and prevent possible infringements on privacy and protection of personal data by public administration, primarily through requirements for transparency (so called "right to know" or "right to information" based on the freedom of information (FOIA); Kovač, 2014). Hence, full transparency is not desirable by most accounts; concerns of its realisation are raised in particular through more digitalised societies and work processes in the EU and beyond (Erkkilä, 2020).

The large databases produced, collected and processed by authorities financed from public resources in the EU are determined and limited by the GDPR in force since 2016 and applicable since 2018. Member States were obliged to harmonise their national legislations with the GDPR by 2018. This is particularly important since public governance in the EU is based on multilevel governance, which only exceptionally applies uniform regulations and rather prioritises Member States' autonomy (Nikolić and Kovač, 2021, pp. 624ff; Trondal and Bauer, 2015). As said, privacy and personal data protection in the EU are regulated by the GDPR, which, in addition to having set the relevant standards, is also important, as it is directly applicable in all Member States (more in Kuner et al., 2020). Interestingly, the GDPR places the above rights explicitly in the nationally autonomous administrative-procedural system, thus effectively combining the common goals while respecting national specifics (Pirc Musar et al., 2020, pp. 39ff). This means that rules are not just a dead letter as their implementation is monitored on an ongoing basis, as evidenced by the vast administrative case law, studies, research, commentaries on the GDPR, training of officials, introduction of compliance systems for public and private controllers, and the like. Hence, it is not surprising that the GDPR is considered the *de jure* and *de facto* constitutional identity of the EU. In addition, it overcomes the problem of information deficit of the citizens *vis-à-vis* the public administration, especially when its tasks are delegated to private controllers. Personal data protection is thus an important civilizational asset of the European society and is considered a fundamental, constitutionally provided human right in the EU and individual Member States (more in Kuner et al., 2020; Avbelj et al., 2019; Cullen, 2016; Kent, 2013).

The protection of the right to privacy and personal data as well as other human rights is the key obligation of any authority. As a rule, every human right is accompanied by three different obligations: to respect and not interfere with it; to protect it from possible interference and infringement by third parties; and to enable its implementation and exercise (Cullen, 2016, pp. 585-592). Thus, in addition to the GDPR, the right to privacy and personal data protection are

defined already in the UN Universal Declaration of Human Rights (1948). The European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights (2010) are also important in this regard. The purpose of such regulation of both rights is to show that the rights to privacy and personal data protection are, especially in the EU, considered fundamental human rights and an important standard of the democratic values and functioning of the European society. Moreover, since all EU MSs have signed the ECHR and are the members of Council of Europe, they are obliged to personal data protection under the Convention no. 108, and subject to eventual judicial review by ECtHR.

In terms of operational enforcement, personal data protection and the related information privacy are reflected, especially in the EU, in the rights of individuals under the GDPR (Table 1). GDPR has been prepared, coordinated and adopted in several years, based among others on the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, so this piece of legislation served as a precursor for finally enforced Regulation in 2018.

Table 1. Rights to privacy in Europe under the ECHR, the EU Charter, and EU Regulations

Rights under the ECHR (1950)	**Article**
Right to respect for private and family life	8
Rights under the EU Charter (2010)	**Article**
Respect for private and family life	7
Personal data protection	8
Rights under the GDPR (2018), based on the former Directive 95/46/EC (1995)	**Article**
Right to information	13 & 14
Right of access by the data subject	15
Right to rectification	16
Right to erasure (right to be forgotten)	17
Right to restriction of processing	18
Right to data portability	20
Right to object	21
Rights concerning automated decision-making and profiling	22
* Rights under EU Regulations on e-privacy (2017) & artificial intelligence (2021)	* Proposals

Source: GDPR, more on GDPR provisions in Kuner et al., 2020; Pirc Musar et al., 2020.

Article 6 of the GDPR stipulates that controllers – be they authorities, private companies, other individuals, etc. – provide an adequate and lawful legal basis for the processing of personal data of data subjects. Thus, for example, Article 6 defines the following legal bases for processing data: contracts, legal obligations, vital interests, the performance of public tasks, legitimate interests, and consent by data subjects. Such regulation binds controllers to process personal data on data subjects only if there exists a tangible and specific purpose and only within the legal bases provided for such purpose. The concept of the rule of law thus represents a key aspect and an important safeguard for the regulation of the said issues in the EU, ensuring a high level of protection. In terms of personal data protection and privacy, the GDPR enables data subjects to decide for themselves to whom, when and under what conditions they allow the processing of their personal data. Yet, one must distinguish various legal grounds to protect and interfere with privacy rights, since there is an obvious difference whether data protection is based on the legal statute or public interest in administrative matters (e.g. no right to be forgotten in taxation) as opposed to mainly consent giving in private matters (e.g. when dealing with data collection and rights of consumers in the market). The said difference is based on the power between the data holders and individuals, where public law grounds offer less herachical relation, so significantly stronger protection is given to the individuals in order to prevent more plausible and affecting misuse of public authorities. With the adoption of the GDPR, data subjects in the EU have become even more attentive of the security of their personal data. The adoption and the debate on the GDPR itself have had a significant impact on public awareness of the principles, rights and obligations pursued by personal data protection as the operationalisation of the principle of privacy (Pirc Musar et al., 2020, pp. 15).

