10.32565/aarms.2023.1.9

What Can Privacy Mean in Data-Driven Societies?

The Security Policy Contexts of the Data Management Culture in the People's Republic of China and the European Union[1]

Tünde LENDVAI,[2] András TÓTH[3]

The purpose of this article is to present the basis for building trust within the European Union, through which the authors illustrate the importance of the protection of personal data as a fundamental requirement in both the EU and its Member States' legal environments. In addition, the authors have examined the Chinese Social Credit System, which by its design and operation is not primarily focused on building trust and is therefore not the most appropriate solution for building trust. The authors conducted a SWOT analysis comparing the EU and Chinese principles to achieve their objectives. They also conducted interviews with people who have personal experience with the Chinese credit point system. Based on the results obtained, they sought to justify their basic hypothesis that this type of credit system could not be applied within the EU.

Keywords: *Chinese Social Credit System, data-driven society, personal data, privacy, trust*

The People's Republic of China (hereinafter referred to as China) operates a unique data-based public administration system, the Social Credit System (in Mandarin: 社会信用体系, pinjin transliteration: shehui xinyong tixi). On the other hand, the European Union prioritises protecting the public's personal data, an obstacle to any Member State's efforts in this direction. Therefore, the basic regulation is the General Data Protection Regulation (GDPR), which aims to prevent the collection and processing of data about the public without their consent. Accordingly, it regulates how data is collected, processed, stored, erased, used and transferred.

The study uses a deductive approach and a qualitative assessment of secondary data to show how political and cultural traditions, as well as geopolitical and economic conditions have led to the development of a data management culture in China that is so different from

[1] The work was implemented in the framework of project TKP2020-NKA-09 funded by the National Research Development and Innovation Fund under the Thematic Excellence Program 2020.

[2] Junior IT Security Auditor, Black Cell Magyarország Ltd., e-mail: lendvaitunde96@gmail.com

[3] Associate Professor, University of Public Service, Signal Department, e-mail: toth.hir.andras@uni-nke.hu

European traditions and on which the social credit point system could be built. The Beijing leadership's operation of an extensive data collection and data-driven administrative approach both helps and hinders the state's security policy and cybersecurity efforts by applying a defence framework built around cyber warfare logic. To prove this thesis, the study explores the correlations between how the government's data disclosure requirement limits the ability of the major players in the Chinese IT market (Alibaba Group, Tencent, Baidu) to address cybersecurity vulnerabilities, which in turn reduces trust in Chinese IT services and the overall security of cyberspace. Within the European Union, the authors have reviewed the principles and practices that aim to build the trust that will help people use the systems and services available under the Digital Europe Programme without fear of their personal data being accessed by service providers and the public and non-public actors. To increase the validity of the results, the authors conducted expert interviews as part of primary data collection (see section *Interviews*). These focused on confidentiality, which is central to their research, and concerning which they formulated their basic research question about what confidentiality might mean in data-driven societies. In their analysis of the interviews, they examined what trends emerged in response to the questions related to each hypothesis, from which they could draw relevant scientific conclusions. The hypothesis were the followings:

- The European Union is making great efforts to build trust, but this can be threatened by technological, technical, or sociological influences from outside the Union.
- The Chinese Social Credit System is not based on trust, the reason being that the focus of data protection is on the state perspective and not on individuals, and therefore it is not feasible to implement this type of system in the EU.

The main objective of the research is to conduct a comparative case study of social credit scoring and data cultures controlled by the EU legal framework to prove, by answering the hypotheses, that introducing a credit scoring system is not feasible in a trust-based society. Furthermore, by comparing the two contexts, we can gain a better understanding of the social and legal implications of introducing credit scoring systems in EU countries.

Trust and privacy in the European Union

Many EU reports and strategies state that Europe is built on trust. Trust is essential because it is the basis for well-functioning relationships and is a key element in a system of properly operating democracies. Accordingly, leaders must do everything in the EU and its Member States to ensure that the necessary trust is built and sustained among citizens, businesses and organisations. In the digitalisation of Europe, information security, which is closely linked to trust, should be a key focus of attention at both public and executive levels. Therefore, Europe needs to act in a unified way in all areas of information security to ensure compliance within the Union and at the national level to build the necessary trust. To achieve this, the activities of governments and industry must not stop at EU borders, and cooperation at the global level is essential to ensure adequate security and to maintain the trust that has been built up.[4]

All these considerations indicate that, in addition to efficiency and effectiveness, building legitimacy and trust is an important factor that governments need to consider in their innovation activities for digitisation. Therefore, when we talk about digitalisation, it is important to talk about the ethical use of data, its legitimacy, which can guarantee public trust, as well as privacy, transparency, and the risks that governments and citizens need to be aware of. These are particularly important for understanding:

- the role of public trust in EU leadership and governments in the adoption of new digital services by citizens
- the conditions under which citizens are willing to accept new digital public services
- the compromises citizens make between privacy and the benefits of using new digital public services in different areas

Trust is essential in situations of uncertainty and interdependence. In the digital environment, these two factors are of paramount importance, and building and maintaining trust is one of the biggest challenges of digitalisation. From an individual's perspective, confidence in the digital age is about whether they are willing to spend time, money, or risk revealing their personal data to participate in commercial and social activities and how vulnerable they become if their data is used to monitor their behaviour, discriminate, or violate their privacy. For organisations, trust means that to take advantage of the digital transformation, each organisation assumes a certain level of risk regarding potential digital security, privacy and consumer protection incidents.[5]