Even more so, the GDPR – directly or by reference to national law – sets out the key procedural and institutional elements for personal data protection. Insofar a right does not present such elements; it can only be a dead letter, as shown by analyses in various fields. Thus, for protection to be effective (cf. Kovač, 2014, pp. 33–42; Pirc Musar et al., 2020, pp. 36–62), the following are needed. First, the definition of supervisory institutions, such as the national regulator and/or supervisory authority, and the European Data Protection Supervisor under the GDPR, and, second, the definition of the type of relationship and thus of the rights specific to this type of procedure. In the case of the GDPR, this implies, in particular, national laws on administrative procedure and laws on misdemeanours that implement the types and legal nature of measures defined by the GDPR and the associated legal protection. As regards national institutions, most EU countries have introduced the joint Information Commissioner, which jurisdiction usually comprises personal data protection and right to information simultaneously. Some countries, on the other hand, have opted to establish data protection agency and IC in parallel (e.g. Croatia). The holistic approach, nonetheless, seems to be more effective since it enables to run proportionate tests between privacy and transparency oriented rights on this initial administrative level, not only afterwards when respective disputes come in front of the courts (Pirc Musar et al., 2020). On the EU level,

one should recognise the huge importance of the European Data Protection Board, established by GDPR, which serves as an independent European body, contributes to the consistent application of data protection rules throughout the EU, and promotes cooperation between the EU's data protection authorities (EDPB, 2022). The latter task is carried out through engagement of national supervisory authorities' representatives in the Board from all EU MSs (and partially EFTA EEA states), and the European Data Protection Supervisor.

Second, if procedural law does not take into account or does not regulate the way in which the party's legally protected interest (e.g. rights under GDPR) is implemented, a legally relevant substantive decision can still be made, yet the status of the party that, in such case, lacks legal protection, is likely to be affected. If the authority determines an entitlement under public law, it should also determine the relevant procedure that would enable its effective protection. In fact, only the procedural elaboration of a substantive right truly enables its realisation. Therefore, in most legal systems, insofar as the procedure is not regulated by a sector-specific law, the principles and rules of national Administrative Procedure Act apply *mutatis mutandis* also in non-administrative, yet still public law relationships like in privacy rights enforcement also by private data bases holders. (Administrative) procedure thus serves the purpose it pursues, in terms of implementation of substantive rights and fundamental procedural principles or safeguards. The GDPR, though, only partially regulates procedural issues (see Pirc Musar et al., 2020); while on a systemic level, it leaves such up to the Member States. This seems like a logical choice considering the different administrative traditions of individual countries.

In addition to the GDPR, another two important (proposals for) Regulations have recently been developed in response to ICT development in the EU, namely the ePrivacy Regulation, addressing, in particular, the protection of personal and other data in e-communication, and the Regulation on artificial intelligence (AI) restricting the use of AI in relation to individuals.[3] This shows the need for a more uniform and modern EU-wide regulation that restricts the interferences with the status of individuals. On the other hand, various analyses show (cf. Voss, 2017; Corbet et al., 2021; Nikolić and Kovač, 2021) that such rules may limit the EU's competitiveness when it acts as a political or economic entity against the US or China, which requires a constant trade-off between legal certainty and flexibility.

3.2 The regulation of privacy and the development of the social credit system in China

Being a socialist republic, China presents a completely different political and legal regulation of social issues than Western liberal democracies. The reins of society are in the hands of the Chinese Communist Party, which, with 89 million members, is one of the largest and most powerful political parties in

3 See the two proposals at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010> & <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021P C 0206>.

the world (Lawrence and Martin, 2013). To stabilise the country's one-way system of government, the Chinese Communist Party is working to transform China into the most influential country in the world with the greatest economic potential. Considering its complete control and one-party system of government, however, its activities are non-transparent and, for the most part, considered a secret.

China has been repeatedly in the eyes of the world public for its numerous violations of fundamental human rights and its clear opposition to the ratification of declarations aimed to guarantee and protect human rights (Botsman, 2017). By doing so, China is moving far away from the liberal Western countries and strongly undermining the human rights system. The government quickly silences those who criticise and oppose this way of regulating society (Peerenboom, 2005, pp. 72–162; Kent, 2013). Despite China's constitutional regulation whereby all matters in the country are to be governed by laws, the Chinese legal system is quite unusual, as laws have never been codified. The majority of important decision-making in society is made by quasi-judicial institutions that resolve and decide on most public law matters, while the government runs and implements its governance of public law matters employing information systems and algorithms (Wang and Madson, 2013; Xu, 2019, pp. 153–175). An example thereof is the social credit system, introduced to ensure the greatest possible conformity of the citizens and fulfil the positive obligations of the government.

The social credit system is a Chinese government project whereby the government, by means of big data databases and various information on individuals, monitors and evaluates their social acceptability and trustworthiness. Each citizen gets an exclusive social score and is rewarded or punished based on his or her behaviour. The social credit system was first introduced in 2019 with the launch of a project coordinated by the Central Leading Group for Comprehensively Deepening Reforms of the Chinese State Council (Wong and Dobson, 2019, pp. 220–232). Despite a relatively short development and implementation phase, the system has been fully operational since 2020. The Chinese government has even made pilot algorithms available to eight high-tech companies to help test the integration of its large databases and thus improve the implementation and centralisation of its algorithm model (Cheung, 2009, pp. 275–279; Jiang and Fu, 2018, pp. 372–392). Despite several criticisms, those algorithms are kept secret already in the pilot phases and even today, hence it is not possible to fully determine which data the system is based on and with which algorithms such systems operate and collect process and exchange data (Cheung, 2009, pp. 275 –279; Shen, 2018, pp. 21–31).

Citizens with high scores get rewards (e.g. easier access to loans or visas, Wassler and Tolkach, 2019), while those who score low are sanctioned (see, e.g., Liu, 2019). A pilot project entitled Honest Shanghai, for example, gave individuals the option to voluntarily download and sign up to the app by providing a range of personal data and importing data through the usage of facial recognition technology (Dai, 2018). According to a public project carried out in Rongcheng, a city in the Shandong province, each resident started off with 1000 social cred-

it points to be used for their social grade (Liu, 2019, pp. 22–32). Individuals with high scores were considered to be model citizens, those with a score of 850 to 600 were imposed restrictions, while those with a lower score became 'objects of significant surveillance' (Brehm and Loubere, 2018), did not have access to managerial positions, etc. Also in other Chinese cities where projects for the introduction of social credit systems were in place, e.g. in Dongfeng in the Henan province, various social credit rating algorithms were installed in landline and mobile phone systems. So, one was greeted with an audio message instead of a ringing tone that informed the caller that the person reached was an irresponsible and dishonest person when trying to call an individual who was on the system's blacklist (Wong and Dobson, 2019, pp. 220–232). In the city of Taishan, LED billboards and large TV screens located in shopping malls and other public places were used to expose people on blacklists by displaying their pictures. By 2020, over 50 Chinese government departments signed a memorandum to restrict access to public goods for 'discredited' individuals (Aho and Duffield, 2020, pp. 187-212; Wong and Dobson, 2019, pp. 220–232).

The social credit system can thus be regarded as a covert and deliberate plan to create obedient citizens, which allows mass surveillance of individuals by using large databases and information. Such projects suggest that to make citizens conform and to create an environment of public order and peace, the Chinese government encroaches on many other aspects of society, especially individuals' privacy and personal data protection, as well as their freedom of expression and autonomy in society. The social credit system project is thus a substitute for the Chinese system of individual trials, while the combination of ICT development and the use of power without legal guarantees is just another dimension of lowering democratic standards (Macnish, 2014, pp. 142–153). Such systems do not provide for any mechanism of protection and legal remedies in cases of unjustified placement of individuals on blacklists. By doing so, the government systematically violates fundamental human rights that are decided globally e.g. under the UN Universal Declaration. Thus, even the provisions of the Chinese Constitution remain just a dead letter, leading to digital dictatorship (Zhao, 2015, pp. 29–52; Chen and Cheung, 2017, pp. 356–378; Dai, 2018). In the case of the social credit system, the government deliberately promotes dictatorship, stifles fundamental human rights arising from international pacts, and imposes draconian projects aimed at the restriction of individual rights, surveillance, and citizen obedience. The reasons for this form of government can be found in the lack of an effective electoral system, transparency of government and its work, and democratic governance guidelines in general.

4 Results of the comparison of privacy regulation, trends and safeguards in the EU and China

To study the global understanding and development of privacy from a political and sociological aspect, we performed a comparison between the EU and China based on key findings of scientific literature, expert interviews, and axiological and sociological methods. It was aimed at exploring the com-

monalities and differences between the two systems to tackle our research question addressing global and regional principles of democratic governance, the regulation and understanding of personal data protection more strictly in Europe as opposed to the regulation in China.

The Chinese social credit system is by no means the only one where ICT and big data based algorithms are used in the context of surveillance. Although such systems of society regulation are hardly imaginable in the EU, some cases of individuals' assessment according to their specific actions can already be observed. Behaviour is assessed, for example, by some EU insurance companies that use computer-based data processing to determine whether an individual is a careful or reckless driver, which affects the cost of insurance for the vehicle owner. Similarly, data from various devices for tracking sports activities are used to determine the price of health and sports insurance. Moreover, the assessment of individuals is present in the private sector where customers rate service providers and the system uses the relevant algorithm to assign to this provider – according to its rating – more potential customers and improves its visibility on the platform. Similar assessment methods can be seen on social networks such as Facebook, Twitter, Instagram, etc. These systems operate on a voluntary basis but eventually act as control systems encouraging individuals to take certain actions. Yet, unlike the Chinese social credit system, they are based on individuals' voluntary registration and are not implemented by the government as in the Chinese case. The European assessment systems focus on encouraging citizens to pursue activities that are beneficial to society, thus helping society to create credible profiles of people, places and events (Kasl, 2019, pp. 349–358). However, such a way of society control also resulted in lower participation and visibility of individuals with low ratings. According to the review of the relevant scientific literature, such kinds of assessments on social networks in some way even promote the social credit systems (Shahin and Zheng, 2020, pp. 25–41; Mistreanu, 2018). In comparison, China's system is much more formalised and centralised, laying in the hands of a superior authority without the possibility of logging out and with much more serious consequences, i.e. limited fundamental human rights and tightened social surveillance.