In the European Union, public trust is governed by a combination of laws, regulations and ethical guidelines designed to ensure transparency, accountability and integrity in the activities of public officials and institutions. This includes measures to prevent corruption, conflicts of interest, and requirements from disclosing financial and other relevant information. The European Union's commitment to transparency and accountability ensures that public officials and institutions are held to the highest standards of integrity. Public trust is regulated at the national level, as the EU has no competence to regulate public trust issues. However, the EU has the power to set minimum standards to protect citizens' rights and has adopted various directives and regulations. These directives and regulations are intended to ensure a minimum level of protection across the EU in consumer rights, data protection and competition law. Trust is an essential component of the European Union (EU) and its member states. It is based on the idea that member states will work together cooperatively and in good faith to achieve their common goals. The EU is built on the principle of mutual trust, which means that member states trust each other to comply with EU laws and regulations. This trust is essential for the smooth functioning of the EU and is regulated by a number of mechanisms, including the EU Treaties, EU law, and the EU's institutional framework. The EU relies heavily on mutual trust among its

[4] DigitalEurope 2019.

[5] Misuraca et al. 2020.

member states, which is the foundation for cooperation, collaboration and the successful implementation of EU policies and regulations.

The concept of public trust is an important principle in EU law. It is relevant in many areas of public policy. In general, public trust refers to the trust and confidence the public has in institutions, systems and processes that serve the public good. In the European Union (EU) context, public trust is particularly important in issues such as the handling of personal data, the regulation of financial markets and the management of public resources. To maintain public trust, EU institutions and Member States must be transparent and accountable in their actions and respect the rights and interests of citizens. Furthermore, as the digital transformation progresses and the EU takes advantage of technological developments to improve processes, the EU must continue to ensure that citizens' data is treated securely and adequately protected. As the digital transformation progresses, privacy, particularly personal data protection is increasingly becoming a critical factor affecting trust. The EU has recently considered it important to regulate these areas properly to ensure that the trust established is sustainable within the EU. The EU is strongly committed to protecting the privacy of its citizens. To this end, it has enacted several laws and regulations that can strengthen public trust.

Its founding document is the Charter of Fundamental Rights of the European Union (CFR), which is the cornerstone of the EU's commitment to protect and promote the fundamental rights of its citizens. By guaranteeing these rights and freedoms, the CFR contributes to building public confidence in the EU and its institutions by ensuring that citizens feel protected and secure in their daily lives. Furthermore, by ensuring that all EU citizens have equal access to these rights, the CFR promotes equality, dignity and justice for all.[6]

The next very important document for building trust in the European Union is the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council), a piece of legislation to protect the privacy and personal data of EU citizens. The Directive applies to the processing and storing of personal data transmitted over public networks, such as the internet, and requires organisations to obtain consent from individuals before collecting data. The ePrivacy Directive aims to build public trust by ensuring that organisations handle personal data carefully and that individuals control their data. This includes the right to know what data is being collected, how it will be used, and the right to erasure. The ePrivacy Directive will help promote a culture of transparency and accountability in using personal data, which will contribute to an overall increase in public trust in the EU. By creating a single set of rules across the EU, the ePrivacy Directive will ensure that organisations are held to a higher standard when collecting and storing personal data. It also assures individuals that their data is handled securely and responsibly.[7]

The Law Enforcement Directive [Directive (EU) 2016/680 of the European Parliament and of the Council] is another important piece of EU legislation that provides specific protection for personal data in law enforcement. It applies to law enforcement agencies and

[6] Charter of Fundamental Rights of the European Union.

[7] Directive 2002/58/EC of the European Parliament and of the Council.

other government bodies that process personal data for law enforcement purposes. The Law Enforcement Directive lays down several basic requirements for processing personal data, such as openness, purpose limitation, data minimisation, and data protection by design and by default. In addition, the Directive ensures the rights of data subjects, such as the right access to and the right to modify personal data and protection against unlawful access and use. In addition, the Directive contains many safeguards to protect personal data, such as the requirement of prior authorisation and appropriate security measures and the obligation to respect the concept of proportionality. In other words, the personal processing of data for law enforcement purposes must be necessary and proportionate. Overall, the Directive provides a comprehensive framework for protecting personal data for law enforcement purposes and is a key instrument for ensuring that the privacy rights of individuals are respected in this context.[8]

The Directive on Network and Information Systems (NIS Directive) [Directive (EU) 2016/1148 of the European Parliament and of the Council] is European Union (EU) legislation that aims to enhance the EU's cybersecurity. The NIS Directive is one of the most significant efforts to increase public confidence in the digital environment. It applies to digital service providers and critical infrastructure operators and obliges them to put in place the technical and organisational safeguards necessary to maintain a high network and data security level. The Directive also requires reporting incidents that compromise the security of network and information systems. By establishing a common EU-wide framework for cybersecurity, the Directive aims to facilitate cooperation and information exchange between Member States and to increase public confidence in the security of digital services. By implementing the Directive, the EU ensures that all digital service providers and operators of key infrastructures are prepared to detect, prevent and respond to cyber security threats. It is a key step towards ensuring public confidence in the security of digital services in the EU and is part of a wider EU effort to promote a safe and secure digital environment. As such, this Directive is important to the EU's efforts to build trust in the digital environment.[9]

The European Union's General Data Protection Regulation (GDPR) [Regulation (EU) 2016/679 of the European Parliament and of the Council] is a comprehensive data protection regulation that gives EU citizens control over their data and its use. It entered into force on 25 May 2018 and replaced the 1995 EU Data Protection Directive. The GDPR applies to all organisations operating within the EU and all organisations processing EU citizens' personal data, regardless of location. The GDPR is a positive step towards protecting the privacy of EU citizens and ensuring that their data is handled appropriately in a way that is trusted by the public. It requires organisations to be open about their personal data collection practices and seek individuals' explicit consent before processing it. Under the GDPR, individuals have the right to access and delete their personal data. In addition, businesses must have appropriate technical and organisational safeguards to protect personal data against unauthorised access, loss or destruction. By enhancing data protection rights and promoting responsible data management practices,

[8] Directive (EU) 2016/680 of the European Parliament and of the Council.

[9] Directive (EU) 2016/1148 of the European Parliament and of the Council.

the GDPR contributes to developing innovative technologies and services based on the responsible use of personal data and strengthens public trust in the digital economy. The GDPR is a comprehensive regulation that aims to give individuals greater control over their personal data and hold organisations accountable for how they collect, process and manage it. The GDPR also requires organisations to implement systems and processes to manage data responsibly, including security measures to protect personal data against accidental or unlawful destruction, alteration or loss. It also promotes public trust in the digital economy by strengthening data protection rights and promoting responsible data management practices.[10]

These legislations' primary objective is to develop and preserve trust within the EU by protecting personal data. In the vast majority of instances, these procedures significantly restrict the gathering of information, as no individual, organisation, or government may collect personal data without the consent of the data subjects. This indicates that the right to personal data protection should not be violated even if the information is gathered for security purposes and is proportional to the public interest. Therefore, if the user wishes to protect his personal information, this right cannot be prohibited, which is a relatively stringent information-gathering restriction. According to the regulations, if personal information is collected, the user must be informed beforehand and grant his consent. No organisation should place the data subject in a position where he or she is compelled to waive the right to protect personal data concerning this point. In other words, if the data subject does not consent to collecting and processing his or her data, this cannot be prohibited, even for reasons of public interest. This means that organisations must ensure that any data processing is conducted in accordance with the individual's right to privacy and that the data subject is adequately informed of the purpose of collecting their personal data. For example, from a surveillance point of view, it is particularly important to note that some regulations consider the increasing amount of personal data users make available to the public thanks to newer and newer infocommunication technologies and platforms. For example, this is key to obtaining data from open-source information. However, this provision should be interpreted as an acknowledgement of the need to protect the flow of large amounts of personal data into the information space. From an information-gathering perspective, this narrows rather than expands the possibilities. If we analyse the regulations, the protection of personal data is much stronger than the interests of society. Accordingly, the collection and processing of personal data cannot be based solely on the presumption that it is in the public interest, as the EU strongly regulates this possibility and prohibits these type of activities. Overall, consent plays a key role in data collection. From the individual's point of view, consent should be voluntary, unambiguous and independent of any position of power. From the organisation's point of view, it should be proportionate, ethical, necessary, fair and transparent. This requires an appropriate level of trust between citizens and government, and trust and transparency are, therefore, key success criteria for the data-driven government. Therefore, the design and operation of data infrastructures (enabling the sharing and reusing of personal data) should include mechanisms for trust, transparency and privacy to ensure user acceptance. A focus on trust, transparency and

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council.

privacy should be at the forefront of any data-driven government to ensure a successful transition into an era of digitalisation. Trust is essential to the success of any data-driven government, and it should be ensured by providing citizens with clear information on how their personal data is used.[11]

In addition, it is important to note that these legislations do not cover activities related to national security, so if the information-gathering activity falls into the same category, personal data may be collected. In this case, however, the whole legal issue changes if data collection has a national security basis. This specific case will not be examined here in the analysis of the legal background, as it is not closely related to the general surveillance of citizens. A similar exemption applies to the exercise of public authority. The regulations also provide an exemption for crime prevention and detection activities. The key point is that the law does not apply to national security activities. Although this leaves a large loophole in terms of what can be done in terms of data collection, it does protect citizens from having their data collected for purely malicious purposes. The legal situation surrounding data collection activities is complex, and the lines between what is legal and what is not can be blurry in certain cases. The European Union is trying to regulate this properly to build up the right level of trust within the Union in accordance with these regulations. The new regulations aim to ensure that personal data is only collected, used and stored when there is a legitimate purpose. The above legislation and regulations show that the European Union aims to have a strong legal framework to protect data collection activities, which significantly builds public trust.