In light of the above, the comparison between the EU and China was largely based on expert interviews, taking into account a previous normative analysis. The interview questionnaire contained four sets of questions with standardised answers to allow an easier and more objective comparison. The first set of questions referred to the authorities' role in ensuring privacy and personal data protection, i.e., whether the authorities are entitled to encroach on privacy or, on the contrary, they are primarily obliged to ensure the protection of privacy and personal data. The second set dealt with social surveillance, the third one with the institutional and supervisory function of the government to ensure personal data protection, while the fourth set featured a direct comparison between the EU and China according to previously defined dimensions and criteria. It is clear from expert interviews that in the EU, the methods of social surveillance – such as the social credit system in China or

even in Europe in the private sector and on a voluntary basis – are far from acceptable and are inconsistent with existing legal sources and trends. The European legal order explicitly excludes and restricts such encroachments on fundamental human rights and, if necessary, even restricts authority but this does not necessarily mean that any method of control is illegitimate and illegal. Namely, interferences are permitted when the following elements are cumulatively present: (a) a legitimate purpose prescribed by law; (b) exercised by a body designated as competent by the legislature, and (c) exercised within clearly defined limits of necessity and proportionality and with all safeguards concerning personal data protection and privacy, as well as other human rights. It is precisely the principle of proportionality that underpins any interference with fundamental human rights, even if social control systems had the necessary and thus legitimate purpose. Surveillance through the social assessment of individuals could only be some kind of transitional compensation by the Chinese authorities for the inefficiency of their courts in enforcing sanctions and ensuring conforming conduct by individuals (cf. Macnish, 2014).

Regarding the extent to which the government should regulate the right to privacy and personal data protection, the expert interviewee Chen emphasises that it is first necessary to differentiate between privacy and personal data protection, as only in view of their differences it is possible to argue that the government must allow individuals to have control over their personal autonomy and self-determination. He estimates that there can be no simple solution to what kind of regulation it should be, as the authorities must carefully extract this variable value of personal autonomy from a rather complex concept of privacy. This means that encroachments on such rights need to be treated on a case-by-case basis, as there are no general guidelines for guaranteeing such. Even in more collectively oriented societies such as China, there should be an exceptionally good reason in the public interest for certain government interferences with individual rights (e.g., interventions to limit COVID-19, which must also be well considered and limited in time). The same position is taken by the second interviewee, which confirms what also follows from the literature examined in the previous chapters. Expert interviewee Kallenberger emphasises the duty of the legislator to create a framework that allows citizens to exercise their right to control what happens to their data. Expert Kallenberger further points out that all data controllers, whether in the public or private sector, have the obligation to inform the people concerned about the processing of their personal data and observe all the principles of their protection. In the EU, the GDPR represents an important step towards a more prudent and responsible use of personal data by public and private entities (Ding and Zhong, 2020, pp. 630–644; cf. Pirc Musar et al., 2020 in the definition of private controllers). This reflects, inter alia, in the various forms of control despite the approach and purpose being the same, i.e., digitisation of control systems to increase the security of countries or communities.

Table 2 shows the main findings on the fundamental differences in the control systems of the EU and China, as shown by literature review, normative comparisons and, in particular, expert assessments. The table shows that

there are huge differences between China and the EU, both in political and legal terms. Unlike in China, the legal system in the EU is much more restricted, rigorous and detailed – there is stricter protection of privacy and personal data protection and stricter judicial review.

Table 2. Comparison of frameworks and bases of privacy regulation and control in the EU and China

Comparison criterion	EU	China
Political system	*Sui generis* form of a supra-national union of democratic countries	Authoritarian socialist republic with a single-party government
Legal tradition	A mix of continental & Anglo-Saxon traditions	Continental legal system
Legislation on privacy and personal data protection	More rigorous, uniform and definite legislation, particularly with direct application of GDPR in all Member States	Unclear, diversified and insufficient legislation with many undefined legal terms
Addressing privacy v. transparency	Both principles are systematically seen as a part of good administration	Privacy control is significantly predominant concept, while transparency is understood rather narrowly
Legitimacy	Limited grounds under Art. 6 GDPR (e.g. consent, contract, law)	National security and national interests
Liable entities	Same for public and private sectors	Almost unlimited authority
Procedural guarantees	Systematically enshrined through EU and national (administrative procedural) law	Almost non-existing
Control	As a rule, bi- or multilateral control	As a rule, unilateral control
Judicial review	Strict judicial review in relation to EU Charter & GDPR	Weak judicial review, subordinate to government

Source: own analysis.

The interviewees see the reasons for a more restricted regime in the EU and thus stricter protection of privacy and personal data especially in the system of democracy, the ratification of international human rights treaties, different cultural norms in the EU compared to China, and greater willingness and ability of individuals to participate in public governance and control of the government. Expert Chen notes that the biggest problem with the Chinese regime allowing such systems to prosper is precisely that the concepts and

understanding of the public interest are vague and interpreted in the light of the prevailing political interest. He also notes that the political party in power has monopolised the definition of the public interest, stating that it is in the public interest that the government controls individuals and infringes on their right to privacy. This is further allowed by a lack of regulations such as the GDPR to limit the interference of the government and other controllers. The problems of the Chinese system are thus systemic and culturally conditioned, as the law only reflects social tradition and values. Alongside that, the Chinese courts often refrain from settling the conflict between privacy and transparency by installing the so called "need to know" trend in their ruling of the requesters' interest to access government's information. Therefore, the principle of public monitoring and transparency by ensuring the governments accountability is often undervalued and prevailed by privacy (or other non-disclosure) aspects (Chen, 2015, pp. 275–276).

According to experts, in terms of a global understanding of human rights, the EU has – compared to China – more appropriate legislation that protects individuals from surveillance and excessive encroachment on the rights to privacy and personal data protection. The baselines and safeguards set out in the GDPR have already begun to spill over the EU's borders. Thus, in August 2021, even China adopted its Personal Information Protection Law. This law and the GDPR are quite similar in several respects, from which it can be concluded that the GDPR is the gold standard of protection of the right to privacy and personal data protection both in the EU and more broadly, internationally. This is indeed positive for increasing the provision of these rights worldwide. According to the expert interviewees, the power and weight of individual principles (transparency, privacy, accountability, etc.) depend on political philosophy and the establishment of hierarchy between the two is a matter of political and wider social discourse.