Social Credit System, the data enabled, morally based, high-tech public administration

China has introduced the constitutionally based Social Credit System (SCS) project in full operation from 2020, and its use is mandatory for all residents and permanent residents of China. The Chinese National Development and Reform Commission (NDRC) was made responsible for the development of the national implementation of SCS. Its primary objective is to develop a centralised data infrastructure that allows the integration and search ability of different profiles and databases, furthermore, previously existing public and private social credit platforms. In 2015, the NDRC started to build the National Credit Information Sharing Platform, integrating the assessment and database of private credit systems of 50 private data providers (like corporates and banks), 42 central government and 32 local government bodies. Going into more detail, this consists of the judicial and criminal information, consumption data of daily goods, traveling or taxation, and market giants' mandatory public data reporting mechanism, which monitors users' online activities. E.g. the Ant Financial platform of Alibaba Group and its Sesame Credit or Baidu (provides search engine, social media platforms) and Tencent Holdings Ltd.'s (provider of WeChat application) Tencent Credit. From the practical to technical point of view, the construction of the SCS is based on comprehensive data collection mechanisms

[11] Wimmer et al. 2020.

through the physical surveillance of natural persons, e.g. CCTV, fingerprint scanners and facial recognition systems, and the analysis of their digital footprint utilising artificial intelligence (AI) machine learning (ML) and Big Data analysis technologies and the elimination of pseudonymisation and anonymisation of digital services in practice and by law.[12] Social Credit System is a robust public administration project with multiple moral aims and a diverse set of rules and criteria, which seeks to whiten the economic system and increase social credibility, safety and soundness. The moral criteria of the Social Credit System identify four desired behavioural standards to increase social cohesion and strengthen trust between people:

1. honesty in government affairs (政务诚信)
2. business fairness (商务诚信)
3. social decency (社会诚信)
4. judicial integrity (司法公信)[13]

Within these four categories, the SCS regulates social behaviour using personal reputation (both online and in person) and material means by generating a unique credit score for each person. It is important to note that, there are different credit points (i.e. several subsystems within the SCS project): government affairs credit, judicial credit, social credit and commercial credit.[14] Along these score levels, 'blacklists' (people with a low score, who are considered harmful to society) and 'redlists' (appropriate, society-building examples of people with a high score) are set up on provincial administrative level. Empirical research by an international team of researchers has revealed that there are 273 blacklists and 154 redlists across provincial levels, which has a flexible scoring methodology, including coronavirus epidemic-related norms and regulations. Researchers concluded that these black and redlists mainly prioritise scores consisting of law enforcement and industry regulations-related activity. Nevertheless, they identified redlists that rewarded political and moral behaviour.[15] In addition to the public listing of persons (with their real personal data) with red and blacklists, the SCS has also assigned a system of rewards and penalties to certain scores in the various credit systems. For instance, high commercial scores could indicate the person's business is eligible for discounted loans and be exempt from paying a deposit or advance payment. Meanwhile, low points would make people face e.g. travel restrictions (not eligible to buy airplane tickets) and restrictions on rent, scholarship, and job opportunities due to judicial, social and government affairs credit scores.[16] Overall SCS is a morally based administrative system built on massive government surveillance and data analytics technologies.

Over the years, in its early stage, SCS has received a lot of concern and negative criticism from the international press and rights defender organisations, including Human Rights Watch. The latter has not only accused the SCS of violating privacy and personal rights, but has also published a report on the violations of minorities rights in China (such

[12] Liang et al. 2018: 415–453.

[13] Kovalovszki 2019.

[14] Liang et al. 2018: 415–453.

[15] Engelmann 2021: 78–88.

[16] Lee 2020.

as the Uyghur minority) through the Social Credit System and its interconnected law enforcement platform, the Integrated Joint Operations Platform (IJOP, mandarin: 一体化联合作战平台) and Police Cloud application. The report drew attention to the risks of faulty machine learning, namely that the data analysis outlines possible or suspected patterns of behaviour (so-called "unusual activity" trends) of persons who were previously identified as "risky" rather than reacting to actual events and activity regarding that people. This may result in a violation of the rights of the person concerned.[17] However, the original intent of the platform and application was to enhance public safety and political security by setting up an alert for the overconsumption of certain goods like chemicals and other dual-use goods, which can be combined to create IEDs or other homemade weapons. Both systems could become an effective tool for tracking government adversaries, organised crime networks, or even terrorists because it also can establish trends and visualise patterns of relationships through Big Data analysis.[18]

It is a remarkable fact that China has built the enforcement of its restrictive measures that were applied during the coronavirus epidemic on the infrastructure of the SCS. For example, the health Barcode System generates three types of QR codes (which serve as access codes for public transportation) on people's smartphones based on a daily questionnaire assessing travel information and general symptoms of infection. The generated QR codes stand for green, which indicates healthy and allows travel; yellow, which imposes a quarantine obligation (e.g. on arrival in a new province or following infection) and red, which indicates a case of contact or infection (and naturally quarantine obligation) and may as well generate a notification to the relevant public authorities in case of severity.[19] This use case demonstrates that the goals and moral purpose of this high-tech public infrastructure can be customised at any time, setting an example of development for regimes around the world.

Kostka summarised the diversity of the Social Credit Point System's operation as simultaneously achieving the promotion and enforcement of social behaviour in line with the communist state party's views through total control and the fine-tuning of the Chinese-style market economy model also the transparency and higher reliability of civil rights.[20] According to these findings, Social Credit System has the potential and ability to increase the CCP's political sturdiness all over China through indirect economic and moral influence. This set-up is also theoretically more acceptable to society compared to the use of hard repressive instruments of power and because of the following traditions and status quo of power:

- The cultural and political heritage of the People's Republic of China lay the background of moral governance and authoritarian means.[21] However, that does not mean that society is not ready to go beyond that.
- Along China's geostrategic and geopolitical regions, the largest population density and the country's economic centre are in the coastal area. The social stability of

[17] Human Rights Watch 2018.