These results might suffer from the classic limitations of interviews or survey-based studies (Nitzl et al., 2020; Speklé and Widener, 2018). The conclusions are necessarily based on average evaluations. Hence, we provide an overview of the systematic grounds, sources and trends, not idiosyncratic factors. The subjective evaluations of the respondents may lead to the misrepresentation of some key constructs in our study but by triangulation comparisons, we believe, overcome this weakness, so that final findings present scientific value and practical implications to be taken into account by legislatures and public administrators. From scientific point of view, it is important to mention also that our study is reflecting a specific point of time. A longitudinal research could analyse more long-term changes.

5 Discussion

Society control and the related challenges for privacy and personal data protection are increasingly shaping the course of societal development. Privacy and personal data protection, especially in the light of their provision and possible excessive interferences, also present a challenge in terms of under-

standing their dimensions and impact on other fundamental human rights (e.g. freedom of expression). The analysis of the Chinese social credit system suggests that inadequate provision of privacy and encroachment on privacy and personal data protection related rights/principles lead to a full surveillance society that deprives individuals of their ability to act autonomously. Based on the analysed academic and professional literature, it seems that the EU has developed some important fundamental safeguards under international, constitutional and administrative law (see Galetta et al., 2015, Cullen, 2016, and others) that prevent slipping into surveillance similar to that in China. At the regulatory level, privacy and personal data protection – in relation to the massive, algorithm-based collection of data on individuals – are generally defined by the GDPR. The latter thus represents the gold standard for the protection of the right(s) to privacy and personal data protection, as unanimously recognised by research and expert assessments.

The main objective of the research was to answer the questions of how the concept of privacy can be understood in the context of two entities as politically, culturally and sociologically different as the EU and China, and what safeguards the EU citizens have against (excessive) society control. Comparing the EU and China, however, has its limitations, taking into account the statehood and (de)centralised modes of public, governance, yet the aim of this study was to show cultural framework of legal safeguards and their trends on the field. While transparency and privacy are not antonyms, there is a trade-off between them. Transparency appears both as a concern and as a remedy in the debates over privacy: too much transparency may compromise individuals' privacy, but when trying to control the use of registry data by the public administration, we call for transparency (Erkkilä, 2020). If EU seems to dedicate a lot of attention to the proportionate balance of data protection on one side and (administrative) transparency on the other side, Chinese developments are rather unilateral in terms of more and more strict surveillance mechanisms of the state over its people. This shows fundamentally different understanding of human rights and democratic safeguards, which has comparative scientific but above all practical implications.

In this regard, it is worth pointing out that privacy is a rather complex notion that can be understood in different ways. Although in the EU privacy is considered a fundamental human right that enables the fulfilment of other fundamental human rights, while any encroachment on this right is seen as an encroachment on the autonomy and freedom of individuals, this is not the case in China. In China, privacy is not seen as a human right, nor is it regarded as one of the foundations of freedom, while its člegislative protection is scattered and uncoordinated. Given its dysfunctional judiciary supporting a system of sanctions and punishments for all kinds of violations, the government's main sanction is naming and shaming, which means total loss of privacy and social surveillance. In China, such kind of governance seems to build primarily on systemic problems rooted in the citizens due to the lack of basic democratic elements. The European system, on the other hand, focuses on democracy, the rule of law, lawfulness and strict protection of fundamental human rights. The differ-

ences between the two are cultural, social, as well as political and legal, which means in particular that China, compared to the EU, presents a severe lack of adequate safeguards against government interference with the privacy of individuals and an inadequate system of judicial review. The extensive surveillance of citizens through naming and shaming discredited individuals and allowing sanctions and rewards leads to the gamification of the process of managing public tasks and government obligations, and thus to disproportionate interferences with the privacy of individuals. This result was indeed expected, as historical and comparative experience shows that human rights protection standards are much higher in the EU than in China. As a result, understanding the limits of privacy and its importance in the context of ensuring other fundamental human rights, in particular, is a major guiding principle of Western democracies. Any restrictions on fundamental human rights should always be the result of rigorous consultation procedures, where the real costs and benefits of any measures and interventions in any human right are carefully weighed.

The initial research question, to which extent and why the EU, compared to China, presents stricter and broader protection of the right(s) to privacy was answered taking into account the attributed principles of democracy and the strict provision of fundamental human rights in the EU. The finding might seem (too) obvious, yet is not self-evident in the extraordinary circumstances in major crises (financial, health, migrations or wars related). Consequently, based on both the extensive academic literature on the social credit system, its limitations, evolution and impact on individuals' privacy and personal data protection, as well as on comparisons of regulations and assessments by expert interviewees, it is shown that cultural values serve critically as a framework for individuals' safeguards toward public authorities or the lack of them. The key difference between the European and the Chinese models do turn out to be especially values of Western democracies, with their respect for the principle of proportionality, which applies to both drafting and implementing regulations in practice. The use of technology must thus be appropriate, lawful and within the framework of privacy and personal data protection (Peerenboom, 2005, pp. 72-162; Kent, 2013; Zhao, 2015, pp. 29-52; Kasl, 2019, pp. 349-358). This prevents the development of ICT systems such as the social credit system on European soil. China's system of rating its citizens is incompatible with the core values of European society, which is based on democratic precepts and a strict guarantee and recognition of human rights such as personal data protection. In this respect, the GDPR may well be considered the gold standard on a global level.