[18] Wang 2018.

[19] Lin–Hou 2020: 1–8.

[20] Kostka 2018.

[21] Salát 2009.

this territory is crucial for leadership. Meanwhile, the design and construction make the SCS the most efficient and cost-effective in highly populated urban areas. Yet, the great defence policy dilemma of the Chinese leadership is that this specific geographical area is the most vulnerable by the sea.[22]

- The Chinese-type market economy was created by a social contract created as a result of the status quo after the failed Cultural Revolution and the Tiananmen Square massacre.[23] In simple terms, in exchange for the restriction of political rights (compared to European standards) citizens expect economic growth and a continuous increase in their standard of living. Economic performance is linked to the system's stability, but it also creates an opportunity for the richest market players to develop a new power field.

In a Chinese-type market economy, there has always been the possibility that the most influential and wealthy market players could slip out of government control. Large IT companies (Jack Ma's Alibaba Group, Pony Ma's Tencent Holdings Ltd.) in China and other giant companies that dominate several market segments (Didi) have been collecting data almost limitlessly. However, these data sets were not always fully available to the government. The companies' business interests, reputation and own development ambitions sometimes clashed with the CCP's economic and political policies, for example, concerning the U.S. stock market entry of Ant Financial or Huawei's trust-related security issues that caused a loss in the market margin of manoeuvre. Serious tensions have been triggered in the public–corporate relationship by data leaks on the internet, involving vast amounts of Chinese citizens' personal and highly sensitive data. The excessive data collection practices and inadequate data protection measures and storage procedures of large companies can be held liable for the data breach.[24]

In response to this situation, the CCP, building on the foundations of the system laid down in the 2017 Cybersecurity Act, enacted the Data Security Act at the beginning of 2021, which sets out a security framework for large companies to manage data. In addition, from November 2021, the Chinese Data Protection Law was issued, which mainly focuses on setting up responsibilities and introduces framework regulations aimed at the private sector to archive more reasonable and limited data usage. It contains the opportunity to place data protection fines of up to 50 million yuan (approximately 7.7 million USD or 2.9 billion HUF) 5% of its annual cash flow and expect the appointment of a responsible person for data protection. The law regulates the use of AI-powered CCTV face-recognition cameras in public places, describes the legal basis for data collections, and sets out extraterritorial rules on data transition. Chinese firms shall store data on the mainland; otherwise, a risk assessment shall be conducted with the involvement of Chinese authorities.[25]

[22] Stratfor 2012.

[23] West 2015.

[24] Mészáros 2021.

[25] Kaszián 2021.

SWOT analysis

By examining the EU legislation and directives on trust, the authors have conducted a SWOT analysis to identify the strengths and areas for improvement in efforts to build trust within the EU. For the strengths, the fundamental focus was on the right legislative environment and the existing frameworks, which clearly show the potential of the current conditions. The disadvantages, on the other hand, are those areas that are not properly regulated and, therefore, may have a negative impact on the development and maintenance of trust in the EU and its Member States. Furthermore, the resulting threats were also identified, which could jeopardise the digitalisation process and its potential by negatively impacting people's sense of security and their right to privacy and personal space. The results are shown in Table 1.

Examining the Chinese reforms and the Social Credit System, the SWOT analysis looked at the economic benefits of the credit system and its impact on the population from a state perspective. The opportunities have been examined in terms of the positive impact that the system could have on government and the public. For weaknesses and threats, it looked at how the huge amount of data collected could damage the daily lives of individuals, the economy and affect trust in government. The results are shown in Table 2.

Table 1: SWOT analysis of trust and privacy in the European Union

Strengths	**Opportunities**
• Strong data protection regulations, such as the General Data Protection Regulation (GDPR), prioritise individuals' right to privacy and control over their personal data. • The data protection culture is deeply rooted in the EU, with a long history of data protection that goes back decades. • A commitment to privacy as a fundamental human right and an important aspect of digital sovereignty. • A strong legal framework to protect privacy and respect individuals' privacy rights. The strong data protection regulations and the commitment to privacy as a fundamental human right are seen as positive aspects that contribute to the overall protection of privacy in the EU. Furthermore, the long history of privacy protections and a culture that values privacy also highlights the importance the EU places on this issue. These strengths suggest that the EU has a well-established framework for protecting privacy and ensuring that the privacy rights of individuals are respected.	• The growing importance of privacy and security in the digital age, as consumers become more aware of the risks associated with sharing personal data online. • The rise of new technologies and business models can enhance privacy protections and increase public trust in the digital economy. • Increasing cooperation and collaboration between the EU and other countries on privacy and security issues can help create a more consistent and effective global framework for privacy protection. The opportunities indicate the potential for development and improvement in the sector. The growing importance of privacy and security in the digital age, and the emergence of new technologies and business models that enhance privacy, are seen as good developments that can boost public confidence in the digital economy. Moreover, increasing cooperation and coordination between the EU and other nations on privacy and security issues can create a more coherent and effective global framework for privacy. These prospects indicate that sustainable growth and progress in the European Union's trust and privacy protection is possible.

Weaknesses	**Threats**
• Data protection laws are not uniform across the EU (different Member States may have different legislation), making it difficult for companies to comply with multiple regulations. • Lack of public trust in technology companies and how they handle personal data. • Difficulties in enforcing data protection rules, especially for cross-border data transfers (for manufacturers outside the EU, EU rules are only recommendations, not mandatory). • Data security vulnerabilities can lead to data breaches and privacy violations (data loss, unauthorised access due to supply chain failures may reduce trust). The weaknesses reflect some of the challenges and limitations in the EU's current state of privacy protection. The lack of uniformity in privacy laws across the EU and the difficulty in enforcing privacy regulations can create difficulties for companies trying to comply with multiple sets of regulations. The lack of public trust in technology companies and vulnerabilities in data security also raises concerns about protecting personal data. These weaknesses highlight the need for further efforts to enhance privacy protections and increase public trust in the digital economy.	• The rise of new technologies, such as artificial intelligence and the Internet of Things may raise new privacy and security concerns (there are many areas of the EU's information and communication infrastructures that are dependent on non-EU countries, which can reduce trust in them). • The growing power and influence of technology companies can undermine privacy rights and the ability of individuals to control their personal data (there may be many cases, both at EU and Member State level, where data are handled by a third party outside the EU). • Increased government surveillance and the potential for privacy rights to be eroded for national security purposes. • The growing threat of cybercrime and widespread data breaches and privacy violations. The threats highlighted the challenges that must be overcome to maintain robust data protection safeguards. New technologies such as artificial intelligence and the Internet of Things, as well as the growing influence and power of technology companies can raise new privacy and security issues. In the digital age, the potential for increased government surveillance and the threat of cybercrime both pose significant threats to privacy. These concerns underscore the need for continued attention and action to safeguard the privacy rights of EU citizens, which are essential to maintain trust.

Source: Compiled by the authors.

Table 2: SWOT analysis of the Chinese reforms and the Social Credit System

Strengths	**Opportunities**
• Through the system of scores, listing (publicising) and accompanied benefits consumers can be influenced as well as the development or production goals of businesses. Therefore, the economy can be fine-tuned on political-economic expectations of the CCP. • SCS is able to whiten the economy and increase transparency in certain government matters, which improves the relationship of the people, the market and the government. • Utilising the fear from defamation or desire of praise by the disclosure means of the SCS the expected system-loyal behaviour of citizens can also be achieved with the soft instruments of power. The above statements are explained by the Tiananmen power status quo in addition to the geopolitical situation supplemented with the tradition of moral governance.	• China could be the winner of the new, data-driven technological revolution by its advantage on data collection practices. • The reduction of online anonymity and data analysis capabilities may be able to predictively prevent accidents, violations and crimes. • The creation of a morally customisable, data-based governing model. The possibility for almost unlimited data collection in the public interest is created by legislation as described by the introduction of the SCS. Private sector service providers' practices are based on continuous data analysis, although the new Chinese Data Protection Law seeks to limit this. The health barcode case study also supports the above propositions.
Weaknesses	**Threats**
• Personal data protection is regulated on high level approach. • It is difficult to limit the activities of internal market companies in terms of data provision and cooperation with authorities, so the chance of enforcing extraterritorial scope is low. • The almost unlimited scope of data collection in SCS entails a huge infrastructural burden and a requirement for data storage capacity which financial resources must be continuously secured. • SCS can make the fabric of society inflexible. The review of the Chinese law on data protection assesses the weaknesses in the legislation framework. Meanwhile, the listed fundamental problems of the SCS can be drawn from the urbanisation status and economic weight of China's coastal regions. The above allegations are also backed up by case studies of data breaches by large Chinese companies and by conflicts due to the CCP's economic policies. The weaknesses of the system were highlighted by the interviewees' personal experiences and their perceptions of its social impact.	• There may be many cases where data are handled by a third party outside of China. • The training of the SCS's analysis algorithms or its false positive alerts may cause infringement of rights. The correction of inaccurate data sources could be difficult. These cases provoked a lot of criticism from the international community, damaging China's image. • It can cause psychological damage to individuals that cannot be measured yet and create dividing-lines of trust in society and increase the suppressed aggression toward the government. This creates an environment that is highly receptive and vulnerable for hybrid threats. The SCS's four desired behavioural standards to increase social cohesion and economic prosperity – described in the introduction – is not fulfilled in cases published by international human rights organisations due to technology-related errors. These instances are undermining the international image of the state, which affects the opportunities for global corporations in the trust-based IT markets. The identification of potential threats associated with mental health state and social issues are also supplemented by the deductions drawn from the responses of the interviewees.

Source: Compiled by the authors.

The SWOT analysis shows that the foundations of the EU system are well-regulated and seek to cover all areas that can contribute to building trust. As trust plays a very important role in the EU, the legislators pay serious attention to protecting personal data. Consequently, data protection and security laws have been a part of the EU's policy for several years. The legislation aims to give citizens control over their own personal data. By requiring that personal data be adequately protected, the legislation seeks to ensure that individuals can trust EU institutions and organisations with their information. In contrast, in China, the Social Credit System does not address personal data protection (mostly at the state level) but does not aim to build trust in the government. As a result of people's different ways of thinking, the government there relies much more on acceptance, which means that the population involuntarily agrees to the system collecting and analysing data about them on an ongoing basis.