This is the case not only in terms of substantive privacy rights but also refers to procedural and institutional regimes (cf. Fisher, 2010). For the latter the role of European data protection board and supervisor, as well as national agencies and information commissioners are emphasised for the sake of achieving both, the unified application of EU law in all MSs (EDPB, 2022), and bridging potential gap between the law in letter and administrative practices in force. Moreover, the procedural elaboration of a substantive right defining the participants in the procedure, formality, stages of the procedure, dead-

lines and remedies, enables its realisation, particularly through co-participation of legitimate entities. In consequence, it is important to acknowledge the role of joint procedural and even more the national Administrative Procedure Acts application in enforcing the privacy rights (cf. Kovač, 2014). Besides the GDPR, the future EU Regulation on artificial intelligence (proposed in April 2021) is expected to provide additional protection against interferences with privacy. It is intended to standardise the rules for AI use in the EU and provide additional safeguards for the use of such systems. The main objectives of the Regulation are, in particular, to ensure that AI systems placed on the Union market are safe and respect Union values and fundamental human rights, to ensure legal certainty and predictability to facilitate innovation and investment in the AI sector, and to facilitate the development of a lawful, safe and trustworthy single market for AI. Finally yet importantly, it aims to enhance governance and effective enforcement of safety requirements and fundamental rights applicable to AI systems. The proposed AI Regulation is based on the estimated level of risk posed by AI in terms of achieving the appropriate level of compliance (from unacceptable to high, limited and low risk). It also envisages the setting up of a special EU body – the European Artificial Intelligence Board (EAIB) – to provide advice and expertise to the European Commission, as experience with personal data protection or public information (see Kovač, 2014; Pirc Musar et al., 2020) points to the need for institutional oversight for the effective exercise of rights. The EAIB will foster effective cooperation between national supervisory authorities and the European Commission, coordinate and contribute to guidelines, and assist national supervisory authorities and the European Commission in ensuring a consistent application of the Regulation (Corbet et al., 2021).

We should hereby point out that the GDPR already serves as the main existing protection mechanism and regulatory framework that limits some uses of AI and big data processing in the EU. Not only does the GDPR in Article 25 stipulate the design of any systems processing personal data by being built with the awareness of data protection by design and by default, the GDPR also strictly limits any system (AI or beyond) to strictly take into the account the main personal data principles, such as data minimisation, purpose limitation, transparency etc., when any personal data is being processed. The GDPR also enables (in light of the transparency principle) that the individuals may always request from their data processor any information regarding their data and therefore stipulates in Articles 15, 1(f) that any data subject has the right to obtain information whether their data was processed by automated means and has the right to obtain meaningful information about the logic involved as well the significance and the envisaged consequences of such processing for the data subject. With that in mind, Article 22 of the GDPR also gives the right to the data subject (except in certain conditions set by the Article 22, paragraph 2) to refrain from decision made solely by AI and request that such decision has no effect on the individual. Moreover, Article 35 of the GDPR also invasions that a controller conducts an impact risk assessment of envisioned processing on the protection of personal data, where the processing might result in high risk to the rights and freedoms of the individuals. All things considered, the

not yet finalised AI Regulation will thus, according to the proposed provisions, complement the already existing provisions of the GDPR and provide additional safeguards in the EU to discourage systems similar to the social credit system. As the artificial intelligence systems become smarter, faster and more proficient, their ability to sort out valuable information from the variety of big data becomes easier, granular and immensely more accessible. The faster collection of big data and systems ability to meticulously analyse the data, offers an immense challenge on its ability to intrude on privacy interests of the individual. It is therefore crucial to design such regulation that would on one hand protect individual right to privacy and personal data protection while on the other hand not excessively intrude on the AI development.

China may be seen as a very peculiar national system, especially compared to the supranational one like the EU. Yet, Chinese rather extreme practices and trends offer a reflection on the European cultural values and the consequent EU legal regulation. This study, in spite of given constraints, shows both; first, a high level significance of cultural background for legal institutes and administrative practices to be enforced in any field. Second, the EU is not immune to the erosion of democratic safeguards at protecting privacy when a more centralised need to respond to major crises is required. As in China, also in the EU, one observes the deterioration of the rule of law instead of its strengthening when faced with a need for rapid administrative measures. In sum, this research opens up numerous scientific questions for new prospective field studies. For instance, an issue of crises resilience in public governance, especially in law-making and administrative procedures, occurs. The study also reflects upon the differences of centralised countries regardless of its size (China as an example albeit extreme one) and the decentralised coordination required as in the pursuit of unified EU and national law and institutions in public affairs and related European reforms. Further, we can explore the importance of the principles of separation of powers (legislative, executive, judicial) in the contemporary environment and proportionality, especially in conflicting privacy and transparency rights. As key concepts of public administration, privacy and transparency are relevant for both democracy and efficiency of public governance, despite the fact that they are ambiguous and even paradoxical by nature (Erkkilä, 2020). Actually, too strictly taken or top-down only enforced privacy often acts as the trigger for transparency call (Fisher, 2010). Ensuring the balanced enforcement of privacy and transparency rights, (indirectly) enables the individual to better participate in the process of governing public affairs while also on the other side protects the individuals from possible abuse of power by enhancing the governments' accountability to the public.