As the EU has a relatively well-regulated set of manufacturing requirements to produce certain technological devices, it is quite easy to build trust in devices manufactured in the EU. However, this picture is overshadowed by the fact that there are many areas where it is inevitable that the necessary equipment is sourced from outside the EU. For these devices, there is not always a guarantee that the manufacturer has complied with EU rules, reducing confidence in the service or application. This can lead to a lack of trust from customers, who are not sure that the device they are using complies with the EU's stringent manufacturing requirements. In contrast, China typically uses devices and systems manufactured in-house, which means significantly less exposure. The biggest problem is that much data is being collected; storing and processing is a major challenge for the government. Another problem is that the public is not fully aware of what data is being collected about them and the depth to which it is being analysed. In the long term, this can create a lack of trust in the public, which can negatively affect the perception of the government.

Interviews

The semi-structured interviews were conducted with young academics (under 30 years) with expertise in public administration and research on China, who have personal experience of the Social Credit System. The first set of questions asked whether the system had had any impact on their daily lives during their time abroad and what their experiences had been. The next step was to examine the elements and characteristics of the Chinese society that make the social credit system acceptable and workable and how its application affects the four trust target areas (identified in the design of the data-based governance structure). The following questions examined the impact respondents perceived the social credit system to have had on the Chinese economy. In the final section, we looked at what interviewees think trust means in a data-driven Chinese society and what differences they would highlight compared to the European GDPR-based system. Furthermore, respondents see the possibility of a Chinese-style data analysis system being acceptable in the EU. Four people were interviewed during the study, and the following results were obtained from their responses.

The interviewees typically said that it was only an indirect experience and that it had mostly no impact on their daily lives during their stay, which lasted from two weeks to a year. However, they subconsciously had a risk-averse attitude based on some perceived or real norms. This is referred to as the "chilling effect" in the literature. Interestingly, one respondent said he had looked into the issue with Chinese friends who were very positive about the scheme. This may be due to the basic reasons of discipline, respect for tradition (e.g. a child supports a parent in old age, if not, he risks social exclusion), the high level of digitalisation, and the historical traditions (including decades of authoritarianism), the atomisation of society, the lack of a really strong political opposition, the possibility of using good points to move up in society. Overpopulation and high population density require using new, modern tools to achieve more effective crime prevention or other desirable social goals. Due to its non-democratic set-up, the state has many more resources and data than other states. If the state is to be a good steward, it must harness and benefit from this surplus of resources and data. The application of the social credit system is transforming justice and social/business relations. The retrievable data can now be used to create prejudice against another person. The power of the state or the system that allocates the points is increased, but at the same time, the desire to deceive and manipulate the system is increased, thus refining the methods of perpetration. The fear of negative consequences makes citizens more prudent. According to interviewees, the system appears to impact the Chinese economy positively. Everyone has to have a mobile phone; everyone pays with it, cash is becoming scarce, and payment apps track all spending and status, making it easier to check creditworthiness, which has likely whitened the economy. The system also rewards easy consumption and encourages citizens to consume more. This gives more work to developers and more work to analysts and causes less unemployment. It has also acted as a further stimulus to domestic consumption growth. At the same time, it can hinder the conclusion of certain services and deals, making the economy (and social mobility) more rigid.

In a data-driven Chinese society, the concept of trust is more linked to the state, and since the totality of past actions determines it, there is no question that a person cannot be identified or can only be identified for a necessary period. The point here is precise: the data is tightly bound to the person and is widely accessible. Therefore, citizens are confident that the Chinese state will use the data it acquires exclusively for public purposes, ultimately increasing their welfare. However, the state is not accountable to citizens, so the system's transparency is very limited.

- the purpose of the data collection is not specified
- the state can collect data almost without limit
- facial recognition systems and other new technologies make it easier to identify individuals

The GDPR is much more restrictive on the powers of data controllers and processors, while the Chinese regulation is much more permissive. Therefore, a Chinese-style data analysis system is certainly not acceptable; EU citizens typically have a low tolerance for covert restrictions, while China has "discipline". According to interviewees, the current model would face many legal and moral obstacles in the EU. However, to take advantage of the benefits offered, the main elements of the filtering system could, in their view, be made more flexible with legal and/or constitutional guarantees.

Conclusion

The research confirmed the importance of building and maintaining trust within the EU. The legislative environment has been designed accordingly, and legislators have done their utmost to create situations in all walks of life that are conducive to building trust. The strongest of these is the area of personal data protection, which is extremely well regulated in the EU and its Member States. However, the legislation does not yet strictly regulate the packaging requirements for devices from non-EU manufacturers, nor are the rules for data handling outside the EU fully developed. Accordingly, the first hypothesis was considered to be confirmed.

The Chinese Communist Party has also begun to show a similar attitude to that of EU member states regarding data collection by IT companies and other giant corporations in the state-market relationship. The common feature is that China has also implemented a data protection law that limits the scope of data collection and seeks to force international companies to cooperate with the authorities and provide data security guarantees.