In conclusion, it should be pointed out that the Covid-19 pandemic brought many challenges to society and led to stricter control over citizens to protect public health. Such approaches are often presented as an expression of increased efficiency and responsiveness as the guiding principles of good public governance (e.g. according to Aristovnik et al., 2021). For example, in March 2020, Russia reported that it used face recognition technology – a highly invasive and therefore almost unlawful approach according to the proposed EU

regulations! – to arrest and fine over 200 individuals who breached isolation and quarantine. Although Russia was critical of China's social control system, the threat posed by Covid-19 showed – in Russia as well as in several EU countries, cf. the results of the constitutional review assessing certain measures as unconstitutional or unlawful – that under specific conditions, a system without adequate safeguards can force even a critical authority to do the same. Comparative study, carried out hereby, is therefore of high significance, especially in the light of privacy intrusions and personal data protection during the corona pandemics. Namely, it has revealed the relativity and even fragility of the right to the protection of personal data globally, the EU included. This finding, we believe, is very important for future development of safeguards, albeit or even in particular when facing special circumstances. Not even major crises should allow rather total infringement and denial of such fundamental principles and rights as developed over time in European context or insofar sacrifices prove to be of no avail, which is not acceptable within a democratic framework. Individual human rights should therefore only be limited to the extent of what is appropriate and necessary in order to attain the objectives legitimately pursued by the measure in question which should be proportionate *stricto sensu* given the context of the concrete limitation.

The study shows that broader cultural and societal environment is very decisive when it comes to regulating, respecting and guarding human rights and implementing good administration. Privacy and data protection are hereby often among the first victims of governments' interests to command the critical response to crises occurring in a contemporary world. The Chinese example shows where also European or Western development can lead to if not careful in preserving (regional) democratic standards and proportionate weighing between efficient public governance and good administration principles, privacy rights incorporated. Recognising how fragile the concepts of democracy and fundamental human rights are, we can conclude that the introduction of similar control systems in the future is likely even in the EU. Despite consistent protection of privacy and personal data, which derives from the widespread practice of both national and European courts, and despite the ratification of international treaties (Browne, 2017) it can be concluded that the safeguards of human rights protection in the EU prevent the authorities from creating a surveillance society. It is precisely through the definition of fundamental human rights in the EU that personal data protection preserves its relevance (Kuner et al., 2020; Cullen, 2016). It is therefore necessary – even or especially in crises – to overcome the dilemma between security and freedom, as these are both valuable civilizational assets.

6 Conclusion

The key difference between the EU and China in the regulation of the topic under consideration is the concern for privacy and related rights of personal data protection. The European legal framework on privacy and personal data protection, with the GDPR at the forefront, is robust, modern and able to

adapt to the needs of modern society, notwithstanding the exceptional development of ICT and global crises. However, new technological solutions and practices, as characteristic of the Asian setting, are causing new collisions with established social conditions, and thus with the guaranteed human rights of individuals. This often leads to a series of challenges and the necessity to regulate a certain area in a manner such as to ensure that the collection and processing of personal data employing technology are appropriate, lawful and proportionate. But this is only possible if and as long as personal data protection is systematically understood as a core human right, restricting the authorities' interference with the privacy of individuals.

The main difference between the EU and China thus lies in the systemic regulatory framework that allows for an effective personal data protection and prevents mechanisms such as the social credit system. In the EU, democratic safeguards are in place that guarantee human rights, proportionality, the rule of law and legality, which are not categories that can simply be taken for granted. They call for constant monitoring, awareness raising and improvements of regulations tailored to societal changes. This leads to a final call for the society of the future to be guided by the principles of democratic government based on the European values of high protection of privacy and personal data. Let the path of social development be paved not by technology, but by the values of a particular social community, balancing individual rights and community benefits as the prescribed foundations, measures and limits of the public interest.

References

Aho, B. and Duffield, R. (2020). Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China. Economy and Society, 49(2), pp. 187–212.

Aristovnik, A. et al. (2021). The use of ICT by local general administrative authorities during Covid-19 for a sustainable future: Comparing five European countries. Sustainability, 13(21), pp. 11–65.

Avbelj, M. (ed.) (2019). Komentar Ustave RS [Commentary to the Constitution of the RS]. Nova Gorica: New University.

Bauer, M. and Trondal, J. (eds.) (2015). The Palgrave Handbook of the European Administrative System. New York: Palgrave Macmillan.

Botsman, R. (2017). Big data meets Big Brother as China moves to rate its citizens. At <https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>, accessed 15 December 2021.

Brehm, S. and Loubere, N. (2018). China's dystopian social credit system is a harbinger of the global age of the algorithm. At <https://theconversation.com/chinas-dystopian-social-credit-system-is-a-harbinger-of-the-global-age-of-the-algorithm-88348>, accessed 15 December 2021.

Browne, A. (2017). China uses 'Digital Leninism' to manage economy and monitor citizens. At <https://www.wsj.com/articles/xi-jinping-leads-china-into-big-data-dictatorship-1508237820>, accessed 21 December 2021.

Chen, Y. (2015). Privacy and Freedom of Information in China. European Data Protection Law Review, 1(4), pp. 265–276.

Chen, Y. and Cheung, A. S. (2017). The transparent self under big data profiling: Privacy and Chinese legislation on the social credit system. The Journal of Comparative Law, 12(3), pp. 356–378.