The most striking difference between the two data protection cultures is how they relate to the data subjects' natural persons. The European Union legal framework focuses on the protection of the privacy of the data subject and is designed to impose guarantees of trust and confidence from data controllers and processors. Meanwhile, the data management culture of the Social Credit System requires trust expectations from both the natural persons (the data subjects) and the market actors (the data controllers and processors) to create a secure environment for the public system to operate in which both actors, the company and the natural person, can prosper and develop. This puts the public perspective, not the individual, at the heart of data protection in Chinese data protection culture. These have shown that these types of systems do not address personal data protection and are therefore not applicable in environments such as the European Union, where privacy is a high priority.

References

Charter of Fundamental Rights of the European Union (2012) C 326/02.

DigitalEurope (2019): *A Stronger Digital Europe.* Brussels. Online: www.digitaleurope.org/wp/wp-content/uploads/2019/02/DIGITALEUROPE-%E2%80%93-Our-Call-to-Action-for-A-STRONGER-DIGITAL-EUROPE.pdf

Directive (EU) 2016/1148 of the European Parliament and of the Council (6 July 2016) concerning measures for a high common level of security of network and information systems across the Union.

Directive (EU) 2016/680 of the European Parliament and of the Council (27 April 2016) on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Directive 2002/58/EC of the European Parliament and of the Council (12 July 2002) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Engelmann, Severin – Chen, Mo – Dang, Lorenz – Grossklags, Jens (2021): Blacklists and Redlists in the Chinese Social Credit System: Diversity, Flexibility, and Comprehensiveness. *AIES '21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society,* 78–88. Online: https://doi.org/10.1145/3461702.3462535

Human Rights Watch (2018): China: Big Data Fuels Crackdown in Minority Region. *Human Rights Watch,* 26 February 2018. Online: www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region

Kaszián, Ábel Gergő (2021): A GDPR kínai „unokatestvére" – avagy a kínai adatvédelmi törvény megszületése és várható hatásai. *Jogi Fórum,* 20 September 2021. Online: www.jogiforum.hu/publikacio/2021/09/20/a-gdpr-kinai-unokatestvere-avagy-a-kinai-adatvedelmi-torveny-megszuletese-es-varhato-hatasai/

Kostka, Genia (2018): China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval. *Merics,* 17 September 2018. Online: https://doi.org/10.2139/ssrn.3215138

Kovalovszki, Kartal (2019): A kínai társadalmi kreditrendszer [The Chinese Social Credit System]. *DiploMaci,* 11 April 2019. Online: https://diplomaci.blog.hu/2019/04/11/a_kinai_tarsadalmi_kreditrendszer

Lee, Amanda (2020): What Is China's Social Credit System and Why Is It Controversial? *South China Morning Post,* 09 August 2020. Online: www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial

Liang, Fan – Das, Vishnupriya – Kostyuk, Nadiya – Hussain, Muzammil M. (2018): Constructing a Data Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy and Internet,* 10(4), 415–453. Online: https://doi.org/10.1002/poi3.183

Lin, Leesa – Hou, Zhiyuan (2020): Combat Covid-19 with Artificial Intelligence and Big Data. *Journal of Travel Medicine,* 27(5), 1–8. Online: https://doi.org/10.1093/jtm/taaa080

Maurtvedt, Martin (2018): *Surveillance and Social Manipulation: A Solution to "Moral Decay"?* Master's thesis. University of Oslo.

Mészáros, R. Tamás (2021): Annyi adatot gyűjtöttek, hogy a Kínai Kommunista Párt is megijedt tőle [They Collected so Much Data that even the Chinese Communist Party Was Scared of It]. *G7,* 25 July 2021. Online: https://g7.hu/vilag/20210725/annyi-adatot-gyujottek-hogy-a-kinai-kommunista-part-is-megijedt-tole/

Misuraca, Gianluca – Barcevičius, Egidijus – Codagnone, Cristiano (2020): *Exploring Digital Government Transformation in the EU. Understanding Public Sector Innovation in a Data-Driven Society.* Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2760/480377

Regulation (EU) 2016/679 of the European Parliament and of the Council (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).

Salát, Gergely (2009): *A régi Kína története*. Budapest: ELTE Knfuciusz Intézet. Online: https://btk.ppke.hu/uploads/articles/772735/file/regikinatortenete_teljes.pdf

Stratfor (2012): The Geopolitics of China: A Great Power Enclosed. *Stratfor*, 25 May 2012. Online: https://worldview.stratfor.com/article/geopolitics-china-great-power-enclosed

Wang, Maya (2018): Cambridge Analytica, Big Data and China. *Human Rights Watch*, 18 April 2018. Online: www.hrw.org/news/2018/04/18/cambridge-analytica-big-data-and-china

West, John (2015): China's Political Predicament. *Asian Century Institute*, 30 September 2015. Online: https://asiancenturyinstitute.com/politics/979-china-s-political-predicament

Wimmer, Maria A. – Neuroni, Alessia C. – Frecè, Jan Thomas (2020): Approaches to Good Data Governance in Support of Public Sector Transformation Through Once-Only. *Electronic Government, EGOV 2020, Lecture Notes in Computer Science*. Cham: Springer. Online: https://doi.org/10.1007/978-3-030-57599-1_16