Cheung, A. S. (2009). China Internet going wild: Cyber-hunting versus privacy protection. Computer Law and Security Review, 25(3), pp. 275–279.

Corbet, R. et al. (2021). The EU's new Regulation on Artificial Intelligence. At <https://www.lexology.com/library/detail.aspx?g=ce54d982-fb54-46c4-abad-b6b2c70985b0>, accessed 15 December 2021.

Cullen, H. (2016). Siliadin v France: Positive Obligations under Article 4 of the European Convention on Human Rights. Human Rights Law Review, 6(3), pp. 585–592.

Dai, X. (2018). Toward a reputation state: The social credit system project of China. At <http://dx.doi.org/10.2139/ssrn.3193577>, accessed 15 December 2021.

Ding, X. and Zhong, D. Y. (2020). Rethinking China's Social Credit System: A Long Road to Establishing Trust in Chinese Society. Journal of Contemporary China, 30(130), pp. 630-644.

EDPB, European Data Protection Board (2022). <https://edpb.europa.eu/edpb_en>, accessed 5 March 2022.

Erkkilä, T. (2020). Transparency in public administration. In W. R. Thompson (ed.), Oxford Research Encyclopaedia of Politics. Oxford: Oxford University Press. <https://doi.org/10.1093/acrefore/9780190228637.013.1404>

Fisher, E. (2010). Transparency and Administrative Law: A Critical Evaluation. Current Legal Problems, 63(1), pp. 272–314.

Galetta, U.-D. et al. (2015). The general principles of EU administrative procedural law, Brussels: European Parliament,

Jiang, M. and Fu, K. W. (2018). Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit? Policy and Internet, 10(4), pp. 372–392.

Kasl, F. (2019). Surveillance in digitalized society: The Chinese social credit system from a European perspective. Lawyer Quarterly, 4(9), pp. 349–358.

Kent, A. (2013). China, the United Nations, and human rights: The limits of compliance. Philadelphia: University of Pennsylvania Press.

Kierkegaard, S. (2009). Open access to public documents – More secrecy, less transparency! Computer Law and Security Review, 25(1), pp. 3–27.

Kovač, P. (2014). Significance of and Comparative Trends in Procedural Regulation of Right to Information. Central European Public Administration Review, 12(2-3), pp. 31–45.

Kuner, C., Bygrave, L. A. and Docksey, C. (eds.) (2020). The EU General Data Protection Regulation (GDPR), A Commentary. Oxford: Oxford University Press.

Lawrence, S. V. and Martin, M. F. (2013). Understanding China's political system. Washington, D.C.: Congressional Research Service.

Liu, C. (2019). Multiple social credit systems in China. Economic Sociology: The European Electronic Newsletter, 21(1), pp. 22–32.

Macnish, K. (2014). Just surveillance? Towards a normative theory of surveillance. Surveillance and Society, 12(1), pp. 142–153.

Mistreanu, S. (2018). Life inside China's social credit laboratory: The party's massive experiment in ranking and monitoring Chinese citizens has already started. At <https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory>, accessed 21 December 2021.

Neumann, W.L. (2006). Social Research Methods: Qualitative and Quantitative Approaches. London: Pearson .

Nikolić, B. and Kovač, P. (2021). European administrative space between ideals and reality. In: Stare, J. and Pečarič, M., The science of public administration. Ljubljana: Faculty of Public Administration, pp. 621–641.

Nitzl, C., Hilgers, D., Hirsch, B. and Lindermüller, D. (2020). The Influence of the Organizational Structure, Environment, and Resource Provision on the Use of Accrual Accounting in Municipalities. Schmalenbach Business Review, 72, pp. 271–298.

Peerenboom, R. (2005). Assessing human rights in China: why the double standard. Cornell International Law Journal, 38(1), pp. 72–162.

Pirc Musar, N. (ed.) (2020). Komentar Splošne uredbe o varstvu podatkov [Commentary to GDPR]. Ljubljana: Official Gazette of the RS.

Shahin, S. and Zheng, P. (2020). Big data and the illusion of choice: Comparing the evolution of India's aadhaar and China's social credit system as technosocial discourses. Social Science Computer Review, 38(1), pp. 25–41.

Shen, C. F. (2018). Social credit system in China. Digital Asia, 2, pp. 21–31.

Speklé, R. F. and Widener, S. K. (2018). Challenging issues in survey research: Discussion and suggestions. Journal of Management Accounting Research, 30(2), pp. 3–21.

Voss, G. W. (2016). EU data privacy law reform: General data protection regulation, privacy shield, and the right to delisting. The Business Lawyer, 72(1), pp. 221–234.

Wang, C. and Madson, N. (2013). Inside China's Legal System. London: Chandos Publishing.

Wassler, P. and Tolkach, D. (2019). Orwellian tourism 2020? China's social credit score. At <http://eprints.bournemouth.ac.uk/31654/3/manuscript.pdf>, accessed 15 December 2021.

Wong, K. L. X. and Dobson, A. S. (2019). We're Just Data: Exploring China's Social Credit System in Relation to Digital Platform Ratings Cultures in Westernised Democracies. Global Media and China, 4(2), pp. 220–232.

Xu, L. (2019). The Changing Perspectives of Chinese Law: Socialist Rule of Law, Emerging Case Law and the Belt and Road Initiative. The Chinese Journal of Global Governance, 5(2), pp. 153–175.

Zhao, J. (2015). China and the Uneasy Case for Universal Human Rights. Human Rights Quarterly, 37(1), pp. 29–52.